Monday, July 28. 2008

Neue Sicherheitsrichtlinien und die Auswirkungen

Gerade bei Bruce Scheier gefunden:

Im Yankee-Stadion in New York durfte keine Sonnenmilch mitgenommen werden.

Das ganze wurde nicht auf der Webseite publiziert sondern einfach beschlossen. Die Security-Leute wussten Bescheid, sonst wohl kaum jemand. Leute die mit Sonnencreme kamen mussten diese abgeben - auch die Sonnencreme fÃ¼r Kleinkinder.
Den Zuschauern wurde geraten sich einmal einzucremen und dann die Tuben abzugeben.

Nach entsprechenden Protesten nach dem letzten Spiel im Stadion wurde dieser Ban wohl wieder aufgehoben.

Posted by rince in CCCS at 11:50

Der neue Personalausweis

Das Datenschutz-Blog hat einen sehr schÃ¶nen Artikel zum neuen Personalausweis.

Insbesondere finde ich es erstaunlich dass die Bundesregierung meint dass alles sicher sei bis zum Beweis des Gegenteils.
Gerade bei krytographischen Verfahren (wie fÃ¼r die eID und/oder digitale Signatur) muss man sich darÃ¼ber klar werden dass heute starke VerschlÃ¼sselung nur bedeutet dass sie in 5-10 Jahren leicht gebrochen werden kann - von PCs. DafÃ¼r gibt es sogar ein gutes Beispiel:

In dem UNIX-Systemen der 70er-90er Jahren war als Standard-VerschlÃ¼sselung DES benutzt worden. Die BegrÃ¼ndung damals war dass es niemanden gibt der mit "sinnvoll" viel Geld einen EntschlÃ¼ssler bauen kann der mit Brute-Force (also alles einzeln durchrechnen) DES knacken kann. Der "Point-of-even" wurde damals auf 200.000$ beziffert.

Das ist eine Menge Geld fÃ¼r jemanden der "nur" Passworte von User knacken will; also einfachstes Anwendungsbeispiel. Andere Beispiele wÃ¤ren EC-Karten; aber das zu erklÃ¤ren fÃ¼hrt zu weit; aber DES wurde lange Zeit auch bei EC/Maestro-Karten benutzt.

Nun wurden Rechner mit der Zeit immer billiger und trotzdem schneller / besser und ich glaube Mitte der 90er Jahre haben sich ein paar Leute zusammengesetzt und Ã¼berlegt wie sie mit einem Budget von 200.000$ einen Rechner bauen kann der nichts anderes tut als DES berechnen - aber so schnell dass er fÃ¼r einen PaÃŸwortcracker benutzt werden kann. Nicht um damit Mist zu bauen sondern um zu zeigen dass DES inzwischen schwach geworden ist als VerschlÃ¼sselung.

Das ist auch dann sehr erfolgreich gewesen; O'Reilly hat ein Buch publiziert wo genau diese Geschichte erklÃ¤rt wird und gezeigt wird wie dieser Rechner gebaut wurde. Ich schÃ¤tze, heute wÃ¼rde die Hardware 20.000$ kosten; aber inzwischen gilt als Standard-VerschlÃ¼sselung bei Unix auch AES.

Bei freien Unices war es kein Problem, mit der VerschlÃ¼sselung fÃ¼r Passworte von DES auf Triple-DES oder MD5 zu wechseln; damit war die "Gefahr" durch DES gebannt.

Um zu dem Personalausweis zurÃ¼ckzukommen: Was wir aus dieser Geschichte lernen (die stark verkÃ¼rzt dargestellt ist) ist dass gerade VerschlÃ¼sselungen schwÃ¤cher werden je Ã¤lter sie werden. Das was heute als "stark" gilt ist in einigen Jahren im Bereich der Sachen die in endlicher Zeit geknackt werden kÃ¶nnen - entweder weil die Hardware entsprechend schneller wurde oder weil SchwÃ¤chen im Algorithmus oder der Implementation gefunden wurden - siehe Debian vor einigen Monaten bei OpenSSL.

Man kann sich noch nicht einmal sicher sein dass die Funktion - sofern man sie nicht bestellt hat - dauerhaft ausbleibt. Jeder der irgendwie an das Zertifikat herankommt mit dem die EinwohnermeldebehÃ¶rden die Signaturen generieren (und da wird es also fÃ¼r jede BehÃ¶rde eines geben, also gibt es auch ein paar tausend Leute die darauf Zugriff

haben) kann dann fÃ¼r den Personalausweis eine Signatur generieren und damit ist die elektronische Signatur des Passinhabers aktiviert. Selbst wenn er das gar nicht wollte.

Da frage ich mich warum nicht die Politiker solche Sachen "quasi als Vorbild" als erste austesten und auch die SchwÃ¤chen sehen dÃ¼rfen...

Posted by rince in CCCS at 09:16

Die Pixar-Vorfilme

Es kommt ja in Deutschland im August der neue Pixar-Film raus - Wall-E. Bei jedem Pixar-Film gibt es einen kleinen Vorfilm, der auch immer sehr schÃ¶n und mit viel Detailtreue erstellt wird. Bei Wall-E ist das Presto.

Posted by rince in Kino at 09:13

Friday, July 25. 2008

Wir haben ja nichts zu verbergen

Ein in meinen Augen durchaus schÃ¶ner Text, was mit Datenquellen alles anzufangen ist...

Posted by rince in CCCS at 15:40

Die PlattenlÃ¤den und die kleinen KÃ¼nstler

Nachdem ich ja auf der MÃ¼tternacht Spezial war dachte ich mir, ich kÃ¶nnte ja auch zu den KÃ¼nstlern mir mal einige CDs oder DVDs anschauen. Auf deren Homepages sind die ja alle angezeigt und auch als kaufbar angegeben.

Nun ja, ich wurde eines besseren belehrt. Ich lief gestern durch die KÃ¶nigsstrasse in Stuttgart und ging durch die LÃ¤den.

Zumindest "Eure MÃ¼tter" war ihnen ein Begriff, auch wenn sie von denen nichts da hatten. Martina Schwarzmann hatten sie auch schonmal gehÃ¶rt.

Aber der Rest?

Also ich konnte keine DVD der KleinkÃ¼nstler bekommen; "nur" eine CD der MÃ¼tter habe ich entdeckt.

Bin ich da eigentlich zu kleinkariert dass ich erwarte dass lokale KÃ¼nstler (Zumindest Eure MÃ¼tter kommen ja aus Stuttgart) auch vertreten sind bei den PlattenlÃ¤den?

(Okay, Amazon hat die ganzen Sachen. Aber ich wollte eigentlich nicht den VersandhÃ¤ndler bemÃ¼hen dafÃ¼r).

Also bleibt entweder bei den KÃ¼nstlern selbst bestellen oder bei Konzerten (wo es alle wollen) oder hoffen. Oder habe ich kleine LÃ¤den einfach Ã¼bersehen?

Posted by rince in Kleinkunst at 07:44

Thursday, July 24. 2008

MÃ¼tternacht Spezial: Ole Lehmann, Martina Schwarzmann, BÃ¼lent Ceylan und Bodo Wartke

Ich habe relativ spontan beschlossen (also letzte Woche) doch auf die MÃ¼tternacht spezial zu gehen. Das ist ein Comedyabend mit vier GÃ¤sten, welches auf der FreilichtbÃ¼hne Killesberg stattfand.
Auch wenn es anfangs der Woche nicht nach gutem Wetter aussah; gestern abend war es wunderbar. Wir waren rechtzeitig am Eingang um gute PlÃ¤tze zu bekommen und warteten einfach ab.
Ich sollte dazu sagen dass ich "Die MÃ¼tter" bisher nur von Plakaten kannte. Ich habe ihr Programm bisher nicht gesehen, fand aber die Plakate eher ... seltsam.

Jedenfalls machen sie seit 2 Jahren in der Rosenau einen Comedy-Club; jeden ersten Dienstag im Monat gibt es dort einen Kabarettisten, wobei die Zuschauer bis zum Auftritt nicht wissen wer auftritt; das ist also eine Ãœberraschung. Zum JubilÃ¤um haben sie sich vorgenommen, nicht nur einen sondern vier KÃ¼nstler auftreten zu lassen und (weil der Raum mehr Leute fasst) das ganze auf dem Killesberg stattfinden zu lassen.

Nach einem Opener von den MÃ¼ttern darf Ole Lehmann erstmal von seiner Arbeit auf dem Urlaubsschiff der Aida Diva erzÃ¤hlen - etwas derb, aber gut gemacht und mit viel Witz und Spass auf die Kosten der Heterosexuellen. Zumindest manchmal Ich kannte ihn vor diesem Auftritt nicht, aber seine 20 Minuten hat er gut genutzt um sich vorzustellen; ich denke wenn er wieder hier in der Gegend sein sollte ist das ein guter Tip.

Martina Schwarzmann kenne ich wiederum von einigen Auftritten die im Fernsehen Ã¼bertragen wurden - Pantheon, Live aus dem Schlachthof und anderes. Sie redet "echtes", teilweise schwer zu verstehendes Bayrisch (also schwer zu erstehen fÃ¼r Hamburger wÃ¼rde ich sagen wobei sie von Gelegenheiten erzÃ¤hlt die sich ihr im Laufe ihres Leben ergaben und ergeben. Dazu singt sie dann zwei Lieder die teilweise einen bitterbÃ¶sen Text haben - einfach schÃ¶n um ein wenig zu stÃ¤nkern Sie macht das aber auf eine nette Art, dass sich niemand beleidigt fÃ¼hlt. Es macht auf jeden Fall Spass ihr zuzuhÃ¶ren.

Nach einer kurzen Einlage der MÃ¼tter geht es in die Pause und danach kommt der "Quoten-AuslÃ¤nder" (nachdem Martina Schwarzmann wohl nicht galt) - BÃ¼lent Ceylan. In Wirklichkeit ist er allerdings in Mannheim geboren und redet auch problemlos in dem Dialekt wenn er will. Er wechselt wÃ¤hrend seines Auftrittes durchaus die Rollen (und damit auch die Provokationen) und hat manchmal das Problem sein Programm jugendfrei zu halten (in der ersten Reihe sassen 12jÃ¤hrige)... aber das hat nicht weiter gestÃ¶rt. Zumindest war er sehr unterhaltsam und witzig und hat die Zuschauer immer wieder neu Ã¼berrascht; ich glaube ein Besuch seines Programms wird sich lohnen.

Bodo Wartke ist quasi der bekannteste Kabarettist des Abends und damit auch der HÃ¶hepunkt. Er ist zwar genauso wie die anderen KÃ¼nstler "nur" 20 Minuten auf der BÃ¼hne, aber er fÃ¤ngt die Leute sofort ein und eigentlich wollen sie ihm alle lÃ¤nger zuhÃ¶ren. Seine Lieder sind aus seiner aktuellen Show (und natÃ¼rlich auf den CDs drauf aber live sind sie halt doch ein klein bisschen schÃ¶ner; und wenn man nur die Hoffnung hat dass er sich einmal ein klein wenig verspielt. Das Liebeslied wurde ein wenig gekÃ¼rzt, dafÃ¼r gab es (fÃ¼r mich) neue Sprachen wie Chinesisch, TÃ¼rkisch und Kreuzbergerisch dabei.

Durchaus ein spannender und angenehmer Abend; ich glaube ich werde mir mindestens einmal die MÃ¼tter mit einem ihrer Programme und dann auch ihren Ãœberraschungsabend geben; mal sehen ob diese genau so interessant werden.

Posted by rince in Kleinkunst at 09:52

Canossa X - es jÃ¤hrt sich zum zehnten Male

Zum Zehnten Mal trafen sich die deutschen Internet-Administratoren zum gemeinsamen Grillen und Chili-Kochen. Diesmal wieder auf "der Burg" und es hat richtig viel Spass gemacht - auch wenn ich Samstags tagsÃ¼ber wegwar; Freitagabend mit Vollmond (und guten GesprÃ¤chen) und Samstag abend mit fast-Vollmond, aber einigem Regen (und trotzdem Grillfleisch) war einfach witzig und hat viel Spass gemacht.
Es ist einfach immer wieder schÃ¶n die Kollegen oder Freunde wiederzutreffen - dieses Treffen ist dafÃ¼r einfach ideal. Einfach mal wieder quatschen, auf den Turm steigen, dem Feuer beim Runterbrennen zusehen und sinnige oder unsinnige GesprÃ¤che fÃ¼hren.

DafÃ¼r vielen Dank an die Organisatoren und die Leute die extra dafÃ¼r angereist sind!

Posted by rince in CCCS at 09:43

Wednesday, July 23. 2008

Eine kleine FAQ zum Thema biometrischer Ausweis

Da gerade beim CCC eine entsprechende Anfrage reinkam dachte ich mir ich kann diese Frage ja auch zumindst zum Teil beantworten.

Die Fragen sind:

Brauche ich einen Personalausweis?
Brauche ich einen Reisepass?
Wo werden die biometrischen Daten gespeichert? Nur auf dem Pass oder auch zentral?
Kann ich mich irgendwie dagegen wehren?
Kann ich diesen Chip zerstÃ¶ren, wie steht es dann mit der GÃ¼ltigkeit des Dokuments?

Alle diese Fragen sind "relativ" einfach zu klÃ¤ren.

Jeder BundesbÃ¼rger ist gesetzlich verpflichtet ein amtliches Lichtbild-Dokument zu besitzen - dabei ist es unerheblich ob er dabei einen Ausweis benutzt der ihn als Personal der Bundesrepublik Deutschland ausweist oder einen ReisepaÃŸ. Einen ReisepaÃŸ braucht man wenn man ins nicht-europÃ¤ische Ausland fahren mÃ¶chte; dort werden dann zum Beispiel Visa-Stempel eingetragen. Man braucht aber nur eines von beiden Dokumenten, nicht beide. Beide Dokumente haben ein "Verfallsdatum", das heisst sie sind nur eine bestimmte Zeit gÃ¼ltig.

Die biometrischen Daten werden bis jetzt(!) nicht zentral gespeichert. Es gibt zwar entsprechende Bestrebungen und unser Innenminister ist der Meinung dass es gebraucht wird, aber bisher gibt es diese Speicherung zentral nicht.

Gegen die Speicherung der biometrischen Daten in den Ausweisen kann man sich erst einmal nicht wehren. Es gibt aber bereits entsprechende Verfahren vor Gericht (siehe: Wikipedia-Eintrag).

Den Chip kann man "relativ" einfach zerstÃ¶ren: Es ist ein RFID-Chip, der auf bestimmten Frequenzen arbeitet. Auf derselben Frequenz arbeiten zum Beispiel Schweisstrafos. Wenn diese zuviel Streustrahlung abgeben kann es natÃ¼rlich passieren dass der RFID-Chip durchbrennt.

Die Soll-Bruchstelle ist allerdings eher der Kontakt zwischen Antenne und dem Chip selbst. Wenn dieser Kontakt durchgebrochen wird (zB tragen des Ausweises in der Hosentasche) kann der Chip noch so gut funktionieren; er kann mangels Antenne nicht abgefragt werden...

Posted by rince in CCCS at 13:53

Tuesday, July 22. 2008

Perl zum Merken

Wir schreiben jetzt hundertmal "while () {} ist ungeschickt wenn innerhalb der Schleife wieder benutzt wird"

Das hÃ¤tte mir zwei Stunden eher auffallen sollen.

Posted by rince in CCCS at 14:00

Wednesday, July 16. 2008

Die Krankenkassen und die elektronische Gesundheitskarte

Recht dreist finde ich was die IKK Sachsen (von ihr weiss ich es bisher nur) mit ihren Kunden macht:

Zum Start der elektronischen Gesundheitskarte wollen sie von jedem Kunden ein Foto haben - an sich mag das ja nicht so schlimm sein. Allerdings begrÃ¼nden sie dies mit "gesetzlichen Vorgaben", wonach man verpflichtet sei ein Foto abzugeben.

Im Sozialgesetzbuch V, Â§291 Absatz 2 steht:

Versicherte bis zur Vollendung des 15. Lebensjahres sowie Versicherte, deren Mitwirkung bei der Erstellung des Lichtbildes nicht mÃ¶glich ist, erhalten eine Krankenversichertenkarte ohne Lichtbild..

Das heisst es ist durchaus mÃ¶glich auch ohne Foto eine solche Karte zu bekommen.

Was aber noch spannender ist, sind die AbhÃ¤ngigkeiten die die IKK dort einfÃ¼hrt:

- Das Foto muss biometrisch nutzbar sein - also wie das PaÃŸfoto, welches auch bestimmte Kriterien erfÃ¼llen muss. Im Gesetz steht davon nichts; dort steht nur "Lichtbild".

- Das Foto wird fÃ¼r 5 Jahre bei der IKK (oder deren Dienstleister) gespeichert. Davon steht wiederum gar nichts im Gesetz drin - dies ist nicht notwendig und ich persÃ¶nlich sehe dazu auch keine Veranlassung; aber vielleicht bin ich in der Hinsicht eher paranoid.

Wie sieht das bei anderen Krankenkassen aus? Gibt es dort Ã¤hnliche Briefe und Bestrebungen? Weiss das jemand?

Update:Der CCC hat eine PresseerklÃ¤rung dazu rausgebracht.

Posted by rince in CCCS at 17:16

Monday, July 14. 2008

Zum Thema MedienwÃ¤chter und Umgang mit den neuen Kommunikationsformen...

...habe ich diesen Artikel von Indiskretion Ehrensache gelesen - ich finde ihn gut geschrieben. Insbesondere weil beide "Welten" gezeigt werden.

Posted by rince in CCCS at 14:17

Friday, July 11. 2008

MedienwÃ¤chter und das Internet

Gestern erschein bei Heise ein Nachrichtenartikel der mir fast die Haare zu Berge stehen liess. Dort steht unter anderem:

Norbert Schneider [, Direktor der Landesanstalt fÃ¼r Medien NRW] meint, das Internet habe traditionelle, vor allem am Rundfunk ausgerichtete Modelle der Medienregulierung Ã¼ber den Haufen geworfen. Aus dem Privileg, Rundfunk zu gestalten, werde "ein bezahlbares Jedermann-Prinzip". Dies sei fÃ¼r Regulierer ein Albtraum, da "der Wert der Lizenz absackt".

Er hat das durchaus richtig verstanden: Das Internet hat den Vorteil dass nunmal jeder publizieren kann. Es ist niemand gezwungen die Sachen zu lesen, aber er kann - wenn er will. Das heisst, Rundfunk ist kein Privileg mehr (also Rundfunk im Sinne von "Ich erreiche viele Leute"), sondern eine realistische Sache. Es gewinnt nicht unbedingt der der die stÃ¤rksten MÃ¶glichkeiten hat, sondern eventuell der Kreativere. Was ich durchaus gut finde, sonst gibt es schnell Kartelle oder Monopolsysteme.
Warum daran allerdings die Lizenz absackt kann ich nciht oder nur sehr schwer nachvollziehen. Es gibt doch gerade fÃ¼r das Internet neue Lizenzmodelle (fÃ¼r Software GPL+BSD-Style; fÃ¼r alle Arten von Medien die Common Creative License). Dort kann man ja genau definieren unter welchen Voraussetzungen man eine Verbreitung des Werkes erlaubt (oder auch nicht).
Weiterhin schreibt er:

Die zunehmende Medienherrschaft der Finanzinvestoren, die auf Profite und nicht auf kulturelle Vielfalt setzten, schÃ¼re die Sorge, dass mediale Angebote mit einem Ã¶ffentlichen Mehrwert "unter Artenschutz gestellt werden mÃ¼ssen und Regulierung damit zu einer Art Denkmalschutz wird".

Der Herr zieht zwar teilweise die richtigen SchlÃ¼sse, kommt aber dann zu den meiner Meinung nach falschen Ergebnissen. Es ist gerade gut dass nicht die Finanzinvestoren die Oberhand haben sondern dass die kulturelle Vielfalt (in Form von Webseiten, Blogs und Ã¤hnlichem) die MÃ¶glichkeit hat sich zu artikulieren. Warum das jetzt eine Art Denkmalschutz benÃ¶tige verstehe ich nicht so wirklich.
Und wenn ich mal sarkastisch sein darf:

"Es braucht im Internet auf Dauer ein vollziehbares Verbot von Pornographie, von Kinderpornographie sowieso."

Es tut mir leid, Herr Schneider, auch wenn sie das nicht wahrhaben wollen: Das Internet beziehungsweise die kommerzialisierung ist durchaus durch den Teil Pornographie (Vermarktung, Benutzung) groÃŸ und/oder bekannt geworden. Versuchen Sie bitte nicht, es einfach "wegzusperrren"; das klappt sowieso nicht. Viel lieber sorgen sie durch entsprechende Erziehung dafÃ¼r dass auch Kinder den Umgang damit lernen. Bei Kinderpornographie sind wir einer Meinung, allerdings denke ich dass es viel sinniger ist die Produktion dieser Sachen zu verhindern als "nur" sich auf die Verbreitung zu konzentrieren.

Posted by rince at 16:36

Tuesday, July 8. 2008

Museum fÃ¼r Technik und Arbeit Mannheim: Macht Musik!

Am Wochenende war ich in Mannheim; im Museum fÃ¼r Technik und Arbeit. Sie haben nicht nur eine schÃ¶ne Dauerausstellung (sehr geeignet fÃ¼r Kinder; viel zum Anfassen und Testen). Die Sonderausstellung "Macht Musik" zeigt ein wenig Ã¼ber Musik, wie sie entsteht, was man davon wirklich mitbekommt (Ã¼ber HÃ¶ren, FÃ¼hlen, Verstehen) und wie sie eingesetzt wird - zur Heilung von Kranken zum Beispiel. Man kann vieles selbst ausprobieren - es gibt einen schallisolierten Proberaum fÃ¼r Rockmusik, aber auch klassische Instrumente wie Geigen, Bratschen oder Kontrabass. Zusammen mit den anderen AusstellungsstÃ¼cken ist das eine durchaus interessante MÃ¶glichkeit etwas Ã¼ber Musik zu lernen - ich kann es nur empfehlen.

Posted by rince in Kleinkunst at 18:17

.Mac oder wie die neue Welt bei Apple heisst

Mit dem neuen iPhone sollen ja die GerÃ¤te von Apple zusammenwachsen - dafÃ¼r gibt es .Mac beziehungsweise das neue System von dem ich gerade nicht weiss wie es heisst. Offensichtlich scheint aber Apple nicht zu wissen was dort alles gespeichert wird, oder die Leute im Servicecenter wurde nicht gut geschult: Ein wenig Social Engineering reicht aus um an die persÃ¶nlichen Daten anderer Leute heranzukommen. Dazu gehÃ¶ren auch SSH-Keys, Fotos, Mails usw...

Und das alles in der Hand eines Herstellers?

Posted by rince in CCCS at 18:05

Wednesday, July 2. 2008

BÃ¼rgerbÃ¼ros und der Datenschutz

Gestern bekam ich eine lange Mail als (erweiterte) Reaktion auf meine Anfrage wegen der Meldedaten in den EinwohnermeldeÃ¤mtern - da gab es ja ein paar Probleme mit der Datensicherheit.

Ich war positiv Ã¼berrascht - die Beauftragte fÃ¼r den Datenschutz erklÃ¤rte mir erst einmal welche Daten genau von den BehÃ¶rden Ã¼ber mich gespeichert werden (sofern notwendig), in welchen Gesetzen das steht und - sehr schÃ¶n - schickte mir ein PDF-Formular mit welches ich nutzen kann um meine Daten bei den BehÃ¶rden anzufragen. Inklusive einer Liste von BehÃ¶rden wo die Anfrage gemacht werden soll. Das ganze, damit auch die Anfrage zeitnah bearbeitet werden kann und nicht unnÃ¶tig Arbeit gmacht werden muss.

Das ist eine tolle Reaktion (auch das Formular war Ã¼brigens personalisiert, also Vorname und Name stehen schon drauf) und ich bin durchaus froh dass die Mitarbeiter dort offensichtlich wissen wovon sie reden. Jetzt bin ich mal gespannt was auf mein Auskunftsersuchen passiert

Posted by rince in CCCS at 16:47