

Tuesday, December 23. 2008

Never attribute to malice...

... that which can be adequately explained by stupidity.

Hanlon's Razor

Konkret: der Fall der verlorenen Kreditkartendaten der Berliner Landesbank wurde durch zwei Kurierfahrer verursacht, die Christstollen haben wollten und daher einfach zwei Pakete austauschten...

Posted by Axel Eble in Meta at 10:56

Thursday, December 11. 2008

PCs mit Dreien, Vieren oder eventuell FÄ¼nfem?

Ohne Worte.

Posted by Axel Eble in local at 13:24

ReisebÄ¼ro

Abends in Freiburg kommt man gelegentlich an ReisebÄ¼ros vorbei. Diese haben hÄ¼ufiger auch groÄ¼e Flatscreens als WerbetrÄ¼ger im Schaufenster. Und das kann dabei rauskommen, wenn man Standardinstallationen fÄ¼r sowas benutzt:

Posted by Axel Eble in local at 11:43

Tuesday, December 9. 2008

Qype: Anne Clark in Freiburg

Freiburg - Konzerte & Festivals - Alternative & Indie - Konzerte & Festivals - Pop & Rock - Konzerte & Festivals - Elektronische Musik

Wie erwartet: intimes Ambiente. Ein kleines, aber sehr feines Konzert mit den alten Gassenbauern und den neuen Stücken von der Smallest Acts of Kindness-Platte. Das Preis-/Leistungsverhältnis war gelungen (knapp 20 Euro für 2h Konzert). Endlich mal wieder ein Konzert, endlich mal wieder heiser

Nächstes Mal wieder

Mein Beitrag zu Anne Clark - Ich bin eble - auf Qype

Posted by Axel Eble at 23:29

Sunday, November 2. 2008

Anti-Spam Appliances Considered Harmful

It's no secret: Anti-Spam configuration can be hazardous to your email traffic. If the spamfilters generate too many false positives your email transmission will suffer. This is a major problem in B2B configurations and can bite you out of the blue.

I've had this problem in the past, when the company I was working for was justifiably listed on an RBL. And I had it again, now - only this time I am reasonably sure that the system is a) configured tightly enough not to be usable as an open relay and b) not being used for sending out marketing or other possibly spam-alike emails.

Nevertheless, the system was listed with a commercial anti-spam appliance vendor in their RBLs (which are "reputation based" - meaning, they have a set of criteria that can give you a certain (read: bad) reputation). The only explanation I have for this is that said company has caught backscatter from our system and classified that as spam. If you don't know what Backscatter is: that's bounces sent to innocent people that were listed in the From: address of Spam.

The danger with those commercial anti-spam appliances is the multiplication factor: if you happen to end up as a false positive with those companies, you may lose contact with not only one customer, but with several.

There are several solutions to this:

Don't send out error reports for undeliverable emails. Can only be done if the system does not receive mails at all
Monitor RBLs with your monitoring solution. For Nagios there are RBL checks and I'm sure for other tools as well. The only problem: how do you make sure you're monitoring all (relevant) RBLs? And you will probably not be able to monitor the commercial services as they make a profit out of their services.

How do you cope with these problems? What are your ideas?

Any help appreciated!

Posted by Axel Eble at 00:38

Friday, October 17. 2008

Policy-based routing on Linux

A customer system needed to be upgraded and for several reasons it was supposed to be moved from Windows server to Linux (more on that another time). The server was supposed to be moved from one IP range to another as we are moving from our old Provider Aggregatable (PA) IP addresses to our "new" Provider Independent (PI) addresses.

I set the system up and it was supposed to be a hard cutover on one day. It quickly turned out that this was not feasible (again, for several reasons, e.g. the amount of data to copy over was too big). So, finally, it was decided that the cutover was to be smooth: the majority of data was rsync'ed over from Windows in the days before the cutover date, then the rest on the cutover day. The SSL certificate was to be copied over on day X and the new server running Linux should take over the IP address of the old (Windows) server. As the system was now multihomed we needed to cope with asymmetric routing. First off, we thought it should be possible to hide all incoming traffic to the old IP addresses behind the internal IP address of the firewall - but it turned out our product does not allow for that.

The solution to this is policy-based routing: if the packet goes out on Interfacenew, a different routing decision needs to be taken than when it would go out Interfaceold. Fortunately, Linux does allow for this with the iproute2 package: you can have several routing tables glued together with a routing policy, i.e. a set of rules that controls the selection of the routing table. If a rule matches and a route is selected from a routing table the packet gets routed according to this route. If there is no matching route the rule traversal continues.

In our setup this means, that all packets from IPPI-Space should get routed to the PI-Space gateway whereas all packets from IPPA-Space should get routed to the PA-Space gateway. Currently, the default gateway is the PA-Space one, so we don't have to do much.

In Debian/Ubuntu syntax, the network is then setup through /etc/network/interfaces with a stanza like the following:

```
auto eth0
iface eth0 inet static
    address A.B.C.D
    netmask 255.255.255.240
    network A.B.C.128
    broadcast A.B.C.143
    dns-nameservers some.dns.serv.er
    gateway A.B.C.129
```

And for the Interface in the PI address space, the stanza looks like this:

```
auto eth1
iface eth1 inet static
    address V.W.X.Y
    netmask 255.255.255.240
    network V.W.X.128
    broadcast V.W.X.143
    dns-nameservers some.dns.serv.er
    post-up ip rule add from V.W.X.Y table PI-Space
    post-up ip route add default via V.W.X.129 table PI-Space
```

The two post-up lines are the magick in here: the first adds a rule to the routing policy that, for all traffic originating from the PI space interface, a lookup should be performed in routing table PI-Space. Then, we add a second default route to that very same routing table. Now, whenever a packet goes out Interface eth1, the kernel checks if there is a matching route in routing table PI-Space. As we have a default route, this will always match and the packet gets routed to the

gateway in our PI space.

Obviously, all other traffic originates on eth0 so the "normal" routing table will be used, thus this traffic will go out via the gateway residing in the PA address space.

loose ends

Actually, the kernel does not check a routing table named "PI-Space". It will use a numerical identifier that is mapped in /etc/iproute2/rt_tables like this:

```
#
# reserved values
#
255  local
254  main
253  default
0    unspec
#
# local
#
#1   inr.ruhep
100  PI-Space
```

Posted by Axel Eble in General at 23:18

Sunday, December 23. 2007

BÄcher in liebevolle HÄnde abzugeben

Hinweis in eigener Sache: Im Zusammenhang mit unserem kurz bevorstehenden Umzug habe ich eine Latte BÄcher abzugeben, die ich nicht mehr umziehen werde. Die gesamte Liste liegt unter BÄcherliste. Bei Interesse bitte eine Email oder Nachricht im IRC. Ansonsten fliegen die BÄcher ins Altpapier. Und ja, da blutet mein Herz.

Posted by Axel Eble in Meta at 17:23

Wednesday, December 5, 2007

Spam as Spam can: JobLeads.DE

Und immer wenn du denkst, es geht nicht mehr (schlimmer), kommt irgendjemand, der dir das Gegenteil beweist. Na super. Heute morgen finde ich in meiner geschäftlichen Inbox diesen Spam:

Sehr geehrter Herr Eble,

vor Kurzem haben wir mit einem jungen Team JobLeads gelauncht. JobLeads ist eine "By Invitation only"-Karriereplattform, die sich speziell an hoch qualifizierte Fach- und Führungskräfte richtet. Top-Unternehmen schreiben bei JobLeads ihre Stellenangebote aus und versehen diese mit Prämien zwischen € 2.000 und € 20.000 für die erfolgreiche Empfehlung von Kandidaten.

Um den Anforderungen an eine exklusive Karriereplattform gerecht zu werden, gehen wir bei der Auswahl unserer Mitglieder sehr selektiv vor. JobLeads-Mitglieder haben an führenden Universitäten im In- und Ausland studiert und sind nun in verantwortungsvollen Positionen tätig. Als Absolvent der Universität Freiburg gehören auch Sie zu diesem Personenkreis und wir möchten Ihnen anbieten, die Vorteile von JobLeads zu nutzen (die Mitgliedschaft ist und bleibt natürlich kostenlos).

Als Mitglied hat man exklusiven Zugang zu Top-Stellenangeboten und die Möglichkeit, die ausgeschriebenen Positionen an Freunde zu empfehlen. Kommt es aufgrund einer Empfehlung zu einer Einstellung, erhält man die Prämie. Selbstverständlich kann man sich auch auf interessante Positionen bewerben. JobLeads macht es so möglich, immer über spannende Stellenangebote von attraktiven Unternehmen informiert zu bleiben, Freunden interessante Jobs zu empfehlen und nebenbei noch Geld zu verdienen.

Falls Sie Interesse haben, JobLeads-Mitglied zu werden, können Sie sich über den unten stehenden Link registrieren. Falls nicht, wünschen wir Ihnen auf Ihrem Karriereweg weiterhin viel Erfolg.

https://www.jobleads.de/user_introduction_invitation.php?aid=XXXX

Viele Grüße aus Hamburg

Ihr JobLeads-Team

Das zeugt ja schon mal aus mehreren Gründen von ... fehlender Überlegung. Erstens: woher haben die meine Geschäftsadresse? Mit der gehe ich nicht gerade hausieren. Zweitens: es ist Spam. Ich habe keine Geschäftsbeziehungen mit diesem ominösen Unternehmen noch habe ich Interesse daran, von denen meine Inbox gefüllt zu bekommen. Drittens: schlechte Datenquelle - ich bin kein Alumnus der ALU. Ich war da zwar mal eine Weile eingeschrieben, aber ich habe nicht abgeschlossen dort. Viertens (und damit kommen wir zu den technischen Seiten des ganzen Braindeaths): es gibt keine funktionierende Abuse-Adresse für jobleads.de. Fünftens: dännes Gefasel auf der Webseite, irgendwo ist "Recruiting 2.0" erwähnt (meine Güte, dieser 2.0-Hype ist doch schon wieder vorbei!).

Ich spare mir jetzt irgendwelche offensichtlichen Auslassungen über Investmentbanker. Man soll ja nicht eine ganze Berufsgruppe über einen Kamm scheren.

Nichtsdestotrotz muss man derartigen Machenschaften gleich entsprechend einen Riegel vorschieben:

Hallo,

Ich habe diesen Spam von Euch in meiner geschäftlichen Inbox gefunden. Nicht genug damit, daß Ihr damit eindeutig gegen existierende Gesetze verstößt, zeigt ihr dazu noch

eine erstaunliche Insensibilität (hallo? Jobmarkt-Angebote an geschäftliche Adressen? Geht's noch?)

eine erstaunliche Inkompetenz was Marketing in Zeiten des Internet bedeutet (Spam ist die beste Antiwerbung, die ihr hÄttet machen kÄnnen)

Eine rechtliche Aufarbeitung dieser Email spare ich mir - diesmal. Nichtsdestotrotz beanspruche ich nach Â§19 Bundesdatenschutzgesetz Auskunft darÄber:

welche Daten Ihr Äber mich gespeichert habt
wo ihr diese Daten her habt
an wen Ihr diese Daten weitegegeben habt bzw. weiterzugeben gedenkt

Ich gebe Euch bis Freitag, den 7.12.2007, 17:00 Zeit, dieses Auskunftersuchen zu beantworten. Verstreicht diese Frist ohne Antwort, werde ich rechtliche Schritte einleiten.

DarÄber hinaus untersage ich jedwede Weitergabe oder Verarbeitung der gespeicherten Daten, soweit sie mich betreffen.

Axel Eble

Die Karriere-Bibel sieht das JobLeads-Angebot Äbrigens etwas neutraler.

Posted by Axel Eble in Experiences at 11:02

Tuesday, December 4, 2007

BarCamp Freiburg: Security Metrics

Well, it's been on my mind for quite a while to set up some sort of security meeting in the area.

It should have something to do with security and I want to learn something through it as well.

Over at JollyOrc I got intrigued by the idea of a barcamp and, what can I say: the three items seem to match up nicely.

We've been over the issue of security metrics time and time again in many different places and in many different company - without any meaningful result so far. I think it's time for a get-together and a discussion about what metrics make sense in what context.

The format of a BarCamp seems to be ideally suited for exactly that: a get-together of like-minded people with different backgrounds working on the same topic.

I'm sure the location could be provided, maybe even by my company.

Posted by Axel Eble in local, Meetings at 21:54

Tuesday, February 20, 2007

Crisis Management

So flickr had a hiccup yesterday. Well, truth be told, it was a major problem on their side: the image caches ran amok and delivered the wrong pics - not a few of them a bit on the more adult oriented side (as a sidenote, this proves what we all knew anyway: The Internet Is All About Porn). To the emotional outcry from lotsa lotsa users came the fact that the problem was not resolved by restarting the flaky cache server(s) but instead resurfaced once again. So finally, after quite a few hours of downtime (and I bet beet red engineers working overtime to find the bug and fix it) the system is back up.

So that's the exposition, which just about gives you an idea of the dimension of this thingy. It didn't? Well, then let me summarize: It Was BIG. However, flickr not only took down their site but pointed to their blog - in which Eric Costello did keep the users informed (if only tersely, but this is better than just a few lame marketing lines stating that all is beautiful and the system is just being enhanced yaddayaddayadda). When it was apparent that flickr would solve the problem he sat down and wrote a decent explanation of the problem - in a way to satisfy both non-technical users and the somewhat tech-savvy ones. He explains the issue without emotional overtures nor does he play it down:

To be clear, we regard this as a serious problem, but it is something that goes away as soon as we restart the malfunctioning servers (tonight we found that the servers were going insane again shortly after restarting, but we have isolated the problem and believe we have a permanent fix).

And finally, he concludes with:

We shamefacedly apologize for the inconvenience and the scare. We understand that it probably seems very, very strange and we know that many people got the impression that their photos were lost forever. But they should all be back now, safe and sound. And everyone who works on Flickr's engineering and technical operations teams are working double time to ensure that it never happens again. Thanks for your understanding and patience!

Folks, this is one of the best pieces of crisis management I have ever seen! It states the problem; it states the solution; it takes the blame where necessary and it gives a promise to the future. Now, if we could set this as mandatory teaching for all companies worldwide I would feel so much better.

Posted by Axel Eble in Meta at 08:14

Friday, January 12. 2007

Democracy, Freedom and the Internet.

The German District Attorney of Halle has urged the Credit Card Industry to screen all 20-22 million German credit cards for transactions along some criteria - without having an initial suspicion of any criminal behaviour. Any such screening and searching is only legal through a warrant. Now there are two immediate scandals obvious:

the District Attorney had no warrant whatsoever, but they threatened the credit card companies that non-compliance would be illegal and punishable
the credit card companies' lawyers obviously didn't care to think this would be illegal and complied.

It almost comes as no surprise that the Police Union says that illegal means in investigations are fine to get results.

What it was all about? Child pornography. Which, according to German Law, is about in the same category as Wilful Damage to Property (which would almost be a joke in itself if it wasn't so sad). The screening of the 20 million German credit cards yielded 322 suspects.

Udo Vetter wants to have a court state if the District Attorney's action was legal or not.

I'm wondering what our current government will try next.

Posted by Axel Eble in local at 12:59

German Government plans a Federal Trojan

The German Federal Government plans to have a Trojan created to spy on its citizens help the law enforcement agencies in their investigations.

Currently the legality of this plan is under scrutiny (the first try to get an "online search" done was stopped as illegal by a judge), but the government is not afraid to tout that they will create the legal grounds for it if necessary.

Heise has published more information, among them the factoid that two programmers will be hired to write the trojan and that the development should not cost more than 200,000 €, in total.

The brazenness of this idea is astounding (not to mention dumbfounding) - not to mention that they will have a hard time against people with at least some security skill.

Oh well, it's always good to see perfectly good tax money go down the drain.

Posted by Axel Eble in local at 10:16

Thursday, January 11. 2007

Stückchen

Blacky hat mir vor einiger Zeit ein Stückchen zugeworfen... Alsdenn.

Wo warst du am...

22. November 1963

Noch nicht mal geplant. Spannendes Datum, aber. Fast so gut wie Roswell, was Verschwörungstheorien angeht.

6. Mai 1975

In der Emil-Gütt-Schule in Freiburg. Schätzungsweise. My memory is a bit blurred that far back...

26. April 1986

Im Droste-Hilshoff-Gymnasium in Freiburg. An dem Tag war ich mit meiner Ente gefahren und müßte nochmal kurz raus, um was zu holen - durch den Regen. Die folgende Zeit war bedrückend und bestimmt durch die aktuellen Zahlen in der Zeitung. Sie entbehrte allerdings auch nicht einer gewissen bizarren Komik, weil die Wolken an der französischen Grenze halt machten.

16. August 1993

Mal sehen... '93... wahrscheinlich irgendwo an der Uni Freiburg, schätzungsweise im Institut für medizinische Biometrie oder in der Institut für Informatik. Ggf. auch in der Unibibliothek. Das Ereignis hat mich damals noch nicht sonderlich berührt in Ermangelung geeigneter Hardware.

11. September 2001

In Las Vegas, zwei Wochen unserer vier Wochen USA gerade rum. Aus irgendeinem Grund habe ich morgens beim Aufwachen den Radiowecker angemacht und habe irgendetwas von einem Flugzeugunglück gehört, woraufhin ich den Fernseher angeschaltet habe... um dann noch die zweite Maschine mitzubekommen, wie sie in den zweiten Turm geflogen ist. Es war ein beklemmendes Gefühl und wir haben gemacht, daß wir aus Vegas rausgekommen sind. Es ging dann weiter zum Grand Canyon, leider nicht über den Hoover Dam sondern mit ca. 200 Meilen Umweg. Grand Canyon war komplett ohne Flugzeuge und Hubschrauber - müß ja sonst deutlich anders sein. Und natürlich das Bangen ob wir überhaupt zurück kommen wie geplant. Die Sicherheitsbestimmungen, als der Flugbetrieb wieder aufgenommen wurde, waren dann in etwa vergleichbar mit denen in Europa vor dem Anschlag.

Kennst du die Ereignisse, die zu all diesen Daten gehören?

Das vorletzte müßte ich nachschlagen und beim ersten war ich mir erst nicht sicher.

Ich gebe das Stückchen an Kris, Tilman und Harald weiter.

Posted by Axel Eble at 10:48

Saturday, January 6. 2007

Verbietet Killerspiele! Lockt die Jugend ins Kino!!!(eins elf)

Nach dem Besuch von «James Bond: Casino Royale» stellt sich mir ernsthaft die Frage, was die Diskussion über das Verbot von Egoshootern (vulgo: Killerspiele) soll, wenn derartige Filme ab 12 Jahren freigegeben sind. Mal ganz abgesehen von der sinnfreien Darstellung der Gewalt (den Sex hatten sie ja mal wieder ausgeblendet und bitte was soll das denn?!) finde ich auch die Thematik für einen 12jährigen nicht unbedingt nachvollziehbar.

Was wieder einmal zeigt, daß das reflexartige Geschrei nach dem «Verbot von Killerspielen» eben nicht mehr ist als genau das: reflexartiges Geschrei.

Posted by Axel Eble in Experiences at 18:28

Wednesday, December 6, 2006

Der mediale Internet-Experte und die Berichterstattung

Heute erschien auf der Webseite von tagesschau.de ein Artikel namens "Wieviel Kontrolle braucht das Internet?" In diesem Artikel zitiert der Autor Herr Zirpins einen Hamburger "Internet-Experten" namens Bert Weingart, der für mehr Filter und bessere Kontrolle des Netzes eintritt. Diese Meinung kann man vertreten, so man sie denn entsprechend verargumentiert. Der Artikel beschränkt sich jedoch weitgehend darauf, die Meinung Herrn Weingartens wiederzugeben. Ganz am Schluss des Artikels schließlich gesteht Weingarten die Problematik seiner Vorschläge ein:

"Die derzeitige Anarchie im Internet ist in Ordnung für Menschen, die eine Medienerziehung genossen haben und damit umgehen können. Wir müssen aber medienunerfahrene Personen schützen", sagt er, und gesteht ein Problem ein: "Internet-Filterung kann durch entsprechende Administration zur Zensur werden." Aber genau das schlägt er ja letztlich vor.

Interessant hingegen die Meinung des Waffenexperten der Gewerkschaft der Polizei, Wolfgang Dicke: "Wenn der Waffenkauf so einfach wäre, warum war Sebastian B. dann - zum Glück - so hundsmiserabel bewaffnet?" Interessant, da diese Meinung gerade von der GdP kommt, die ja sonst eher durch markige Sprüche ihres Vorsitzenden Konrad Freiberg auffällt, der stets für mehr Überwachung und mehr Kontrolle in allen Lebensbereichen eintritt.

Zusammengefasst empfinde ich den Artikel als sehr tendenziös, weil er den massiven geschäftlichen Interessen des Bert Weingarten nach dem Mund redet. Hätte man mit Kristian Kahlhopp gesprochen, der wohl genausogut als "Internet-Experte" klassifiziert werden kann (oder mit Andrea Wardzichowski vom DFN-Verein oder mit einem anderen alten Hasen), so hätte Herr Zirpins mit Sicherheit einen anderslautenden Artikel geschrieben - wohlgermerkt: mit Argumenten hinterlegt statt mit Panikmache (und: handfestem Geschäftsinteresse).

Aber das passt natürlich gut zu der aktuellen Stern-Umfrage, da ca. 59% der Bevölkerung a) einem Verbot von Egoshootern (gemeinhin "Killerspiele" genannt) und b) stärkerer Kontrolle und damit der Einschränkung bzw. dem Verlust von Bürgerrechten zustimmt. Ganze 72% sind danach der Meinung, da Egoshooter zu dem Amoklauf von Emsdetten beigetragen haben - was auch immer das heißen mag.

Im ZDF-Politbarometer hingegen sind sogar 72% der Befragten für ein Verbot von "Killerspielen" (Frage 9 von 11); allerdings sind nur 16% der Meinung, da durch ein solches Verbot die Zahl gewaltbereiter Jugendlicher stark zurückginge, 49% weniger stark und immerhin 32% sind der Meinung, da ein Verbot keinen Unterschied bewirkte. Diese Umfragewerte halte ich für bedenklich, zeigen sie doch, da für komplexe Zusammenhänge nur einfache Lösungsansätze gefragt zu sein scheinen.

Zum Abschluss zitiere ich nochmals Herrn Weingarten: "Die derzeitige Anarchie im Internet ist in Ordnung für Menschen, die eine Medienerziehung genossen haben und damit umgehen können. Wir müssen aber medienunerfahrene Personen schützen"

Ich stimme dieser Aussage zu - allerdings sehe ich das Heil hier nicht in technischen Lösungen: wir sehen derzeit an vielen Beispielen der USA, da Technologie nur begrenzt helfen kann. Die eigentliche Herausforderung liegt in der Medienerziehung, insbesondere der heranwachsenden Generationen. Viele Eltern, Erzieher und Lehrer sind damit schlichtweg überfordert, weil sie selbst keine entsprechende Medienkompetenz besitzen.

Posted by Axel Eble in Meta at 16:44

Thursday, November 23, 2006

The European Blackout on November 5, 2006

On November 5th, 2006, a power outage caught about 10 million people all over Southern and Western Europe unawares, half of them in France alone. The cause of the problem? Human error - and a cruise ship leaving its dockyard for the North Sea. From around 10pm CET to around 11pm Western Europe was black.

The following is a summary of the official report by e.on to the Bundesnetzagentur. The new cruise ship Norwegian Pearl was supposed to be pulled from the shipyard in Papenburg through the river Ems into the North Sea. For this to happen, a high voltage line across the Ems has to be turned off to prohibit flashover. This is nothing new and has been done numerous times before. This time, however, things didn't work out according to the plan.

The engineers responsible for the powerflow in the e.on control HQ for Northern Germany considered the remaining capacities after shutting off the line across the Ems as adequate - which was a correct assessment. They did not, however, calculate whether the n-1 criterion was still valid. The n-1 criterion mainly says that power can still be supplied even if another line fails besides the one being shut off. This in itself would not have been bad - had not a sudden power surge occurred which led to an overload of another line connecting e.on with their counterpart RWE and the line having different safety margins on each end (of which the e.on engineers did not know at first). e.on lines can be overbooked for a certain amount of time, so they did not consider the surge critical at first.

The real mistake came then, after finding out the safety margins on the RWE end were lower. Instead of calculating the expected results they bundled up some other lines to distribute the power flow and thus reduce the load on the overloaded line. At first glance, this measure should have been successful. A control calculation would have shown them, however, that instead of reducing the load more load would hit the already overbooked line. They didn't do the calculation (due to limited time for reaction to the already critical situation), so the line switched off. This safety switch-off then propagated southward with the known effects.

The separation of the Eastern and Western parts of Europe with one side lacking power and the other side having a huge surplus of power led to different power frequencies in both parts. It took only 37 minutes to equalize the power flow so the two network parts could be reconnected again. During the equalizing power companies all across South Western Europe had to turn off part of their supply in order to sync the frequencies again.

In total, around 10 million Europeans were without power for about an hour, five million in France alone. The power outages reached down to Southern Spain, even Morocco is said to have been afflicted.

The Norwegian Pearl finally left the dockyard two days late(r).

Posted by Axel Eble in General at 22:55

Tuesday, August 22. 2006

Language Log: Translating leadership, creating verbiage

Language Log: Translating leadership, creating verbiage
"Translating thought leadership...creating business results"

Wonderful, just wonderful! I've nothing to add to it, actually.

Posted by Axel Eble in Experiences, Meta, Off-Topic at 12:37

Monday, August 7. 2006

The Quest to Shutdown A Credit Card Fraud Site

In Viruslist.com - Analytiker-Tagebuch (German only) a Kaspersky Labs technician describes how they found a Russian web site hosting data of about 300 credit cards, some with only basic information, some with deluxe information like ATM PIN, email address and phone number of the owner.

Kaspersky labs then called the Bundeskriminalamt , the German Federal police - to no avail. All three people they were named as responsible for this sort of information were already gone for the weekend. The same at the State police authorities. What is really scary is the fact that they didn't reach anybody from MasterCard or VISA, both. The hotline for lost cards wanted to know the credit card number of the calling party. Ouch.

Well, Kaspersky is not without resources. They finally contacted their US branch office which in turn got in contact with the FBI - and the Russian headquarters took care of shutting the site down.

I'm curious if this experience will change something at the German police institutions. However, I really doubt it.

Posted by Axel Eble in Experiences, local at 12:54

Monday, June 26, 2006

Requiescat In Pacem, WinFS

Today, Heise Newsticker (German only) mentioned that Microsoft finally killed WinFS for good. Of course, they are going to call it differently (like: "[...] WinFS has always been about many things â€" a new model to enrich how users manage information, rich storage technology, and sometimes also a packaging of technology.[...]" according to Quentin Clark from the WinFS team). But, let's face it: there won't ever be a separate piece of software to install that will enable us to use advanced features and fast search procedures.

Why? Difficult question. Personally, I guess that they got overwhelmed by the complexity and the tight integration philosophy that is so deeply ingrained into Microsoft products. Trying to fit too much into it until they realized that pulling the plug is the only valid solution.

What does it mean? Well, it's a big deal for Vista (or, rather, a huge blow to Vista) as the only really useful advanced feature for Vista won't ever be available. Obviously, Microsoft miscalculated something quite important. While I won't go so far as calling it a Domsday scenario for Microsoft, as an analyst I would be wary and start investing in other companies.

And the security linkage? Well, if you really want to have one - think for a bit about what something like this could mean to the security initiative and the overall state of Microsoft software. Will they ever be able to handle their boatloads of highly complex software? I doubt it, but then, I'm a heretic and a sceptic anyway.

Posted by Axel Eble in General at 15:13

Identity: Information, Theft, Cards - Culture!

With the continuing theft of personal identifying information (PII) in the US the old question pops up all over: why is what Americans understand as "identity theft" not a problem in Europe? I think three main factors need to be taken into account here:

European data privacy and data protection legislation forces companies to only collect as much data as they really need to process. That limits the amount of data that can be stolen (or, rather, illegally disclosed) in the first place. Besides, it is highly unusual for contractors to have private, production data on their personal systems.

No "Easy Credit" culture like in the US. From what I've been told by quite a few US citizens by now, the US have a culture of buying things on credit - and thus rely on receiving credit fast and without hassle. In Europe, people tend to inquire for credit only for large sums and usually only for buying a car, a house, an apartment - or other larger investments.

Europe (with the exception of the UK) has government-issued identity cards that uniquely identify the person. There simply is no need for a social security number that can be shared easily without accompanying documents (and pictures. And whatnot).

These issues in combination make illicit information access much riskier in Europe than it is in the US. Oh, and it shows that identity documents don't have to be such a bad concept as many US and UK citizens make them out to be.

Over at the Identity Corner, Stefan Brands has an interesting series of articles about the UK identity cards:

- Final UK study on digital identity (Part I)
- Final UK study on digital identity (Part II)
- Final UK study on digital identity (Part III)
- Final UK study on digital identity (Part IV)

Posted by Axel Eble in General at 13:12

Germany: Greens Urge Government To Force Companies To Disclose Information Breaches

The German Party Bündnis 90/Die Grünen filed an application to the legislative body (the Bundestag) to enact a law along California State Act 1836 to require companies to disclose breaches of information.

The representatives are concerned about what they call "identity theft" - however, what they mean by it is the growing number of credit card information abuse. In Germany and, with the exception of the United Kingdom, in Europe in general there is nothing that resembles what in the US is known as "identity theft". Credit card (data) abuse over here has practically no risk for the client as the credit card companies refund you for money lost. And there is no such thing as your credit rating going bonkers because you can identify yourself with an official government-issued identity document (either your identity card or your passport).

How do you in the US prove you are who you claim to be? How do you get yourself off the no-fly list? Exactly: you can't - at least not without severe hassle. So, in my eyes, the application by the Greens is a smoke screen, aimed at gaining votes. The proposed law will not be effective in reducing credit card data abuse.

Posted by Axel Eble in Meta at 12:12

Blog Export: The Quiet Earth, <http://blog.balrog.de/>

Monday, June 12. 2006

WTF - Apple's OS X is NOT As Secure As a Fortress?!

Oh holy Guacamole! OS X has lots of heap and buffer overflows! Quick, buy Vista and all will be well again! Oh, right. Vista isn't out yet. You've just switched to Apple because of all the exploits and dangers of running XP or some *gasp* older version of Windows. And now you're still insecure?!

Why, yes, of course. There is no such thing as a free lunch 100% security. Every reasonably complex piece or suite of software will. be. buggy - to some extent at least. Granted, there's lots of talk out there about how secure OS X is - and, actually, it still is. It's just not invincible, as it's cracked up to be. But, when Apple says it's products are the best, why would you believe them when you don't believe Microsoft? All vendors are alike in that regard.

And let's not forget that OS X is a revamped version of NeXTSTEP, the OS of the famous NeXT computer. That one was said to be riddled with local exploits, so don't expect OS X to be much better. As OS X is gaining market share, it will become more and more the target of choice for malware programmers.

What is different, though, is the use of administrative accounts (like on Windows where accounts by default are administrator accounts). On OS X, the only administrator account, root, is disabled, and to run administrative tasks one has to enter the password (this is a better-working equivalent to the runas command in Windows).

Moral of this? If someone tells you they are offering perfect security, chances are they are lying and only want your money. Be careful, always - it's a dangerous world out there.

Posted by Axel Eble in General, Meta at 14:18

ESAG vanished

I've written twice before about the European Security Advisory Group. I thought I'd check up on them again - only to find they have gone as quietly as they appeared. telepolis guesses (I believe correctly) that it was just a smokescreen for the US DoD propaganda group called Office of Strategic Influence.

Good riddance - another open book closed.

Posted by Axel Eble in General at 13:36

Flight Data Transmission from EU to US illegal

The European Court of Justice has declared the treaty between the European Commission and the US Federal Government for the transmission of passenger data to US officials as illegal. That sounds like a big win for data protection and privacy at a first glance - but is it really?

Well, no, it's not. The original intention of the complainants was to have the European Court of Law state that the treaty does not conform to European Data Protection Legislation. However, all the Court did was rule that there was no legal basis for the treaty at all.

The European Commission had signed the treaty because they claimed that they were responsible because the data concerned was collected by private organizations and companies. The Court in turn clarified that the EU Directive did not cover Penal uses of data and since the data would only be collected for purposes of criminal prosecution the directive does not apply. Thus, the Court carefully managed to avoid the trickier side of politics and navigated around those particular rapids.

So, what does this ruling mean? First of all: the EU has until the end of September 2006 to come up with a new treaty. So far it looks like the Commission will try to push through new legislation to create the legal grounds for the treaty with the US Administration. Mind you, this is not easy because Criminal Legislation is still in the courts of the individual States - there is nothing like a common criminal legislation in Europe. EU law would have to be changed - unanimously by 25 member States. You can bet that political issues (both European politics and local politics) will greatly influence the stance of each State. If the change does not happen, each State would have to negotiate a separate deal with the US.

Blog Export: The Quiet Earth, <http://blog.balrog.de/>

Ah, so finally we have our rights back and have full control over our data! No, unfortunately not. If the airlines don't transmit the passenger data to the US, they will experience heavy sanctions by the United States of America.

The best way to keep control about your data is by not going to the USA for now.

Posted by Axel Eble in Meta at 13:13

Thursday, June 8, 2006

The Sky Is Falling (This Time For Real!) - or is it?

Lately Andy Tanenbaum got into the news once again because a few of his students have created a scenario where RFID tags could be used to compromise databases. Upon looking at the news item a bit closer it clearly has little to do with the RFID tags.

Basically, what it boils down to is that RFID tags could be used to compromise databases through SQL injection. Big deal, innit? The threat may be real, but that doesn't make it a new one. Granted, the attack vector is different, but the attack itself is age-old.

So why make such a fuss about it? Need to get in the news again? One cannot help but wonder.

However, this shows clearly that people still scramble to adopt new technologies without considering security in the first place. It's about time that secure application design is taught in schools and universities.

Posted by Axel Eble in Technology at 08:28

Friday, February 3. 2006

What Kind Of Weather Are You?

You Are Lightning

Beautiful yet dangerous
People will stop and watch you when you appear
Even though you're capable of random violence

You are best known for: your power

Your dominant state: performing

What Type of Weather Are You?

Posted by Axel Eble in Off-Topic at 10:49

"Nah, we don't need no steenkin' study!"

As could be expected the European Commission "sees no need" for a study about the effects of the advance collection of data they have decided to enforce. Heise covers this yesterday (German only).

Posted by Axel Eble in General at 09:47

RFID Based Passports With BAC Vulnerable

In a current news item Heise reports that the Dutch security company Riscure found a way to brute-force attack the encryption of the Dutch ePassports. Let's recap: the ICAO has issued a set of guidelines on "Machine Readable Travel Documents" that basically states that passports and other travel documents should use an RFID chip that can be used to read the individual's data contactless. Apparently the field strength is strong enough to be read from several meters distance. However, the transmission is encrypted by "Basic Access Control" (BAC) where the key is comprised of the serial number of the document itself, it's issue date and it's invalidation date. This gives about 56 bit of key length (which is not really that much and it's questionable if it will be safe to use on a mid-term timeframe. Now, the issuer of the Dutch ePassports uses sequential serial numbers and the number of documents issued is basically constant per time unit. This gives a linear connection between the issue date and the passport serial number, thus effectively reducing key length to about 35 bit - which is easily breakable in a few hours without special hardware equipment.

This attack vector is valid for every document that uses BAC and uses predictable serial numbers for the documents! What hasn't been stated so far is the fact that once the key is known the RFID chip could theoretically be read everywhere. Consider a country that's gone off the deep end with hysterics about terrorism and thus has installed RFID scanners throughout what they consider critical points. Now they only need those scanners hooked up to a central database where all keys to all passports ever seen entering has been stored and they can easily find out where a person goes (given they take their passport with them).

Posted by Axel Eble in General, Technology at 09:41

Blog Export: The Quiet Earth, <http://blog.balrog.de/>

Saturday, December 24. 2005

Merry Christmas

Not that I'm religious in any way, but happy end-of-year festivities and a happy new year to all of you.

Posted by Axel Eble in Off-Topic at 22:42

Monday, November 28. 2005

What type of RPG player are you?

You scored as Method Actor. You think that gaming is a form of creative expression. You may view rules as, at best, a necessary evil, preferring sessions where the dice never come out of the bag. You enjoy situations that test or deepen your character's personality traits. Method Actor92%Storyteller83%Tactician67%Power Gamer50%Specialist42%Casual Gamer17%Butt-Kicker8%Law's Game Stylecreated with QuizFarm.com

via kris

Posted by Axel Eble in General at 21:53

Databases and Normalization

Relational Database Management Systems (RDBMSs) use special forms to keep data from being kept redundant: normalized tables. If you're like me, you haven't memorized or completely understood normalization up to now. If you do, however, want or even need to know how it works and enjoy cat content in blogs, you might want to reference Azundris' Introduction. German version available as well.

Posted by Axel Eble in Off-Topic at 15:35

Wednesday, November 23, 2005

Stupidity, Applied

Isn't it amazing how stupid some people can be? I did get some business cards from an organization I'm member of. They managed to put not one, not two, not even three but four errors into two lines of the cards. And, of course, they did not send me a version ahead to check for mistakes. I now have about 100 or 200 business cards that are worthless. They did cost money, both for printing and sending them across the Pond from the USA. Go figure.

The mistakes were: instead of "Trienter Str." they wrote "Tricenter Str.", the number was changed from "6b" to "66", the city was mis-spelled from "Kempton" to "Kempton" and the region "Allgäu" was spelled "Allgu". I can understand the last mistake as they were printed in the USA and they have no idea anyway how to create those darn Umlauts, but that's about all. The rest is simple stupidity. Oh my.

I have the cards printed locally now. Even though the printer is just around the corner (literally) they did communicate with me by email and sent the preliminary sheets before starting to print.

Posted by Axel Eble in Off-Topic at 20:21

Evil Is Who Evil Does

As Germany's best known for it's organizational talent (which always make we wonder whether I really am German, but that's another story), which some also prefer to call bureaucracy I'm very happy to have stumbled upon a nice manual on how to drive administrative officials into stark raving madness.

German only, so if you don't understand the language, I'm sorry, but you're outta luck.

Posted by Axel Eble in Off-Topic at 19:16

Fachsimpler-Test

The Fachsimpler-Test is a test by one of Germany's larger political (?) magazines, Der Spiegel (or rather their online counterpart, Spiegel Online). It is a test aimed at helping school students to find out what subject they should take at University.

ToJe, Zugschlus and ThildkrÄtze all took the test and found large differences between their field of interest/work and the suggested subject of their studies. The test should be taken with a grain of salt as we all are slightly older and experienced than we were right after school, but, well, it's quite interesting to see the discrepancies.

Thinking about it the result is not that far off: I am a generalist with a broad spectrum of interests after all.

Posted by Axel Eble in Meta, Off-Topic at 19:03

Airline Passenger Data Transmission To US May End

In 2003 the US ordered airlines to transmit flight passenger data for all flights ending in, stopping over in or just crossing US American territory. It was made clear that all data was to be stored in raw form and would be subject to further analysis, leading to profiling of passengers, all, of course, in the name of fighting terrorism. It is completely unclear what sort of profiling will be done and what else the US government will be doing with the data (e. g. handing it over to some commercial data brokers like gasp ChoicePoint for analysis). The Washington Post has a good summary as well.

The EU Commission and the EU Council caved in instead of taking a strong position against this practice and declared the US data handling processes as equivalent to European processes and, in general, good enough. This led to a huge outcry from the EU Parliament and several Civil Rights organizations (like the European Digital Rights Initiative) but both the Commission and the Council wouldn't budge.

Now, however, things start to look a bit brighter: the Advocate General at the Court of Justice at the European Communities recommends to annul the Council decision about the agreement. The Court will have to rule about a law suit by the Parliament against the Commission and the Council decisions. The recommendation of the General Attorney are not binding but in most cases the Court will follow advisory opinions.

References:

Heise Newsticker (German)

Washington Post

Posted by Axel Eble in General, Meta at 10:28

The City of Dis

Well, what do you know? I've landed in Dis after taking the Dante's Inferno test:

The Dante's Inferno Test has banished you to the Sixth Level of Hell - The City of Dis! Here is how you matched up against all the levels: Level Score Purgatory (Repenting Believers) Very Low Level 1 - Limbo (Virtuous Non-Believers) Very Low Level 2 (Lustful) Very High Level 3 (Gluttonous) High Level 4 (Prodigal and Avaricious) High Level 5 (Wrathful and Gloomy) High Level 6 - The City of Dis (Heretics) Extreme Level 7 (Violent) Moderate Level 8- the Malebolge (Fraudulent, Malicious, Panderers) Very High Level 9 - Cocytus (Tracherous) High Take the Dante Inferno Hell Test

Thanks to Adam.

Posted by Axel Eble in General at 07:08

Thursday, November 17, 2005

Security Convergence

"Security Convergence" is the subject of The Alliance between ISACA, ISSA and ASIS. Seeing what the focus of all the three groups is it really does make sense: ISACA's main operational field is Governance, especially IT governance; ISSA is "the global voice of information security" and ASIS is primarily concerned with physical security.

It's pretty clear that those three fields do converge more and more, so The Alliance is an important step in the right direction. It will help to open the eyes of security professionals worldwide to the other fields. It will, thus, help to raise a more business oriented security program in enterprises. We shouldn't expect too much in too little time, however: I don't believe that many companies understand at the moment that security is something that needs to be considered in a (I hate to use the term, but it does fit so nicely) wholistic way.

So, at the Network Security Conference/Security Management Conference of ISACA in Amsterdam last Monday the panel discussion was just about this: "Security Convergence". I was invited to represent ISSA at the panel. It was rather interesting to see the different points of view on the panel - and in the audience. Another member of the panel, Carl Thorp, stayed on for the day (I had to get back unfortunately) and reported that there were quite a few interesting discussions about the convergence thing. However, it seems to be of prime import to define what "Convergence" really means.

It will be interesting to see the discussions around the term in the near future.

Posted by Axel Eble in General, ISSA, Meta, Organizations at 20:30

Monday, November 14, 2005

First time to the Netherlands

I've been invited to represent ISSA at a panel discussion at the ISACA Network Security/Security Management Conference in Amsterdam. It's my first time to the Netherlands and, unfortunately, I won't have any time to do some sightseeing.

The panel discussion is about The Alliance between ISACA, ISSA and ASIS about the convergence of physical security and information security. The folks are great and I wish I had more time to spend here.

Posted by Axel Eble in General, ISSA, Organizations at 07:44

Thursday, November 3, 2005

The Dangers of Inference

Here I am, taking a strong stance about government agencies that collect data and use inference to think about what it might possibly mean. There's no lack of wrong inferring to be done that way, starting from false assumptions about coherence of incoherent data or by simply interpreting too much into too little data.

And suddenly I find myself here, doing exactly the same: thinking F-Secure jumped on the bandwagon of Mark Russinovich's posting at sysinternals for their excellent work of analyzing the Sony DRM Rootkit. Independently, I should say, because that is what they did. They did not, however, manage to make it clear how they got wind of the thing (which they did earlier than Russinovich and were in contact with Sony to discuss the issue). After Mark published his findings, F-Secure thought it was now time to publish theirs, too.

Can't blame them, really. I blame myself, however, for jumping to unjustified conclusions. Ah well, as I said: inference is bad.

Posted by Axel Eble in General, Meta, Off-Topic at 01:47

Tuesday, November 1. 2005

Ch-ch-ch-changes

Jon Toigo is annoyed at the lack of progress the information security field has made since the Medieval. I feel his pain, too. But what are the alternatives? Or rather, why are we still using the same concepts? Are we just too stupid to come up with something new or are the concepts just so basic and so sound that there is no better way? Let's take a look at the items Jon mentions.

Access Control: moats and stockades then, firewalls now. Access control is still one of the soundest principles of information security. Control who may access information when and how and you have removed several vulnerabilities and reduced your risk dramatically. However, the technologies being used for access control change considerably over time. Up until the 1980s to 1990s access control meant control of physical access. Computers were large and heavy and access to them could be controlled pretty strictly and fairly easily. Enter The Network - and things shift completely. Or, to be fair, they get expanded. Physical access control is by then pretty much a commodity: people just do it anyway. What's new is that access to the computers is not only available by physical access but by network access as well.

While the Light Side had control for an enjoyable while it was only a matter of time until the Dark Side jumped on the bandwagon and started to use the Net for their sinister purposes. So well, Marcus Ranum writes the DEC SEAL and it starts to get a success quite fast: companies hire firewall administrators to take care of these arcane beasts that are tough to tame (alliteration not intended but gladly taken). Fast forward to today: every simple DSL router for home use has a NAT firewall included; the network guys do the firewalls on the side and up come web services with the nice side effect of tunneling "stuff" across HTTP (yes, and other protocols, but HTTP really is ubiquitous by now and a nice example of the ever changing technologies, thank you). So now we have web application firewalls which really are nothing else than application layer proxies. And so it goes, goes round again. (Kudos to Joe Jackson)

Signet Rings and Trusted Certificates - now there you've hit a sore spot, Jon. I don't trust the PKI model with a commercial head - much less even if said head is Verisign. The last piece in the puzzle was their Sitefinder "service" which accidentally broke half the Internet. But really, why do we trust signatures, signets or certificates at all? Chances are, the signature is illegible anyway so a cursory glance of similarity is all we get. Same with certificates (without even the added benefit of Verisign). No solution there, I'm afraid.

Edicts and Policies - good point, Jon. However, I consider them to lay out the rules by which we play. We agree upon a set of rules to be able to note deviant behaviour and sanction it. Thus, policies and edits are rather useful tools as they prepare the ground for legal skirmishes or, in some cases, provide the opportunity to find out unwanted behaviour in the first place. I wouldn't want to live without them.

Codes and Encryption are powerful tools, too. Unfortunately, many people tend to forget that encryption is a temporary safeguard at best. Even if the encryption algorithm has no known weaknesses it still will fall given enough time. There's the rise in computing power and the change to other technologies (can you say Quantum Encryption? I knew you could!). As long as people recognize this, they are quite secure. All they have to do is select an algorithm that will possibly keep the information secure as long as it has to be classified.

Interestingly enough, the bad guys don't seem to have learned either how to circumvent the safeguards we set up. Either they are as caught in our ways of thinking or there simply is No Better Way at the moment.

What do you think?

All of this, however, has nothing to do with vendors coming up with new products all along instead of listening to what the customers want - just like in the storage market. Thanks for the eye-opener, Jon!

Posted by Axel Eble in General, Meta, Technology at 00:03

Saturday, October 29. 2005

SYSTEMS

So, SYSTEMS today. Rather disappointing, I have to say. Contrary to what the expo management said it didn't look like there were more exhibitors there this year than last. And certainly there were more booths empty in those halls that were open. I had the impression that at least one hall could have been saved.

Only few of the big players were present and even some of the companies that were there last time were missing this year. It was a strange experience today, seeing the importance of the SYSTEMS expo decline each year. It'll soon be a rather regional experience. Sad, really.

Posted by Axel Eble in General at 01:05

Wednesday, October 26, 2005

Conservatives going off the deep end

heise reports that the CDU/CSU parties warn of potential terrorist threats to IT infrastructure. Yawn yawn. I just love it how terrorists are responsible for anything and dangerous for everything. And, being the conservatives, one could expect them to scream for direct data exchange between governmental, law enforcement and intelligence agencies. Why, sure enough that is exactly what they want.

"International terrorism and information technology are related in a multitude of ways," Mr. Koschyk explained today. The information infrastructure was a potential target for international terrorism, he observed.

Oh yes, bringing the Internet down will strike terror in the hearts of the people like nothing we have seen before. Tell that to the people in Pakistan, to the people in Far East caught by the Tsunami, the people in New Orleans, to the people in Florida and whoever else has been struck lately by nature's catastrophes.

Posted by Axel Eble in General, Meta at 12:52

Tuesday, October 25. 2005

SYSTEMS 2005

I'll be visiting SYSTEMS 2005 on Friday, October 28. If anyone of you is there then, let me know and we can hook up.

I seem to have missed Richard Stiennon as he'll be outbound on Wednesday already.

Anyone else?

Posted by Axel Eble in General at 08:18

Friday, October 21. 2005

RSA Conference: Conclusion

A final look at the organization of the RSA Conference in Vienna seems appropriate. Rather unexpectedly, the organizers of the conference found themselves with around 1,400 participants. That's quite a lot and certainly a lot more people than the last times if I'm to believe what I'm being told by others.

It remains a mystery to me, though, why they scheduled both talks by Ira Winkler and Bruce Schneier in somewhat small rooms instead of in the one large hall. In that light it was a good idea to shift the sessions that seemed to generate larger interest into other, larger, rooms. This, however, made the pre-made signs and schedules incorrect which in turn led to largely inaccurate plans and a whole lot of unnecessary walking. It would have been a good idea to set up screens to show the current (revised) schedule in front of every room instead of fixed, printed signs. It would also have been helpful had there been a schematic of the building at each room entrance for easy orientation.

And, as a final note, even if I seem to be the only one blogging about RSA Conference Europe 2005, it would have been quite helpful if the lecture halls had been equipped with WLAN.

What I did like was the provided lunch. It consisted of some fruit (banana, apple), a sandwich or two, some piece of dessert, some snack and a bottle of water. Granted, it wasn't anything warm, but one can't expect everything, now can we?

Posted by Axel Eble in General, Meetings at 08:39

Thursday, October 20. 2005

RSA Conference: Networking

From a networking point of view the RSA Conference was a great success. I finally got to meet Candid Wäst, met with Frank Ackermann from the Munich Security Group and Steffen Müller from the Frankfurt one, met Patryk Geborys from ISSA Poland, saw Paul Wang (CISSP from PwC Geneva), Klara Wilhelm from (ISC)² Europe, Yves LeRoux (fellow CISSP and ISSA member) and Jon Colombo, a fellow member of the CISSP Forum mailing list. Through him I met Andreas Mitrakas from Enisa. We had a lot of fun (and the wine was actually rather good, at least the white one). Besides getting signed copies of books by Bruce Schneier and Ira Winkler, I got to know Katrin and Juri(?) from the F-Secure Antivirus Research Team and had a nice chat about mobile/cell phones, Nokia and SonyEricsson

Posted by Axel Eble in General, Meetings at 15:26

RSA Conference: European Information Security Awards (EISA)

After the Keynotes on Monday the European Information Security Awards were published. I found it rather interesting that two of the four awards went to Accenture. They must have changed a lot since I had anything to do with them. Quite a few other people I spoke to at the conference had equally bad experiences with them.

Posted by Axel Eble in General, Meetings at 15:03

Wednesday, October 19. 2005

Continental Europe

One thing that's fascinating me all the time is the influence of the Gulf stream on Europe's climate. Vienna is too far away from it to still receive its benefits, so this morning it was rather cold here. Back home it should be around 3-5°C warmer. Really amazing, the difference between continental Europe and Western Europe.

Posted by Axel Eble in General at 11:19

Tuesday, October 18. 2005

RSA Conference: Trends in Information Security, Bruce Schneier

Contrary to the abstract Bruce Schneier was talking about trends in information security and their economic equivalents. The basic message was that the scene is constantly professionalizing - away from amateurs and toward professional crime. One noticeable quote was:

We now have more technology than we are willing to use

which is another way of saying "If you think technology can solve your problems you don't understand technology and you don't understand your problems."

The economic terms that influence security on a larger scale are

- Trade-offs
- Agenda
- Externalities
- Loss Allocation

Not many new things, but it's always a pleasure to hear Bruce speak and listen to his examples.

Posted by Axel Eble in General at 17:24

RSA Conference: Security of Web Services, Vic Morris

Vic Morris gave an interesting overview of Web Services and the specific security nightmares going along with them. The usual combination of SOAP, WSDL and UDDI is extremely powerful, but, alas, can get extremely complex in an extremely short amount of time. Thus, many companies use Plain Old XML (POX) instead of the tools above.

Rather than thinking of how to implement security in each part of the web services Morris suggested implementing security as web services themselves. He advocated security in depth by using existing features like directories and web access authorization and the like (which makes sense, no reason to re-invent the wheel time and time again). XML introduces a lot of new security threats like SQL injection through XML payload, XPath Injection, unexpected attachments (and how to deal with those), malformed XML etc.

As we have witnessed in other parts of the field, security is continuously moving up the ISO protocol stack and is about layer 7 now.

Summarizing the threats of web services are:

- creeping complexity
- unauthorized access
- XML threats

XML Gateways (web application firewalls) can help a bit but should be complemented by web service security.

Posted by Axel Eble in General at 17:19

RSA Conference: Secrets of Superspies, Ira Winkler

Winkler started off by telling about his days at NSA, describing some common vulnerabilities that were prevalent even in the ultra-secure NSA. From there he went on to explain why both "superspies" James Bond and Sydney Bristow are actually bad secret agents: they get caught by the (well-designed) security of the bad guys.

The large difference between "Hackers" and "Spies" is that the former don't work in a structured, "scientific" way whereas the latter do exactly that. Spies tend to implement countermeasures to mitigate vulnerabilities, not threats, and they work hard to get security in depth. All in all, it's about optimizing risk: deciding how much (potential) loss you want to live with.

If you haven't heard Ira before and should ever get the chance, don't hesitate (given you understand English spoken fast

like in "real fast"). He's one of the exceptional speakers in the security theatre, like Marcus Ranum and Bruce Schneier.

A couple of anecdotes from the talk:

A cell phone was ringing in Ira's talk. Suddenly he went: "Is that mine?... My, that's obnoxious!"
"Then we had to change the whole thing from a penetration test to an incident response. Kinda ruined the day."

Posted by Axel Eble in General at 17:05

RSA Conference: Keynotes

First keynote was David Taylor, the host for all the keynotes, introducing the 1920s and the era of prohibition. Nice, but nothing overwhelming.

Second keynote was Dame Stella Rimington, former Director General of the British Secret Service MI5. She was terrific! Like most security professionals she has a very level-headed approach to law enforcement and legal regulations. She warned against feel-good security and acknowledged that striking the right balance between security and civil rights is hard, but that the latter should be scrupulously guarded (at least, that's what I read from it).

Third and last keynote was by Art Coviello, CEO of RSA Security. He was talking about identity. While what he said rang true, I think Dick Hardt has a more visionary approach.

Posted by Axel Eble in General at 12:39

Monday, October 17. 2005

RSA Conference: Matching CobiT, ISO17799 and ITIL, Yves LeRoux, CA

Yves LeRoux compared the three frameworks CobiT (oriented toward IT Governance and Audit), IT Infrastructure Library (geared toward Service Management in IT) and ISO17799 (International Standard for Information Security Management). His conclusions are that all three complement each other. CobiT could be used in conjunction with ISO17799 for evaluating the current IS state of an organization. ITIL can be used with CobiT to organize and improve processes and, finally, ITIL and ISO17799 together can be used to improve the security management posture of an organization.

Posted by Axel Eble in General, Meetings at 15:10

RSA Conference: (ISC)2's Professional Workforce Study, Sarah Bohne

Sarah Bohne, Director of Business Communications and Constituent Services, held a talk about (ISC)2's Professional Workforce Study. (ISC)2 is evaluating currently certified IS Professionals with regard to the development of their jobs and their education.

Interesting fact is that APAC has the largest requirement of IS professionals while at the very same time having the lowest salaries. Either the job market is askew there or we need to take the general standard of living into account. The talk leaves a few open questions, but those might be answered in the full-fledged report that will be out in December.

Posted by Axel Eble in General at 15:09

RSA Conference: Tim Mather on Changes in Information Security And The Implications For CISOs

I attended Tim Mather's talk on the Changes in Infosec and what it means for CISOs. It was rather disappointing as Mather didn't say anything new or anything out of the ordinary.

What he stated was more or less that from technical information security in the 70s the focus has shifted to processes and will shift more in the direction of Risk Management. Well, yes, Big Deal.

I had expected slightly more than this from the CISO of Symantec.

The one rather funny highlight was that he was talking about "point solutions" with isolated management consoles - alas, he talked about them as if they were a thing from the past. The console Symantec has in their portfolio is definitely nothing better. While it can integrate other security devices, there is no vendor-neutral standard for consolidating log entries, much less management of security devices. Symantec is nothing special in that regard, though. All the security vendors do it the same way. They offer some "vendor neutral" management approach. On looking closer one sees that it can only aggregate so much of other vendor's capabilities.

Posted by Axel Eble in General, Meetings at 12:51

First Impressions: RSA Conference Europe 2005

Just arrived this morning in Vienna. I'll be here at the RSA Conference Europe 2005 until Wednesday evening.

Great networking so far, even met someone I didn't know would be here. The big program starts tomorrow, so expect some more comments during the next two days.

Posted by Axel Eble in Meetings at 12:25

Sunday, October 9, 2005

The difference a year makes

In 2004 DARPA issued the first Grand Challenge: having fully autonomous vehicles run a challenging (sic!) course. The best vehicle ran into a ditch after 12 km and caught fire.

This year, however, things were to be a bit different: five vehicles from 23 reached the finish. The best one was the Stanford team with a stock Volkswagen Touareg R5 TDI motor. Congrats!

[Links will be added later]

Posted by Axel Eble in Off-Topic at 23:03

Thursday, October 6, 2005

Another One Bites The Dust™

Martin pointed me to Sourcefire being bought by Check Point. I'm annoyed at that because Check Point is like any big player in any field: they buy a company and suck them dry. I am very apprehensive what they are going to do to Snort and how Marty Roesch will get along.

If I were to look in the crystal ball I'd predict that Check Point will kill the GPL and open source version of Snort or at the very least will try to squash it or drop support.

Of course, we'll see what pans out. I'd really love to be wrong on this account. Oh, and for the record: I hope Marty Roesch got a good deal out of it.

Posted by Axel Eble in Meta at 22:42

Wednesday, September 14, 2005

Silliness, Thy Name Is Infosec Companies

I hope Shakespeare forgives me the mangling of Hamlet's line about Fair Ophelia, but really, enough is enough.

I've heard quite a few vendor presentations in the last while, most of them by big players in the information security market. Quite a few of them started with antivirus products and moved on to swallow greedily every company that didn't manage to climb the trees upon counting to three. One of those companies seems to have swallowed one bite too many in too short a time and ended up splitting itself apart (that'd be mitosis for you, by the way). But I digress.

Every one of those vendors has an Intrusion Prevention System (IPS) Appliance in their product portfolio. So far, so good. However, the latest ploy of their markedroids is to sell it like this:

[â€]In the past we've seen the rise of Intrusion Detection Systems and every company and their neighbor ran to get one. Upon deploying they noticed they got tons of false positives which they'd never wade through and thus phased those systems out again after a while. And let's not forget these things are reactive!

Now we have our brand spanking new Intrusion Prevention Systems that can actually do something about unwanted traffic - it can block it automatically![â€] Yada yada yada.

I take issue on this statement on no less than three four points:

An IDS throwing so many false positives is not configured correctly. An IDS is a wonderful tool for analyzing your network traffic and then tweaking your IDS ruleset to adapt to your particular set of protocols and traffic patterns. An IDS in my eyes is also a very wonderful tool to analyze network problems (which rather tells why I don't like the moniker IDS - it's a pattern and traffic analyzer with a configurable ruleset). It is not, however, a silver bullet.

So basically what the vendors are saying is that the IDS systems we bought off them five years ago were pieces of crap and we should buy the same pieces of crap with added bells and whistles? Because they never mention that the false positives are gone in their IPS... sneaky weasels, those markedroids, aren't they?

So an IDS is reactive. Big deal, most security measures are - simply because it's a mathematically hard problem to enumerate all potential threats and tag them with meaningful probabilities.

Hey, vendors, you're s0, like, w4y c001 that you are proactively blocking traffic with your IPS systems. Only if you didn't manage to sell me decent products in the past that did what you marketed they would, can you tell me why I should want to buy another of your systems that goes so far to automagically block network traffic? I'd want to be damn sure that I didn't block anything business related! And, finally, what's so wonderfully proactive about blocking traffic? It's still reactive, only a bit earlier on in the connection setup. Proactive would mean to anticipate malicious traffic and patch the appropriate systems before the malicious and mobile code can reach them.

Which brings us full circle round to what really works: thinking about your problems instead of your symptoms. Rather than liberally deploying IPS appliances across your network you might want to analyze the traffic patterns with dedicated network analyzers (you may even call them IDS if you're cocky!) and then segment your network into different zones with well-defined traffic patterns that can be safely secured by firewalls and other blocking technologies. Take, for example, a web server. It doesn't need to be available via SMB. So block ports 135, 137, 139 and 445 ingress and egress all traffic save that you know is good and valid for the given network. Flat networks are a nightmare for trouble shooting, no matter if they're switched or not. So segment them in any way you can. That's being proactive.

Posted by Axel Eble in Technology at 20:49

Bad Case of Referer Spam

Just a quick note before we commence with the evening program: I've been experiencing a bad case of referer spam lately which led to some outages over the last couple of days.

I apologize wholeheartedly for the inconvenience and hope that with the time I took right now to analyze the problem and the entries I added to my .htaccess things will improve.

Thank you for your patience.

Posted by Axel Eble in General at 19:35

Sunday, September 4, 2005

Silly 'droids

Okay, I know it's silly. However, some things I just can't pass...

Posted by Axel Eble in Off-Topic at 18:50

Thursday, August 25. 2005

Don't Bark Too Loud

Maximillian Dornseif writes in *Barking at Banks* that German banks sell indexed transaction numbers (iTANs, authorization codes for individual transactions) as the best thing since sliced bread and that all security woes would be magically cured by their use. He goes on to say that the banks spread misinformation and points to an advisory by his students about how iTANs are of no use against Man-In-The-Middle-Attacks. Which, of course, is right. However, iTANs are a good tool against phishing - a phisher won't have any idea which TAN will be the next and even if they phish two or three TANs chances are they are of little use to him. And that's not even mentioning that users should get some funny feeling upon a) reading phishing emails as they are translated so extremely bad that it should be obvious they're not from the bank and b) the form asking for the TANs doesn't ask for TANs with specific indexes. So, while iTANs don't help against trojans they are pretty useful against phishers.

Dornseif's and his students' underlying premises are true, however: if the banks would use a sufficiently good mix of low-level and high-level security things would be much harder for phishers. What do I mean by low-level security? Things like not sending out HTML emails but simple text/plain messages, sent from the email servers and domains of the bank itself. And what do I mean by high-level security? Well, a time based one-time password (OTP) would be a better idea than a list of pre-generated TANs. However, the cost/benefit ratio probably won't see us going there. Even better would be HBCI with a Class 3 chipcard reader. In that case, however, the user interface is clumsy (as is often the case with security: it's not exactly user-friendly). So I don't see much happening on that front, either.

As a final note, it's quite interesting how diverse different countries' banks can be. In some countries banks hand out time-based OTP tokens, in the USA on the other hand banks don't seem to get a grasp of the concept of transaction authorization. Quite interesting, actually, as I'm sure it ties down to the mentality and society of the corresponding people.

Posted by Axel Eble in *Experiences*, *Technology* at 15:07

Tuesday, August 23. 2005

Drowning

Be advised that this blog might just be offline for some time. We are experiencing heavy rain and the local river, the Iller, has already flooded parts of the area. Downtown Kempten is in serious danger of getting flooded, too. While we wisely decided to live up on the surrounding hills it might well be that the electrical power company or the telecommunication provider can't guarantee my uptime. I'll try to get some pictures for those curious enough .

Update: So, we obviously survived. For the curious, the local newspaper has a few pictures available.

Posted by Axel Eble in Off-Topic at 09:32

Thursday, August 18. 2005

Honeyclients

In my earlier post about Microsoft's HoneyMonkey project I mentioned that the HoneyNet Project will probably latch on and develop something along the same lines. In the meantime, I was notified of Kathy Wang's Honeyclient project and the client-side honeypots diploma project at the Laboratory for Dependable Distributed Systems at Rheinisch-Westfälische Technische Hochschule in Aachen.

Thanks to Thorsten Holz and whoever else pointed me at the Honeyclient project (I can't remember. Must be age creeping in).

Posted by Axel Eble in Technology at 09:07

Sunday, August 14. 2005

Sneakers

I was just watching Sneakers on DVD. While quite a bit of the movie is Hollywood, another large part is still true - or rather, gets true more and more.

What's that, what Cosmo is saying?

There's a war out there, old friend. A world war. And it's not about who's got the most bullets. It's about who controls the information. What we see and hear, how we work, what we think... it's all about the information!

So true.

Posted by Axel Eble in General, Meta at 22:31

Monday, August 8. 2005

Microsoft (In-) Security Rehashed

I confess: I am a Microsoft basher. By now it's probably a die-hard habit, too. However, what I'd like to write here and now is: it is soooooo 90s. In other words: it's boring the heck out of me to listen to myself whine about how bad Microsoft is security-wise.

There are actually two issues here:

Microsoft is getting better and the freedom they give their employees to blog and work with grassroots journalism publication is a great thing. Astroturfing happens less and less and this is A Good Thing. The underlying problems are what should be looked at. It's not "Microsoft is Evil, thus Microsoft needs to be bashed. Microsoft is The Enemy". Instead, let's take a look at the core of the problems MS is having with security.

So, expect some blog entries in the near future about what I don't like about Windows and why I think there are design flaws in it that make security a hard problem. Quite a bit of this will spotlight on behavioural patterns, too.

Oh, and I'll spare us the ubiquitous comparison with Linux or other *ix variants. This has been done before by people that have a much better understanding of each kernel than I have (or possibly ever will have).

Feel free to bash (pun intended) me if I cross these self-adopted limits.

Posted by Axel Eble in General at 23:55

Are You Reading Me? or Curiosity Killed The Cat

To all you Out There™ reading me: would you mind telling me that you do and if so, how you found this blog and whether you like it?

I know of a few people (The Usual Suspects™ - you know who you are!), but the ones I don't know I'm interested in.

Feel free to use the comments or drop me an email.

Posted by Axel Eble in Meta at 23:46

Identity Theft Ring Uncovered

Sunbelt, a Florida security software provider seems to have uncovered a huge identity theft issue. Their blog entry [More on the identity theft ring](#) tells more.

Via Deb Radcliff.

Posted by Axel Eble in General at 21:57

Making IT Matter

Jon W. Toigo (of "Desaster Recovery Planning" fame, the only decent book about the topic) blogs in Making IT Matter about his upcoming book juxtaposing Nicholas G. Carr's article IT Doesn't Matter. As said article was featured in the current issue of the Gesellschaft für Informatik's Informatik Spektrum journal it's a neat coincidence and I rise to the occasion to voice my point of view.

I only skimmed Carr's article but noticed that it was full of commonplace stuff and really nothing new except for the somewhat provocative theme. Then it dawned on me: it's nothing new to me because it's the typical point of view of someone coming from an environment where IT is constantly being used and pushed forward without delivering any real value. In other words: it describes an organization that is controlled by the IT, not vice versa.

Blog Export: The Quiet Earth, <http://blog.balrog.de/>

The company I'm working for is using information technology since the 70s and 80s. It's a transportation and logistics company and we're making heavy use of IT to control the flow and storage of goods. IT delivers a huge amount of value to the organization and we've come a long way along the path where it will simply not be possible any more to live without it. Our business processes were and still are optimized due to the discriminate use of information technology. Without it, we wouldn't be able to optimize the flow of goods both with respect to the shortest path and the shortest amount of time to deliver. It does indeed give us a competitive advantage - and one that doesn't diminish, for that matter.

True, I've seen more than one organization that had all the latest fads in technology - but usually those organizations lacked a lot on their processual front or they are very IT centric. Those don't count.

So, to sum it up: does IT matter? If business is done right, yes, it does matter. It will support the business, not vice versa. Everyone saying something different just doesn't understand the current landscape.

And that's exactly what Toigo says.

Posted by Axel Eble in Meta at 20:07

Sunday, August 7, 2005

The Strider HoneyMonkey Project

Browsing the web through my News Aggregator I came across the Strider HoneyMonkey Project. Microsoft has added to the honeypot concept (which is passive) with an active component: The Strider HoneyMonkey project takes the static concept of a honeypot in a new direction. A "honeymonkey" is a computer or a virtual PC that actively mimics the actions of a user surfing the Web. A series of "monkey programs," which drive a browser in a manner similar to that of a human user, run on virtual machines in order to detect exploit sites. The browsers can be configured to run with fully updated software, or without specific updates in order to look for exploit sites that target specific vulnerabilities. In this manner, the attacks more likely to impact customers can be analyzed and detected.

Sounds like a pretty neat idea. Too bad they don't plan to publish any product. But I'd bet that the HoneyNet Project guys will jump on the bandwagon (if Microsoft won't be patenting this, that is).

Off-topic Update: Take a look at the Google Ads underneath the article. Guess "Strider" is pretty strongly linked with Lord of the Rings

Posted by Axel Eble in Technology at 19:44

Thursday, August 4, 2005

ConfessionsReport of a Lawyer

Jennifer Granick tells the Michael Lynn story from her perspective. Quite an enjoyable read and quite interesting to hear read an assessment of the legal issues at stake.

Posted by Axel Eble in General at 13:23

Wednesday, August 3, 2005

ISS Replies

As I mentioned in my earlier post I have sent emails to ISS and Cisco with some questions about the incident. I have received ISS' answers today and find them interesting both in what they say and what they don't. I will leave the comments up to you. Here are the original questions again:

Was ISS informed about Mike Lynn wanting to present this particular topic at Black Hat?

If so, was ISS okay with it in the beginning?

When did Mike Lynn finish the presentation prior to presenting?

Was Cisco informed about the planned presentation?

Was Cisco fine with it in the beginning?

When was it decided to cancel the presentation?

Why was the presentation cancelled?

Who decided to cancel the presentation?

And here is the document I received back from ISS:

Has ISS been informed about the intention of Mike Lynn to give the presentation at the Black Hat Conference?

The intent of ISS's participation at the Black Hat conference has been to share information amongst security professionals and create a heightened awareness of specific security threats that companies need to protect themselves against. Therefore it has been agreed to present at the show by a spokes person of the ISS X-Force research team - in this case Mike Lynn has been assigned to do so - preliminary research in the area of potential attacks on router networks and not uncovering any new vulnerabilities. According to that, demonstration on how existing flaws could be exploited has been in focus of the offered presentation. Reason for that is mainly ISSs believe that if our researchers are able to figure out these exploits, then hackers are as well. Aim of our presentation has been correspondingly to bring security professionals up to speed on what hackers out there are already doing or attempting to do, leveling the playing field between the two groups.

If so, has ISS agreed originally that he will held his presentation?

As said, of course it has been agreed that a member of the ISS X-Force team will held a presentation with the intention to present information about preliminary research in the area of potential attacks on router networks. But this area of research is both significant and serious. Thus in the interest of customers it does not make sense at all to disclose any findings until the broader scope and impact is fully understood. Upon completion of full characterization of issues, information are not ready for publication. Because of that knowledge, we have an established vulnerability disclosure policy in place that underlines our commitment to continually improve the security and reliability of customers' and partners' networks. But the presentation held by Mike Lynn at the conference has been not aligned to these disclosure guidelines and in making the presentation he was acting independently and in contrary to ISS instructions.

When has Mike Lynn finalized the presentation he intended to hold?

As already mentioned the original presentation presented preliminary research in the area of potential attacks on router networks. We take the disclosures of vulnerabilities very seriously - in fact we disclosed one involving Cisco two weeks ago - and we pride ourselves in the extensive research that we do. Nevertheless, we have a well established vulnerability disclosure policy, which we follow. Therefore we believed that making the presentation is not appropriate at this time. As said with his final presentation Mike Lynn was acting independently and in contrary to previously discussed ISS instructions.

Has Cisco been informed about in advance about the planned presentation?

Blog Export: The Quiet Earth, <http://blog.balrog.de/>

Cisco has been aware of our preliminary findings, because prior to releasing details on security flaws in certain products to the public we always work directly with the vendor to make them aware of the issues and assist them in fixing the issues before exploits are developed. ISS followed this same procedure in regards to the technologies its researchers presented at this particular conference. By sharing the results, ISS and Cisco have determined that ultimately, the best use of this research is for improving the security of router networks and ISS and Cisco are collaborating in this area.

Has Cisco agreed initially?

Of course Cisco agreed to share essential information amongst security professionals in order to create a heightened awareness of specific security threats that are critical to customers business operations. Cisco takes all security vulnerabilities seriously and because of the fact that the research did not disclose a new vulnerability but helps uncover new vulnerabilities, both companies believed that sharing findings supports customers and partners to identify and protect their infrastructures from flaws in the future. But both companies are dedicated to furthering their understanding in this area for the benefit of customers and partners. So it has been decided by both parties that a full characterization of this issue, the findings and results shall be completed and then responsibly disclosed in a manner consistent with each organizations processes.

When has been decided to withdraw the presentation?

When both teams met again in mid-July, the decision was made to cancel the presentation and to pull the materials from the proceedings.

Why had the presentation to be cancelled?

Upon internal review, ISS felt that the original tone of the presentation was a bit too instructional and wanted to make sure it was in alignment with ISSs established disclosure guidelines. Thus, in the interest of our customers and given the preliminary nature of the research, the decision was made to pull the research.

Who has decided that the presentation will be withdrawn?

When both teams met again in mid-July, the decision was made to cancel the presentation and to pull the materials from the proceedings because ISS felt the research was not complete. Nonetheless, this area of research is both significant and serious. Both companies are dedicated to furthering their understanding in this area for the benefit of customers and partners. Once ISS and Cisco have completed the investigation into these findings, and in accordance with our guidelines, we will disclose details in a responsible manner.

Posted by Axel Eble in General, Meta at 20:51

Congratulations, Risks!

The F-Secure weblog reminds of the RISKS Digest's 20th anniversary today. Thanks to Dr. Peter G. Neumann for handling the digest!

What was new to me was the fact that the Digest is also available as an RSS feed nowadays.

Posted by Axel Eble in Experiences, General, Technology at 12:43

Cisco Continued

According to this Heise Newsticker article (sorry, English translation not yet available, but try checking the English newsticker excerpts later) it is currently impossible to log in to Cisco's website as they have determined that the login process or the password database was compromised. They quickly reset all passwords, thus effectively disabling people on accessing any software downloads (including the latest security fixes).

I don't want to rush to any conclusions without further evidence but considering that hacker teams are currently ganging

up against Cisco there might well be a connection. Either this is completely unrelated to last week's episode or they already have a working exploit want to buy time for working on the exploit by keeping administrators from fixing the vulnerabilities or want to emphasize that Cisco could have managed this better or ...

I'm curious about how Cisco will deal with the situation. I guess they are starting to realize that they are quite a target at the moment.

Update: Cisco has released a "security alert" according to which the customer passwords were accessible through a search engine on cisco.com. Funny in itself, I guess. As long as you're no Cisco customer.

Posted by Axel Eble in Meta at 12:22

Monday, August 1. 2005

Waterloo in Vegas

The Story So Far

By now you all have read about Michael Lynn's presentation at Black Hat 2005. Let's, nevertheless, recap: ISS X-Force did contract for Cisco to check IOS for (possible) security vulnerabilities. It comes as no surprise that they found enough of them (as did others before them, like FX from Phenoelit). The really new thing that makes this very interesting is the fact that Lynn found a design flaw in IOS enabling practically any vulnerability to lead to a local enable shell. The specifics have been written up by TomsNetworking. According to rumours abounding on the 'Net, they informed Cisco about them in April. Funny enough, during March and April Cisco cleaned up the available IOS images from their site, leaving only ones that are supposed not to be vulnerable. Since then Michael Lynn, the ISS researcher in this case, was accepted to talk about this flaw and how it could be exploited remotely. Cisco was informed of this and had wanted to send one of their people along with Lynn.

Now, on the Monday before the Black Hat Briefings, Cisco and ISS suddenly decided they would not have the talk being held and prepared for a different talk about "Internet Security". They even went so far to cut the 10 pages out of the proceedings. Lynn quit ISS on very short notice and held the original talk, knowing full well that it would have legal repercussions. The crowd, however, cheered. Cisco and ISS ordered an injunction ("gag order") for Lynn and Black Hat. Cisco offered a press release stating that Lynn reverse-engineered their code which he was expressly forbidden to do and, furthermore, did not keep to the "responsible disclosure" conduct. Besides, they were in fear for their "Intellectual Property".

Not to worry (and just as expected), the slides of Lynn's presentation were available in PDF format shortly after this whole affair blew up. Now Cisco and ISS are actively legally pursuing everyone hosting the slides. Meanwhile, Lynn seems to have taken a legal celebrity as his lawyer, Jennifer Granick.

The Results

Does it come as a surprise that the reputation of both Cisco and ISS are rapidly going down the drain? What's even more interesting is the fact that neither Lynn is available nor have Cisco and/or ISS decided to put the story on their front pages. So all we are going to get is rumours, blog reports from people at Black Hat and some press releases by the companies in question. I'm trying to get some answers that might shine some more light on the matter. The jury is still out about whether Lynn did The Right Thing™, something illegal, something unethical or all of the above. Let's examine each:

The Right Thing™

Was it good to show a room full of security professionals, hackers and crackers what could be done to the primary routing platform of the Internet? Hell, yes! Security by obscurity has been proven to fail, so we all need to know if there's a grue lurking in the dark. A vulnerability known is one that one can defend against (or least die trying). If it's unknown to me I can never be sure it's unknown to my neighbor with the black basecap.

Something Illegal

Lynn held the presentation which was done on ISS company templates. This shows an endorsement by ISS that wasn't there any longer since he had resigned from them. [Note: Lynn had removed everything referring to ISS from the slides, according to Kat Lacher, who sat in the audience. I apologize for judging from the circulated PDF version.]

He said he had done his research on his personal Cisco equipment that he bought second-hand. As far as I remember IOS licenses don't automatically transfer when selling the hardware. So he might have run IOS illegally in the first place. If he did his research in his spare time on his private equipment and he reverse-engineered the code he broke the license agreement. If he did do his research on ISS equipment, he probably wasn't allowed to disclose his findings without the endorsement of his employer.

So, my conclusion is: he probably did something illegal.

Something Unethical

Independently of any professional organizations he may be member of (which practically all have a Code of Ethics) it may be considered unethical to eff your (former) employer and possibly bring them into a tight space with their principal. On the other hand, there's the duty toward society and Mankind. I don't think this is an easy dilemma to solve.

Concluding this train of thought, I wouldn't know how to weigh those three different aspects against each other. However, there are still other issues at play here. For example, Cisco's use of "Intellectual Property" as the big club to stifle any discussion of flaws in their products. This is a very, very suitable example to show that the Digital Millennium

Copyright Act (DMCA) is severely flawed. The underlying vulnerabilities have nothing to do with Intellectual Property but quite a lot with bad coding. Obviously, IOS is so bloated and so hard to maintain by now that Cisco is rather throwing lawyers at the problem than restarting from scratch (which would be the only valid way to go, in my eyes). That the DMCA is exactly the tool they need for this approach is annoying and only shows how short-sighted said act is.

Officialicisms

In order to get more information first-hand I have sent off emails to Lynn's roommates asking whether he'd be answering some questions, one to Cisco PR person Mojgan Khalili with the following:

Was Cisco informed about the plan of Mike Lynn to present this particular topic at Black Hat 2005?

If so, did Cisco agree to it in the beginning?

Is it true that Cisco had planned to send a representative to Black Hat to co-present with or accompany Mike Lynn?

When came the decision to cancel the presentation?

Why was the presentation cancelled?

Who decided to cancel the presentation?

and, finally, an email to the German branch of ISS asking

Was ISS informed about Mike Lynn wanting to present this particular topic at Black Hat?

If so, was ISS okay with it in the beginning?

When did Mike Lynn finish the presentation prior to presenting?

Was Cisco informed about the planned presentation?

Was Cisco fine with it in the beginning?

When was it decided to cancel the presentation?

Why was the presentation cancelled?

Who decided to cancel the presentation?

I'm curious to see if I receive any replies.

The Underestimated Masses

So now we come to the final point of this by now rather lengthy bulletin article diatribe piece of writing: the underestimated power of weblogs and the way corporate communications can go bad. Cisco seems nowadays be run by marketing and PR. They try to set the spin. What they are just beginning to see is how security works - and one of the fundamental principles of security: what is disclosed can't ever be controlled again. Pandora's Box is open: let the games begin.

The "underestimated masses" from this section's heading are the bloggers: both the ones attending Black Hat and informing us at home about what was going on and us, sitting at home, adding what we see lacking in others' reports and finally enabling the world to get a (biased) picture of the situation. Cisco will be finding out that these grassroots efforts (I hesitate to call them "journalism") are very effective and will do more damage to their reputation than they thought possible. There is an example of exactly such a fiasco in Germany with a mobile phone ringtone provider called Jamba that was selling subscriptions for ringtone downloads (in small script, of course). There was a weblog article with a bit of chuzpe so the company decided to have their employees post comments in their favor which was found out by the blogger and all of a sudden the issue was all over all the online news services and even print media in Germany. The company didn't have egg on their face, they were face down in an egg pan.

Update: Wired News has an interview with Michael Lynn. It's not completely coherent, but it gives his answers to the questions I asked ISS and Cisco. Go read it. Now.

Kudos to Richard Stiennon.

Posted by Axel Eble in Meta at 21:54

Saturday, July 30. 2005

Google Ads on this blog

I've added Google Ads to this blog down below in the sidebar. It's a test and I'm not sure if I want it yet. However, the advantage of Google Ads is that the text ads aren't annoying and intrusive and it's only two of 'em. I don't even expect them to generate much revenue (if any at all).

Let me know if you think that's silly or if it annoys you (and if so, why).

Thanks for reading - And Now To Something Completely Different™.

Posted by Axel Eble in Meta, Off-Topic at 10:25

Thursday, July 21. 2005

Hollywood's Influence

According to a Yahoo! news report from USA Today it seems like the US government now has gone completely bonkers. They are testing anti-missile lasers aboard commercial airliners because those might be targeted by communist terrorist missiles.

We all know the reliability of anti-missile lasers based on the ground. They won't be any better in a moving plane. I guess the current administration watched one too many Hollywood flick.

Thanks to Bruce Schneier for a hilarious blog entry.

Posted by Axel Eble in General at 18:30

The Psychology of Change

Security is not a product, security is a process. Yah, we know. However, "process" is not nearly enough. The process and the products can be the best there are - if the infosec professional can't get it across all is moot.

What am I stating here? I'll try to explain in the following. "Getting secure" means change. It means changing old (die-hard) habits, it means changing workflows and processes and it means changing products. All in all, it means changing the work environment. For future projects, it even means taking security into the equation right from the start instead of kludging it on afterwards (because that, as we well know by now, doesn't work in most cases).

Changing things is not that hard. Changing process is harder by an order of magnitude. Changing people is nigh impossible. That's why so many change processes go wrong in most companies. And this, in turn, is why so many security initiatives go wrong, as well. The security managers in most cases don't understand the complex psychological processes running in the background and thus don't communicate efficiently with their intended target group. Said group will react adversely: "We've done it like this for ages and we're doing it right now and everything works well - there is no need for change!". It is important to take this (negative) criticism into account, talk with the parties in question and try to get them do some of the work for you. Ask them what they think they could contribute to the overall security of your organization. Ask them why they think it's not important to do anything where you see a big problem looming. Ask them where they see the biggest security problems in your organization.

All of this may not work, either. That's why it is important to get management aboard when you plan your initiatives and projects. Communicate what you see as a problem, point out what you consider the risk. There's no need for a quantitative risk analysis - but be well prepared if your manager challenges your assessment. If you can't get your message across, make at least sure you have made the risk transparent and get them to sign off on that - they have to understand it and willingly make it their residual risk. If they take you up on it and back you, you're pretty much set. If your colleagues still insist on blocking you, you will have to go to your management for support. Sometimes it may be necessary to force the change on some people. This instrument should, however, be kept to an absolute minimum. It's always better to have people understand you and work willingly with you.

However, don't think for a moment that all people will react the same. You'll probably find all sorts of people starting from the ones that enthusiastically support you and the changes to the ones who will be against it and are vocal about it. You'll have to talk to all of them and try to convince them in their very own way. It will be a challenge, but there just is no silver bullet. Unfortunately, I might add.

So, what's the executive summary of this diatribe? Now that's easy: stop focusing on technology. Focus on psychology, read books of succesful change management and project management. Learn to read people.

Posted by Axel Eble in Meta at 13:47

Wednesday, July 20, 2005

Off-Topic: Google Moon

Matching the 20th anniversary of Man's landing on the Moon Google has added Moon maps.

Nothing too spectacular, one would think. However, try to zoom to the largest zoom factor.

Posted by Axel Eble in Off-Topic at 12:27

Tuesday, July 19. 2005

Owning a box - film at 11!

Well, actually it's not only at 11, it's any time you like: The Security Monkey points to a site that has various movies displaying and showing what can be done with Knoppix-related distros. The one he points to shows the Owning of a Windows based webserver via an insecure IIS installation, but there are other movies, too.

Posted by Axel Eble in General, Technology at 10:08

Thursday, July 14. 2005

The Institute of Backup Trauma

Thanks to lilit for the pointer to a hilarious commercial ad starring John Cleese of Monty Python fame. I don't know the featured company nor its products so I don't endorse them. However, I found that video too hilarious not to share it.

Too bad I don't understand lilit's language.

Posted by Axel Eble in Off-Topic at 12:08

Tuesday, July 12. 2005

Law and Order

In the aftermath of the London bombings politicians, secret service and police officials are popping up all over the world to urge new, tougher laws into being to control everyone and everything.

At the same time, data protection officers and information security people, equally distributed, are warning against the very same thing for the lack of efficiency. Most of them also say that the laws already in place are sufficient to reach the goals of finding, pursuing and bringing terrorists to justice.

I find it ironic that the point of view of people doing risk management all the time diverges so much from that of law enforcement personnel and politicians. In my eyes, it shows clearly that the former have a very narrow view of the world and the latter have their very own agenda.

Aftermath: Funny enough, last night someone mentioned the difference between police and (pragmatic) security people. Police put the rules above the meaning, pragmatics put the meaning above the rules.

Posted by Axel Eble in General, Meta at 08:21

Sunday, June 26. 2005

Aachen University Teaches Hacking

According to Heise Newsticker the Laboratory for Dependable Distributed Systems at the Rheinisch-Westfälische Technische Hochschule (RWTH, a technical university) Aachen will hold the "Summerschool Applied IT-Security". The Summer School will consist of lectures in the morning and extensive hacking and penetration trials in the afternoons. They expect students not only to try out proven techniques but develop their own ones. RWTH Aachen hopes to come up with a more scientific approach to computer and network security.

This is a bad idea. First of all, hacking and penetrating systems will not lead to a better understanding of security. Security is not that hard to grok - it's just boring to design systems that are secure. RWTH Aachen would do much better to teach secure programming techniques like avoiding buffer overflows and all that nonsense all those other well-known vulnerabilities. Second, some companies will react adverse to this program. They may not employ anybody who went through it. Is that really worth it?

Posted by Axel Eble in General, Meta at 20:11

Friday, June 24. 2005

Re: Audit Those PCs

Audit Those PCs says Fred Avolio, telling of confidential data leaking out of a PC loaded with file sharing software and infected by a virus/worm/...

While I agree with what he says about having policies and dealing with infractions current viruses and worms bring their own file sharing software. It's not even necessary to have something pre-installed.

Posted by Axel Eble in General, Meta, Technology at 23:13

Nostalgia: Good Bye, My Friend

I just revoked a PGP key I had created 1995. It's really sweet to remember all the stories to all the email addresses that the key was tagged with.

Good bye, my friend.

Posted by Axel Eble in Experiences, General, Meta at 22:43

Biometric Passports: A Nightmare In Several Acts

Germany's Minister for the Interior, Otto Schily, insists on introducing passports with biometric data AND an RFID chip in fall 2005.

He insists further that data protection and privacy is guaranteed (and quite a few of the data protection officers on the federal and state levels are not at all convinced of this) and that we need it because of the added security. Unfortunately, fraud with passports and ID cards was almost negligible in 2004. Where we need the added security is not clear - he doesn't tell. He is, however, very intent on silencing the public Data Protection Officers and denouncing them as incompetent or exceeding their competencies. It would be fun to watch the ensuing mudfight from a safe distance if we citizens weren't so directly involved.

What Schily does tell, however, is one of two reasons for this haste: German companies are supposed to lead research and development in biometrics and biometrically enhanced ID documents. The other reason he'll never publicly say, but I'm quite sure he wants to lay down the infrastructure for a better surveillance. Right now laws prohibit the setting up of a central database for ID data (including biometric and DNA data), but I'm not sure if this is being retained in the long term.

Besides, since the RFID chip protocol has to be readable all over the world an ICAO protocol will be adopted. What data will be readable is supposed to be declared by the issuing country for every other country. No one, however, will be able to keep any other country from setting up central databases and entering the data they can get off the RFID chip in it. Granted, some countries will not get much information from it, but countries like the USA will probably have a very thorough access profile. And we all know that the US of A still don't understand data privacy (especially not when it comes to aliens) nor do they care about the qualms of foreigners.

In order to access the RFID chip's information a cryptographic key has to be determined. For this, a special optical zone will be scanned. This is supposed to keep everybody from accessing the chip and thus easily build movement profiles. Remember, there is no legal provision for a central database of those access keys - in Germany. Now, what happens if someone travels to, e.g., the USA? Why, they'll scan the optical zone, calculate the key and store it in a database. From then on, they could theoretically access the RFID data all the time without the person ever knowing it. However, the crucial information that I have not been able to find so far is the range of the RFID chip. Is it only millimeters? Is it centimeters? Is it meters? This makes the world of a difference!

Oh, and finally: the costs of the passports more than doubles from 26 €, to 59 €.

So, to sum it up: not enough data is being published for the people to check Schily's claim that it's all safe and sound and that there's no need to worry; the process is being pushed forward with unparalleled speed; critiques are being

Blog Export: The Quiet Earth, <http://blog.balrog.de/>

silenced or denounced and the whole sense of this project (other than schmoozing with Bush's Junta over there in Washington, D.C.) is strongly debatable.

Isn't it nice to live in a democratic and free country?

Posted by Axel Eble in General at 22:20

Friday, May 27. 2005

Winn Schwartau Mac-ified

In Mad as Hell: Why Over The Top? Winn Schwartau tells about his switch to the Mac.

However, my own experience shows that Apple is pressing equally hard at not having to exchange hardware. When the mainboard (or the internal 128 MB RAM) on my iBook were b0rken (right from the start, it showed intermittent kernel panics that couldn't be traced back to the third party RAM or any software I had installed), they kept running me through test upon test (reinstalling and running a clean OS etc.) until I finally sent it in for a check. They, of course, didn't find anything (as the panics came very intermittently - sometimes three in a row, sometimes none in three weeks) and charged me with their service fee.

I then wrote a complaint and mailed it in (snail mail this time - it shows that I feel it important enough to not only write it but put it in an envelope, put a stamp on and walk to the post office to get it mailed out to which they at last agreed to exchange the Logic Board. It was a major hassle and I'm still waiting for the refund on the service fee I paid for the exchange of the Logic Board itself. So, whenever you're dealing with HW problems, companies usually don't trust your expertise - no matter if it's Apple, Dell, Sony or whatever.

All in all, however, I'm very very satisfied with my Macs.

Posted by Axel Eble in Off-Topic at 09:02

Tuesday, May 24, 2005

I don't hate Security

In Five Reasons I Hate Computer and Network Security Fred Avolio tells us why he is getting more curmudgeonly by the year.

His five reasons are valid - however, that's where I believe the true value of IT Service Management (ITSM) comes into play. ITSM is a methodology and a way of thinking. It's thinking in terms of your users and what they expect from you as an IT organization. It's thinking out of the box, not technology centric but customer centric. In short, it is a whole new perspective - and, frankly, one that may be difficult to grasp for network, computer or security administrators. Their job is being technical-minded, to stay current with advances in technology, to stay abreast of the ever moving wave of progress.

ITSM doesn't necessarily. It's concerned with delivering quality. It's concerned with satisfying the user. To achieve this, it's necessary to define your processes and live by them. If you start with that, you can start looking for (meaningful!) metrics for those processes - and from there on start to improve the processes themselves. This is not technology. This is not necessarily fun work. It is, however, talking the talk and walking the walk to understand the business side and, thus, the very management that only wants to save money. Which just might be a positive benefit of ITSM.

In short, ITSM leads to a more business oriented IT, not a more technology oriented business. And that may be just what we need.

Posted by Axel Eble in Meta at 18:50

Winning as a CISO with Rich Baich (CISO of ChoicePoint)

Some things are plain hilarious: Executive Alliance Publishing House Announces Release of New Book on 'WINNING AS A CISO'. If you're a CISO you can learn from the winner of the 2004 Information Security Executive of the Year in Georgia Award. Let me quote their press release:

"The role of the CISO carries tremendous accountability for the mitigation of risk and therefore, successful operations of the business," said Baich. "Ultimately, the success of any business depends on a leader's ability to build a team, market and sell the product and run the business; the CISO is not an exception to the rule."

Funny he should say that, especially in light of the scandal around ChoicePoint. Sometimes attack looks to be the best kind of defense.

Thanks to ChoicePoint Information Sentinel Adam Shostack!

Posted by Axel Eble in General at 09:37

Decision Making and Risk Management

In Context is everything Chandler writes about how context changes data into information and how it can change Decision Making and influence Risk Management.

Let me elaborate a bit: in companies like banks, insurances and other financial institutions both integrity and confidentiality of data is of highest importance. For an automotive engineering company, confidentiality is of highest importance. For a transportation company, availability is the crucial point (because the data they keep is exceptionally fleeting anyway and finding out about the flow of goods is equally possibly by following some trucks).

If one does risk management by the book, i. e. without looking at the context of the company, the result is meaningless and won't have anything to do with the given company. "What is the risk of an intrusion [from the Internet]?" is one of those questions I see asked time and again. Well, for what type of business? Again, for the bank the risk is quite high, of course (and I won't go into giving any numbers - and the reasoning is for another blog entry) - for our transportation company it's pretty much negligible: their customers often don't understand the possibilities of the Internet and networking at all and for the usual hacker the company does not offer enough to bother.

Chandler has made a very important point here. To conclude this post I'll just let him talk: Next time you're asked to estimate risk, don't forget that there's a lot more to be considered than the data. So many analyses of risk examine just on the Usual Suspects from some checklist, best practices guide or standards list and then stop. They ignore the unique context that is their business and the accuracy and cost-effectiveness of the solution suffer accordingly.

Blog Export: The Quiet Earth, <http://blog.balrog.de/>

Posted by Axel Eble in Meta at 09:15

Monday, April 4. 2005

Antwort auf den offenen Brief von Andreas Pfitzmann an Udo Helmbrecht, Präsident des BSI

The following post is in German as it concerns primarily a German issue. If you want to know what it's all about, take a peek at my last entry.

Hallo Herr Pfitzmann,

mit ihrem offenen Brief haben Sie eine große Aufmerksamkeit in der Blogosphäre (und demnächst vermutlich auch in weiteren Kreisen, siehe den heutigen Artikel im Heise Newsticker) hervorgerufen. In dieser Email möchte ich persönlich und direkt dazu Stellung nehmen.

Es ist richtig, daß die Art und Weise der Absage durch Herrn Helmbrecht extrem seltsam und auch persönlich beleidigend ist. Allerdings müssen Sie sich vorwerfen lassen, daß Ihre Antwort auch nicht wesentlich "besser" oder niveaullvoller ist. Ich werde diesen Vorwurf im folgenden detaillieren.

Sie erwecken in Ihrem Brief den Anspruch von Wissenschaftlichkeit, indem Sie schreiben: "Statt sich den Überlegungen und Argumenten der Wissenschaft zu stellen, [...]". Damit stellen Sie sich als personalisierte Wissenschaft dar und alle Ihre Ausführungen des Vortrags auf dieselbe Stufe wie wissenschaftliche Arbeiten. Sieht man Ihr Papier durch, gelange zumindest ich zu der Überzeugung, daß Sie diesem Anspruch aber in keinsten Weise gerecht werden: der Vortrag legt viele Meinungen und persönliche Befindlichkeiten dar, ohne selbige wissenschaftlich oder sonstwie zu untermauern.

Auch die Aussage, daß Ihre Meinung "zensiert" werden soll, ist vollkommen überzogen: würden Sie zensiert werden, würden Sie weder Ihren öffentlichen Brief publizieren können noch könnten Sie anderweitig veröffentlichen. Alternative Plattformen sind Ihnen jedoch unbenommen. Insbesondere mit dem Hintergrund, den Zensur in NaziDeutschland und der DDR hatte, machen Sie sich durch diesen Superlativ unglaubwürdig. Ein letzter Kritikpunkt an Ihrem Brief an Herrn Helmbrecht: es gibt keinerlei glaubwürdige Hinweise auf eine mittelbare Einflußnahme des BMI auf das BSI. Es mag nahe liegen, an einen derartigen Einfluß zu denken, Beweise jedoch existieren nicht. Insbesondere im Gebiet der Informationssicherheit wird viel zu häufig mit Halbwahrheiten, Mutmaßungen und Extrapolationen gearbeitet, für die es keinerlei Belege gibt. Diese Vorgehensweise ist für das Gebiet nicht fürderlich. Gerade von einem Wissenschaftler erwarte ich eine zurückhaltende und sachorientierte Arbeitsweise - etwas, was Sie in Ihrem Brief vermissen lassen.

Daß Sie ein Experte auf Ihrem Gebiet sind, mag ich Ihnen glauben (insbesondere durch die Aussagen meiner Peers, die Sie und Ihre Arbeit wohl besser kennen als ich). Daß die von Ihnen aufgeführten Argumente gegen die Vorhaben des BMI sprechen, ist unter Informationssicherheitsleuten sicher konsensfähig. Auch ich stehe den Plänen von Herrn Schily und der wiederholten Mißachtung von Parlamentsentscheidungen durch die Bundesregierung sehr skeptisch gegenüber. Daß Sie aber nicht über diesen Methoden stehen und nicht professionell agieren, ist nicht nur ungeschickt, es dient im Gegenzug weder der Sachlage noch Ihnen als Person. Durch Ihren offenen Brief, der sowohl von der Form als auch vom Inhalt das Ziel verfehlt, werden Sie keine öffentliche Debatte über die Themen erreichen, sondern lediglich über Ihre Person und Ihre Integrität. Das ist nicht nur schade für Sie persönlich, es dient vor allem nicht der Sachlage und macht Sie angreifbar. Ihre Argumente werden "by proxy" illegitimiert, was sicher nicht in Ihrem Sinne ist.

Vielleicht gab es ja eine covert channel Kommunikation zwischen Herrn Helmbrecht oder anderen Mitarbeitern des BSI und Ihnen, in der zumindest der Zusammenhang mit dem BMI, den Sie vermuten, angedeutet wurde. In diesem Fall nehme ich meinen diesbezüglichen Vorwurf selbstverständlich gerne zurück.

Mit freundlichem Gruß,

Axel Eble

Cc: an diverse Mailinglisten sowie als Eintrag in meinem Blog.

--

Blog Export: The Quiet Earth, <http://blog.balrog.de/>

Axel Eble, CISSP Trienter Str. 6b 87437 Kempten (Allgäu) Germany
fon: +49 831 5753978 cell/fax: +49 178 2853265
email: [censored for the blog] blog: <http://balrog.de/security/>

Reply by Andreas Pfitzmann:

Von: [email address censored for the blog]
Betreff: Re: Ihr offener Brief bzgl. der Ausladung zur 9. Sicherheitskonferenz des BSI
Datum: 5. April 2005 03:49:43 MESZ
An: [email address censored for the blog]
Cc: [email addresses censored for the blog]

Hallo Herr Eble,

Am 04.04.2005 um 22:38 schrieb Axel Eble:

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Hallo Herr Pfitzmann,

mit ihrem offenen Brief haben Sie eine große Aufmerksamkeit in der Blogosphäre (und demnächst vermutlich auch in weiteren Kreisen, siehe den heutigen Artikel im Heise Newsticker) hervorgerufen. In dieser Email möchte ich persönlich und direkt dazu Stellung nehmen.

Es ist richtig, daß die Art und Weise der Absage durch Herrn Helmbrecht extrem seltsam

sicherlich

und auch persönlich beleidigend

das würde ich nicht behaupten

ist. Allerdings müssen Sie sich vorwerfen lassen, daß Ihre Antwort auch nicht wesentlich "besser" oder niveauvoller ist. Ich werde diesen Vorwurf im folgenden detaillieren.

Sie erwecken in Ihrem Brief den Anspruch von Wissenschaftlichkeit, indem Sie schreiben: "Statt sich den Überlegungen und Argumenten der Wissenschaft zu stellen,[...]". Damit stellen Sie sich als personifizierte Wissenschaft dar

haben Sie genau gelesen? Es geht überhaupt nicht um meine Person, ich empfinde das ganze auch keinesfalls als beleidigend, es geht um den Austausch von Argumenten.

und alle Ihre Ausführungen des Vortrags auf dieselbe Stufe wie wissenschaftliche Arbeiten. Sieht man Ihr Papier durch, gelange zumindest ich zu der Überzeugung, daß Sie diesem Anspruch aber in keiner Weise gerecht werden: der Vortrag legt viele Meinungen und persönliche Befindlichkeiten dar, ohne selbige wissenschaftlich oder sonstwie zu untermauern.

Vielleicht haben Sie nicht genau genug gelesen (mir ist bewusst, dass ich klar meine Meinung geschrieben habe, persönliche Befindlichkeiten geschrieben zu haben, ist mir nicht bewusst), vielleicht ist Ihnen nicht bekannt, was ein eingeladener Vortrag (im Gegensatz zu einem eingereichten) soll: Ein eingeladener Vortrag soll Orientierung (swissen) vermitteln und nicht alle Details inkl. Belege dafür wiederholen, was typischerweise in eingereichten Beiträgen steht.

Ich habe dies, da aus meiner Sicht eine Entwicklung ziemlich falsch läuft, sehr kurz und deutlich getan, denn ich wollte mit meinen Argumenten (und da wo exaktes Wissen bisher nicht verfügbar ist: mit meiner warnenden Meinung) Menschen erreichen, die nicht die Zeit haben (oder sie sich nicht nehmen), lange Texte zu lesen.

Oder noch deutlicher gesagt: Ich wollte mit meiner Vortragsausarbeitung keinen Text schaffen, aus dem dann jede(r) das herausgreift, was ihm in den Kram passt, da der Text so lang und kompliziert ist, dass ihn keiner ganz liest. Ich halte

den Text für kurz und einfach genug dass ich mich traue zu sagen: Bitte ganz lesen - und manchen vielleicht sogar: Bitte mehrfach und genau lesen ...

Auch die Aussage, daß Ihre Meinung "zensiert" werden soll, ist vollkommen überzogen: würden Sie zensiert werden, würden Sie weder Ihren öffentlichen Brief publizieren können noch könnten Sie anderweitig veröffentlichen. Alternative Plattformen sind Ihnen jedoch unbenommen. Insbesondere mit dem Hintergrund, den Zensur in Nazideutschland und der DDR hatte, machen Sie sich durch diesen Superlativ unglaubwürdig.

Halten Sie es für möglich, dass Begriffe je nach Verwendungszusammenhang etwas anderes bedeuten können, dass Zensur im Zeitalter von e-mail und www etwas leicht anderes bedeutet als früher? Ein Hinweis (falls Sie genau lesen) ist in meinem Brief, dass ich von Zensurversuch spreche.

Es geht mir allerdings nicht um diesen Begriff, sondern um einen Sachverhalt, den ich durchaus genauer beschreiben kann, allerdings nicht in ein Wort verdichten:

Im Umgang mit WissenschaftlerInnen fragen Politik und Wirtschaft in der Regel nur diejenigen, von denen Sie eine genehme oder interessante Antwort/Gutachten, was auch immer, erwarten. D.h. bereits hier wird die Realitätssicht stark selektiv und die Wissenschaftler aus Sicht der Öffentlichkeit lassen sich bereits hier teilweise missbrauchen.

Noch mal selektiver ist ein Vorgehen, wenn Politik und/oder Wirtschaft erst aufgrund der Antwort entscheiden, ob sie sie hören wollen.

Gegen ersteres habe ich keine einfache Methode, sich zu wehren, gegen letzteres wehre ich mich als Wissenschaftler sehr deutlich (und wie ich mit Freude feststelle, durchaus erfolgreich).

Wenn Sie für diese Zeilen einen guten Begriff haben, der einfacher als "politisch motivierte ex-post Antworten/Gutachtauswahl" ist, nehme ich den künftig statt "Zensurversuch".

Ein letzter Kritikpunkt an Ihrem Brief an Herrn Helmbrecht: es gibt keinerlei glaubwürdige Hinweise auf eine mittelbare Einflusnahme des BMI auf das BSI.

Die gibt es zuhauf: Lesen Sie genau, denken Sie nach und unterstellen Sie bitte dabei, dass ich keine weiteren Menschen in so einem Brief nennen möchte.

Ich habe mal 1986/87 in Vorläufern der Kryptodebatte Kollegen schriftlich zitiert: Die wurden auf der Basis dieses Zitats von Ihrem Chef zu sich bestellt und vor die Wahl gestellt: Arbeitsplatz oder Gegendarstellung. Es gab Telefonate, wo sie sich bei mir für die Gegendarstellung entschuldigt haben, aber sie mussten ihre Familie ernähren. Kurzum: Bitte denken Sie auch darüber nach, ob es Dinge geben kann, über die man nicht schreibt.

Es mag nahe liegen, an einen derartigen Einfluss zu denken, Beweise jedoch existieren nicht. Insbesondere im Gebiet der Informationssicherheit wird viel zu häufig mit Halbwahrheiten, Mutmaßungen und Extrapolationen gearbeitet, für die es keinerlei Belege gibt. Diese Vorgehensweise ist für das Gebiet nicht fürderlich. Gerade von einem Wissenschaftler erwarte ich eine zurückhaltende und sachorientierte Arbeitsweise - etwas, was Sie in Ihrem Brief vermissen lassen.

Bitte lesen Sie ihn noch mal unter dem oben genannten, Ihnen möglicherweise neuen Aspekt.

Da Sie ein Experte auf Ihrem Gebiet sind, mag ich Ihnen glauben (insbesondere durch die Aussagen meiner Peers, die Sie und Ihre Arbeit wohl besser kennen als ich). Da die von Ihnen aufgezählten Argumente gegen die Vorhaben des BMI sprechen, ist unter Informationssicherheitsleuten sicher konsensfähig. Auch ich stehe den Plänen von Herrn Schily und der wiederholten Mißachtung von Parlamentsentscheidungen durch die Bundesregierung sehr skeptisch gegenüber. Da Sie aber nicht über diesen Methoden stehen und nicht professionell agieren,

Das sehe ich anders - und ich hoffe, Sie nach dem Lesen meiner kurzen Antworten auch.

Ist nicht nur ungeschickt, es dient im Gegenzug weder der Sachlage noch Ihnen als Person. Durch Ihren offenen Brief, der sowohl von der Form als auch vom Inhalt das Ziel verfehlt, werden Sie keine öffentliche Debatte über die Themen erreichen, sondern lediglich über Ihre Person und Ihre Integrität.

Blog Export: The Quiet Earth, <http://blog.balrog.de/>

Warten wir es ab. Ich bin zuversichtlich, dass es um Argumente geht, und nicht um Personen.

Das ist nicht nur schade für Sie persönlich, es dient vor allem nicht der Sachlage und macht Sie angreifbar. Ihre Argumente werden "by proxy" illegitimiert, was sicher nicht in Ihrem Sinne ist.

Vielleicht gab es ja eine covert channel Kommunikation zwischen Herrn Helmbrecht oder anderen Mitarbeitern des BSI und Ihnen, in der zumindest der Zusammenhang mit dem BMI, den Sie vermuten, angedeutet wurde. In diesem Fall nehme ich meinen diesbezüglichen Vorwurf selbstverständlich gerne zurück.

Ich habe mir mit meiner Antwort viel Zeit gelassen und kenne in diesem Feld viele Kollegen in der Wissenschaft, in der Politik und natürlich auch im BSI seit mehr als 20 Jahren, teilweise sehr persönlich.

Ich habe mir grundsätzlich überlegt, was ich schreibe. Ich sehe (bisher) keinen Anlass, daran inhaltlich irgendetwas zu ändern.

Mit freundlichem Gruß,

Axel Eble

Cc: an diverse Mailinglisten sowie als Eintrag in meinem Blog.

-- Axel Eble, CISSP Trienter Str. 6b 87437 Kempten (Allgäu) Germany
fon: +49 831 5753978 cell/fax: +49 178 2853265
email: [email address censored for the blog] blog: <http://balrog.de/security/>
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.2.4 (Darwin)
Comment: Axel Eble, CISSP

iD8DBQFCUaWuwI7cdv6NorsRAu2UAJsGWXesiEtNnEFHh4S1MdLq9/+pBgCelqMI
H2dr5D+7Hndi8prhrflQsfU=
=OAz2
-----END PGP SIGNATURE-----

Viele Grüesse

Andreas Pfitzmann

Technische Universität Dresden Phone (mobile) +49 170 443 87 94
Fakultät Informatik (office) +49 351 463 38277
Institut fuer Systemarchitektur (secretary) +49 351 463 38247
01062 Dresden, Germany Fax +49 351 463 38255
<http://dud.inf.tu-dresden.de> e-mail [email address censored for the blog]

Posted by Axel Eble in General, Meetings, Meta at 21:46

Sunday, April 3. 2005

Censorship in Germany?

I had wanted to keep this blog largely free of politics but obviously information security is so political a topic that this is no longer possible.

For the 9th German IT Security Congress, organized by the Bundesamt für Sicherheit in der Informationstechnologie (BSI, the Federal Office for Information Security), the BSI had invited a talk by Prof. Dr. Andreas Pfitzmann about the current state of biometrics and if a widespread deployment really will bring so much more security.

About eight weeks before the congress Udo Helmbrecht, the president of the BSI, wrote to Pfitzmann telling him that his talk had to be removed because there were several new topics that were more interesting. Well, bad style, one might say. However, what really makes this smell fishy is that a) there's still a talk scheduled about a study by the BSI that has recently been cancelled and re-scheduled; b) the talk by Pfitzmann is pretty critical about the benefits of a widespread use of biometry and, c) the Federal Ministry for the Interior, to which the BSI is subordinate, wants to deploy biometry wherever possible.

Pfitzmann has replied to Helmbrecht suspecting that the Ministry has influenced the decision. Of course, it does smell fishy, and, if was true, it would be really close to censorship (although Pfitzmann is not denied the opportunity to publish his opinion).

Independent of the quality of the talk (which I find rather disappointing, more an opinion than a scientific article), the question remains: why did the BSI cancel the talk with a rather thin justification? However, I don't want to believe in any conspiracy at the moment.

Via Kristian K hntopps Wunderbarer Welt von Isotopp und Matthias Langes Abenteuerliche Abenteuer s dlich der Elbe (Beitrag von Markus Hansen).

Posted by Axel Eble in General, Meetings, Meta at 19:23

Thursday, March 24, 2005

ISO17799

I've just come back from a very good event in Brussels, Belgium. The ISSA Chapter Bruxelles European had organized a one day event about ISO17799/BS7799 titled "Making progress on a work in progress".

The talks were excellent, ranging from the future of the standard to case studies. Apart from the educational aspect the networking part was really good: I met some people for the first time in person (like Lois Gamon and the notorious famous Richard Starnes).

On a related note, ISSA is currently working on taking part in the development of ISO 17799.

Posted by Axel Eble in General, ISSA, Meetings, Organizations at 00:07

Friday, March 4, 2005

ElcomSoft breaks EFS on WinXP and W2k3 Server

According to Heise Newsticker, the current version of ElcomSoft's Advanced EFS Data Recovery is able to break the encryption of Windows XP's and Windows 2003 Server's Encrypted File System (EFS).

Posted by Axel Eble in General at 15:59

Thursday, March 3. 2005

The "X.509 Certificates With MD5 Hashes" Sky Has Fallen

Scientists seem to have found a way to create different X.509 certificates with the same MD5 hash. This is critical in that CAs usually only sign the MD5 hash. With that, the certificates can later be exchanged without anyone noticing.

The attack is only possible if the attacker can generate both the "official" and the "unofficial" certificate - pre-image attacks (creating a fraudulent certificate to a given MD5 hash) are still not possible and SHA-1 hashed certificates are safe too - for the moment.

Source: Heise Newsticker (german)

Original Paper: <http://eprint.iacr.org/2005/067>

Posted by Axel Eble in General at 17:09

To ID Card Or Not To ID Card

I am living in a country where ID cards and registration with the town authorities are mandatory. I don't find an ID card system as intrusive as Adam Shostack describes. This is due to several points. Let me try to explain:

Our ID card system was introduced after WWII

The culture and mindset of Europe are completely different than the US ones. European history has forged our minds to accept and welcome a centralist government, to even rely upon it. On the other hand, US citizens distrust their government and absolutely abhor the idea of it interfering with their everyday life, the way they want to live their life and with their freedom.

Germany has a long standing record of Identification Systems. I don't believe this is either a bad or a good thing. It just is - what we as a society make of it is what makes it good or bad. Granted, it offers potential for abuse. Yet in the almost 60 years we're having it, it has not been abused, partially because people are vigilant to this.

This point somewhat corresponds to the last one. I believe wholeheartedly that one of the largest reasons our ID card system has not been abused so far is that it was implemented in the 1950s. Back then, people thought differently and there were practically no ways of automating surveillance. There was no Internet, there were no Credit Cards, no computers, telephones and TVs were rare (perhaps one per house or even street). This very much minted the minds of people and their children and their grand-children - and last but not least, the laws. If we were to implement an ID card system today, I'm pretty sure the current terrorism craze would make us have a very intrusive surveillance oriented society. As it is, we don't have it.

Finally, Adam sees the ID card being used as an authenticator because it might be declared "trustworthy". This is the age old discussion about the use of identifiers for authorization. The concept alone is breathtaking. Why, oh why would anyone want to do that without further checks? It makes my head hurt just to think of that. An ID card is exactly what it says: it identifies you - nothing else. The difference between an ID card and a Social Security Number (SSN) if it's done correctly is that it's harder to fake and forge an ID card than a single string of digits and possibly characters (I have no idea what an SSN looks like). The second difference is that an ID card can be back-checked with the authorities issuing it.

Again: I'm not here as a missionary for ID cards. All I can say is that with our system we have practically no abuse whatsoever and we have no ID theft whatsoever. I'm sure there are lots of reasons for both of these non-issues and I'm reducing it too strongly, but I'm equally sure that an ID card might actually help for identification purposes.

Posted by Axel Eble in General, Meta at 16:29

How To Be A Millionaire Movie Star Internet Celebrity Security Con\$ultant

Due to reader questions (well, one reader at least, and I don't even know if he read the English portion of my web site, but anyway, here you go), I'm going to jot down a few hints and tips on becoming a Security Consultant.

First of all: why would you want to do that? If you're still at school, chances are you'll think this venue glorious - after all,

the usual reports in newstickers and magazines talk about self-acclaimed security experts in highest regard. If you're out of school already, my question still holds true. It's not as if this sort of life is glorious - you won't be in the limelight and you won't have two "babes" (or "hunks" for the few girls out there) on each finger admiring you for your awesome skillZ. So you think security is c00l. Well, let me tell you: it isn't. It's mostly boring work, nagging your colleagues to think a bit more about security or to get them doing stuff you think absolutely necessary. It's fighting against windmills because more often than not top management wants "The Job To Be Done"™; and security just looks like an obstacle.

Okay, so you still want to consult in information security. Don't expect that to be a quick moving process. To be taken seriously by your peers you'll have to show them a lot of work experience. And I'm not talking "security work" here. I'm talking the nitty-gritty down-to-earth getting-your-hands-dirty kind of work. That means you either have to know a somewhat narrow topic in depth or a broad list of subjects a bit more on the shallow side. Either way, you'll need to learn it. If you want, you can go to University (or take any other sort of higher education that's available in your culture). It won't do much harm as long as you question what they teach. At the very least it should teach you how to learn and how to attack a problem in a structured way (and lets you have a blast every now and then if you're doing it right). I'd recommend a study of computer sciences, but really, it's up to you. However, you'll have to have an in-depth understanding of the technology you're going to consult about.

You've taken your studies, you're looking for work. Don't go rushing for any top-of-the-notch security company. Go work in the trenches for a system integrator or maybe even a vendor. Or work as a system and/or network administrator for an end user company. Do that for a few years. Talk to security people. Watch the products you administrate for security issues. Don't believe in vendor pitches (not even when you're working for one!). Go to conferences, take courses. Talk to your security people. Do it again. Keep on talking to them. Ask them what their work is all about and ask them where the biggest obstacles are. You'll pretty soon notice that security isn't rocket science. In fact, if it looks like rocket science, you have botched something severely, probably right from the start. It's a lot about common sense and good design - as wrote Marcus Ranum some while ago.

If, after those years, you still feel security is worth the effort, if you still feel like it's a calling: go for it. If along this way you have found a venue that you find more rewarding, don't feel bad.

Posted by Axel Eble in General, Meta at 11:43

Monday, February 21. 2005

Possible intermediary processes for SHA-1 and MD5

Even if SHA-1 and MD5 are somewhat compromised (there's as yet no real breaking of the algorithms) I'm wondering why the two algorithms aren't used in conjunction?

The main problem is that the cyphertext space has gotten a lot smaller suddenly and collision attacks seem to be feasible. However, if both algorithms are used to compute the hash and both hashes will have to be checked it would mean to generate another (meaningful) message that gives collisions for both algorithms.

This will, of course, cost computing time. But it might give the community a bit of breathing space.

Posted by Axel Eble in General, Technology at 06:18

Wednesday, February 16, 2005

Bruce Schneier: SHA-1 Broken?

Slowly but surely the number of usable cryptographic hash algorithms is falling asymptotically against zero. You're reading correctly. Zero. MD-4: broken. MD-5: all but broken.

Now Bruce Schneier blogs that SHA-1 is the next candidate for that. Apparently there's a paper circulating describing how they received »collisions in 269 hash operations, much less than the brute-force attack of 280 operations based on the hash length.«.

According to Bruce, it does not affect applications like HMAC for which collisions don't play a role. It sure would make SHA-1 unusable for cryptographic hashes.

Posted by Axel Eble in General, Technology at 08:32

IDN - The Sky Has Still Not Fallen?

Last week has seen a flurry of news articles about the abuse of International Domain Names for phishing and spoofing. Let's sum it up: Domain names in URLs can be spoofed by using characters from another character set that look similar or identical to their ASCII counterpart. For example, a cyrillic 'a' looks practically the same as an ASCII a. That means, paypal.com could be written with the cyrillic letter `а`; `р`; `у`; `р` or even `р`; `у`; `р`.

The solution to the problem seems easy: turn off support for IDN names. Internet Explorer never supported them anyway, but even the Mozilla Foundation decided to turn their support of IDNs off from now on.

However, nobody did their homework in that regard: the originators of the IDN system already thought about this spoofing scheme. Paul Hoffmann writes about possible solutions that are still intrusive yet retain functionality.

Read it, it's good.

via Kris

Posted by Axel Eble in General, Technology at 00:21

Monday, February 14. 2005

"Security" seems to have a future

Heise reports that Novell is now starting to sell their Novell Security Manager, a rebranded version of Astaro's Security Linux distribution, a small Linux distro running off a CDROM. Apparently both companies will co-develop it in the future.

Please, Novell, concentrate your efforts on SuSE and a decent integration in existing Novell NetWare and Microsoft networks. That makes a whole lot more sense and brings a whole lot more revenue in the long run.

Posted by Axel Eble in Meta at 08:37

Sunday, February 13. 2005

Web-of-Trust based Certification Authority

As getting certificates for mail and web encryption is somewhat expensive for the average Joe and Jane User there is a rather new initiative that applies the same trust model as PGP.

Whoever wants to start playing in the League has to have their identity confirmed by at least two already accredited «assurers». The candidate must bring official documents (ID Card, Passport, ...) with them. In return, the applicant receives «points». The more points, the more trustworthy they are and the more they can do in the system.

Of course, that only confirms the identity of the candidate, not their integrity. The information to be found on the web site is so far pretty limited, but I'll be diving into it in the next time as I find this model pretty interesting.

Their primary goals at the moment are getting their root certificates into the different browser certificate stores, which seems to be an adventure - see their General FAQs under CAcert's Root cert is not included in my browser - what's up with that?.

Posted by Axel Eble in Meta, Technology at 19:05

Thursday, February 10, 2005

ISSA is taking off in Europe

It looks like ISSA is finally taking off on the Continent. There are several new Chapters and several new Chapter Presidents in Europe. We're currently in the process of founding the German Chapter and the Belgians will host a European event on March 22nd. Apart from that Infosecurity Europe will host a few events for (ISC)2 constituents and ISSA members. ISSA Int'l. is recognizing Europe as a growing market and is working with the local chapters on sponsoring, support and event organization.

All in all, it is a pretty exciting time right now.

Posted by Axel Eble in CISSP/(ISC)², ISSA at 00:13

Thursday, January 27, 2005

Unintended Consequences

Scott Granneman has an interesting article on SecurityFocus about unintended consequences. He's urging people to do more risk and threat evaluations, more thinking out of the box. I couldn't agree more.

Posted by Axel Eble in General, Meta at 10:27

Do you have antivirus software for your Lexus?

In an exceptionally information lacking article SC Magazine states that Lexus cars may be vulnerable to viruses transmitted by bluetooth connections.

It's completely unclear if the navigation and communication system runs the Symbian operating system that recently saw itself vulnerable to a certain sort of viruses or what other operating system is running.

It's equally shrouded in mystery if the communication system is connected to the driving system. I hope not.

Using existing operating systems for car electronics and on-board computers is tempting as it saves a lot of development time. Alas, it brings the problems from the computer world to cars - and I really don't think this is a good idea. While we get more and more electronics in our vehicles, the tendency is growing to use computers for it instead of discrete circuits. Of course, they're easy to use, they're programmable, they're versatile.

But we import not only the versatility - we import the vulnerabilities as well, only this time into an environment that understands something complete under "security" than we infosec professionals do. Automobile engineers think "safety" when they hear "security". They think of physical security.

Is it a good idea to use environments like embedded Linux or Windows Automotive or Symbian for automotive equipment? What do you think?

On a side note: the article in SC magazine is another good example for how insubstantial coverage often is. It's great to inspire fear in people; it's possibly great to put a dent in Lexus sales - but does it contain facts? No, it doesn't. As the saying goes, nothing's wasted - it can always be used as an example how not to do it.

Posted by Axel Eble in General, Technology at 10:23

Monday, January 24, 2005

IT&W /ed

Industrial Technology And Witchcraft, a fun weblog by a media company, is being slashdotted since this morning. The reason: they have hunted down and reconstructed the only remaining copy of the official Apple Macintosh premiere 20 years ago. His Steveness didn't look half as cool back then as he does nowadays. Wearing a bow-tie doesn't really suit him

Right on, majo! It was worth the wait!

Posted by Axel Eble in Off-Topic, Technology at 11:42

T-Mobile USA Hacked Revisited

I had talked earlier about how T-Mobile USA has been hacked.

According to a fellow CISSP who works there the SecurityFocus article was somewhat out of perspective. Jacobsen has had access to about 400 customers' data. These have been notified under California State Act SB1386.

The initial attack on customer records in October 2003 didn't "go unnoticed".

It's good to know people in the appropriate places!

Posted by Axel Eble in CISSP/(ISC)², General at 08:25

Sunday, January 23, 2005

Mediocrity is ruling us

Frau Berg erklärt die Welt. An article about the current mediocrity in Germany and how it rules it that way. Very polemic, very bitter - and very true.

Only it's not only about Germany. I can see that in a lot of places and I have seen it in a lot of places in the past. There's not much that can be done - except for doing it better.

If you happen to know German, read it.

Posted by Axel Eble in General at 22:36

Tuesday, January 18. 2005

Off-Topic: Thanks, Apple

Soon after my iBook G4 arrived it showed the first signs of a defect: it froze with a kernel panic. This happened every now and then (sometimes three times in a row, sometimes after three months running smoothly) until, finally, I was fed up with it and opened a case with Apple. I was suspecting the 3rd party 512MB RAM I had installed, but the system panic'ed even with the original Apple RAM installed. I followed every advice Apple gave me (fresh installation of the OS without any additional software; running it on the internal 128 MB RAM only; running it off an external disk) - to no avail. So, finally, after almost a year, almost at the limit of warranty, I sent it in to Apple for repair.

I almost expected what happened then: Apple returned it without finding a defect and sent an invoice for their Service Lump Sum. What to do? I decided to complain, stating that in any Unix dialect I know a kernel panic is a symptom either of a defective driver or a defective hardware. I told them how my fondness of Apple was severely tarnished and I further asked them politely to please replace the logic board (that's the mainboard for all you iA32/iA64 types) and refund the service fee.

Nothing happened for a few weeks. I gave them the benefit of the doubt and, lo and behold, they finally called last Friday with the news that they would repair the device and refund the service fee.

Thanks, Apple!

Posted by Axel Eble in Off-Topic at 07:13

Monday, January 17. 2005

Walter Ernsting *13. Juni 1920 †15. Januar 2005

And now to something completely different: Saturday, Walter Ernsting (german) (Artist's Name: Clark Darlton) died in a Salzburg, Austria, hospital. He was one of the most influential SciFi-Writers in Germany and one of the earliest, as well. He was a long time member of the pulp fiction series Perry Rhodan.

May He Rest In Peace.

Posted by Axel Eble in Off-Topic at 06:24

Sunday, January 16. 2005

Toll Collect - Another Neverending Story

Toll Collect, the German Autobahn toll company, finally started this year (with a mere two-year delay - but that's almost beside the point). They transmit the tracking data either via snail mail or via email as a PDF document or a CSV document. To make sure that these documents can only be read by the appropriate recipient the documents are packed into a .zip-File which is being encrypted (the key is signalled more or less out-of-band, i.e. in a separate email).

Now, is that stupid or not? Who in their right mind allow password-protected .zip-Files to enter the premises of their responsibility after the MyDoom and NetSky viruses abused that medium for their means?

Of course, their call center acknowledges that they only have these two alternatives to transmit the data. I've yet to receive a reply to an email I sent Toll Collect that their CISO would please get back to me. I'm not holding my breath, though.

Update: And a good thing I didn't. It's now February 16th, one month after my initial post. I of course haven't heard back from them...

Posted by Axel Eble in General at 01:06

Thursday, January 13, 2005

Schneier on Security: Secure Flight Privacy/IT Working Group

In his latest blog entry (Schneier on Security: Secure Flight Privacy/IT Working Group) Bruce Schneier talks about how he has been invited to a special Working Group that shall assess several issues about Flight Security. Actually, it's about the successor of CAPPs II and its efficiency.

The main point in his entry however, does not seem to be about the fact that he is a member of this group, but about the fact that he had to sign an NDA to be able to join. The original NDA the Department of Homeland Security wanted him to sign would have given them the right to search his premises without any warrant(!).

The question is: how much do US citizens trust their government not to make up "facts" and lie outright? Remember the record of said administration: it's all about secrecy, it's all about Fraud, Uncertainty and Doubt. They have proposed a lot of very invasive measures that incise deep into personal rights and privacy space - all with the provision that the terrorist threat is exceptionally high and that these measures will help in detecting terrorists and dangerous people. Their suggestions seem to be valuable when seen from the outside, but more often than not, when viewed from a security perspective, they are anything but. In fact, they are worthless because they either yield false positives or false negatives or no results at all. Take, for example the mandatory transmission of flight passenger data for all flights that stopover or land in the US. The US requires the airlines to transmit the complete Personal Name Record where many interesting things are recorded (amongst others, menu preferences). This information is allegedly being stored in raw format and used upon need. How long it will be stored is not disclosed. It's clear that the data would be wanted for computing a risk index for each passenger, yet without enough data to yield a believable result. Additionally, it's clear that much of this risk index would have to be guessed, not calculated - or, to use a somewhat more acceptable term, inferred. Inference is prone to very high amounts of false positives or false negatives if the boundaries are not exceptionally strict and the target is a pretty homogenous set. Would you describe humans as homogenous? Neither would I.

So go figure - think about the reasons the US government wants more and more control. Oh, wait, go and read George Orwell's "Animal Farm" before thinking...

Posted by Axel Eble in General at 20:01

T-Mobile USA Hacked

According to SecurityFocus 21 year old Nicolas Jacobsen from Portland, OR, hacked into the T-Mobile USA customer database and had access to it for over a year. He sold social security numbers and other identity theft related information up to voicemail PINs and candid photos taken by celebrities like Paris Hilton (of course, eh?) and Demi Moore.

What's really funny is that Mr. Jacobsen's resume is on the net and one of his stated goals is a CISSP certification. Maybe he should have taken a look at the (ISC)² Code of Ethics before engaging in illicit activities.

via Martin McKeay, CISSP

Posted by Axel Eble in General at 13:35

Blog Export: The Quiet Earth, <http://blog.balrog.de/>

Wednesday, January 12, 2005

Check This!

John Hargrove shows how little signatures on credit card receipts are checked. Hilarious - and a lesson to behold about the security of credit cards, the carelessness of vendors and the failure of security mechanisms.

Thanks to Udo.

Posted by Axel Eble in General at 17:58

Monday, January 10. 2005

Linux Kernel Development Problems

Richard's TaoSecurity has a very apt article about the stability problems of the 2.6 Linux kernels lately. I am on his side, the current image the kernel developers and their products offer is not very professional.

Tobias has ranted blogged several times by now about the strangeness of some design decisions surrounding Gnome/GTK+2. This goes along the same lines according to my gut.

Funny, the more mainstream Linux gets, the more problems pop up. Maybe a development model that's a bit more rigorous would be in order?

Posted by Axel Eble in General, Meta at 23:32

OH MY GOD, THE SKY IS FALLING!

Every decent security related blog is mentioning the latest Vulture article about non-secured web-based cameras on the Net.

Come on folks, that's not even worth a news item. Those cameras have little embedded computers, so what makes you think that people Out There would really secure those computers better than their own home systems? We all know where all the Spam originates (Own3d home computers, of course) and we all know that more often than not systems will be run directly on the Net in their default configuration.

So what else is new? Get over that particular tidbit and think about what you can do instead of what you can buy to make your setup more secure.

Posted by Axel Eble in General at 22:39

(ISC)² website up and running again

The (ISC)² website had been taken down for "scheduled maintenance". They seem to be up and running once again, now with a new, flashy (pun intended) front page.

I have yet to understand why websites need Flash to be deemed worthy websites. Oh btw, did I mention that the Flash menu does not render well with Safari?

Posted by Axel Eble in CISSP/(ISC)² at 22:06

Blog Export: The Quiet Earth, <http://blog.balrog.de/>

Friday, January 7. 2005

Trackback Spam

Due to massive trackback spam I have turned on comment moderation at the moment. We Apologize For The Inconvenience. [Sorry, Douglas Adams]

Update: thanks to the awesome guys and girls on #wordpress at irc.freenode.org!

Update 2: the storm seems to have settled down for now. Moderation is once again turned off. I'll watch it for a while...

Update 3: I've added Spam Karma to the plugins. Although Captchas don't work (I'm using authimage for that anyway) the rest seems to work. I'll be having an eye on it, but keep me posted if something does not work the way you expect it.

Update 4: Comment Moderation is once again turned on. Spam Karma doesn't seem to work too well on trackback spam...

Posted by Axel Eble in General at 20:06

Thursday, January 6, 2005

New Blog On The Roll

I can highly recommend John S. Quartermans blog Perilocity. I know Quarterman's works from way back in the '90s when I was still a greenhorn and fiddled around with the fascinating world of Email as a student employee.

Quarterman obviously emerged as well and funny enough, he's into risk management nowadays. His latest entry is pretty interesting, even if it has nothing to do with information security per se.

Posted by Axel Eble in General at 22:44

Wednesday, January 5, 2005

The Seven Cardinal Sins: Greed

With a two year delay Germany finally had a successful start of the toll system for trucks on the Autobahnen. The system works with GPS tracking and automatic digital imaging and OCR of the number plates off so-called "toll bridges". These images get transmitted to Toll Collect HQ and checked if the truck has registered with the system.

In a current article Heise Newsticker quotes a state police officer who wants to use the number plate images from the toll system to check for drug dealers and other capital crimes. Hessian already started the legal provisions for this kind of surveillance, Saxonia-Anhalt seems to be the next.

It's incredible how much privacy gets undermined in the last few years - even if people warned of the ineffectiveness of the suggested methods. It's pretty much the same as in the USA - form is more important than function.

Posted by Axel Eble in Meta at 17:32

Tuesday, January 4, 2005

Pardon?

Okay, so I'm possibly (very probably even) the last one to see this, but what on Earth are these sorts of trackbacks? It can't possibly be referrer spam and it comes from diverging IP addresses.

Any information welcome.

Posted by Axel Eble in General at 20:18

Security is not a product... once again.

In Category-based Web content blocking... a bit useless really Rory gives another fine example why technology can at most be part of the solution... and often is the problem.

Posted by Axel Eble in Meta, Technology at 14:42

Technological Complexity Bites Back

Dana Epp talks about the Top 10 Threats in 2004 (According to McAfee). While he's right in that most of these exploited long-known vulnerabilities that could have been patched, I see this only as an effect, a symptom, not the root cause. Why? Because even the notorious Microsoft vulnerabilities are not the root cause. It's the people and the complexity of the technology they use but refuse to learn enough about.

Our current computer and network technology is sufficiently easy to use for most people to jump aboard and do it. It is, however, at the same time sufficiently complex that most people will make errors in their configuration which in turn lead to vulnerabilities in their installed base.

Even people who should know it better (read: paid administrators in small to large companies) often enough have no clue whatsoever why something needs to be done in a certain way. Example? Take Wireless LAN - there's an abundance of people (and companies) setting up their access points without any security settings turned on. Take DNS: one of the most used and most abused protocols and applications on the Internet.

I believe that we need to work on the complexity: if things were less complex or at least well enough hidden behind a decent, intuitive GUI, I think we might better off. This would include safe and sensible default settings that work. And yes, we would possibly have to revamp some of the core protocols. The Internet has emerged from a small and safe place into an anarchic labyrinth where the old technologies simply don't scale any more. They were sufficient for the old times when there was trust abundant Out There. Today we need a complex design phase that caters to the complex problems and tries to find easy solutions to complexity.

And in the meantime it would help a lot if our dear vendors would start shipping their gear with security options turned on by default.

Posted by Axel Eble in Experiences, General, Meta, Technology at 02:01

Sunday, January 2. 2005

ESAG revisited

I've written before about the European Security Advisory Group. After some more research it looks like it's financed through straw men by the DoD. If it's true (and it definitely looks that way) it's part of D. H. Rumsfeld's propaganda group, there to shine a better light on the USA, particularly in "friendly countries" that are criticising the USA's unlawful war in Iraq.

There is some source material on telepolis, but it's only available in German.

Posted by Axel Eble in General, Meta at 20:40

Ethical Behaviour

At the 31st CSI Conference this year CSI had invited Frank Abagnale as Keynote Speaker. When several people of the Grand Old League heard of this, they refused to participate in the congress and/or decided not to speak at it. Some gave reasons along the line of "I make a point of never speaking if a convicted felon is speaking, too", some were less direct and said that Abagnale was selected as a keynote speaker because of his notoriety and that this would send the wrong signal to the participants. All agreed, however, that it was their ethical duty to abstain from talking. A heated discussion ensued on the CISSP mailing list about self-righteousness, about "forgiving" etc. When Abagnale learned of this, he offered to pull back. He even went so far that he will never speak at Information Security events again.

In my opinion, Abagnale has paid for his crimes. Considering that he did help the FBI considerably in the years after his conviction, I would consider him reformed (no matter that some of my peers say "once a con man, always a con man"). Still in my opinion, the first reason given above is self-righteous and a holier-than-thou attitude. On the other hand, the second one is a valid concern that I share, too. As much as Abagnale has done for the security profession, I'm sure CSI wouldn't have elected him keynote speaker hadn't Leonardo DiCaprio and Tom Hanks played in a quite successful movie depicting Abagnale's criminal life.

There's an ethical dilemma hidden in there alright. But it has nothing to do with the obvious good-guy-vs.-bad-guy. It's, as usual, thoughtlessness on the side of CSI. It's clear that hiring Abagnale was a clever marketing ploy to get more people interested in the conference and to make them sign up. Should we be mad at Abagnale for taking the opportunity? I don't think so. Should we laugh about our peers of high morale? To each their own.

But once again the real culprit is the industry that is primarily out to increase their sales. As long as the industry does not take responsibility for their actions and/or develops things the market doesn't need we should not wonder about how the information security profession is not taken seriously. We as professionals should actively work to get the industry to recognize not only their quarterly accounting data but What Is Right™.

Posted by Axel Eble in CISSP/(ISC)Â², General, Meta at 13:02

Blog Export: The Quiet Earth, <http://blog.balrog.de/>

Saturday, January 1. 2005

News and Updates

Starting with 2005, I'm hopeful to once again blog more regularly. I'll be closing my Rants down in favor of security related entries.

Since MT 2.x was a bit on the slow side and pretty vulnerable against comment spam I've decided to try out WordPress. The new blog is Gravatar-enabled (see example in the comment section) and has Captchas for commenting. Yes, email address and names are mandatory. Sorry 'bout that.

The old Information Security Blog entries have been imported into WP and are thus still available. There's a mod_rewrite rule that directs to the new pages.

Posted by Axel Eble in General at 16:09

Wednesday, December 22, 2004

OS X 10.3 Security Guide

NSA has published the MacOS X 10.3 Security Configuration Guide.

OS X and Solaris 8 are the only non-Windows operating systems for which a guide exists.

Posted by Axel Eble in Technology at 16:55

Saturday, October 30. 2004

Employment of Sasser Author Fires Back For Securepoint

According to Heise Newsticker (german only) H+B EDV, a company developing the Antivir software, has cut ties with Securepoint, the company that hired the author of the Sasser and Netsky worms.

If you would like to applaud them for their decision, write to them and let them know!

Posted by Axel Eble in Meta at 11:23

Friday, October 29. 2004

Security Risk Management Guide by Microsoft

Careful, Rant Ahead.

Microsoft has released their Security Risk Management Guide.

It seems to be a PDF document, so that's a huge improvement to earlier publishing efforts on their side. However, one has to have a .NET Passport ID to download the document. Thus, I can't say anything about the quality of the Guide because I refuse to register with an inherently insecure service that is essentially a data collector about all things relevant and irrelevant. Besides, I am pretty sure it does not differentiate between EU citizens and North American ones. For those of you who don't know, the EU has very stringent data protection laws which companies in the US have to adhere to under the Safe Harbour agreement between the USA and the European Union.

So, close, Microsoft, but still no cigar.

[Kudos to Dana Epp]

Posted by Axel Eble in Meta at 09:58

Monday, October 25. 2004

Fear Mongers Unite

Just saw a TV commercial for another fear monger group: www.esag.info. They claim to fight terrorism in Europe by educating people. However, they don't publish the persons behind the idea.

The whois-entry points to one Christophe Legrand of Paris, France.

All in all, it's pretty dubious. Kids: stay away from them. Your parents know better what to do and what not to.

Posted by Axel Eble in Meta at 23:51

Monday, September 13. 2004

Sender ID is dead

At the moment Microsoft does not have a lucky streak. First of all Longhorn has been postponed several times by now. Second, some key features will be missing like the database filesystem or the new programming framework. Third, they are biting on granite (as the German proverb has it) with the Internet standards process. MARID dropped the Microsoft-based Sender ID proposal to fight SPAM - and it's not the first of these defeats.

Looks like they don't Own The Market anymore and will have to work with it, not against it. It's really pathetic to see them whine about how they won't be making as much profit in the future as they have in the past because of Open Source software.

On the other hand, this is a nice way to show that software patents can be a bad thing for a company, too.

Posted by Axel Eble in Meta at 22:14

Indictment of Sasser Author

In Anklage gegen Sasser Autor Heise Newsticker reports that Sven J. - the Sasser author - has been indicted on charges of Computer Espionage. In addition to the criminal charges he'll be sued for damages for about 130,000 €

He's lucky that's it not much more - and that we don't have a legal system similar to the US where the sums would be way higher.

I hope he'll face a severe sentence to learn from his mistake. And, he should start thinking about a new career. I can't see how any company dealing with computers would think of hiring him with this background - let alone a security company, which he's hoping for.

Posted by Axel Eble in Meta at 21:05

Thursday, June 24. 2004

Organization Maturity

Ian writes in Financial Cryptography: Phishing II - Front Page News:

[phishing being mainstream news] is in itself an indictment of the failure of Internet security, a field that continues to reject phishing as a threat.

I don't share Ian's assessment. It's not "Internet security" that has failed. It's the people that have. I can't count the "security guys" who have no clue whatsoever what information security means. They still think it's a technical problem and some of them still wait for Microsoft to fix its (and thus: their) problems. They Don't Get It™. The people I know and respect all recognize phishing as a serious problem. They are preaching the awareness sermon to anybody who wants to hear it and then some.

This brings me to the basic theme of this article: the maturity of organizations. The capability maturity model for software development actually works for pretty much any part of an organization. It is just a generalization of the fact that the more formal an organization gets the more advanced and mature it is. The background being, of course, that formalisms are achieved after thinking about the underlying basics or a certain process - or, plainly, thinking about processes and refining them.

This seems to be just another view of mature descriptive processes like ITIL.

To sum this up with a somewhat provocative statement: a company's maturity is directly related to the professionalism of the employees. Well-defined processes are just a documentation of this.

Posted by Axel Eble in Meta at 17:31

Tuesday, June 22. 2004

NAI to be swallowed by Microsoft?

heise online - Spekulationen über NAI-Übernahme durch Microsoft talks about huge rebuilding taking place at Network Associates where not only massive layoffs are planned but a complete sell-out of the company is supposed to be possible.

As rumours have it, Microsoft is interested - which would match the statement that MS would add a virus scanner to their portfolio but not bundle it with Windows.

NAI hasn't had much luck with their one time strategy to buy countless companies and never managed to integrate them into one company. This led to bad integration of the products and disgruntled customers.

Recently, NAI has sold out PGP once again into a separate company.

The problems and the layoffs come as no surprise, however the suggested buy-out by Microsoft is a new twist that will make the other antivirus vendors like Symantec and Sophos wonder about the future.

Posted by Axel Eble in Technology at 16:36

Sunday, June 20, 2004

The Crystal Ball Threats

Haven't you often wondered about those billions of [insert currency here] damages by some new and extremely virulent worm? Haven't you often wondered how they know exactly how many systems were vulnerable and how many were attacked? Haven't you questioned the figures some big marketing research group came up with to hype the latest buzzword technology?

I knew you did! And what did you do then? Let me guess: you possibly thought "whoa! Those guys have research methodologies I'd like to know about", believed most of what they wrote with a grain of salt and moved on. Well, I know I did and I don't think I'm something special (or a special sort of dolt, for that matter).

Do me a favor - no: do yourself a favor and ask, nay, nag these guys about where they got the data from and how much of it is extrapolation to make their case. Doubt them and think about the sense those numbers make - especially compared to claimed damages in law suits. And I'm not talking the astronomical sums that are claimed in US law suits, mind you.

Posted by Axel Eble in Meta at 23:18

Saturday, June 19. 2004

Responsibility and Age

In Entwickler des Sasser-Wurms befürchtet hohe Schadenersatz-Forderungen on Heise Newsticker Heise reports that Sven K., the author of Sasser and the Netsky worm family is worried about his future, as the expected claims for damages will ruin him until the end of his life.

Well, tough luck. The guy is 18 which is legal age in Germany (although up until your 21st birthday you can be judged by juvenile law). I expect from people a certain amount of responsibility and thinking about their actions before all hell breaks loose. I've seen a large amount of discussions out there where people are saying the poor guy shouldn't be judged guilty at all because he was trying to do something good, because systems could only be affected if they weren't patched and yaddayaddayadda.

A worm is a worm is a worm is a worm - independent of any reasons for writing one. That's the first thing to behold. The second thing is that while people lack the diligence in patching, some just plainly and simply can't. Either because they run software that doesn't work on a patched system or because their integration test of patches takes way longer than the worm authors gave them. Locking a network from the outside is mandatory, of course. There are a lot of network design issues that can mitigate the dangers of malware. However, if one of your users brings an infected laptop in chances are, all hell breaks loose. Third, the non-patching home users often lack the understanding of security. They use the system like they use their car: sit in it, turn it on and drive. If something breaks, they'll bring it to the garage down the street to have it fixed. Computers as they are today need a lot more knowledge to use. And Microsoft's claims that they have made computing easy for the average person out there may be largely correct - however, the administration is not. Microsoft has maneuvered themselves into a tight spot: it's a very fine line between automation of patching and easing system administration and the need for privacy. I'm not sure they understand that there are different mindsets all over the world that prioritize differently.

Anyway, back to the topic: if a guy of 18 years can't estimate the work and damage he's going to cause by releasing several worms into a world-wide computer network, then I'm sorry, but he isn't suited to use a computer.

As a final funny side-note, he's looking for an apprenticeship now, preferredly in a company working in the field of IT security. As he's already proven his lack of integrity and adulthood, one can only but hope that no such company will hire him.

Posted by Axel Eble in Meta at 11:25

Wednesday, June 9, 2004

XML Firewalls vs. Controls

Jiri talks about XML firewalls and thinks that they are somewhat superfluous as controls can be implemented on the application side (Jiri's Notepad: The case of XML firewalls). He's right, of course. On the other hand, this is only valid for your self-developed applications. What happens when you buy third party products that exchange data in XML format over which you have no control? Since I work in a shop where we make heavy use of EDI for B2B I know that sometimes external applications and connections have to be implemented where one does not have the source to put appropriate controls in place.

It seems like XML security has been analyzed quite a bit. There are several resources out there that deal with encryption, signature, key management and remote execution (XML-RPC) in XML documents (and the possible security problems with XML documents traversing your firewall for RPC reasons). However, it seems pretty hard to me to create products that can analyze the documents for conformity to security policies.

Posted by Axel Eble in Technology at 09:56

Witty Worm Analysis

Stefan Keller has dug up some analysis about the Witty worm.

I agree with the paper: we were lucky that it did not attack a ubiquitous vulnerability of Windows this time. We would have been seriously bugged had that been the case (pardon my French).

Posted by Axel Eble in Meta at 09:35

Threat Modeling Tool

Michael Howard has a couple of blog entries about the Threat Modeling Tool published by Microsoft. While primarily geared toward application developers, it can be used for practically any Threat Modeling. It's a bit beta at the moment, as Michael explains in Updated info about Threat Modeling tool.

If you're running Windows and don't mind installing the .NET Framework 1.1 I suggest you try it out.

Posted by Axel Eble in Meta at 09:26

RSS Feed For MS Security Bulletins

Microsoft's Security Bulletins seem to have an RSS feed nowadays [via Michael Howard]

Posted by Axel Eble in Meta at 09:21

Tuesday, June 8. 2004

IT Projects - A Secure Way To Sink Ships

In SAP-Projekt der AOK kriselt one more of the usual IT projects is described: one of the Health Care companies (Krankenkassen) has started to implement SAP. Now suddenly the project will be late by three years and it will cost at least 540 million € instead of the planned 360 million. According to the Vice President of the organization they underestimated the complexity of the software. That's a serious reality check here. Underestimating the complexity of SAP is tantamount to saying software has no bugs or the Titanic is unsinkable.

Another nice example that controls are necessary and that large projects should be broken into small sub-projects and include detailed planning and evaluation phases before committing money and signatures.

Posted by Axel Eble in Meta at 09:40

Outsourcing Trust And The Failure of PKIs

Ian has a pretty interesting article about the failure of PKIs at Trust Cannot be Outsourced (via Financial Cryptography).

He's right, using some PKI that you have no control over is tantamount to outsourcing your trust. I've often wondered about what's supposed to make PKIs and CAs like Verisign so special. Obviously, it's nothing, really: it boils down to giving someone money and having to trust them without any good controls.

Of course, this is not the only reason why the PKI model failed commercially. It's one of the reasons, but that didn't keep some people from throwing money at the vendors in return for less work.

Another major reason why PKIs failed is the fact that vendors claimed they could solve any problem at all. Companies started to implement PKIs without any good idea what they wanted to accomplish with them. Thus, the projects often became bloatware and died a quiet death. Or, they were successfully implemented but there were no applications making use of them. Quiet death once again.

Mind you, I'm all in favor of Service Level Agreements - but there is only so much one can put into an SLA. A second point to take into account is the fact that with PKI vendors and the CA trust model there are no controls that can be audited. So what do you match your SLA against? Availability alone? That just doesn't cut it.

It's actually a good example of what went wrong in the Dotcom years and that technology without a business case is money thrown out the window.

Posted by Axel Eble in Meta at 09:07

Monday, June 7, 2004

Alan Mathison Turing

*June 23, 1912

† June 7, 1954

Posted by Axel Eble in Meta at 10:52

Friday, June 4, 2004

John Thompson's Remarks On The Security Of Linux And Windows

According to Symantec CEO hits out at Microsoft... and Linux (via silicon.com) John Thompson said he doesn't believe that Windows is inherently less secure than Unix dialects and that the Malware creators will be attacking Windows for some time still because Windows has such a high profile.

Generally, I think he is right. However, comparing Unix dialects (let's focus on Linux here because it really is the most prominent one and most points are valid for commercial Unix dialects as well) and Windows shows a few crucial differences.

Windows is more widely distributed than Linux - that's a given. It does have a worse default configuration security-wise: network services are accessible by default and are turned on by default. This is slowly changing, but we won't be seeing much of that before the release of Longhorn (which won't be released before 2006). And finally, Windows users are in majority much less knowledgeable and interested in the workings of a computer than Linux users are. It is clear that many of these people will run the default configuration of the OS they bought the computer with - and they won't bother to upgrade without any need. If this isn't clear to you, take a look around in your families and take note how many people still use Windows95 or 98 without having installed any patch. All of this factors into the vulnerability of Windows.

Linux, on the other hand, sees a definite rise in usage - and not only in the server department but on desktops as well. Distro vendors do their best to sell Linux as "desktop ready" and the workings of the KDE and Gnome groups have gone pretty far already. So, users are going to try it out. That means the profile will get higher and it will become more attractive to the average malware author and skript kiddie. It also means that more people will use it who aren't as technologically savvy as the current user base, thus more people will run with default configurations. Linux distro vendors have recognized this and ship their respective distros with more secure base settings. They start to hide the inner workings from the users to make it more appropriate for the tech un-savvy users.

Thinking about it, this was one of the most surprising things to me: the main influence on system security is the default configuration.

As a final note, let me state where I think Thompson errs: Integration. The Windows systems are highly integrated. While Microsoft sells that as it's biggest advantage over Linux, in my eyes that's the biggest disadvantage. If you can't remove the browser from the system without rendering it inoperable, something is clearly amiss. Another example? If you need over six months to release a patch for a vulnerability in the ASN.1 parser because you need to do so many regression tests that doesn't bode well for the future: complexity in Windows rises, more and more gets integrated into the operating system.

Unix systems integrate through interfaces: there are well defined input and output systems of small programs that can be chained together. This makes it flexible without bloating. A bug in a library or program? Fix it - just make sure you keep with the interfaces. You'll only have to test the program or the library - not the whole system.

Summing up, this means that Thompson is more or less right: Windows will stay the primary target for some time. However, Users will try out Linux and thus Linux will become more attractive in the future.

I don't really agree with his assessment that neither Windows nor Linux are inherently more secure compared to each other. The integration aspect and the fact that the default configuration is more secure with Linux systems make me believe that Linux is more secure. Just how much is open to anyone's guess.

Posted by Axel Eble in Meta at 22:04

Thursday, June 3. 2004

(ISC)2 Privacy Leakage

Today the Vultures have published the article
Security cert body gives lesson in insecurity.

(ISC)2 has recently published a "constituent survey" that the constituency is asked to fill out. The survey obviously was outsourced to a contractor that a) had the appropriate infrastructure in place and b) sent the mass mail.

Obviously, the survey company didn't do their homework with respect to security and privacy.

I have a whole lot more to say to this but will refrain from doing so. For the moment.

Posted by Axel Eble in CISSP/(ISC)² at 22:26

BayStar Capital pulling out of The SCO Group Deal

In a press release the SCO Group states: The SCO Group to Retire All Shares of Series A-1 Convertible Preferred Stock, meaning essentially, BayStar Capital pulls out of their deal with The Company That Made Insubstantial Sueing Their Business.

It remains an interesting comedy.

Posted by Axel Eble in Meta at 10:59

Anti-Spam Solutions Soon Under Legal Attack?

'twas in the News yesterday: NAI has been granted a very broad patent on antispam technology. Rory thinks this is An example of software patents being a bad thing™.

I guess we'll just have to see how aggressive NAI will attack other vendors.

As I have little knowledge about the legal implications abroad, I can only speak about German patent law which states that if a technology was already in use for some time before the patent was granted, the patent is void. Since software like SpamAssassin or bogofilter use Bayesian filtering for some time now, I don't think NAI will stand much of a chance in monopolizing this particular technology. What they can monopolize, however, is their particular implementation. How effective that is has yet to be determined, though

Posted by Axel Eble in Meta at 10:43

Thursday, May 27. 2004

Economics and Security

Many people often see security as a technological problem. To this point of view I often reply with the quotation attributed both to Bruce Schneier and Marcus Ranum: "If you think technology can solve your problems you don't understand technology and you don't understand your problems".

Looks like Ross Anderson has taken this to heart and collected a page of resources about Economics and Security.

Definitely bookmark material.

Posted by Axel Eble in Meta at 13:58

Thursday, May 20, 2004

The Truth And Nothing But The Truth

Andrew Tanenbaum of Minix fame wrote down Some notes on the "Who wrote Linux" Kerfuffle where he talks about the notorious Ken Brown of Alexis de Tocqueville Institution. Yes, the one who keeps publishing rumours and FUD about Linux and how it's actually dangerous to use it in a corporate environment.

Apart from Andrew's conviction that he owns the truth when it comes to the old Microkernel vs. Monolithic Kernel debate and his diminishing of Linus' accomplishments he really offers more interesting facts than the ominous de Tocqueville Institution ever did.

It's interesting to note that the so-called "path-breaking study" is not available for free and a free review copy for the press and academics needs a copyright agreement. It would be most interesting to see this same agreement. Obviously, Brown is being paid by either Microsoft or the SCO group - otherwise how should we interpret the "review[...]" in light of repeated expressions of contempt for intellectual property rights by Torvalds and some (but by no means all) open source programmers.?"

Posted by Axel Eble in Technology at 22:15

Saturday, May 8. 2004

Germany: two points

Funny, isn't it? Suddenly Good Ole Germany is back in the limelight. Both the authors of Sasser and of Phatbot are German citizens, the latter even lives pretty close to my hometown of Freiburg.

Who would've guessed?

What's going to be interesting is whether the Netsky variants are going to end as well - the self-called skynet said that Sasser and the Netskys were written by the same authors.

Update: Looks like the Sasser author indeed is the Netsky author as well. The only downside is that he will be judged by juvenile standards as he turned eighteen (legal age in Germany) only a short while ago. However, that won't make any difference for the damages the victims will want amends for... I'm almost sorry for the guy.

Posted by Axel Eble in General at 18:31

Monday, May 3. 2004

Companies Don't Get It™

The F-Secure : News from the Lab Blog is a source of interesting information. Today the following was posted:

Sasser rumours Posted by Mikko @ 11:12 GMT

In August 2003, Blaster worm outbreak disrupted bank systems as well as air and train traffic.

This seems to be happening all over again. According to the sources quoted below, there have been Sasser-related problems in at least two large banks. RailCorp rail traffic was halted in Australia on Saturday, leaving 300,000 travellers stranded - CEO of the company is quoted saying a virus might be the reason. Also, according to several sources, Delta Airlines had their planes grounded in USA on Saturday for several hours, because of a "computer glitch"...but this case has not been confirmed to be related to Sasser.

Links are available at the F-Secure Blog.

If this is true and if it is related to any one of the newer worms, then this is a clear sign that companies Don't Get It™; they don't seem to have learned from Blaster and consorts.

Can we please get a tad more professional?

Posted by Axel Eble in General at 16:17

SLAs are news items nowadays

Microsoft unterstützt Bundesinnenministerium bei IT-Sicherheit is a news item stating that Microsoft will support the Bundesamt für Sicherheit in der Informationstechnik (BSI) in securing the operation of critical infrastructure (like TelCo or Electrical Power). The BSI is supposed to help operators of critical infrastructure in securing their information technology equipment.

It does sound like nothing more than a simple SLA about vulnerability information, even more so since they don't want to publish the nature of the information that Microsoft will share.

Anyone willing to bet that it's nothing more than a simple information service about vulnerabilities?

Posted by Axel Eble in local at 15:17

Friday, April 23. 2004

RoSI: R.I.P.

It looks like Return on Security Investment (RoSI) is dying a more or less silent death. I'm seeing more and more articles that say it makes no sense to expect a return on investment from expenditures for security. One of the latest in this series is a report from Information Security Decisions Conference published in SearchSecurity. In it, Edward Hurley summarizes some alternatives that were discussed at the conference. While I don't agree with the proposed alternatives I am hopeful that people will Get It™ finally.

My critique with the quoted "return on seatbelt investment" is the same as with the common ROSI: it's simply not calculable because you have no additional revenue by spending for security.

The message is correct that security, like IT, is an enabler to the business: it gives certain guarantees about availability and it takes care of the appropriate (and, possibly, given) level of confidentiality and integrity.

Let's hope the profession and it's professionals mature in more ways like this.

Posted by Axel Eble in Meta at 11:33

Wednesday, April 21. 2004

Junk Mail Is Not A New Problem

In his recent entry Spam -- a brief historical perspective Fred Avolio points to late Jon Postel's rfc706: On the Junk Mail Problem.

What's so surprising is not that Jon Postel wrote it or that the topic is mentioned in an rfc. What I really found astounding is the date: November 1975.

Update: since there seems to be considerable misunderstanding about this entry, here's a bit of an explanation. Naturally, in 1975 spam was no issue. That's why Jon thought about black- and whitelists for server systems to take care of unwanted email (like, from badly configured systems). However, these principles apply just the same to any sort of unwanted email, be it spam, excessive bounces or anything else.

Posted by Axel Eble in General at 11:10

Friday, April 9, 2004

security companies

I have blogged before about the business model of security companies, especially companies that sell anything related to reactive security.

The current case of Intego about the Proof of Concept MacOS X trojan highlights this clearly. They are FUDing the community to sell their product.

What light does this shine on the security industry in total? Maybe Andy Briney is right after all when he says in his logoff column in Information Security that the profession is "struggling to gain respect, credibility and funding." Fred Avolio doesn't think so, but seeing companies like Intego acting so transparently stupid makes one wonder.

How can we expect to be treated with respect and belief when our peers (and at least for argument's sake I'm assuming that Intego employs security professionals) act so foolishly?

Posted by Axel Eble in Meta at 23:24

Thursday, April 8, 2004

Oh The Wonderful Things Mr. R. Can Do

In his blog, Martin McKeay tells about a thread that flew by the CISSP Forum a couple of days ago.

Having had the pleasure of Marcus Ranum's company a few weeks ago at a TruSecure roadshow, we got into a discussion about politics pretty quickly. From this I had a hunch that the letter Martin mentioned and the views of Marcus Ranum didn't really fit together. Never one to wonder for long I sent Marcus an email asking him, basically, "What the heck?"

Seems like Marcus thought the same.

We've been discussing the issue of cyberterrorism and cyber warfare for some time in the CISSP mailing list a while ago. The consensus of the people I respect most on that list was that cyber terrorism is inefficient as it doesn't instill the same terror in people than explosives do. Okay, so switching off the power for half a country is pretty darn bad. However, it is nothing as concrete and direct as flying airplanes into the heart of US economy and bringing it down into a heap of rubble. Opening a dam thus flooding a large part of a country is bad, no doubt. But wouldn't it be way easier to stick a few kilograms of plastic explosives to the base of said dam and watch it explode? The power and force of an explosion will always invoke stronger emotions than the controlled opening of flood gates.

Which leads me to the next cow I'm having with cyber terrorism: it's complicated: there is a large amount of knowledge involved. There is a lot of energy involved on the part of the terrorists to get where they want: it's not as if the computers controlling the dam are on the Internet without security systems (contrary to the dam itself which is usually accessible directly through hiking). Another thing to consider: the perpetrator leaves tracks and traces. Granted, those are pretty much worthless at the moment (thanks to lazy system administrators) but on the other hand: They. Do. Exist. Finally, having remote control over a system is different. It's like steering a pickup truck by remote control. Anything can go wrong: the system is not reliable and the communication is pretty much one way. A lot of information about the actual surroundings of the system will be missing. The perpetrator will always have to wonder whether they are on a clever honeypot or on the Real McCoy.

The same obviously holds true for warfare - actually, even more so. Why remotely try to hack into a munitions depot or other critical infrastructure of the enemy when you can fly an unmanned drone or a cruise missile directly into it? At least that money will be well-invested...

[just in case you're wondering: the title is an adaptation of a line from the book by the wonderful dr. seuss: "mr. brown can moo! can you?"]

Posted by Axel Eble in Meta at 23:15

Plaxo and the like

In his article [Opting out of Plaxo](#) Jay Allen talks about Plaxo and why he'd never use their services.

Just one of those funny coincidences, I guess. Just this afternoon I was talking with my colleague about them and their services and the potential security implications. While their privacy statement explicitly states they wouldn't pass your information to anybody else, I have yet to understand how they make money. Their business model is completely unclear to me if they promise me my privacy.

Aside from this, I'm pretty sure their service will be used heavily - in the US. I'm equally sure they'll not have as many customers in Europe. Our privacy needs and wants are completely different from the US ones.

Posted by Axel Eble in Technology at 22:56

Tuesday, April 6. 2004

Certified Authentication May Be Worthless

We are currently evaluating VPN clients for mobile users. Several of those offer the capability to authenticate with digital certificates against the corporate endpoint. However, thinking about it, it becomes fairly obvious that certificates may not be the best way to go for mobile users. The user must have the private key encrypted with a password. Thus the security of the VPN link is reduced to the security of the password. If said password is captured by any way the certificate basically is compromised.

Certificates are useful multipurpose tools: they can be used e.g. to encrypt, to sign, to authenticate. However, to really make them useful, they would have to be issued by a corporate wide certification authority (CA) and included in the corporate PKI framework. Most technologies nowadays come with their very own CA and do not fit into a PKI (even if one were already established).

Digital certificates have their place: in static gateway devices that are secured properly both physically and organizationally so they may not be accessed by unauthorized persons (try doing this with a laptop and you end up with it in a concrete block at the bottom of the Sea).

There are other solutions for this specific task: using one-time passwords (OTP) and/or n-factor authentication. Like using an OTP generating token together with a personal identification number (PIN) or other secret information (like a password).

The conclusion is easy: for simple authentication and identification of mobile users against a VPN gateway digital certificates are far inferior to one-time passwords.

Posted by Axel Eble in Technology at 13:26

Sunday, April 4. 2004

Im Westen nichts Neues

Fred Avolio talks about how the same old, same old discussions seem to pop up in information security.

He's right, of course. I heard Marcus Ranum a few days ago and he said basically the same thing: Information Security isn't rocket science and the most effective techniques have been around since at least 20 years.

So, what does it mean? To be cynical, it means that the information security industry is a big part of the problem. They don't seem to want to come up with solutions to our problems, they don't seem to want to do research. Of course, if they make us secure, they won't sell anything anymore. And if they want to keep on selling us their stuff that more or less works, they'll have to re-label it. So that's why we have Intrusion Prevention now.

The real hard problems haven't been solved, like log file correlation; like insecure default settings; like... you name it.

Posted by Axel Eble in Experiences at 20:20

Friday, March 19. 2004

Control Freaks

In an article called *Reisepass mit RFID-Chip* the Heise Newsticker reports that the German Federal Printing Office ("Bundesdruckerei") is ready to create Passports and Identity Cards with RFID chips. The implications of this are far-reaching: it means that it's completely out of the control of the holders of said passports and ID cards when and how they are scanned.

What does it mean? Always keep a generous amount of tin foil at home.

Posted by Axel Eble in Technology at 15:22

Sunday, February 29. 2004

Connection Managers

I've recently encountered the problem of wanting to have a remote dial-in solution that uses any available technology: broadband, wireless, modem, ISDN. If possible it should be integrated with a personal firewall, a VPN client and software checks (like: A/V patterns, software version checks etc).

It looks like there are at least two globally available solutions out there: iPass and Fibrelink. Both seem to be pretty interesting.

Posted by Axel Eble in Technology at 09:56

Friday, February 20. 2004

To Patch Or Not To Patch

The lately released MS Security Bulletin MS 04-007 raises important questions. Since there is no known exploit in the wild that does more than a Denial-of-Service attack it is valid to ask whether all systems need to be patched. On the other hand: the vulnerability is at such a critical place in the Windows infrastructure that it's really, really, really unclear to me whether we really should wait until we get bitten into our buttocks.

Being the security fascist I am I'd rather patch - but how long will it take until the next vulnerability of this quality will be out in the open?

The highly integrated architecture of Windows makes creating patches - and testing them - a real nightmare. Microsoft really could benefit from an open source approach.

Posted by Axel Eble in Technology at 14:03

Monday, February 2. 2004

Holistic A/V

Sometimes everything seems simple until one starts to actively address a problem.

Take Antivirus, for example. Sure, perimeter security. We might want to take a look at server security, as well. And while we're at it, let's not forget the personal firewalls on the desktops and laptops to help us enforce policy.

Sounds still easy? Wait until you delve down into the nitty-gritty and have to check for all the connections to the outside, for the services offered and whether there's a product covering every one of them (because, remember: security is only as strong as the weakest link).

I'm feeling somewhat like opening Pandora's Box.

Posted by Axel Eble in Technology at 15:29

Saturday, January 24. 2004

Anfänger

How to tell a human from an automatic probe? Easy:

```
Out: 220 Heimdal.Balrog.DE ESMTP Postfix
In: HELO
Out: 501 Syntax: HELO hostname
In: QUIT
Out: 221 Bye
```

Posted by Axel Eble in Experiences at 22:39

Friday, December 5. 2003

Networking

I've sent an email to all the local groups Stefan and I know. We'll try to set up a meeting about where each of the groups wants to go and see where collaboration makes sense and where we can promote each other.

Stefan and I think of our group as a means to share information, to glimpse into areas where people may not have that much experience so far.

I'm curious how many people we'll get together and if and how we're going to collaborate. Sounds intriguing so far.

Posted by Axel Eble in Meta at 21:14

Thursday, November 27. 2003

Security-Meeting

Heute, 27.11.2003, 19:30 bei Avinci Mitte.

Posted by Axel Eble in Meetings at 19:05

Wednesday, July 9, 2003

Just because they're out there doesn't mean we have to be paranoid

In the Washington Post article *Dissertation Could Be Security Threat* a grad student is described whose dissertation is considered to be a possible security threat. So far, so good.

The information that he used to write his paper is publicly available, however. That means, anybody else could do it, too. Thus people are trying frantically to re-classify their once public information as confidential. The catch here is, you can't. There is no way of knowing how many people have already accessed the information and made a copy for future reference or for redistribution. Once it's in the open, you can't pull it back into the closet and declare it private. Ask any film star about their quest of suppressing the nude photos they foolishly had done before they were famous.

The underlying point, however, is a completely different one: it's simply about the feasibility of risk assessment/analysis. There is no notion whatsoever how many people accessed and compiled the information. There is no way of knowing how distributed it is. And, finally: there is no way of knowing or predicting the probability of an attack, much less an attack with or through this public information. So how do they know it's dangerous? Simple answer: they don't. Risk Analysis is impossible when you have so many variables and so little hard, factual input. Thus the only reason for the proposed action is: paranoia.

Which leads me to the following conclusion: It's Fear, Uncertainty and Doubt (FUD) they talk in order to widen their power, in order to have excuses to spread their military (and sooner or later their economic) power throughout the world. "Am Amerikanischen Wesen soll die Welt genesen." This didn't work in the past for Germany, it won't work in the future for the USA, either.

Posted by Axel Eble in Meta at 13:40

Blog Export: The Quiet Earth, <http://blog.balrog.de/>

Monday, March 24. 2003

Need! More! Input!

Well, the first meetings of the local security group have gone by. The second time we were very few people and I do believe by now that it makes no sense to hold CISSP-only meetings. Let's open up and invite people from all over. I've started a list of companies in the area that I would like to invite, too. I'm concentrating on the well-known brands for now, but hey: we welcome anybody interested in security and able to participate.

Posted by Axel Eble in Meta at 22:22

Blog Export: The Quiet Earth, <http://blog.balrog.de/>

Monday, January 20. 2003

meta work

The first meeting of the local CISSP group lies behind us now. It looks promising: we seem to have a group of interested people that seems to be dedicated both to continued professional education and to the networking aspect, too.

Speaking of which, one of the guys from the list mentioned the CAST Forum which does seem to have interesting but expensive seminars (200€ for non-members early subscription; member fee is 1500€/a). The GI does have a Security SIG that meets a few times per year in Frankfurt.

The question arises whether that appeals to people "out there" as the GI in my eyes has a pretty academic approach to things. We'll see - the next talk is on January, 31 and I plan to join them. I'm still thinking the international aspect of the ISSA might give a new angle to the meetings and the things people expect of them - but I'm happy to give it a try. The goal, no: my goal is to find people to network and to share thoughts about current developments and ideas and tools and whatnot - in three words: continued professional development.

Posted by Axel Eble in General at 00:22

Thursday, October 24. 2002

Discussions

I would like this weblog as a means to discuss those topics in information security that are not so much of a technical aspect. In my eyes, there are lots of discussions about 'technical' aspects out there - however, no technical measure can help if human compliance is missing.

Posted by Axel Eble in General at 10:59