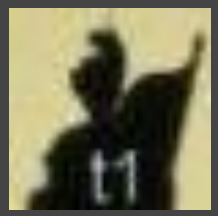
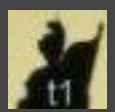
Bezpečnost dnes v 7 hodin ráno tentokrát v roce 2011

bodik & čuba++





Vítejte po 0x04-thé

And now something globally different

Keynotes:

DigiNotar, Comodo hack - PKI v kopru
RSA hack a jak na to přišli...
Mobilní telefony ukazují kde jste ...iPhone + Android
BEAST SSL Attack explained

... ale nejdřív uspíme techniky

Upozornění na mrvý úhel

Parkovací kamera
Upozornění na hrozící srážku
Automatická brzda
Řidičský alerting
Detekce chodců
Adaptivní tempomat
ABS ESP
12 Airbagů

Pilíře bezpečnosti

Znamená to, že se ve Volvu nezabiju?

Pilíře bezpečnosti

Pilíře bezpečnosti

No není to Volvo, ale zase Ford.

Technické prostředky pomáhají...

... ale průšvihy dělají lidi
nehledě na technické možnosti
(Lady Gaga CD + WikiLeaks
)

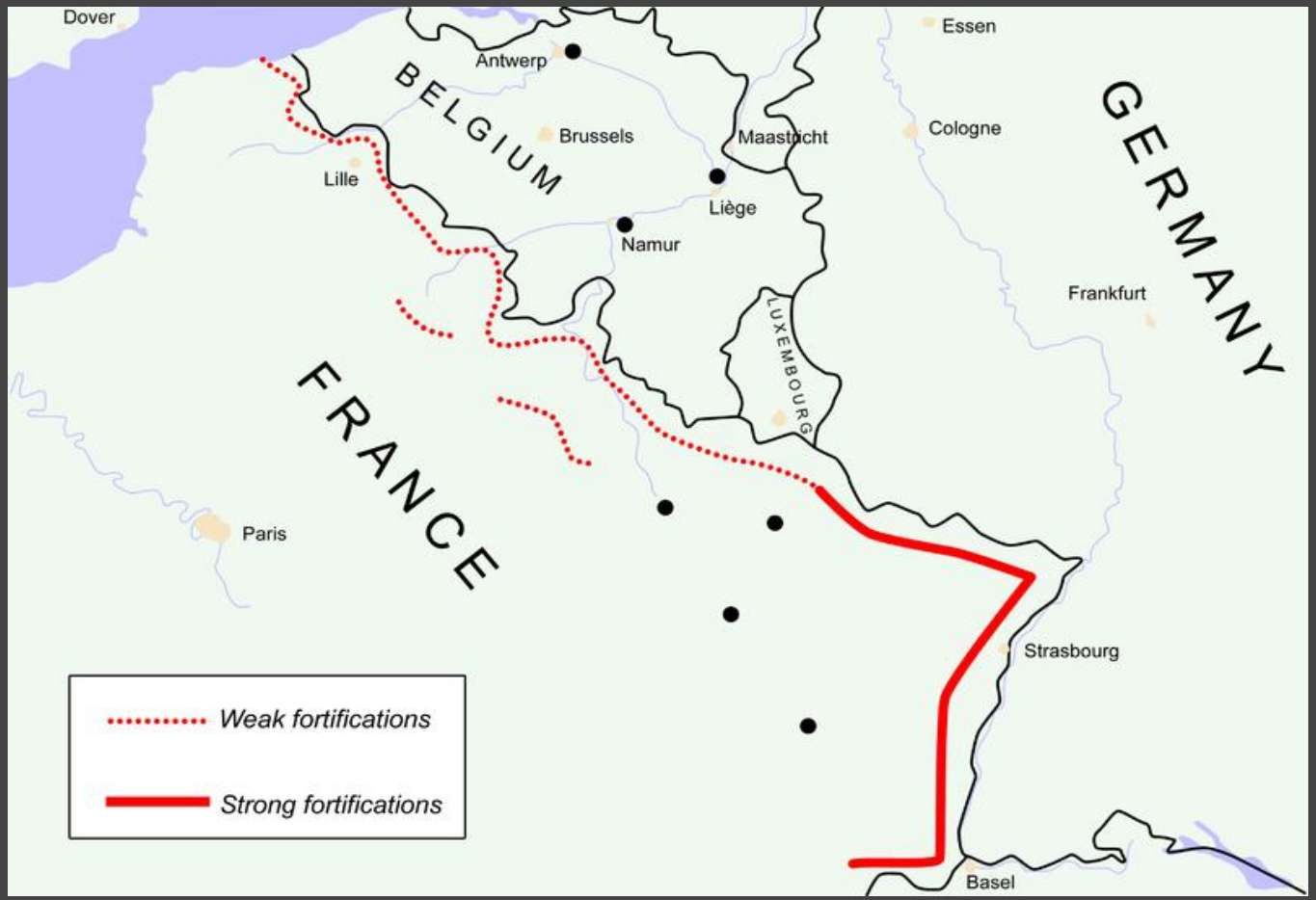
Pilíře bezpečnosti

Pilíř I: bezpečnostní systémy nefungují na útoky mimo kontext

Útoků "mimo kontext" je víc
Při projektování systémů je potřeba věnovat širokému pohledu na věc. Je potřeba odpovídat na mnoho otázek
"Co když...? "
Př.
Xterm (LPS admini, Xterm, ssh. krb. su. vše jak má být, ale X11 se dalo odposlechnout, hehe)

Pilíř I: bezpečnostní systémy nefungují na útoky mimo kontext

proč se .... s firewallem, když mají otevřený zadní vchod...



Pilíř II: očekávej průšvih, upleť bezpečnostní síť a adaptuj se.

Ukaž lidem, jako hodnotu mají informace, jak snadno mohou utéct a jak mohou pomoc při obraně dat.

Společnost XY ... 2 roční rozpočty na bezpečnostní školení, které funguje. Teď má společnost 2000 zaměstnanců - 2000 bezpečnostních senzorů.

…there are three kinds of companies:
one that has been broken into, one that is going to be, and one that
is going to be again.

Pilíř II: očekávej průšvih, upleť bezpečnostní síť a adaptuj se.

Ukaž lidem, jako hodnotu mají informace a vysvětluj!

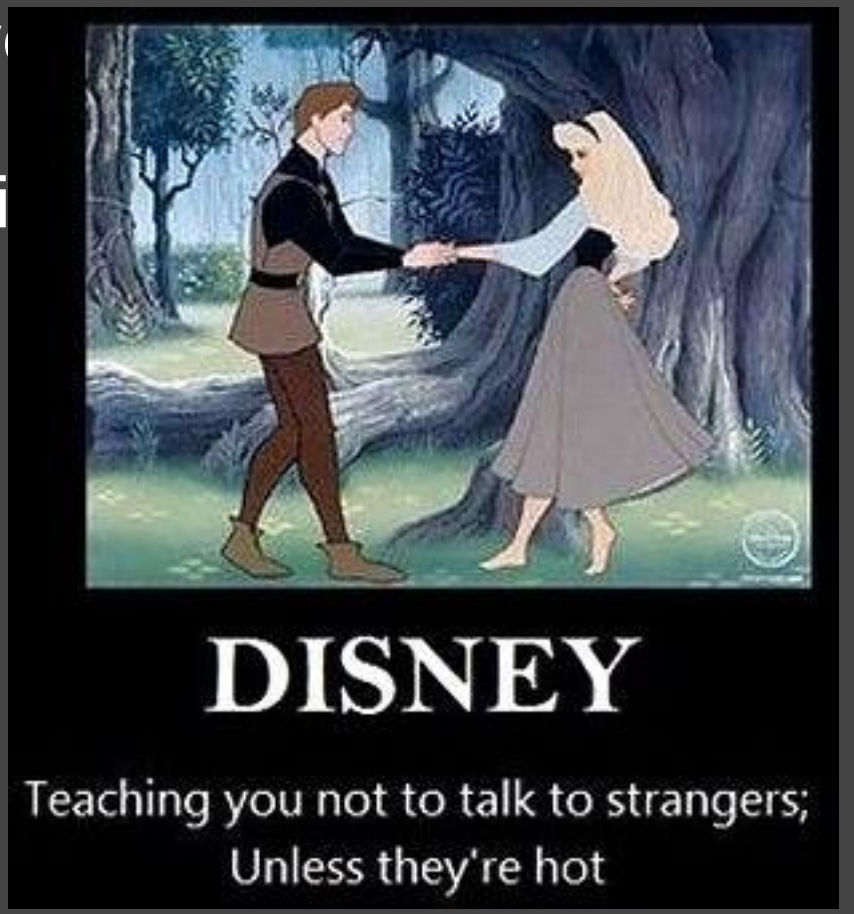
Richard Feynman: Oak Ridge Facility problem:

Přijel jsem do Oak Ridge a nejdřív jsem se dal provést závodem. Nic jsem neříkal, jen jsem si všechno prohlížel. Zjistil jsem, že situace je dokonce horší, než Segré hlásil. Všiml si spousty krabic v jedné místností, ale ušlo mu, že za zdí, v druhé místnosti, jsou další - a takových věcí bylo víc. A když máte příliš mnoho štěpného materiálu pohromadě, tak to bouchne, chápete?

Pilíř III: očekávej, že lidi udělají chybu a připrav se na to.

"Expect that people will make bad trust choices"

Sociální sítě mohou obsahovat odpov
na kontrolní otázky, které používáte
jinde na webu... nebo dokonce v práci



Pilíř IV: předpokládej, že tvoje prostředí je již napadené. To je, co?

He also said it’s easier than ever to fool a well-intentioned insider into doing bad things. It’s becoming harder and harder to differentiate boring work email from boring phishing email, because they look very similar.

Stuxnet at its best!

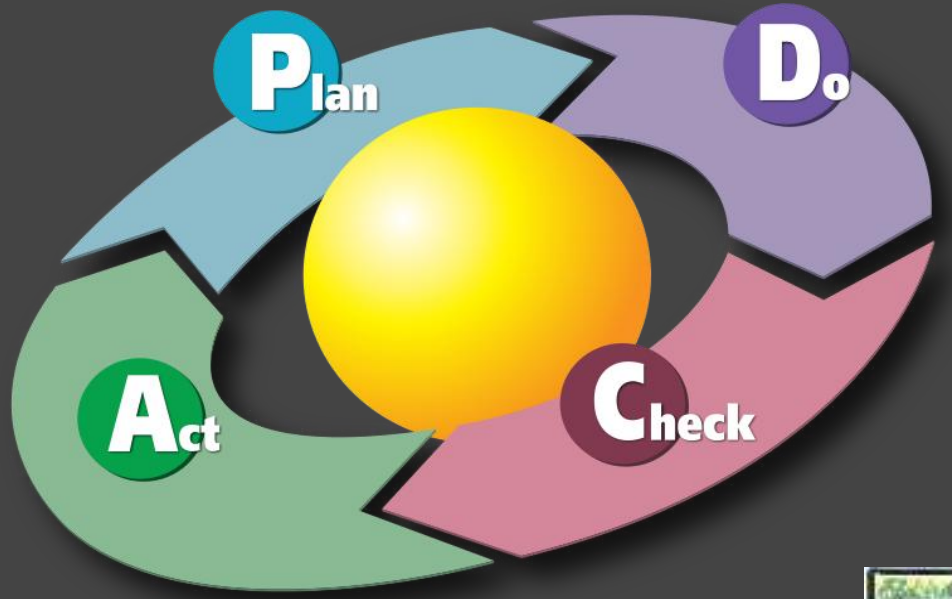
Prosím vyplňte tento dotazník TPoS pro HR oddělení...

Z důvodu zlepšování fídbeku pro ejčár a kontinuálního impůvmentu ajtý servises prosím vyplňte tento kvesčnér a to do konce seknd QÁ

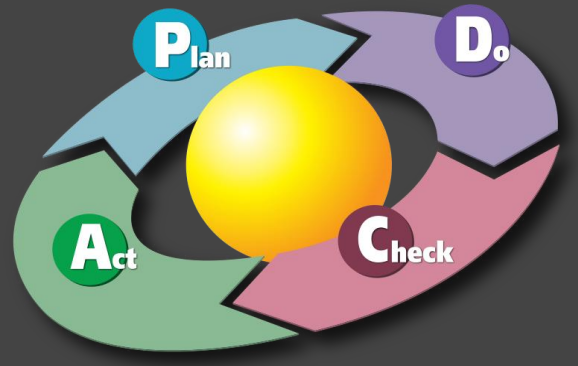
Pilíř V: Pořád přehodnocuj předpoklady

"Reasonable targeting" on the part of attackers no longer applies, said Thompson. It's no longer safe to assume that those with access to the most valuable data within an organization are the most vulnerable targets. "**The pillars of trust, the things that we rely on, are starting to erode**", he added.

RSA attack probereme posléze,
ale kdo usne, tak to neuslyší



... osel ....

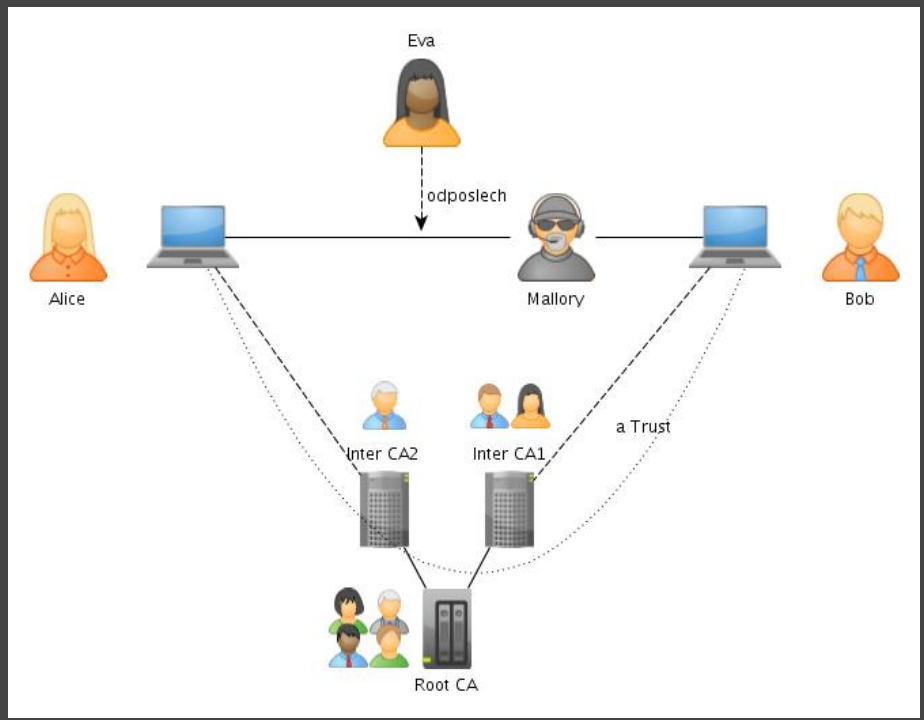


- ... no tak to bychom měli trochu manažerských keců ...
- zkusme je tedy aplikovat do praxe ...
  - aha, takže jak to tak vidím, tak leto jsme na poli bezpečné komunikace na internetu ve fázi PLAN ..
    - po 20ti letech jsme opět v PLANkách ...

PKI, World CA ... final review

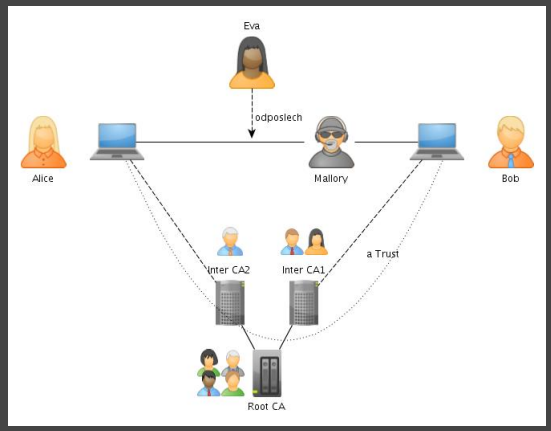
- bezpečná komunikace přes internet
  - šifrovací algoritmy
  - šifrování je super, ale je potřeba vědet s kým (key mgmt) a proto máme PKI
  - sestavení bezpečného kanálu mají nastarosti protokoly -- SSL/TLS

motto:
"Víš s kým spíš? "



PKI, World CA ... final review

- na tento systém se dá útočit na všech úrovních a také se tak děje (stará písnička)
  - útoky na uživatele
    - SSL Strip (fišink :)
  - útoky na implementaci
    - IE5 basic constraint, x509 null byte DN
  - útoky na protokol nebo crypto algo
    - TLS renego, BEAST (2k11)
  - útoky na infrastrukturu
    - Domain validation, CA penetration (2k11)



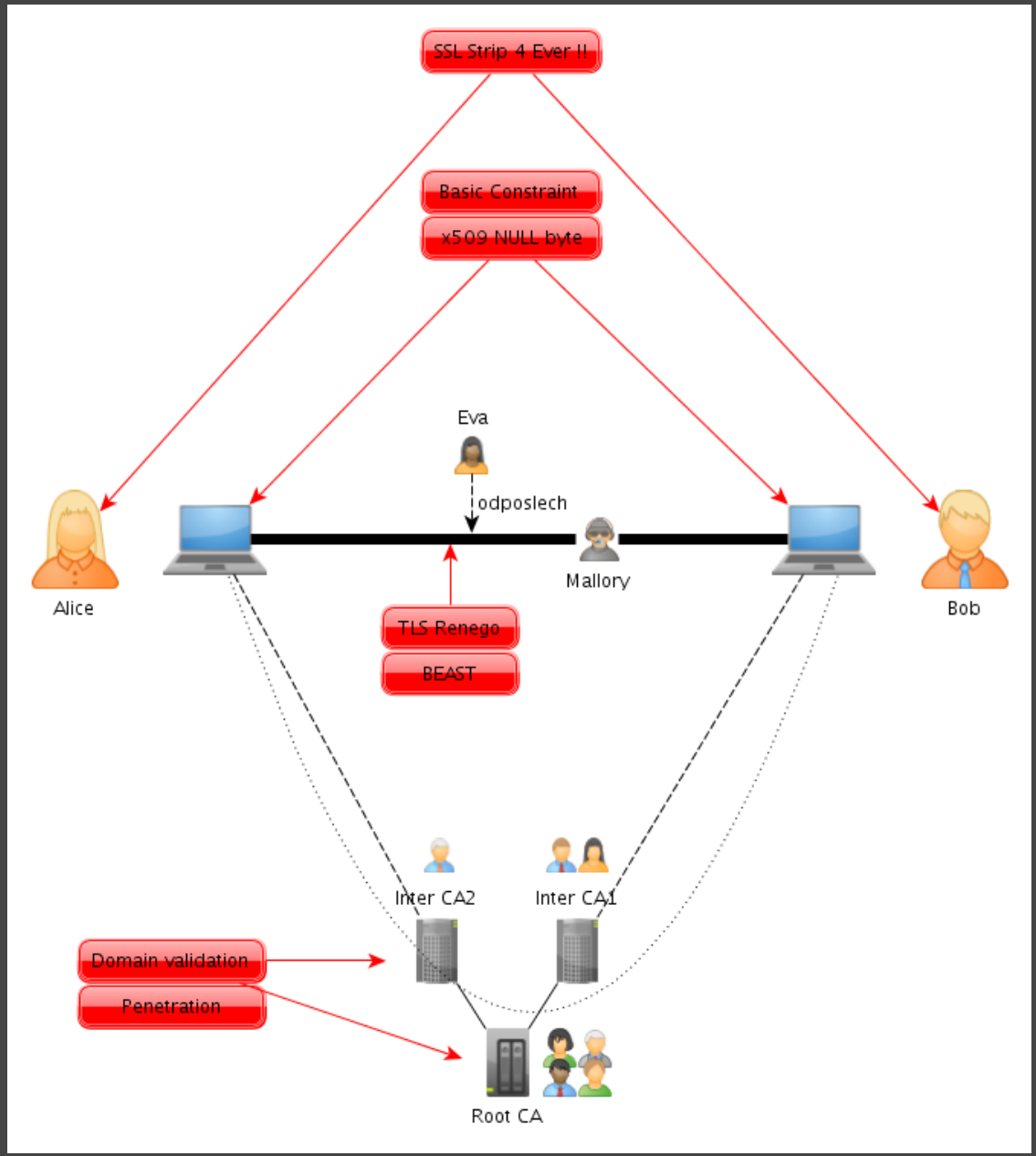
BEAST (2k11)

- kráska a beast
- 7:@)
- *špatná implementace CBC šifrování*
  - *co je to CBC, k čemu je IV*
  - *první IV by měl být velmi náhodný, bohužel ...*

- Předpoklady: MITM, JS, znalost následujícího webu, čas
- Převezmeme klientův prohlížeč ... třeba BEEFem (2010)
- BEEF otevře spojení na https://www.paypal.com (a drží ho)
- Klient mrkne na paypal, ale my vidíme do spojení...
- "chosen-plaintext-recovery" útok => dostaneme IV
- odhalení/dešifrování autentizačních cookies
- cookie replay attack a jsme tam, hurá!
- Chápete to?

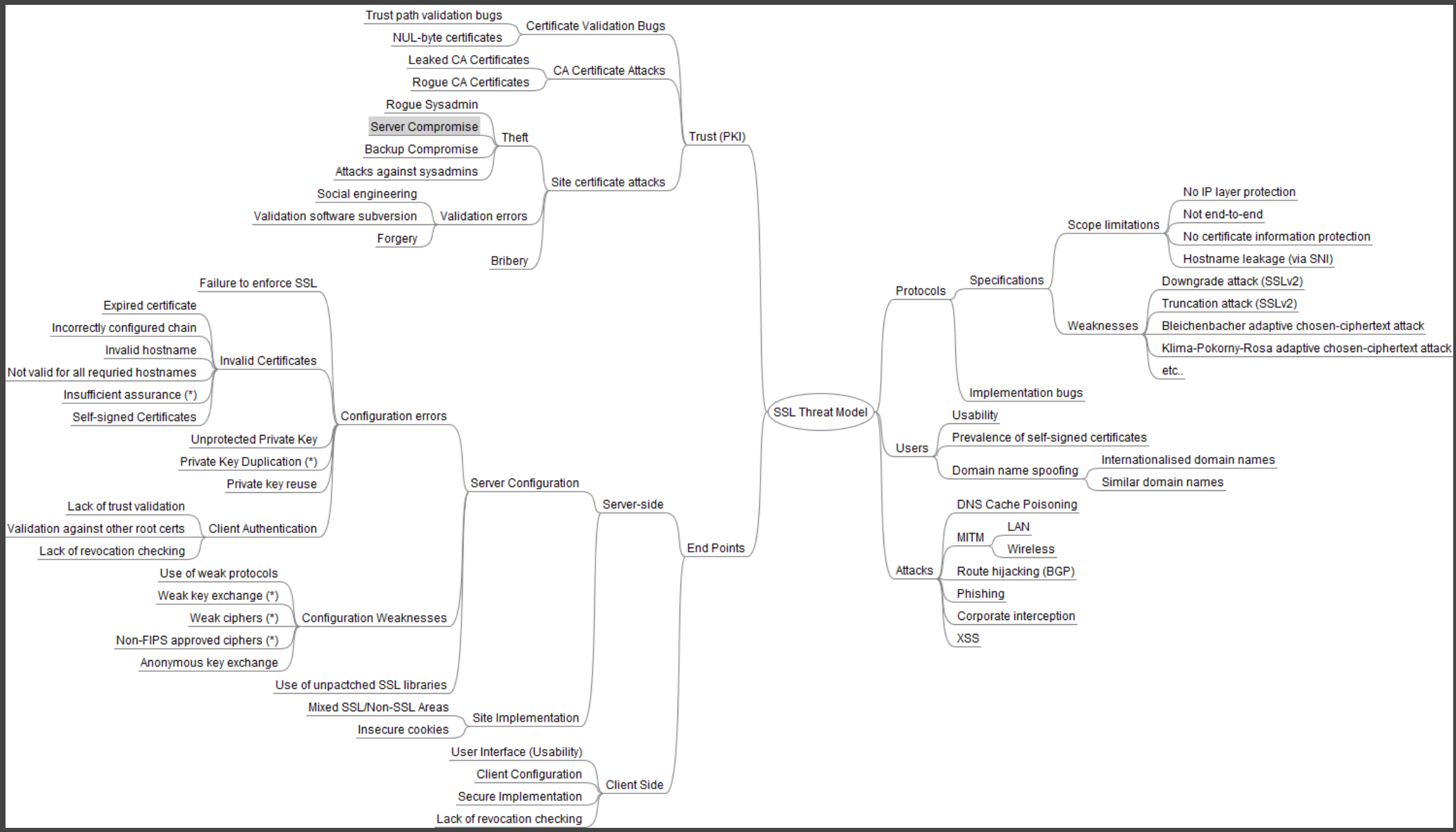
PKI, World CA ... final review

- na tento systém se dá útočit na všech úrovních a také se tak děje (stará písnička)
  - 2011
    - beast
    - ca penetration



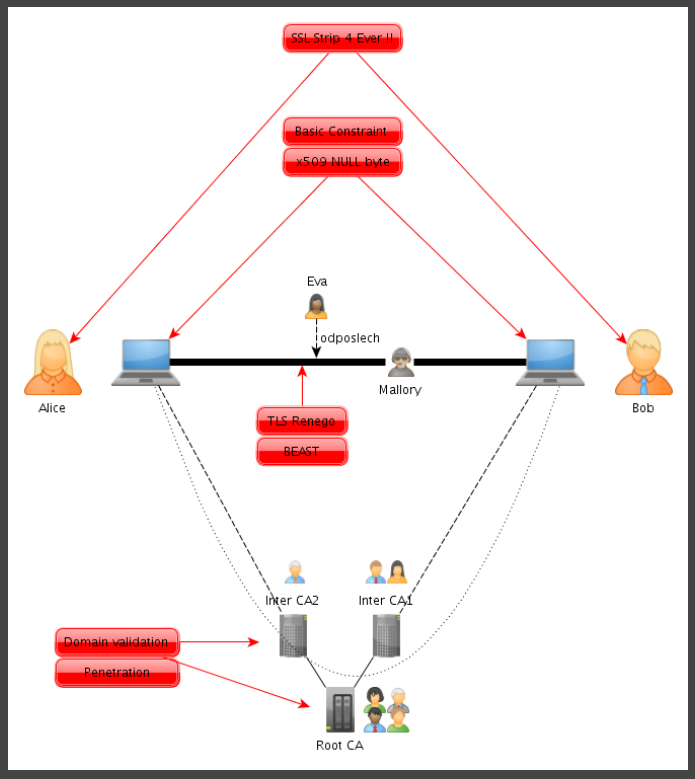
PKI, World CA ... final review

- .. ve skutečnosti je o něco složitější ...
- Ivan Ristić: SSL Threat model



PKI, World CA impl .. final review

- jsou zde 2 extrémy, útoky na "konce"
  - sslstrip (aka fišink) na uživatele bude fungovat vždy
  - penetrace CA bude fungovat vždy, letos přitekla poslední kapka ...

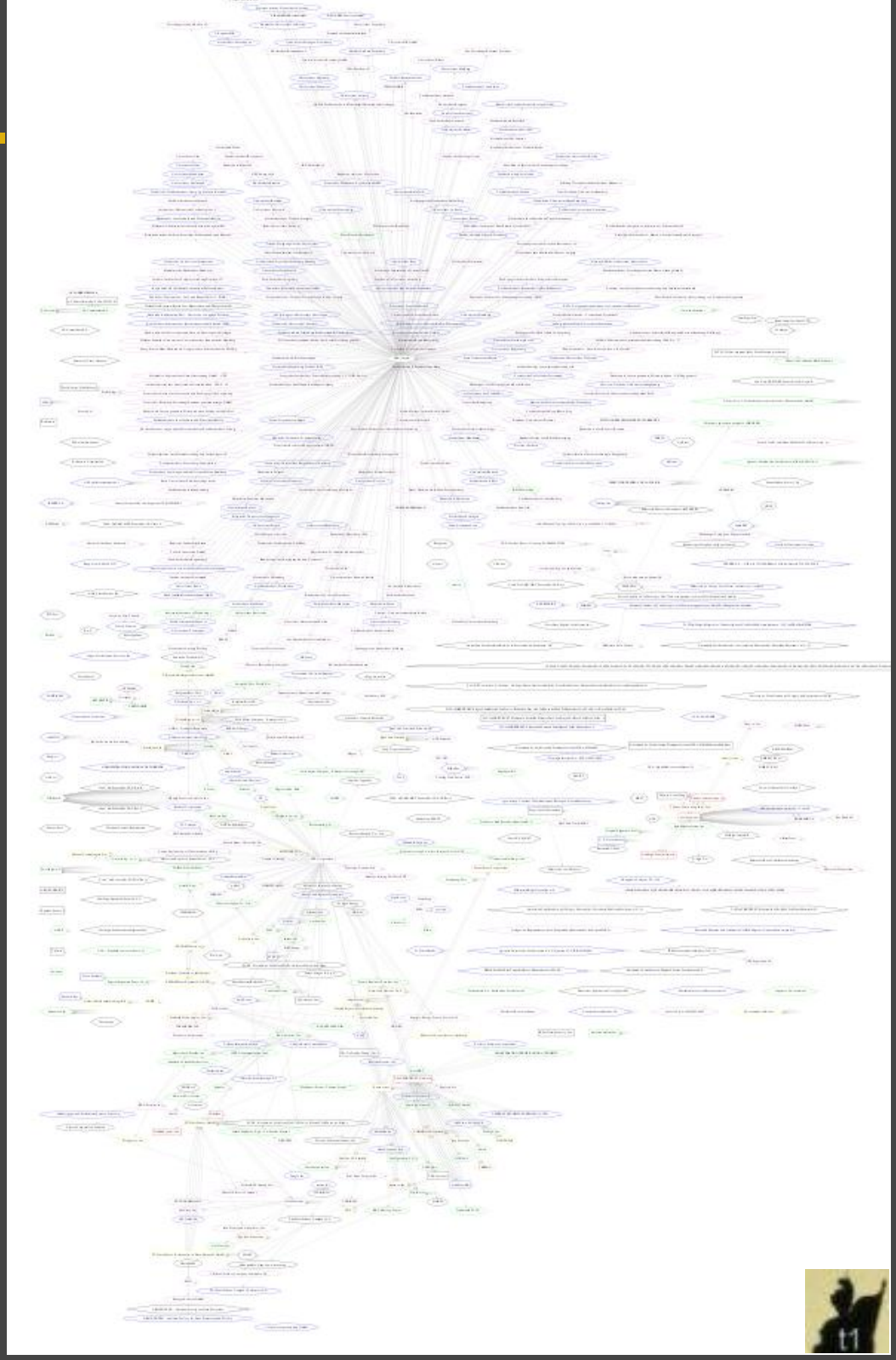


PKI, World CA impl .. final review

- Comodo (23.3.2011 †)
  - 2há největší CA
  - dceřiné autority podepsaly: mail.google.com, login.skype.com, www.google.com, ...
- DigiNotar (30.8.2011 †)
  - malá CA v Holandsku
  - podepsala: *.google.com,*.thawte.com,www.update.microsoft.com
- ... ???
- ... a takových CA je fakt hodně a všechny jsou si rovny
  - ... i přesto že jsou v hierarchii :)

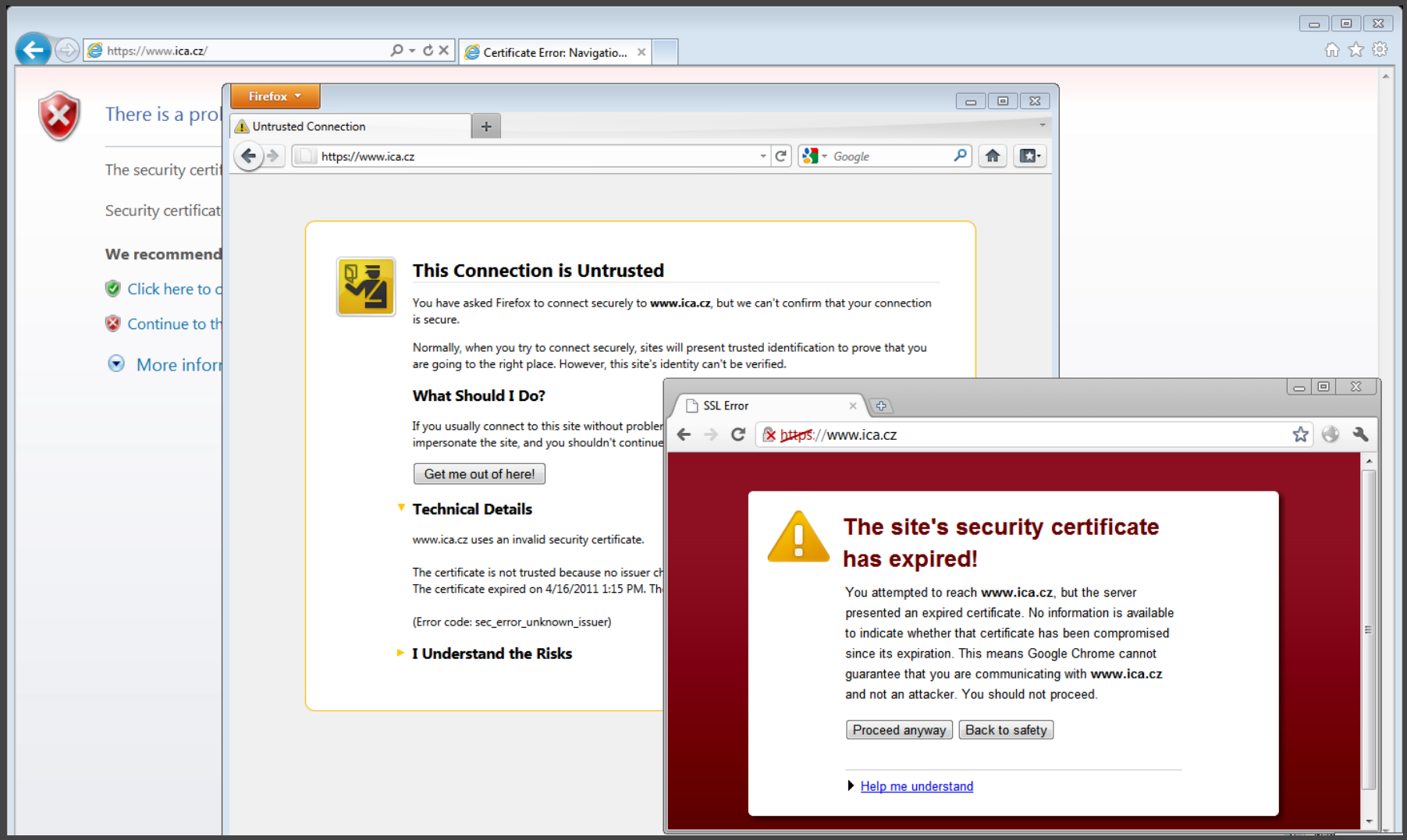
PKI, World CA impl ..

- Browser based PKI
  - cca 650 firem
  - všechny mohou vydat certifikát pro kohokoliv
- Ok ... PKI jako systém není špatný návrh
- v praxi však kompromis zabezpečení vs. použitelnost zašel příliš daleko ...



PKI, World CA impl .. final review

* ... a jak vypadají státem pověřené organizace které se mají starat o PKI nebo DNSSEC ...
ica.cz a jeji SSL certifikat vyprsel 16.4. … jeste 20.4. tam ale byl … 21.4. je to opraveno, Cert ma datum vydani 19.4.2011 … ;-)



PKI, World CA impl .. final review

- co s tím ?

PKI, World CA impl .. final review

- co s tím ? -- browser based trust
  - úložiště certifikátů řízené uživatelem
    - ručně ořezat strom PKI
      - ... těžko si představit uživatele který se vyzná v 650ti zaškrtávátkách
  - izolované ostrovy důvěry
    - všechny certifikáty si uživatel musí explicitně naimportovat
      - kde je vezme ? jak je ověří ? dopadne to stejně klikánií ...
      - nicméně takle je to správně, uvidíme posléze u notářů ;)
  - úložiště certifikátů řízené *doménou-organizací-firmou*
    - v korporacích řídit trust politikou a centrálním nastavením
      - těžko si to představit pro domácí uživatele (viz ^^^)

PKI, World CA impl .. final review

- co s tím ? -- dns based trust
  - DNSSEC
    - distribuovat informace o věrohodných certifikátech pomocí DNS
    - pouze "vaše doména" může vydat certifikáty pro vaše servery
    - i přes následující řádky vězme, že to je možná cesta !!!
  - což znamená ...
    - při koexistenci PKI a DNSSEC/DANE se útočný povrch ještě zvětší (systémy CA + interní systémy organizace)
      - ale nejen koncové sítě, ale také registrátoři budou v řetězci důvěry
      - registrátor ? (.cz|.cn|.usa ...) to je vládou pověřená organizace >> LOL
      - v každém případě měníme jedny za druhé, systém je pouze více rozmělněn
    - výrobci browserů budou muset dále implementovat varování o nesouladu informací mezi DNSSEC a PKI ...
      - ... uživatel tomu stejně nerozumí už teď ...

PKI, World CA .. final review

- co s tím ? --
  - Dan Bernstein
    - DNSSEC jako další systém zanáší systémové chyby (implementační, architektonické)
    - pouze doručuje adresy, ale zabezpečit stejně chceme stránky (skutečná data)
      - pokud ochráním stránky podpisem (PGP), co pro mě dělá DNSSEC ? ...
    - CurveCP + DNSCurve
      - navrhuje šifrovat každý paket zvlášť
      - upřímně řečeno není mi jasné jak je zabezpečena distribuce klíčů ?

PKI, World CA impl .. final review

- nějaký další nápad ?

CA Transparency and Auditability

Ben Laurie <benl@google.com>
Adam Langley agl@google.com

1. Každý veřejný cert bude publikován do veřejného audit logu certifikátů.

2. Každý cert v tomto logu má u sebe auditní důkaz (hash tree) - seznam hashů odshora až dolů viz Merkle signat.

3. Server pošle tyto "důkazy" společně s certifikáty a browser je MUSÍ ověřit

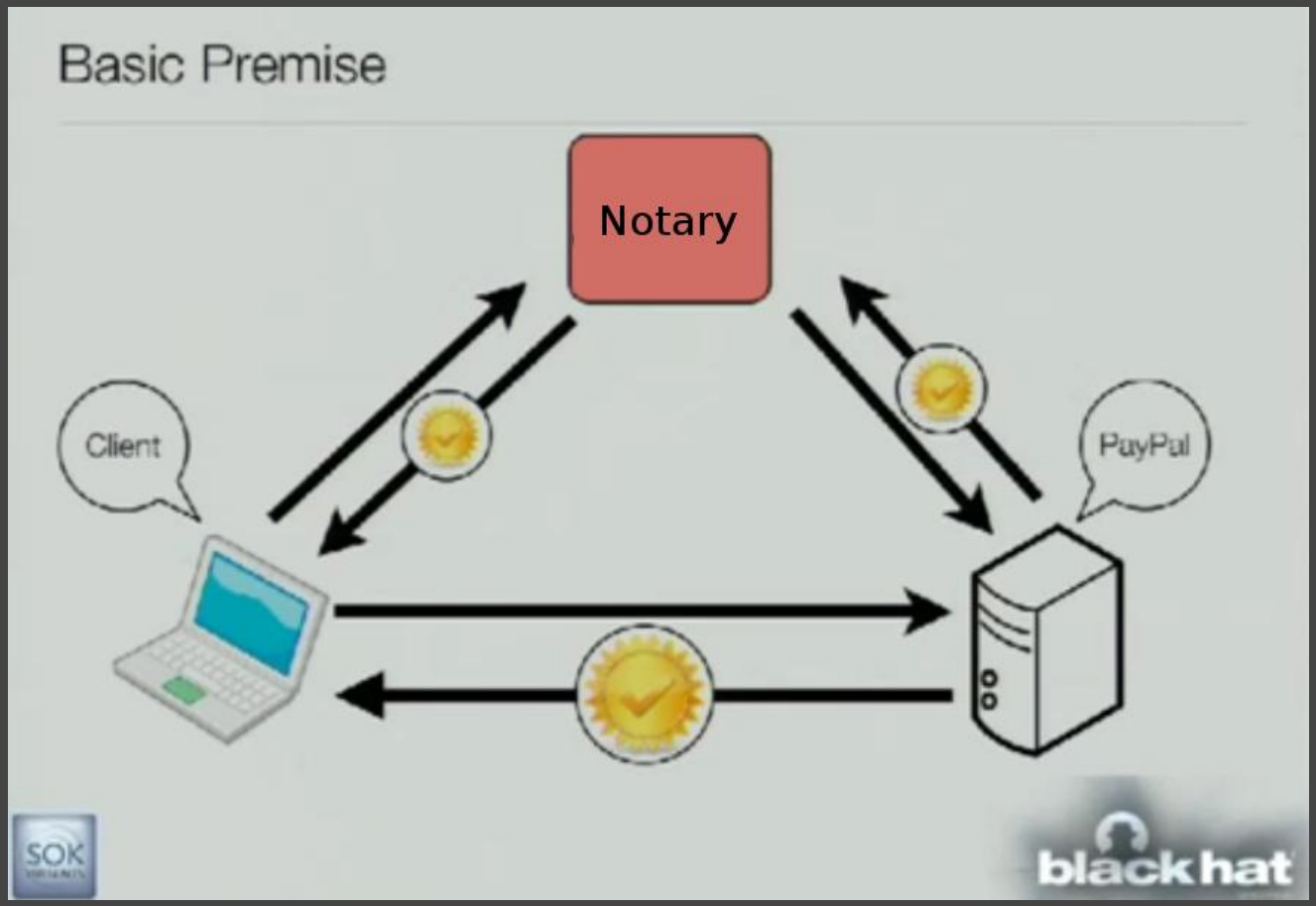
4. **Vlastníci domén** musí procházet veřejné audit logy aby mohli najít problematické certy.

PKI, World CA impl .. final review

- nějaký další nápad II ?

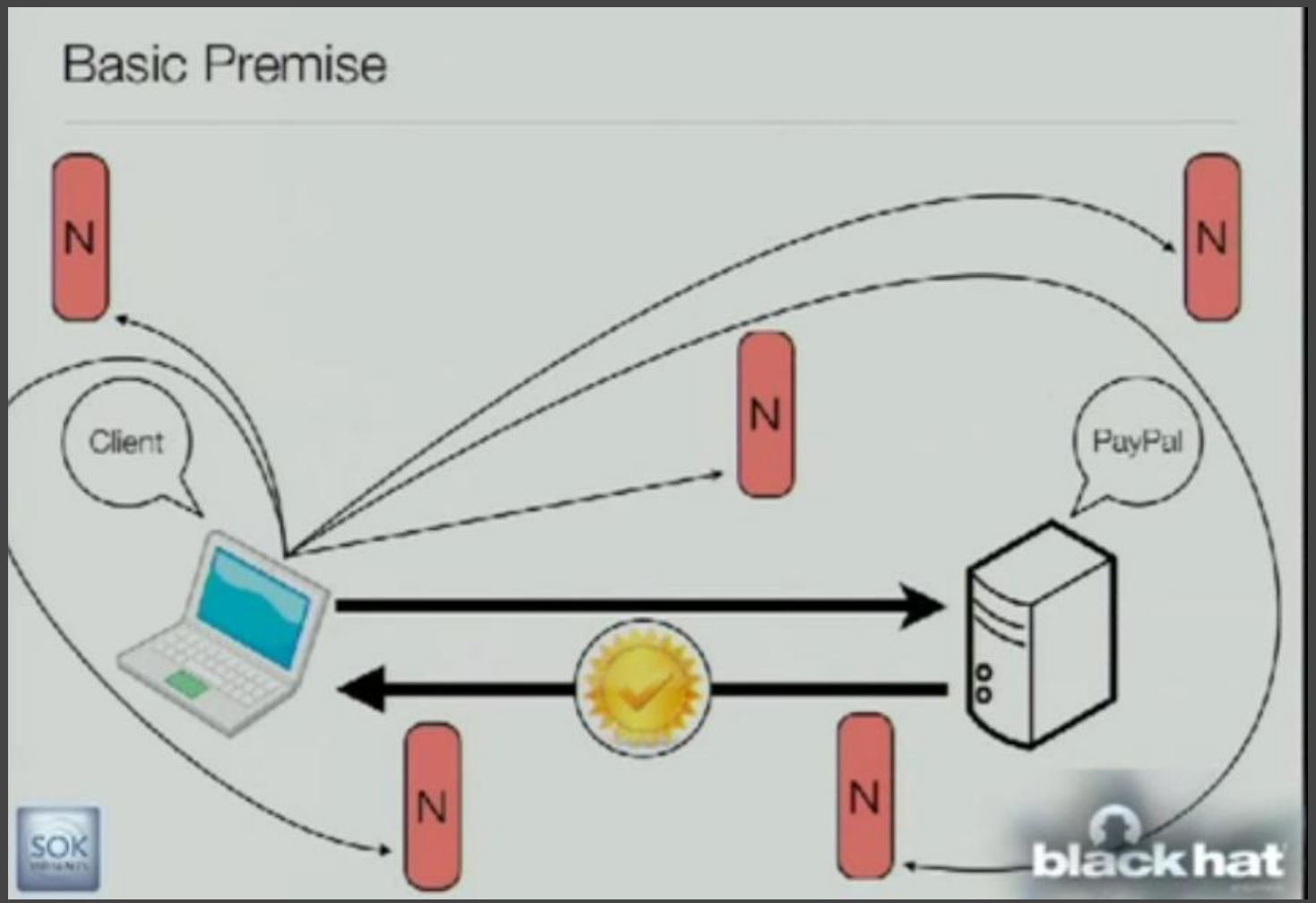
PKI, World CA .. final review

- co s tím ? -- consensus based trust
  - Convergence.io
    - použít třetí stranu pro ověření nabízeného certifikátu z jiného úhlu pohledu



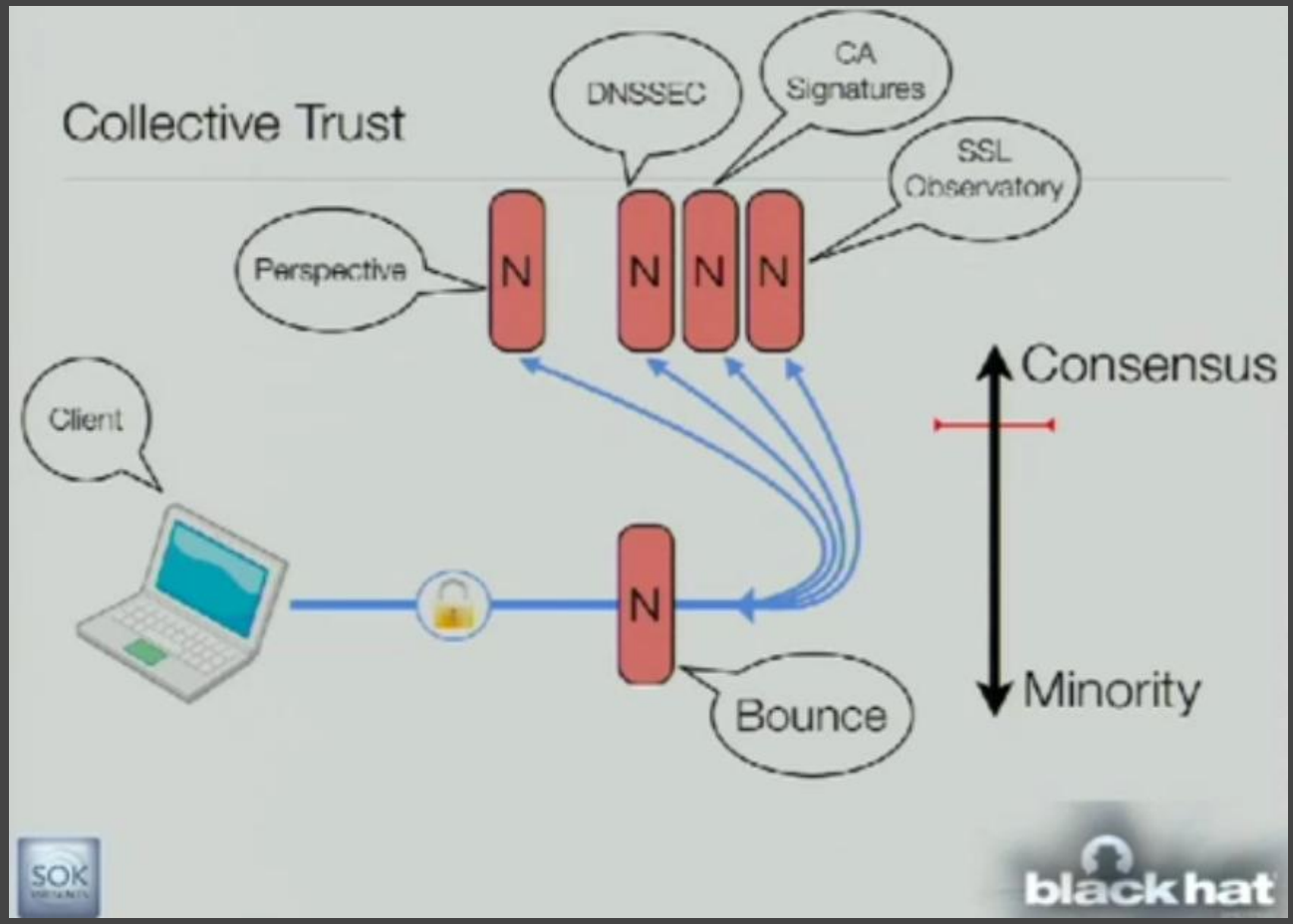
PKI, World CA .. final review

- co s tím ? -- consensus based trust
  - Convergence.io
    - .. nespoléhat se však jen na jednoho notáře ...



PKI, World CA .. final review

- co s tím ? -- consensus based trust
  - Convergence.io
    - .. notáře je možné si vybírat ...
    - *systém knížete Svatopluka*
      - jeden proutek se zlomí snadno, ale 3 najednou ?

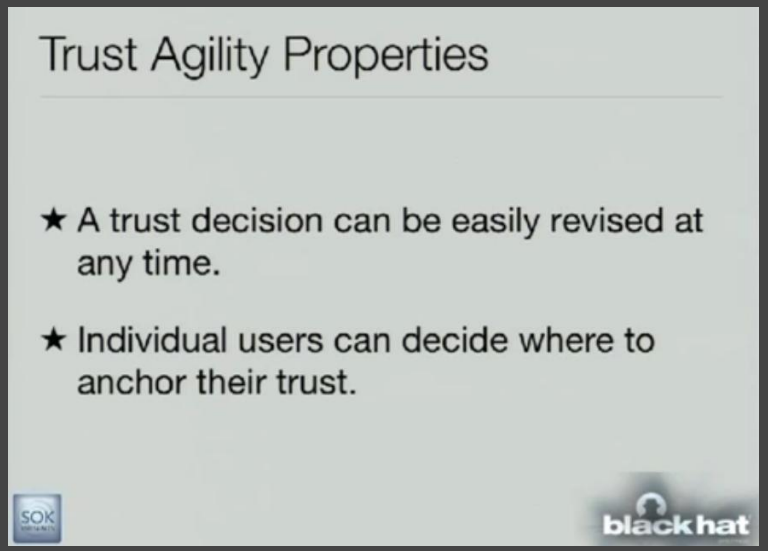


PKI, World CA .. final review

- co s tím ? -- consensus based trust
  - Convergence.io
    - na straně serverů není potřeba nic měnit
    - na straně klienta je potřeba plugin
      - super, ale uživatel tomu rozumí stejně jako PKI, vyskočí hláška o nevhodném certifikátu a co dál ?
      - ! uživatel by si měl seznám notářů sám řídit (trust agility)
      - kde je pro něj rozdíl mezi CA, DNSSEC a notářem ? nikde, stále jej otravuje varovné okénko ...
    - pokud jeden z notářů říká něco jiného než ostatní, znamená to že lže, nebo lžou všichni ostatní ?
      - ... a když to bude 50:50 ?

PKI, World CA .. final review

- co s tím ? -- user controlled trust
  - convergence.io je technikálie, ALE návrh se opírá o několik zajímavých vlastností ...
    - rozhodnutí o důvěře nezávisí na jednom systému,
    - myšítkem si může vybrat míru důvěry,
    - každý sám za sebe, nikoliv výrobce prohlížeče za něj,
    - není to hyper, ale je to možnost nejen změna algoritmů ...



PKI, World CA impl .. final review

- co s tím ? -- reality based trust
  - jak vzniká důvěra v reálném světě ?
    - zkušenosti a bolest
    - známosti a přátelství
      - trusted introducer

  - PGP -- Pretty Good Privacy
    - systém pro ověření důvěryhodnosti šifrovacích klíčů založený na důvěře mezi lidmi kteří se skutečně znají ...
    - crypto facebook ;)

  - Co místo notářů (kteří jsou *anonymní*) použít systém osobních známostí ? ať už pro předávání klíčů nebo vytváření SSL bran do internetu, provozu bezpečných terminálů ? coze ????

PKI, World CA impl .. final review

- TO (ca,dns,conv, ...) vs. ONI

GSM

- SSL je naprd, antiviry nezachytí všechno
  - no co tak mi vezmou heslo k bance, já mám SMSky !

GSM

- GSM šifruje pomocí A5/1
- 2000 -- Bykurov, Shamir, Wagner -- A5/1 se dá zlomit pomocí předpočítaných tabulek
- 2007 -- Universities of Bochum and Kiel -- A5/1 cracker založený na FPGA
- 2009 -- veřejný projekt crackovacího SW
- 2011 -- realita kolem nás ...
  - 1x GPU, 12 TB disk, Kraken
  - Motorola, osmocon
  - 1 - 2 znudění g33kové

    - ... a nebo taky jeste jednodušeji ;)))

Vodafone Access Gateway/Femto cell

1. Koupíme si femto cellu : ... *The box costs 160 GBP.*
2. Otevřeme, napájíme seriový port... nastavím baud rate na 115200... a root password je 'newsys'....

3. Vodafone backdoor na sledování polohy celly ... odpájíme. V pohodě...

4. vypneme alarm a auto-update (jeden XML soubor...)

5. protože VOIP data jsou šifrována, tak před IPSECem je odkloníme, zalogujeme a necháme je projít... a slyšíme vás...

Odposlech GSM ?

komu to může být dobré ?

Odposlech

... no přece panu Bártovi ...

Odposlech GSM

... pardon, tomu druhému ...

Odposlech GSM

- ups ...
  - Napadnout browser nebo internetové spojení > heslo
  - Postavit kraken a quadkoptéru
  - odeslat si penízky na vlastní účet, SMS odchytnout, dešifrovat a použít OTP ...

- Klasické SMS již účty nechrání :(
  - speciální bankovní SIM aplikaci
  - nebo hardwarový token ...

Das RSA Schwierigkeiten

prosvištíme si slovíčka:

APT - Advanced Persistent Threat - dlouhotrvající sveřepý průšvih

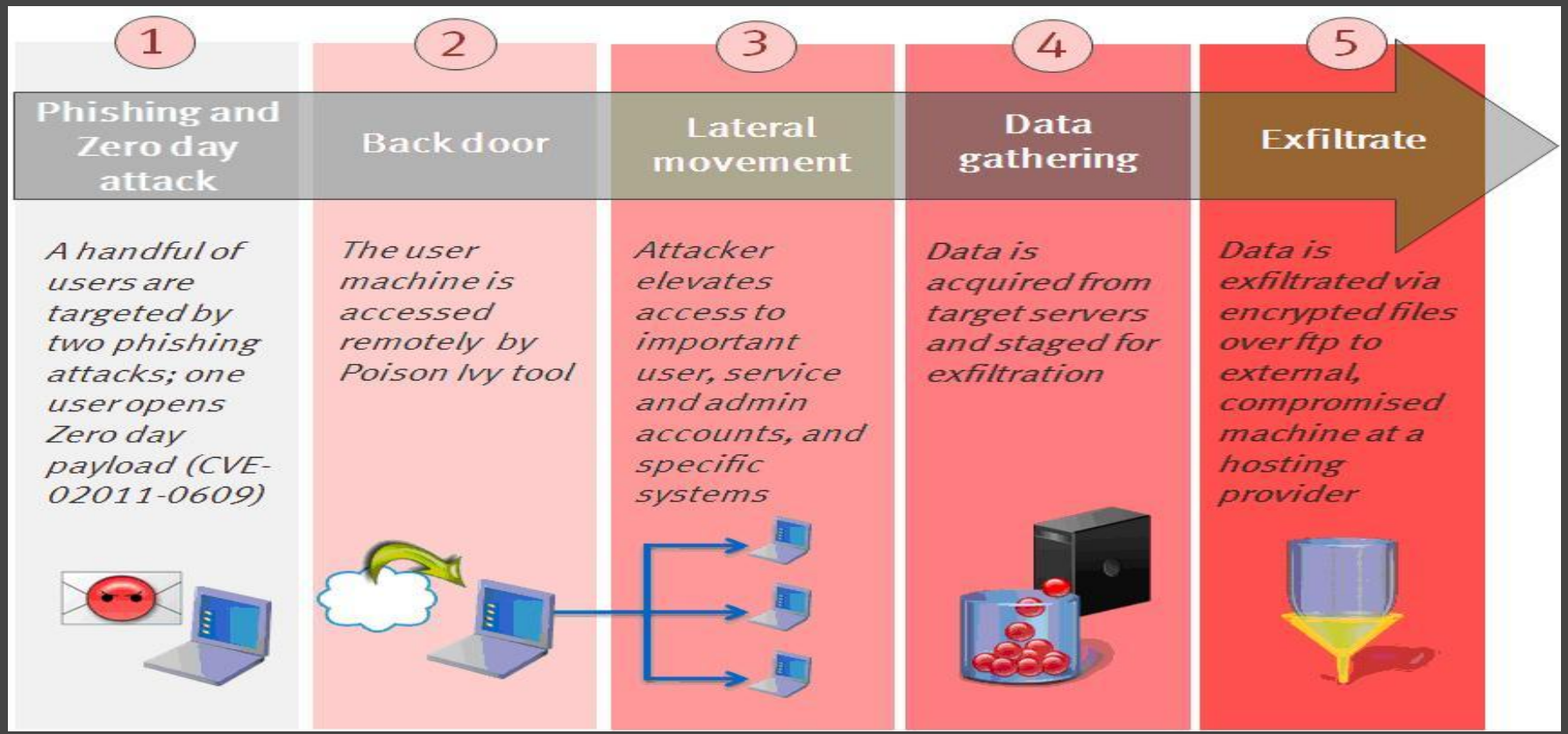
RAT - Remote Administration Tool - nástroj vzdálené správy

Spear Phishing - Drahoušek zákazník ... is so 2007

RSA - firma na bezpečnost (kupte si 5kg bezpečnosti, chcete to taky nakrájet?)

Das RSA Schwierigkeiten - Zeit

1. "2011 Recruitment Plan.xls" s Poison Ivy RAT ve Flashi - spear phishing - DONE
2. útočník se učil - kdo je kdo a jak je postavený, napadá ostatní systémy, učí se dál



Das RSA Schwierigkeiten - Zeit

Jak na to přisli?

dlouhá tenká linie .... až na FTP servery

Good.mincesur.com (venezuela)
up82673.hopto.org (usa)
www.cz88.net (čína)

.... co z toho plyne ....
I mistr tesař se utne? Nebo lépe APT a jiskra jsou zvídavé, rádi cvičí a jsou všichni pracovití

Dz wrъld sekюrity ...

- ať děláš jak děláš, dycky ti někdo nakope zadek. každej to zná ...
  - každý systém má své chyby

- virtuální realita je prostě *rovina existence* se vším všudy, tedy i riziky a každý se musíme bránit sám za sebe a ne spoléhat na ty internety ...

Dz wrъld sekюrity ...

- Štedronín 2011 -- Globalizace
  - podívejme se tedy na internet jako na *datasféru* (dan simmons TM)...
- USA oficiálně prohlásila internet za sféru bojových operací !
  - Různé subjekty (nejen spameři) na planetě mají regulérní jednotky pro boj v datasféře a ty chtějí NAŠE stroje/prostředky
    - EU/NATO, USA, CN, RU, ...

Dz wrъld sekюrity ...

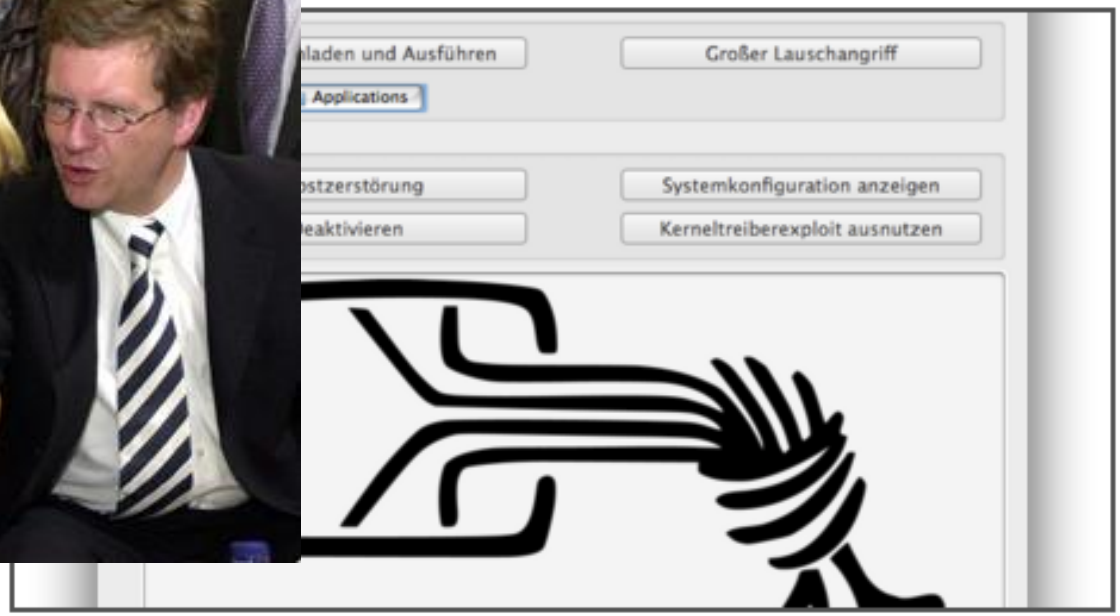
- seriózně tu operují i vlády, a mastí viry jak na běžícím pásu, a je to vidět ;)
- botnet update ;)

German State Co... | CCC | Chaos... | Fixed: Remove A... | 2011 Bezpečnos

Chaos Computer Club analyzes government malware

2011-10-08 19:00:00, admin

The largest European hacker club, "Chaos Computer Club" (CCC), has reverse engineered and analyzed a "lawful interception" malware program used by German police forces. It has been found in the wild and submitted to the CCC anonymously. The malware can not only siphon away intimate data but also offers a remote control or backdoor functionality for uploading and executing arbitrary other programs. Significant design and implementation flaws make all of the functionality available to anyone on the internet.



Even before the German constitutional court ("Bundesverfassungsgericht") on February 27 2008 forbade the use of malware to manipulate German citizen's PCs, the German government introduced a less conspicuous newspeak variant of the term spy software: "Quellen-TKÜ" (the term means "source wiretapping" or lawful interception at the source). This Quellen-TKÜ can by definition only be used for wiretapping internet telephony. The court also said that this has to be enforced through technical and legal means.

Dz wrъld sekюrity ...

- máme tu nejen PČR, ale i ozbrojená vojska -- ccdcoe.org

Foreword from the Director

In the era of information technology we have become dramatically dependant of information technology in our everyday activities. The army is from that perspective no exception to the rule. The bigger the power controlled by IT solutions, the higher the risk of their abuse. There are uncountable possibili-

Funding and Structure

CCD COE is not funded by NATO, but by its Sponsoring Nations. Estonia as the Framework Nation is responsible for providing all Host Nation Support, which includes the infrastructure and administrative costs of the organisation.

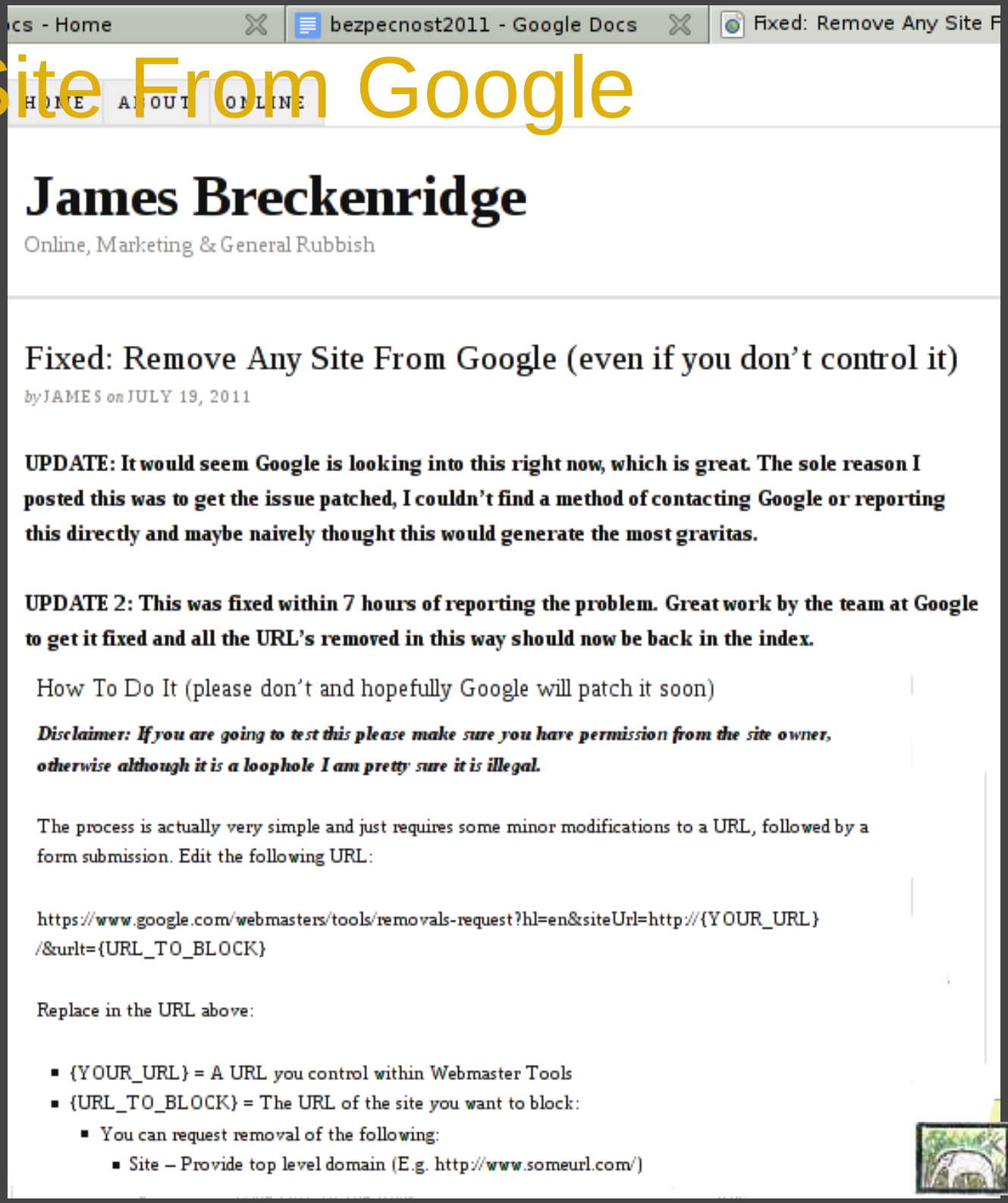
osel

- ... dosti gottwaldizace, pojdme už konečně zlobit ;)

Remove Any Site From Google

- feature of the year ;)
- kdo má webmaster account požádá o ...
- ... vymazání libovolného URL z indexu ;-)
- 7h a je opraveno

kudos 2 google



cs - Home | bezpecnost2011 - Google Docs | Fixed: Remove Any Site F

HOME ABOUT ONLINE

James Breckenridge

Online, Marketing & General Rubbish

Fixed: Remove Any Site From Google (even if you don't control it)

by JAMES *on* JULY 19, 2011

UPDATE: It would seem Google is looking into this right now, which is great. The sole reason I posted this was to get the issue patched, I couldn't find a method of contacting Google or reporting this directly and maybe naively thought this would generate the most gravitas.

UPDATE 2: This was fixed within 7 hours of reporting the problem. Great work by the team at Google to get it fixed and all the URL's removed in this way should now be back in the index.

How To Do It (please don't and hopefully Google will patch it soon)

Disclaimer: If you are going to test this please make sure you have permission from the site owner, otherwise although it is a loophole I am pretty sure it is illegal.

The process is actually very simple and just requires some minor modifications to a URL, followed by a form submission. Edit the following URL:

https://www.google.com/webmasters/tools/removals-request?hl=en&siteUrl=http://{YOUR_URL}/&urlt={URL_TO_BLOCK}

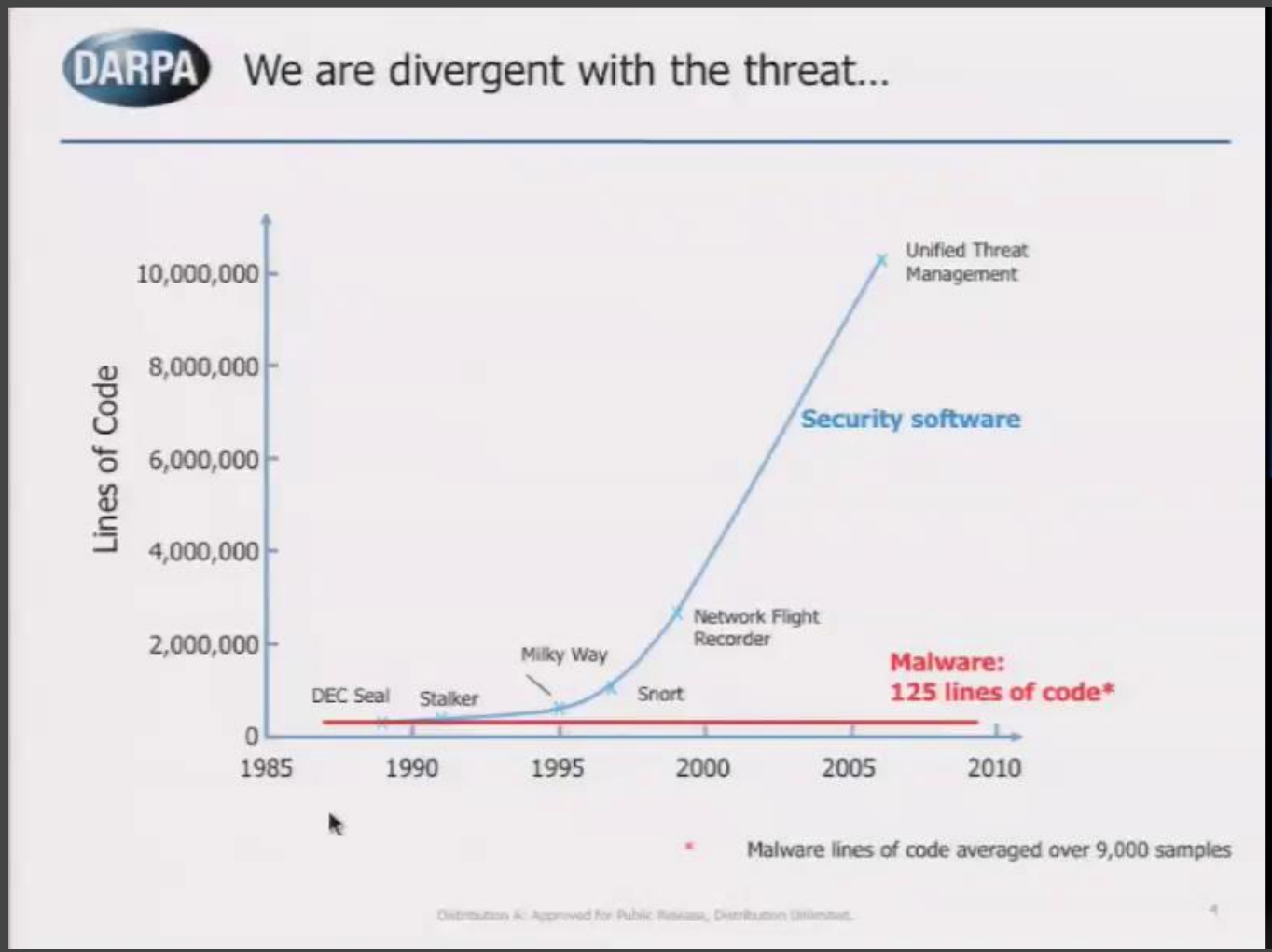
Replace in the URL above:

- {YOUR_URL} = A URL you control within Webmaster Tools
- {URL_TO_BLOCK} = The URL of the site you want to block:
  - You can request removal of the following:
    - Site – Provide top level domain (E.g. http://www.someurl.com/)

Tagging

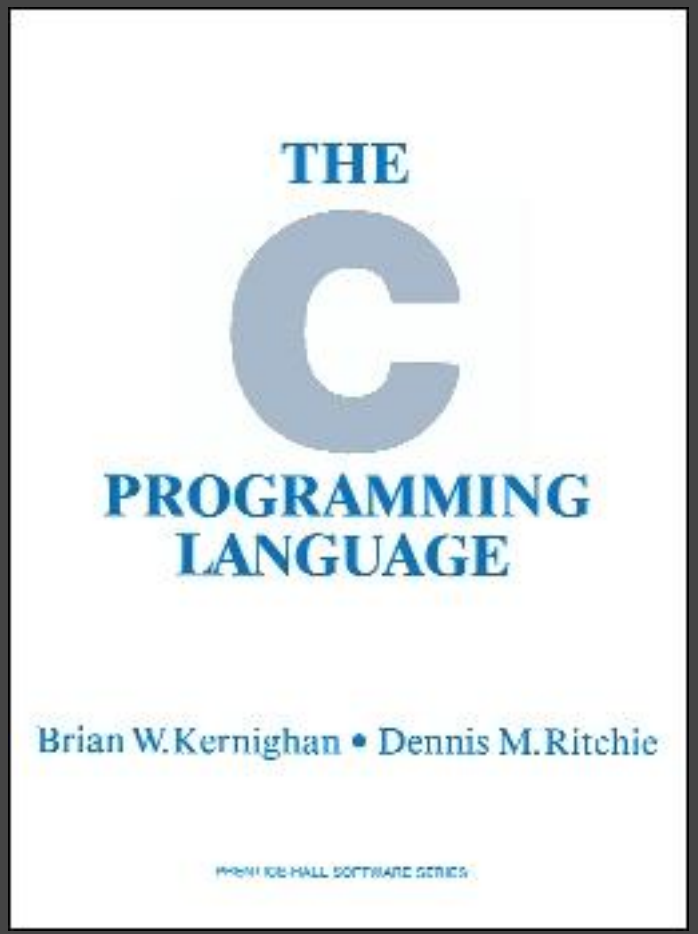
Výhled do budoucna

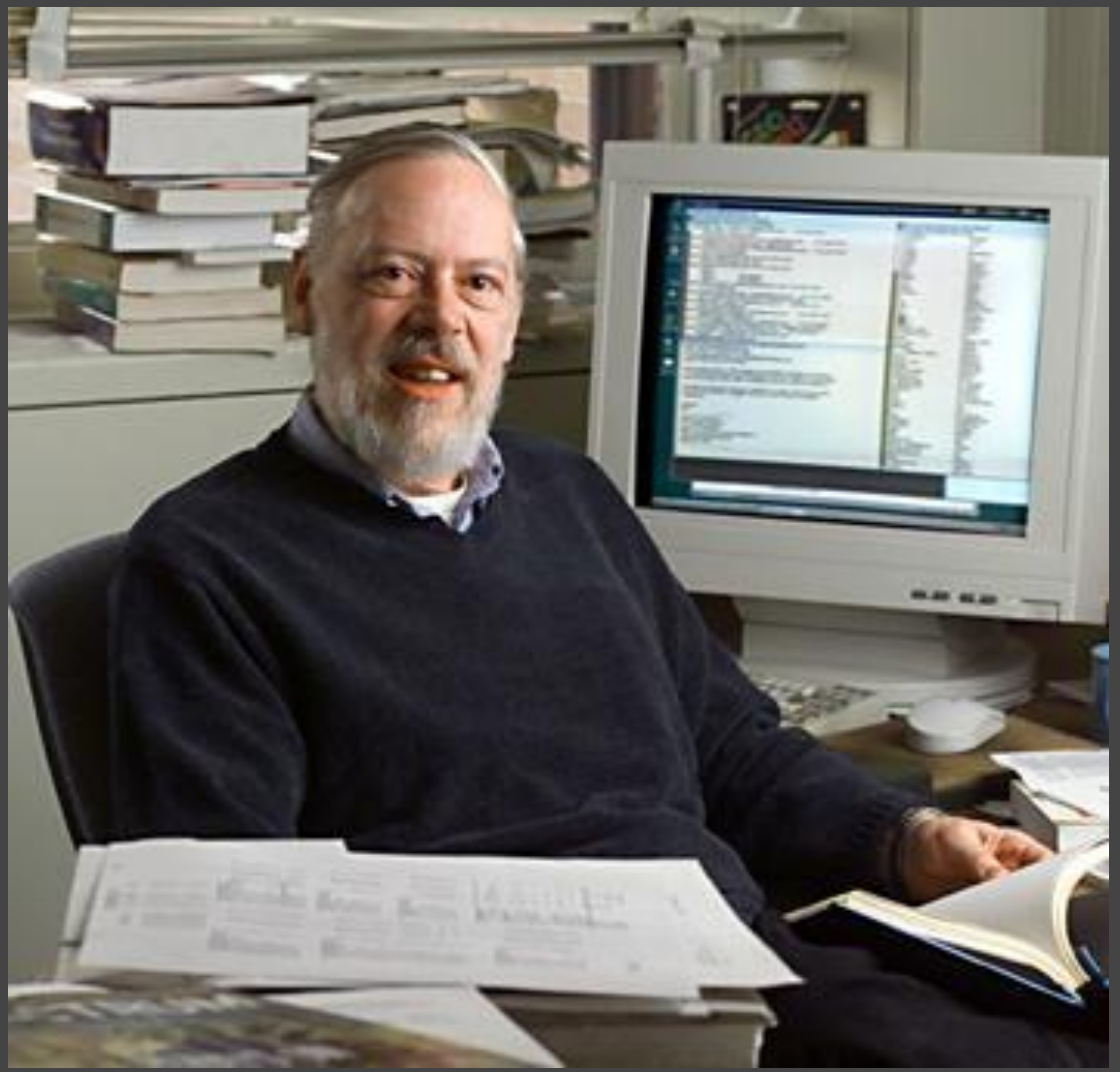
- virů, průniků a všelijaký havjeti je pořád dost, ale nechtěli jsme vás už letos nudit ...



Denis R. (9. září 1941 -- 12. října 2011)

- main(){printf("goodbye, dmr. RIP.\n");}
- R v K&R C





Sweetest Password of the Year ;)

- cokolada
  - 2678 CPU, 30TB, ...

Člověče nezoufej ...

.. stále jsou mezi námi lidé, kteří jsou vůči internetovým bezpečnostním incidentům skutečně imuní ..

Počasí 2011

2.12.2011	2011		2010	2009	2008
Sun Alerts http://blogs.sun.com/security/?cat=alerts&date=200811	71		89	216	173
Debian Security Advisories http://www.debian.org/security/2009/	214		162	246	235
Microsoft Security Bulletin http://www.microsoft.com/technet/security/current.aspx	86		68	68	69
Gentoo Linux Security Advisories http://www.gentoo.org/security/en/glsa/index.xml	47		42	151	191
FreeBSD Security Advisories http://www.freebsd.org/security/advisories.html http://www.vuxml.org/freebsd/	158		132	167	161
CVE Candidates http://cve.mitre.org/data/downloads/allcans.txt	4637		4333	4037	6432