

Cybersécurité au quotidien

Une fragilité et porosité souvent ignorée

Benoît Morel, Carnegie Mellon University

La Chaux de Fonds, le 5 Mars 2014



Charquemont

France
Switzerland

Les Breuleux

16

nnétage

e Russey

Canton of Jura
Canton of Bern

St-Imier

Parc naturel
régional
du Doubs

sur la Côte

Sonvilier

Sur le Ring

16

La Chaux-de-Fonds

20

Canton of Bern
Canton of Neuchâtel

ets

Le Locle

Boinod

La Biche

Dombresson

Lignièrès

Châtillon

Twann

Ligerz

Lake Biel
Bielersee

La Neuveville

Erlach

Cernier

Savagnier

Cressier

La Ruine

La Sagne

La Sagne

Fontaines

Fenin-Vilars-Saules

Saint-Blaise

Cornaux

Brüttelen

Brüttelen

Sise

Les
nts-de-Martel

Peir Martel

Coffrane

Peseux

20

Neuchâtel

Saint-Blaise

Marin-Epagnier

Gampelen

Ins

10

Rochefort

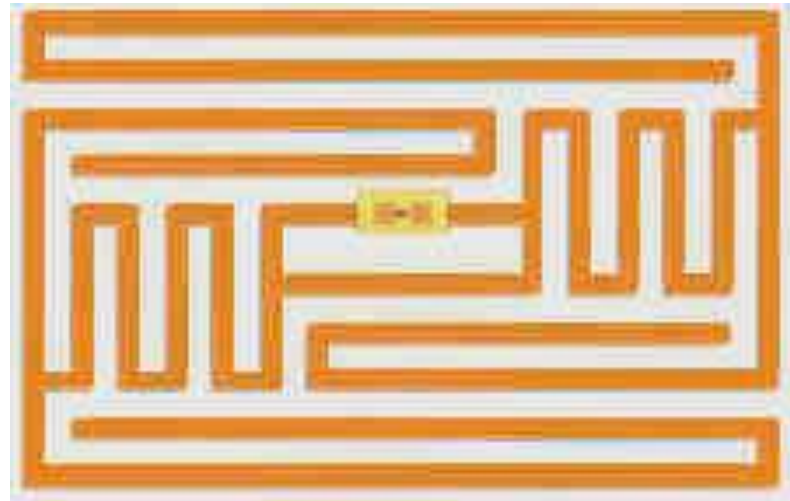
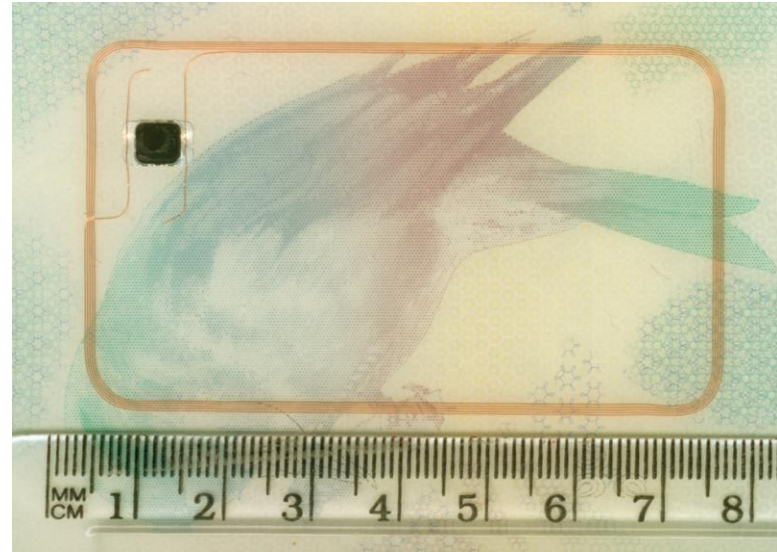
Auvernier

Canton of Bern
Canton of Fribourg



RFIDs...

- Carte d'identité
 - Pour passer une porte
- “SmartCards” (Carte à puce)
- Biometrique (Passeports)
- Clés d'hôtel
- Ski pass
- Bagages
- Identification de produits
- “implants humains”
- Senseurs



Le monde moderne?



On peut mettre un malware dans un objet qui a moins de 1kb de mémoire?

- Un système RFID a plusieurs composantes: un lecteur RFID et un software/middleware.
 - Le software/middleware est sur un PC ordinaire ou un serveur. Il contient la logique de l'application du RFID et (important) une base de données (e.g., Oracle, SQL Server, Postgres, MySQL) pour enmagaziner l'information sur les "tags".
- Un tag infecté peut exploiter les vulnérabilités du RFID middleware pour infecter la base de données.
 - Une fois que le virus, "vers" ou autre malware a atteint la base de données, les tags suivants venant de cette source peuvent propager cette infection.

Scenario hypothétique

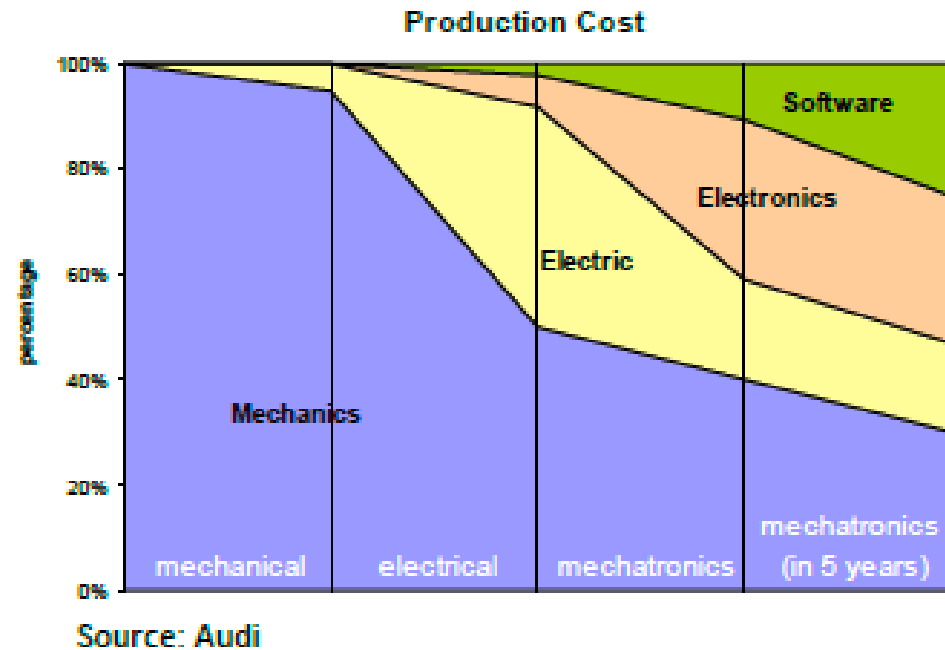
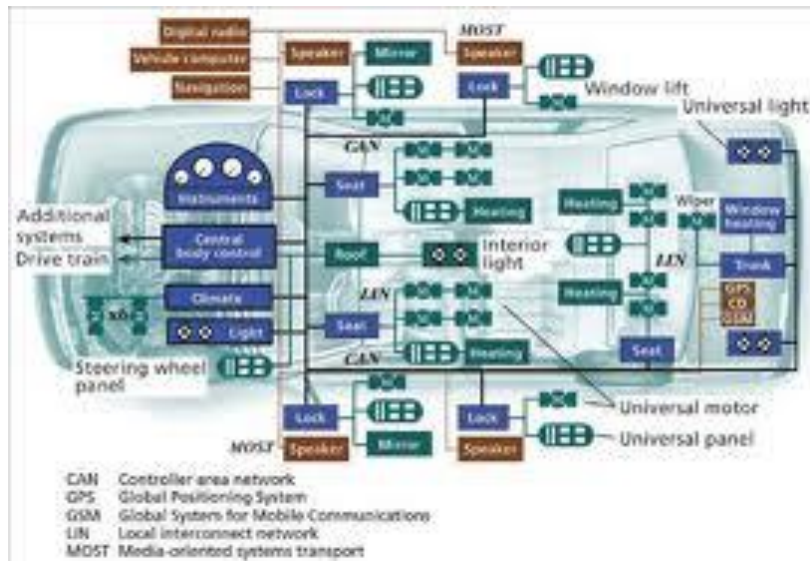
- Les aéroports envisagent de munir les baggages enregistrés avec des RFID
- Ça a potentiellement beaucoup d'avantages: plus d'information plus facile à lire.
- Si un voyageur met en douce un tag infecté sur une valise, l'intégrité de tout le système pourrait être affectée
 - Le tag peut infecter la base de données.
 - Tous les tags produits après ça seront aussi infectés (en plus d'être defectueux).
- Non seulement les baggages pourraient être envoyés à n'importe quelle destination y compris des baggages contenant de la drogue.

Comment écrire un virus pour RFID

- RFID tags sont trop petits pour contenir un virus (ou vers).
- Comme la plupart des malwares, le tag ne contient qu'un code petit qui connecte à un serveur pour télécharger un code malicieux...



Voitures modernes: Electronique devient la composante la plus importante ...



Baucoup plus de “computer power” que le support logiciel d’Apollo 11 lors de l’atterrissage sur la lune.

Quelque chose à méditer: a-t’on besoin d’autant de support logiciel??

Factoids (I)

Trojan-Horse MP3s Could Let Hackers Break Into Your Car Remotely, Researchers Find

By Rebecca Boyle Posted 03.14.2011 at 4:57 pm 15 Comments



Dashboard Karl Frankowski via Flickr



Source:


<http://www.popsci.com/cars/article/2011-03/bluetooth-music-and-cell-phones-could-let-hackers-break-your-car-researchers-say>

Des chercheurs à l'université de Californie à San Diego (UCSD) ont démontré qu'il était possible de hacker une voiture, à distance.

En fait depuis la situation s'est "aggravé" avec l'introduction de "l'infotainment" et il est possible de faire toutes sortes de choses aux voitures à distance...

Factoid (II)

Hacker Disables More Than 100 Cars Remotely

By Kevin Poulsen  March 17, 2010 | 1:52 pm | Categories: [Breaches](#), [Crime](#), [Cybersecurity](#), [Hacks and Cracks](#)

More than 100 drivers in Austin, Texas found their cars disabled or the horns honking out of control, after an intruder ran amok in a web-based vehicle-immobilization system normally used to get the attention of consumers delinquent in their auto payments.

Police with Austin's High Tech Crime Unit on

Au Texas, un système informatique qui immobilise les voitures, a été développé pour punir les gens qui ne paient pas leur voiture.

Le système a été compromis pas un hacker pour faire claxonner les voitures hors contrôle...



Source:

<http://www.wired.com/threatlevel/2010/03/hacker-bricks-cars/>

Problems with smartphones

- A node for communications: NFC, Bluetooth, Wifi, cells.
- High processing power
- Low power supply
- New OS: Android, iOS instead of Windows
- New Browsers: Chrome, ...
- World of Apps offer as many new points of entry for hacking.
- Plus many more...

There is no limit for new “apps”.



They offer serious threats
And inspire intriguing stories

Demonstrated use of Smartphones

- Hacking into [cars](#)



- To Steal Credit Card Information, just by Being Near [Them](#)
 - Culprit: NFC



Typical “security tips”

- Keep it locked
- Make sure your phone’s screen lock is on – at all times – so there’s less at risk if your phone falls into the hands of a cybercriminal.
- Encrypt your sensitive information
- Monitor how apps behave on your phone Be aware of permission access / requests from applications running on your phone. It’s especially important to do this for Android smartphones.
- Protect your phone and your data
- Be aware of the risks of jailbreaking / rooting
- Switch off Bluetooth... when you can
- Choose a smartphone security solution with anti-theft features
- **Logical conclusion:**
 - Do you really want or need a smartphone..



Heureusement il y a la NSA



Fort Meade



E. Snowden



Angela Merkel



La NSA cible tout le monde...



Avoir la responsabilité de la cybersécurité

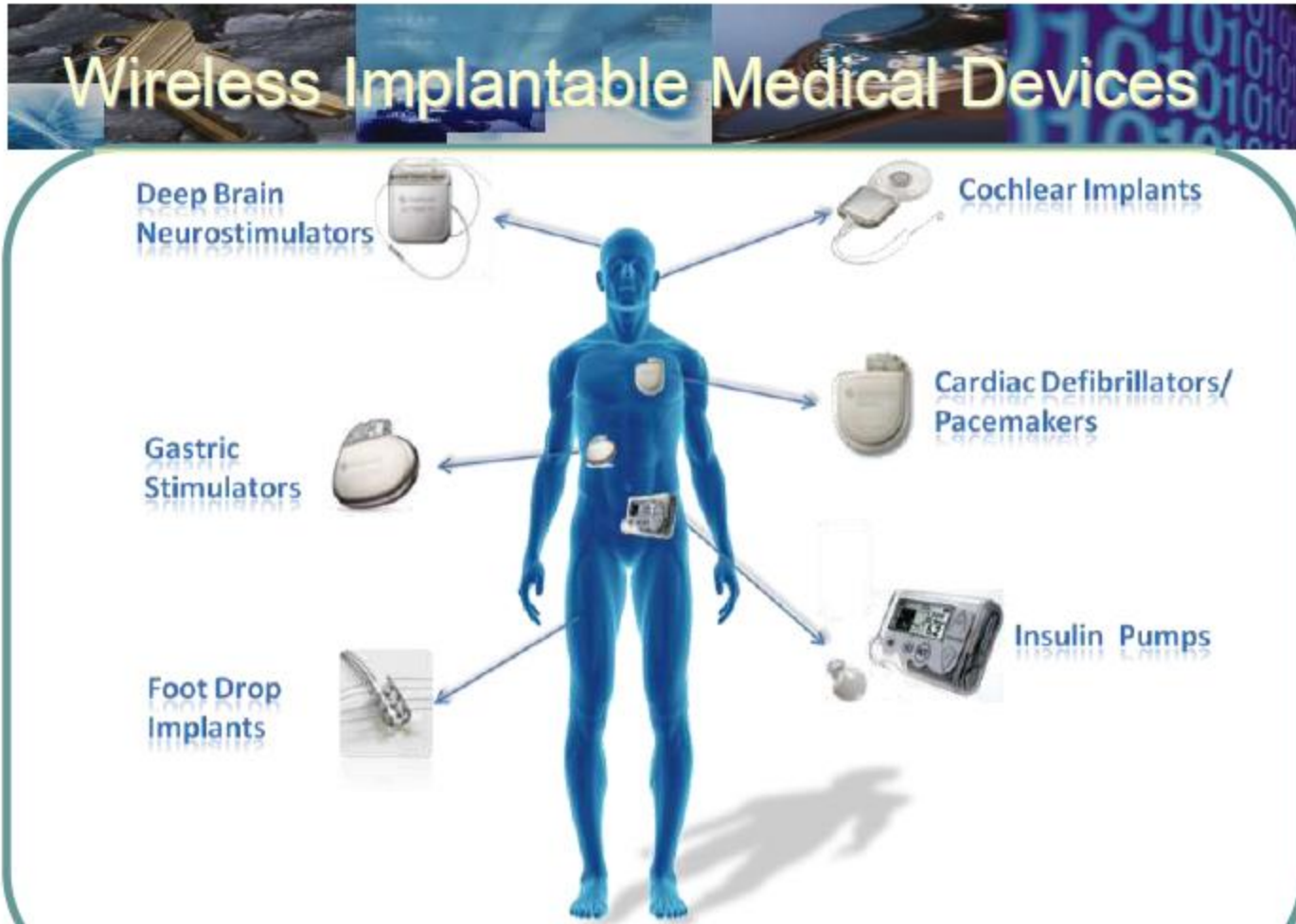


Général Keith Alexander
Chef de la NSA (jusqu'à la
fin du mois de Mars)

Difficultés:

- 1- La mission est complexe parce que
 - la cybersécurité est naturellement complexe
 - Les grosses erreurs ne sont pas permises
 - Les “autorités” ne comprennent pas le problème... et ne réalise pas a quel point!
 - Les États Unis souffrent d'une assymétrie de situation contre eux

“Implantable Medical devices”



The “internet of things” et les dentistes



Systemes cyberphysiques

- ***Communication, calcul contrôle intégrés.***



Transportation

- Faster and safer aircraft
- Improved use of airspace
- Safer, more efficient cars



Energy and Industrial Automation

- Homes and offices that are more energy efficient and cheaper to operate
- Distributed micro-generation for the grid



Healthcare and Biomedical

- Increased use of effective in-home care
- More capable devices for diagnosis
- New internal and external prosthetics



Critical Infrastructure

- More reliable power grid
- Highways that allow denser traffic with increased safety

Le “smart grid” est un nouveau champ de bataille potentielle

Ce sont quelques unes des
“menaces” émergentes

Il y a les menaces/attaques passées
et ce qu’elles nous ont appris

“Browser hijacking”

- C’est une modification du Browser par un malware.
- SilentBanker est un exemple de “Man in The Browser attack”, (MIB):
 - Pendant une transaction bancaire, Silentbanker change les détails du compte du client, fait transférer de l’argent dans un autre compte, sans que le client voit la différence.
- OddJob: maintient la connexion après le log-off est fait un “CSRF attack” (Cross Site Request forgery)
- Il marche sur IE et Firefox

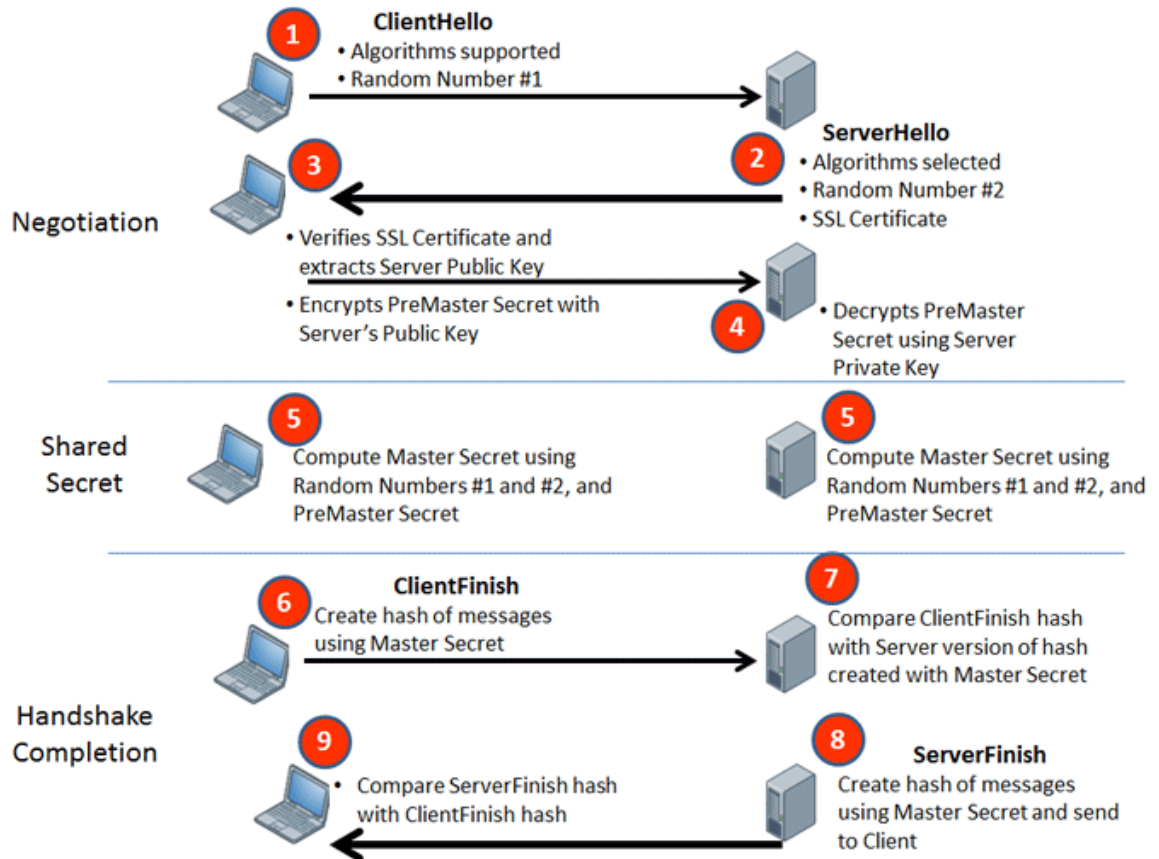
Zeus et ses descendants

(Ref: <http://www.thetechherald.com/article.php/201120/7165/Overview-Inside-the-Zeus-Trojan-s-source-code>)

- Le code source du Zeus Trojan est devenu public en Mai 2011.
 - “Un programme qui valait des milliers de Dollars est maintenant accessible gratuitement, par qui veut, inclus les cyber criminels”...
 - Il était compliqué, Modulaire, (i.e. il pouvait être adapté aux besoins des acheteurs) et avec service après vente...
- Spyeye: est apparu en 2009.
 - Moins cher que Zeus (\$500).
 - Une version (V1.0.7) contenait une fonction qui s’appelait: “Kill Zeus”
 - SpyEye de façon automatique ordonnait des transactions si vite que les banques refusaient de les faire.
 - Dans une version plus récente, il se comporte comme un être humain...
- Semblait copier Zeus et a fini par s’associer avec eux.

Tatanarg

- Tatanarg apparu en Mars 2011, neutralise les Antivirus, neutralise Zeus , se met entre l'utilisateur et la banque
 - Il crée son propre certificat et intercepte la clé d'encryption



“Chip and Pin” is Broken (brisé)



Prof. Ross Anderson
<http://www.cl.cam.ac.uk/~rja14/>

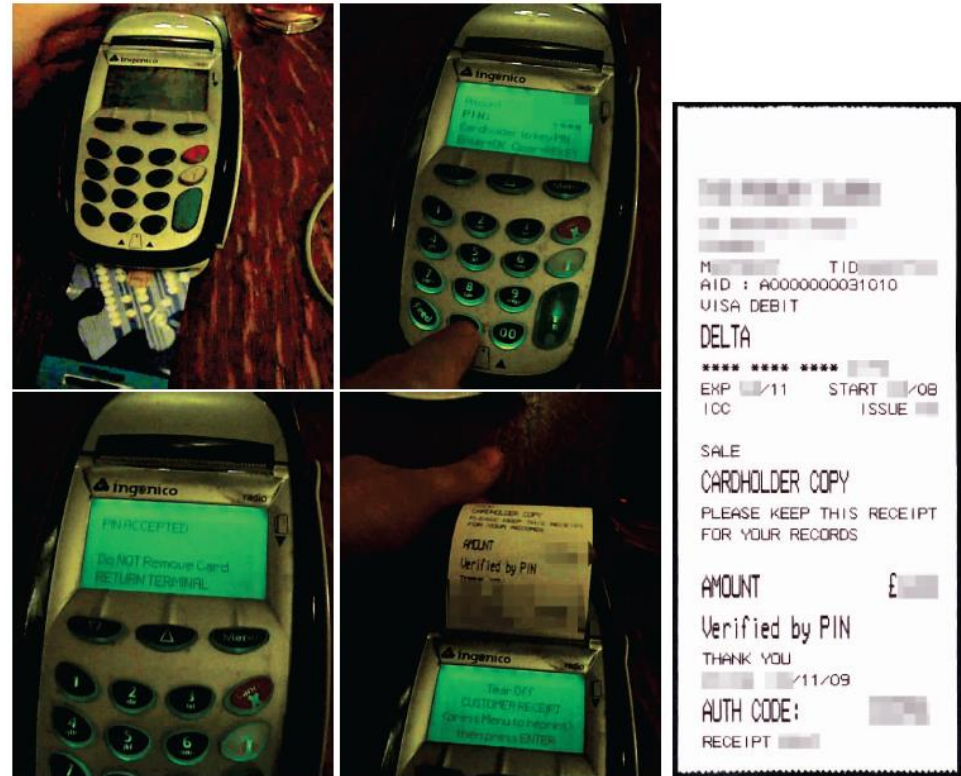


Figure 5. Carrying out the attack. Although we entered the wrong PIN, the receipt indicates that the transaction was “Verified by PIN”.

Il s'ont entré un pin number faux...

Hack sur un bancomat (ATM machine)



Barnaby Jack, a fait une démonstration àDEFCON d'un hack sur une "ATM machine".

Il a montré en public qu'il était possible de les faire donner tout l'argent qu'elles ont, de loin...

http://www.wired.com/magazine/2011/01/st_howtoatm/

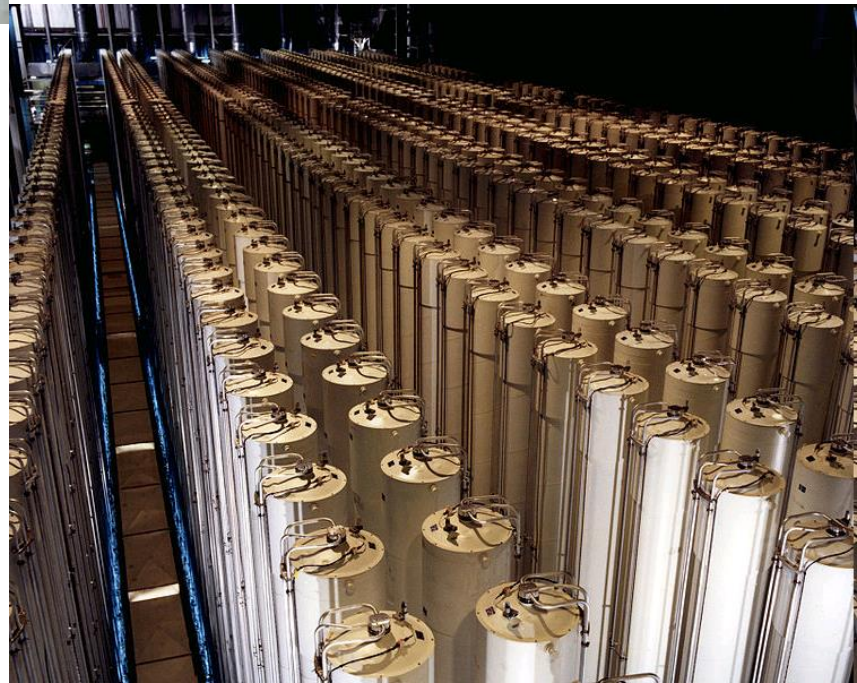
Stuxnet et la vulnérabilité des infra-structures critiques



The control center of the Bushehr nuclear power plant



Enrichment centrifuge cascades



SIEMENS

Siemens S7
Programmable Logic
Controller (PLC)



Présentation de Bruce Dang at 27C3

Characteristics	Aurora	Stuxnet
Exploitation vector	MS10-002 (0-day)	MS10-046 (0-day) MS10-061 (0-day) MS10-073 (0-day) MS10 -092 (0-day) CVE-2010-2772 (0-day) MS08-067 (patched)
Targeted malicious program	Win32/Vedrio	Win32/Stuxnet



Ghostnet

Le diagnostic de [Virus Total](#)

Antivirus	Version	Last Update	Result
AntiVir	-	-	EXP/Word.Dropper.Gen
Authentium	-	-	CVE-2006-2492
Avast	-	-	MW97:CVE-2006-2492
eTrust-Vet	-	-	W97M/SmartTags!exploit
F-Prot	-	-	CVE-2006-2492
Fortinet	-	-	MSWord/ObjPointer.A!exploit.N20062492
GData	-	-	MW97:CVE-2006-2492
Ikarus	-	-	Virus.MW97.CVE.2006.2492
Microsoft	-	-	Exploit:Win32/Wordjmp.gen
Sophos	-	-	Troj/MalDoc-Fam
Webwasher-Gateway	-	-	Exploit.Word.Dropper.Gen

11 out of 34...

“Social engineering” utilisé par ghostnet

From: "campaigns@freetibet.org" <campaigns@freetibet.org>

Date: 25 July 2008

Subject: Translation of Freedom Movement ID Book for Tibetans in Exile

Translation of Freedom Movement ID Book for Tibetans in Exile.

Front Cover

Emblem of the Tibetan government in Exile

Script: Voluntary Contribution into common fund for Tibetan Freedom Movement

Inside Cover

Resolution was passed in the preliminary general body meeting of the Tibetan Freedom Movement held on July 30, 1972 that the Tibetan refugees in exile would promise for each individual,Ãs share of the voluntary contribution into the Tibetan Freedom Movement Receipt book. This resolution was later reaffirmed by the 11th Tibetan People,Ãs Deputies and passed into the law on April 01, 1992 (Tibetan King Year 2119)

Until the last page of this book is used, the book stands valid until August 15, 2012

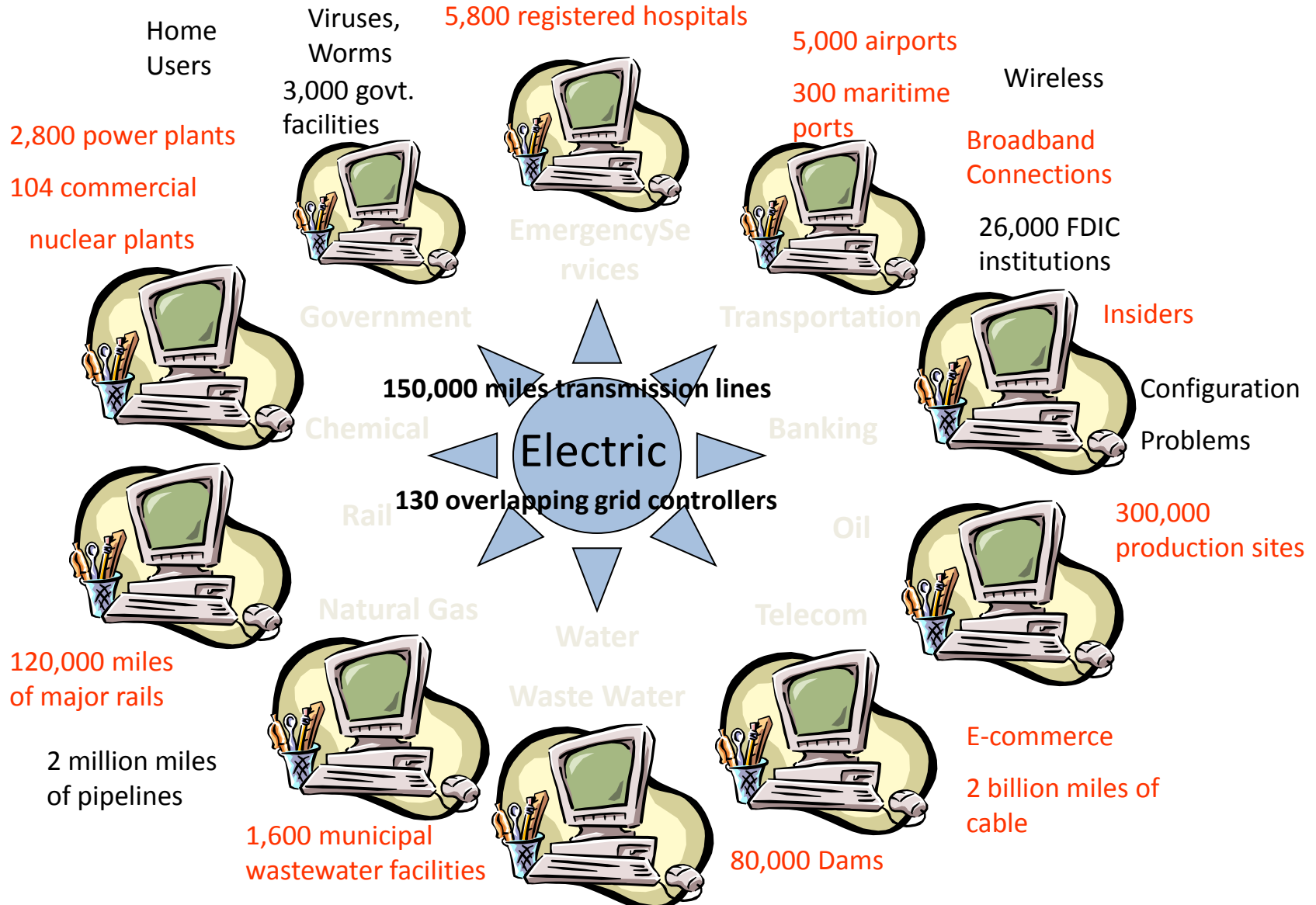
Date: August 16, 2008

Emblem of the Tibetan Government in Exile

Official Signature

Attachment: Translation of Freedom Movement ID Book for Tibetans in Exile.doc

Cybersecurity une menace complexe sur les sociétés modernes



Cybersécurité

- La menace la plus complexe sur les sociétés modernes?
- Qui sont derrière cette menace

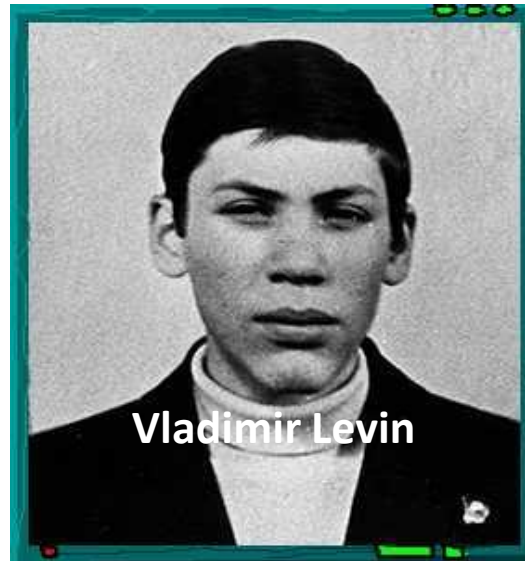


FBI director: Robert Mueller

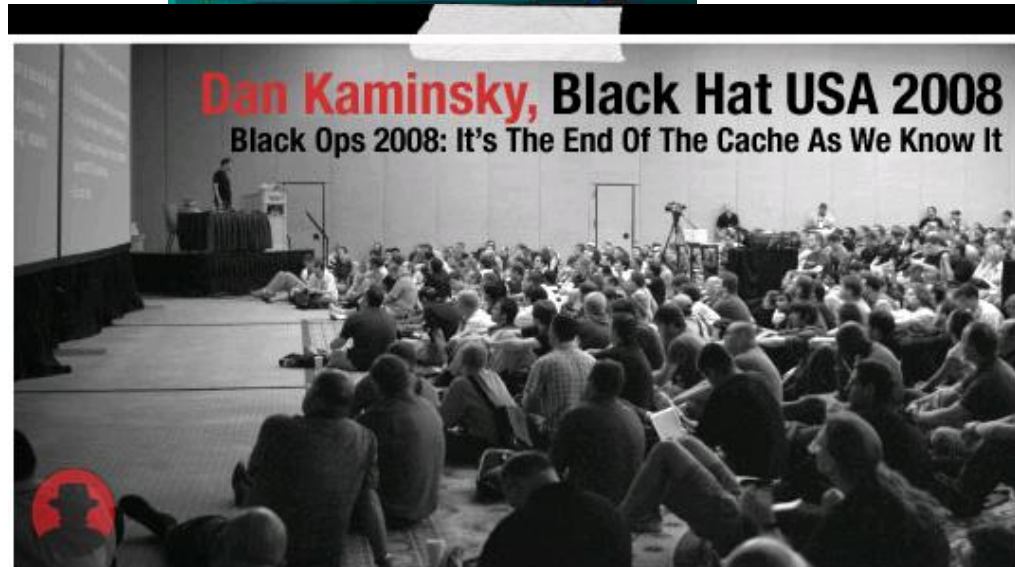
These are the kind of people who
outsmart the FBI...



R.M. Morris:
MIT Prof



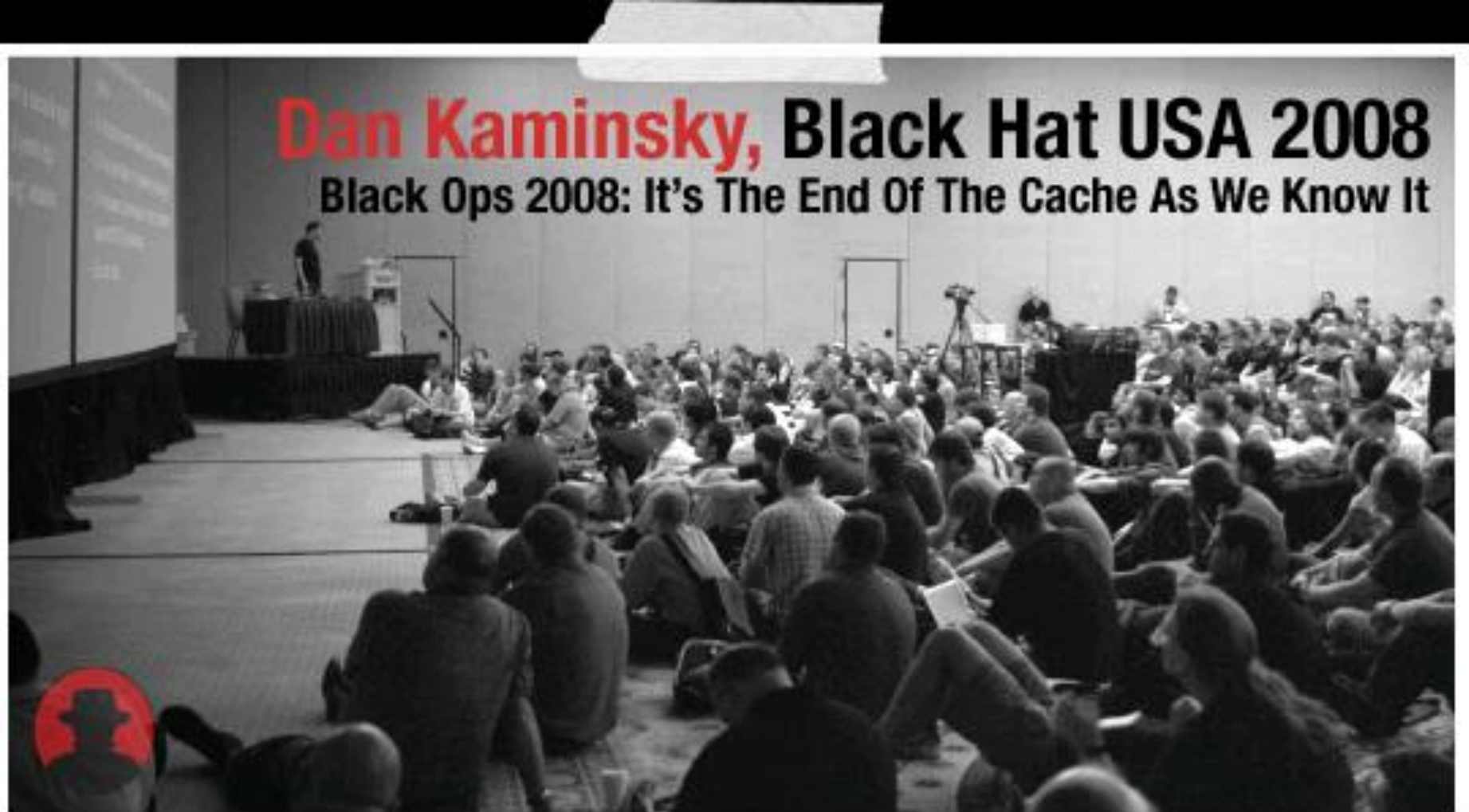
Mudge
Peter Zaitko:
DARPA
Program
manager



La présentation "historique"



Dan Kaminsky, Black Hat USA 2008 **Black Ops 2008: It's The End Of The Cache As We Know It**



(Dr.) Mudge a.k.a. Peter Zatkó

In May 1998, Mudge and the rest of L0pht were invited to testify to the Senate



2011: Mudge is program manager at DARPA



Les ennemis modernes

- Anonymous
- Russian business network
- Syrian Electronic Army
- Les auteurs de Shamoun
- Avant ils s'appelaient: "The cult of the dead cow" ... Ils devaient des malware appelés "back orifice", etc...
- Les choses ont changé, bien (i.e. mal) changé



Dark/Deep Web

<https://sites.google.com/site/howtoaccessthedeepnet/working-links-to-the-deep-web>

Financial Services: a sample...

Banker and Co. - Professional money laundering and consultation service.

Paypal4free - Hacked Paypal accounts for cheap, with balances

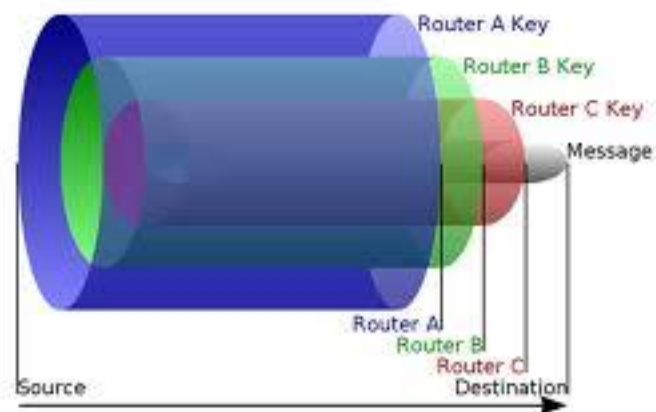
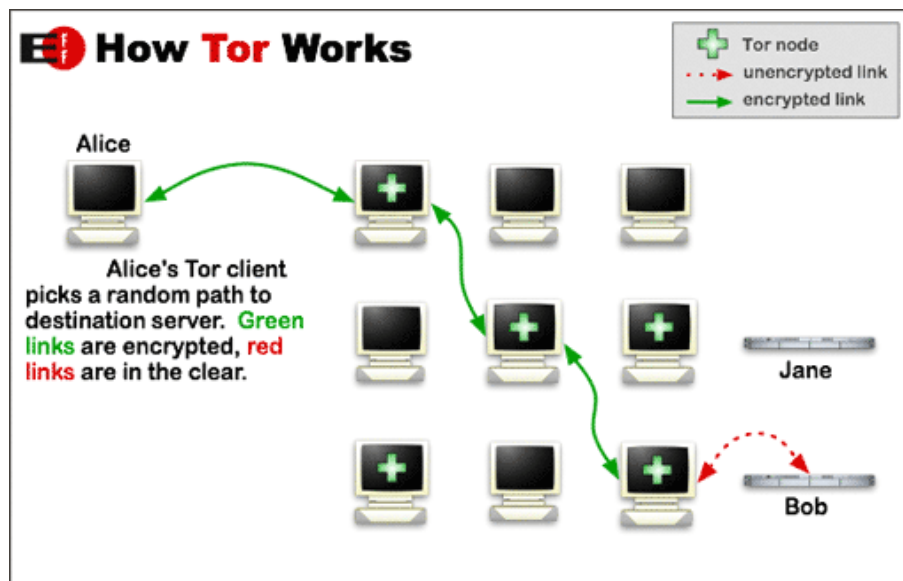
Commercial Services:

DiamondsandGold - Sells stolen diamonds and gold.

Marketplace

See also: The separate Drugs and Erotica sections for those specific services.

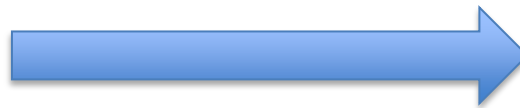
The Onion Router (TOR)



Edward Snowden used the Tor Network to send information about PRISM to the *Washington Post* and *The Guardian* in June 2013

Comment se fait-il que le FBI n'ait pas pénétré ces réseaux: dark web and dark internet?

Progrès??





Fyodor's site

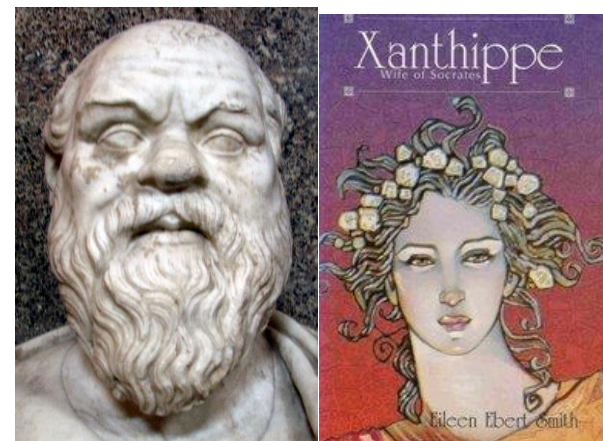
Gordon Lyon, alias:
Fyodor



- [Antimalware \(3\)](#)
- [Application-specific scanners \(3\)](#)
- [Web browser-related \(4\)](#)
- [Password crackers \(12\)](#)
- [Encryption tools \(8\)](#)
- [Debuggers \(5\)](#)
- [Firewalls \(2\)](#)
- [Forensics \(4\)](#)
- [Fuzzers \(4\)](#)
- [General-purpose tools \(8\)](#)
- [Intrusion detection systems \(6\)](#)
- [Packet crafting tools \(6\)](#)
- [Port scanners \(4\)](#)
- [Rootkit detectors \(5\)](#)
- [Security-oriented operating systems \(5\)](#)
- [Packet sniffers \(14\)](#)
- [Vulnerability exploitation tools \(11\)](#)
- [Traffic monitoring tools \(10\)](#)
- [Vulnerability scanners \(11\)](#)
- [Web proxies \(4\)](#)
- [Web vulnerability scanners \(20\)](#)
- [Wireless tools \(5\)](#)

Que dire de la cybersécurité?

- Une menace réelle?
- Un épisode?
- Une forme de pollution?
- Une gangrène??



– **La cybersécurité est le produit des hommes, Est-elle en dehors du contrôle des hommes??**

Des Suisses???



Aurora (極光): un autre épisode ambigu



Google, Dow Chemical, Morgan Stanley,
Northrop Grumman etc...

US se plaint...

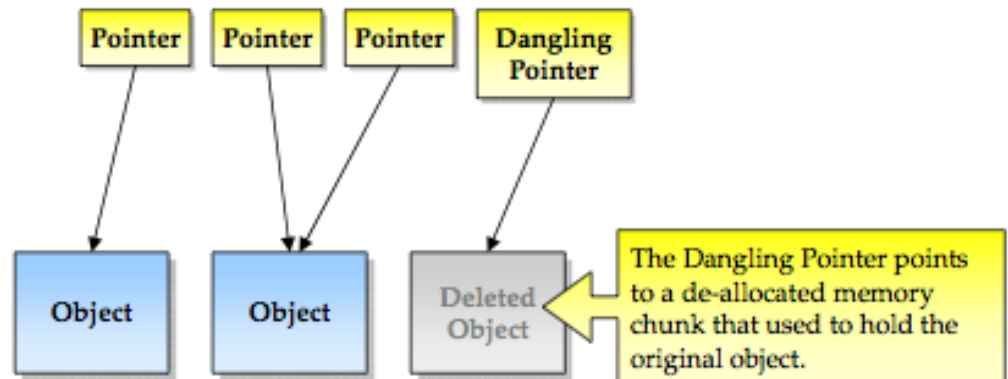
Microsoft sloppiness

Superficiality of the Press coverage

我想知道你的一切

Wǒ xiǎng zhīdào nǐ de yīqiè

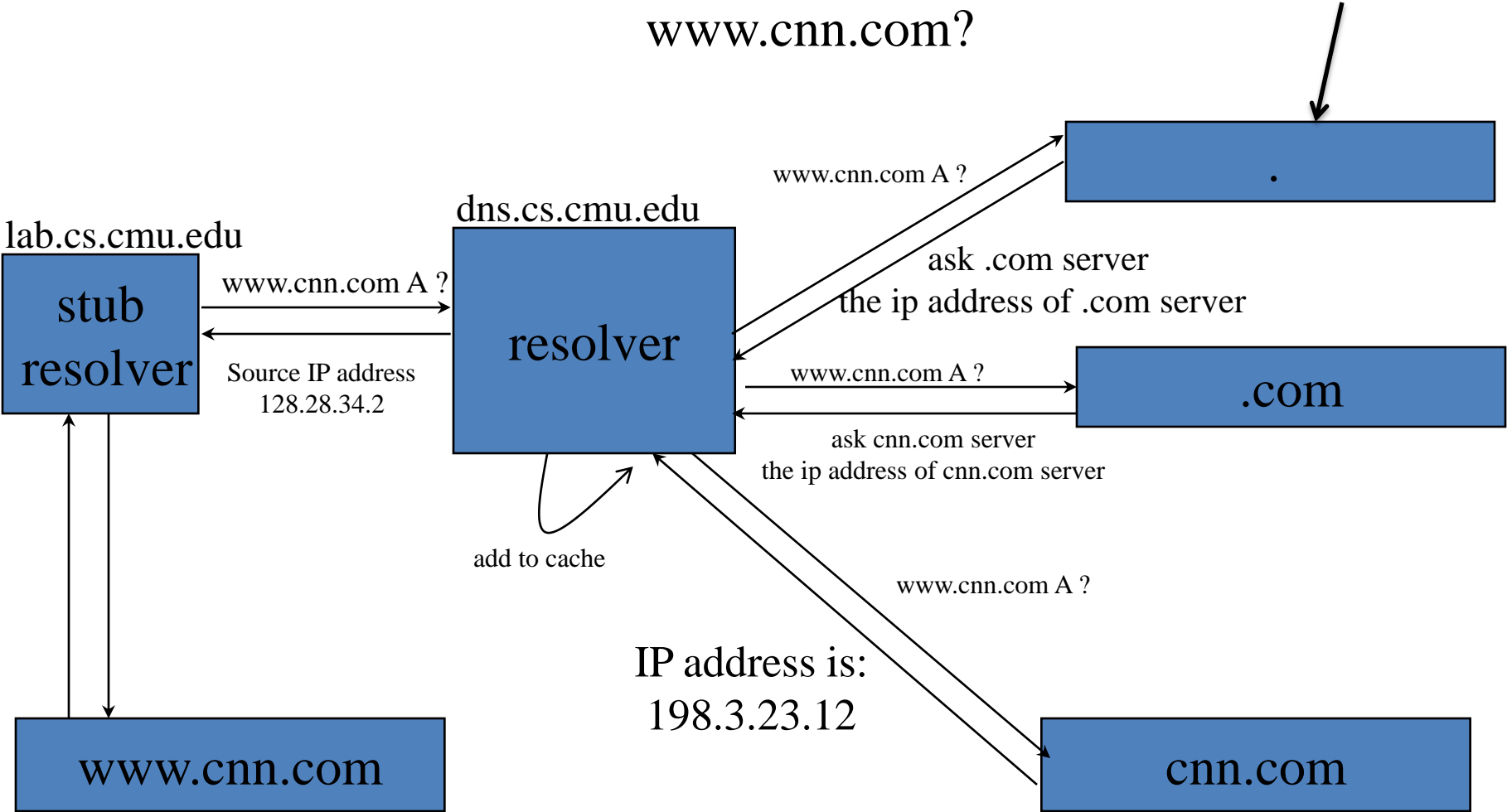
Je veux tout savoir sur vous...



DNS Address Resolution

Question: quelle l'adresse IP de :
www.cnn.com?

La racine



The importance of the “cache” of DNS servers: they save time...

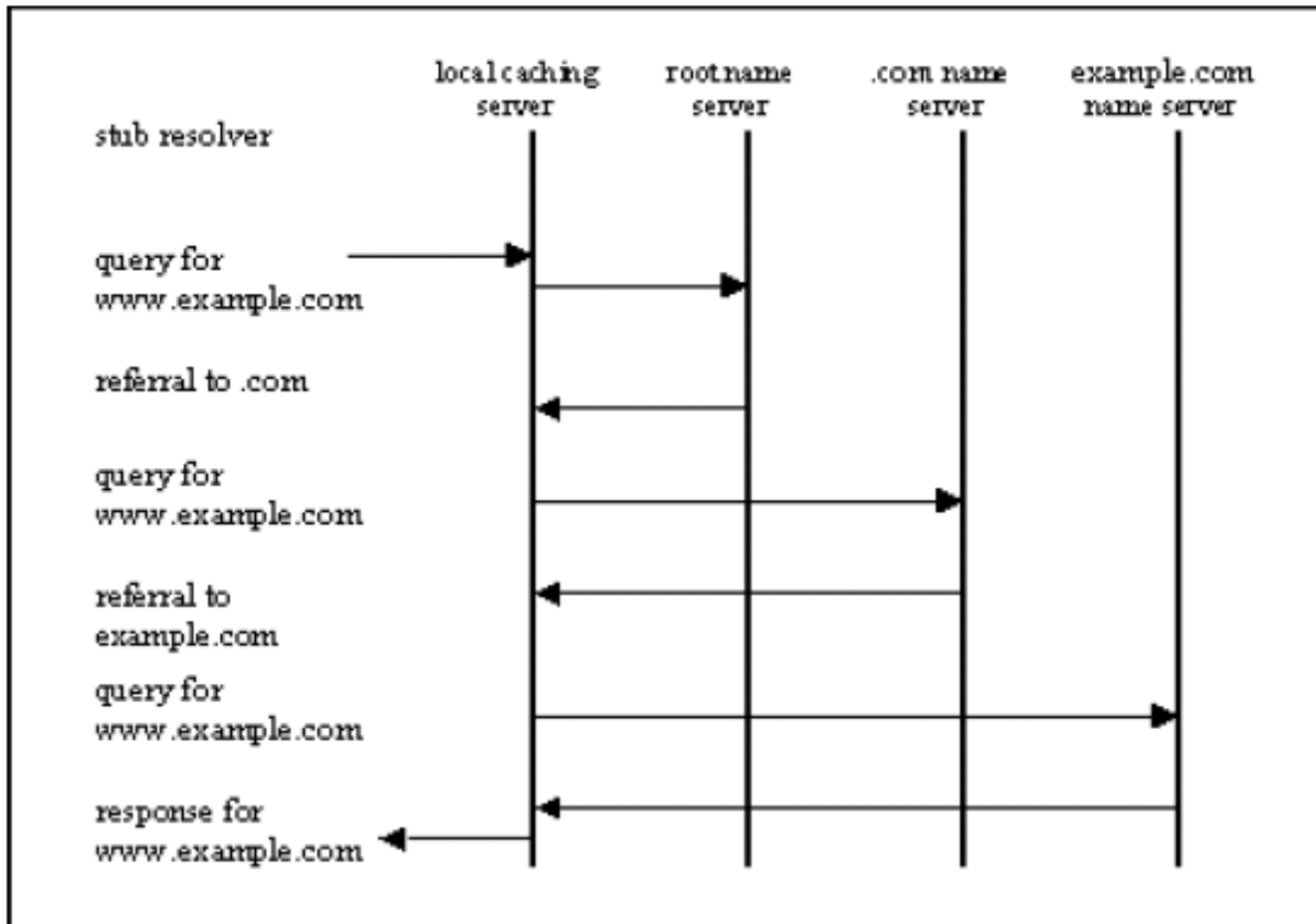
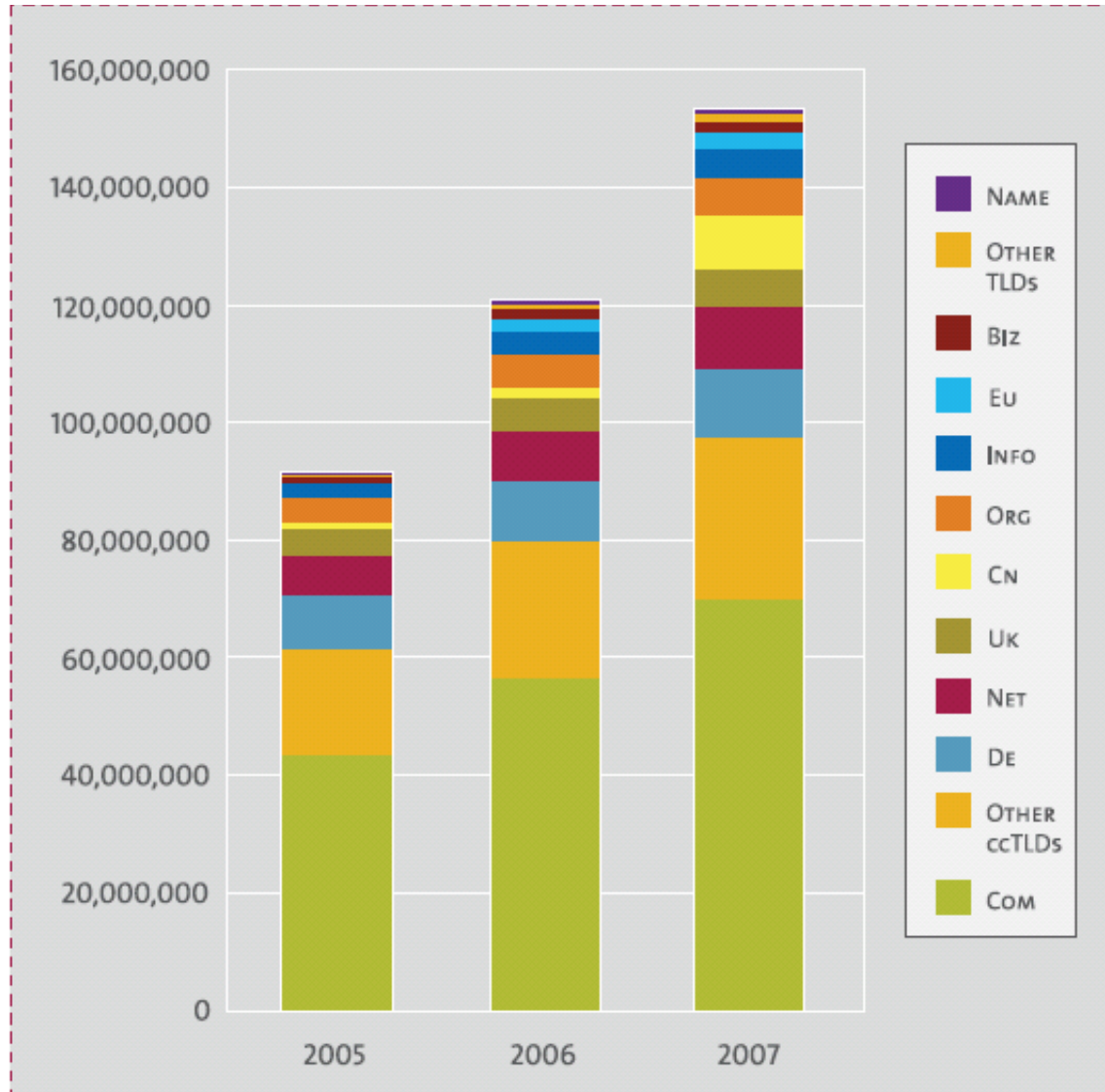
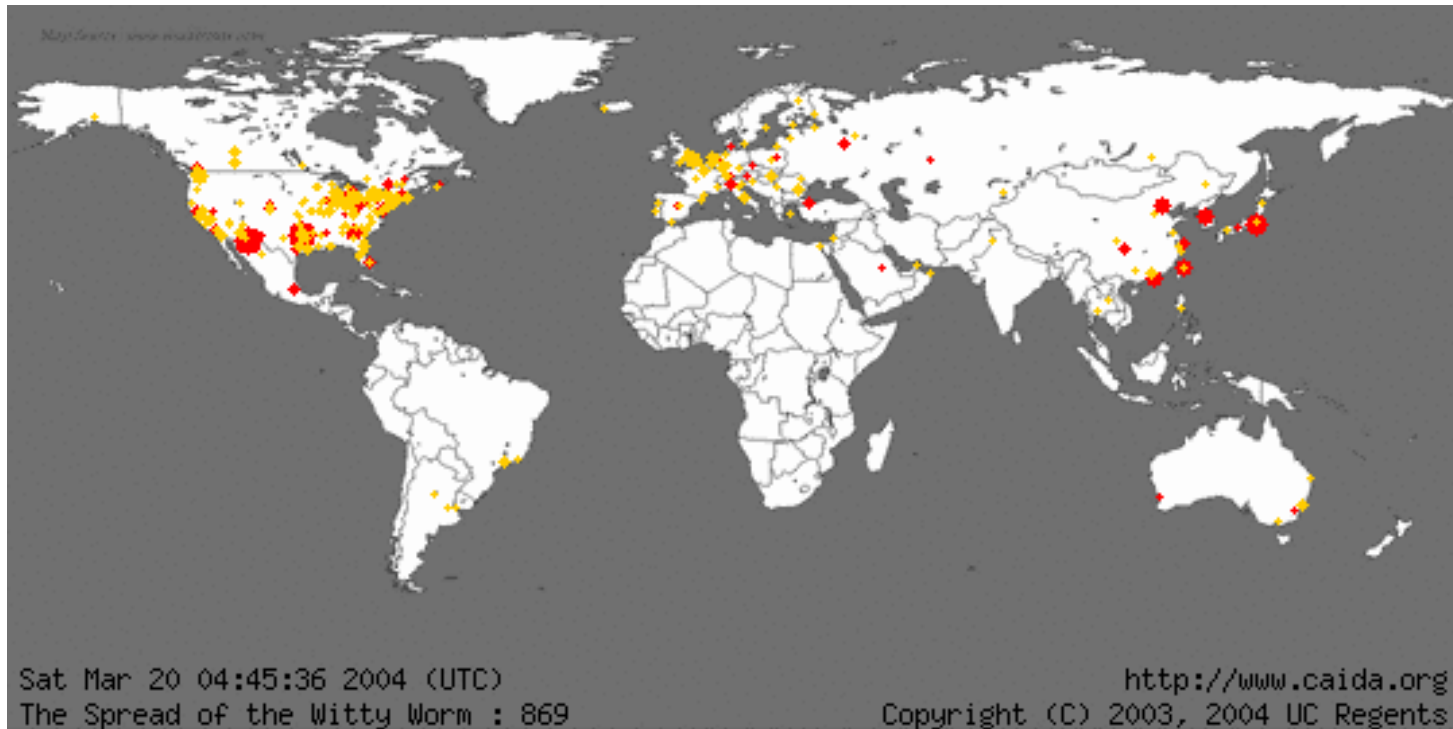


Figure 2-2. Name Resolution Process (without cache search)

Relative size of the TLDs



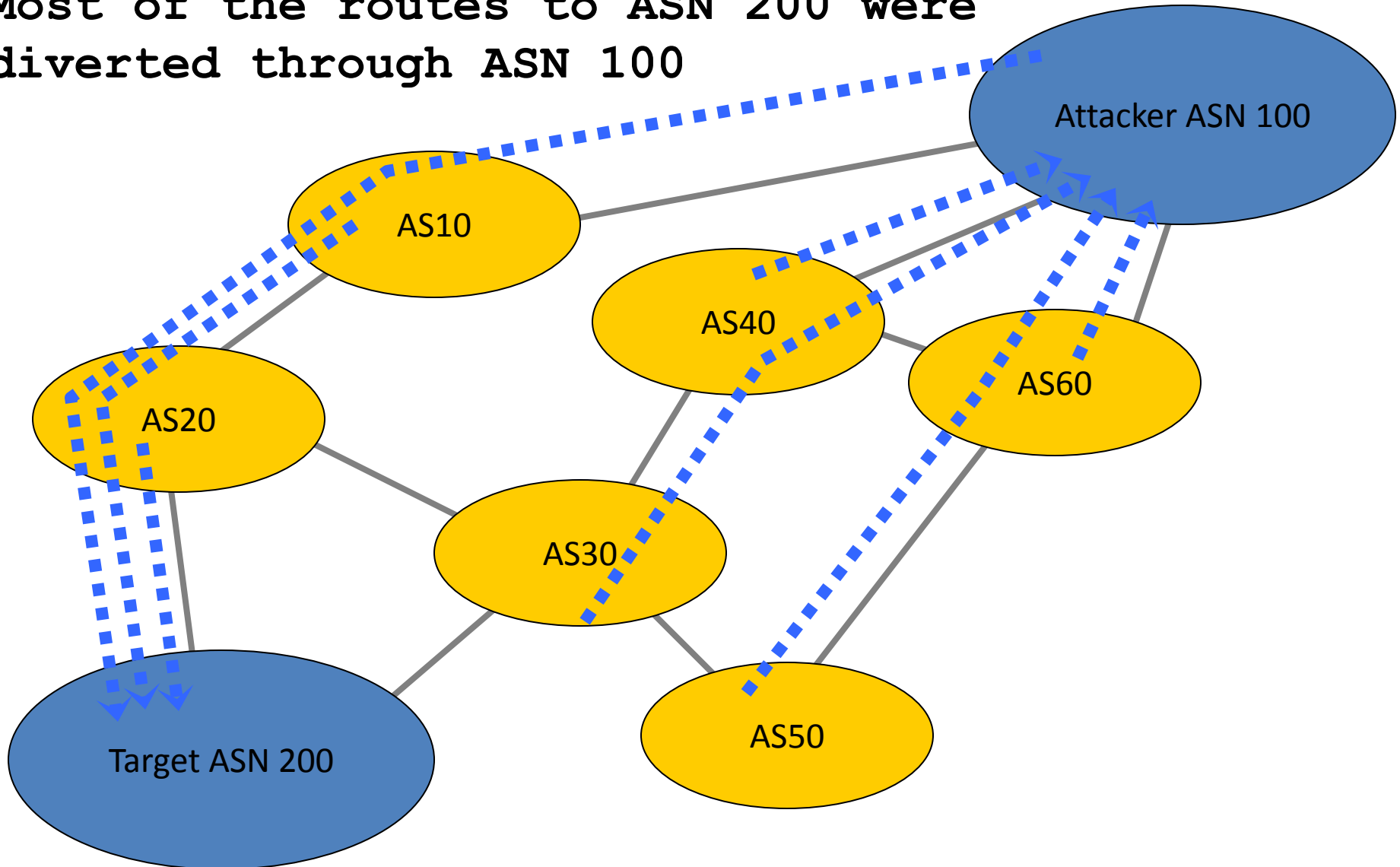
“Witty” (^.^) est un exemple de logiciel malicieux (malware) qui se propagent vite (flash threat)



En rouge les locations infectées dans les premières 60 secondes,
En jaune les locations infectées après 60 secondes.

BGP MITM – Setup Routes

Most of the routes to ASN 200 were diverted through ASN 100



Pakistan Govt. Notice (24 February 2008)



Corrigendum- Most Urgent

GOVERNMENT OF PAKISTAN
PAKISTAN TELECOMMUNICATION AUTHORITY
ZONAL OFFICE PESHAWAR

Plot-11, Sector A-3, Phase-V, Hayatabad, Peshawar.

Ph: 091-9217279- 5829177 Fax: 091-9217254

www.pta.gov.pk

NWFP-33-16 (BW)/06/PTA

February ,2008

Subject: **Blocking of Offensive Website**

Reference: *This office letter of even number dated 22.02.2008.*

I am directed to request all ISPs to immediately block access to the following website

URL: <http://www.youtube.com/watch?v=o3s8jtvvg00>

IPs: 208.65.153.238, 208.65.153.253, 208.65.153.251

Compliance report should reach this office through return fax or at email

peshawar@pta.gov.pk today please.

An IRR (Internet Routing Registry) Update

...Which Should Have Been Questioned

From: db-admin@altdb.net
To: xxx@wyltk-llc.com
ReplyTo: db-admin@altdb.net
Subject: Forwarded mail..... (fwd)
Sent: Aug 7, 2008 9:48 PM

Your transaction has been processed by the IRRd routing registry system.

Diagnostic output:

The submission contained the following mail headers:

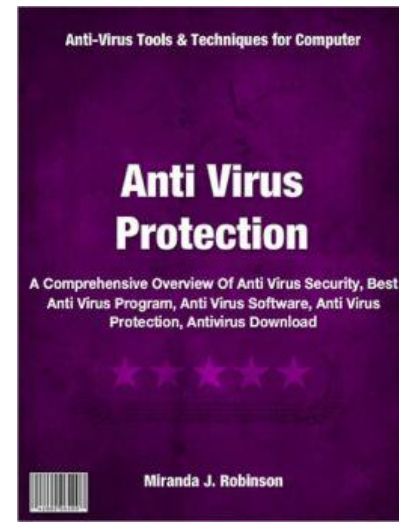
- From: xxx@wyltk-llc.com
- Subject: Forwarded mail..... (fwd)
- Date: Thu, 7 Aug 2008 21:48:53 -0400 (EDT)
- Msg-Id: <Pine.LNX.xxx@wyltk-llc.com>

ADD OK: [route] 24.120.56.0/24 AS26627

If you have any questions about ALTDB,
please send mail to db-admin@altdb.net.

La détection des virus

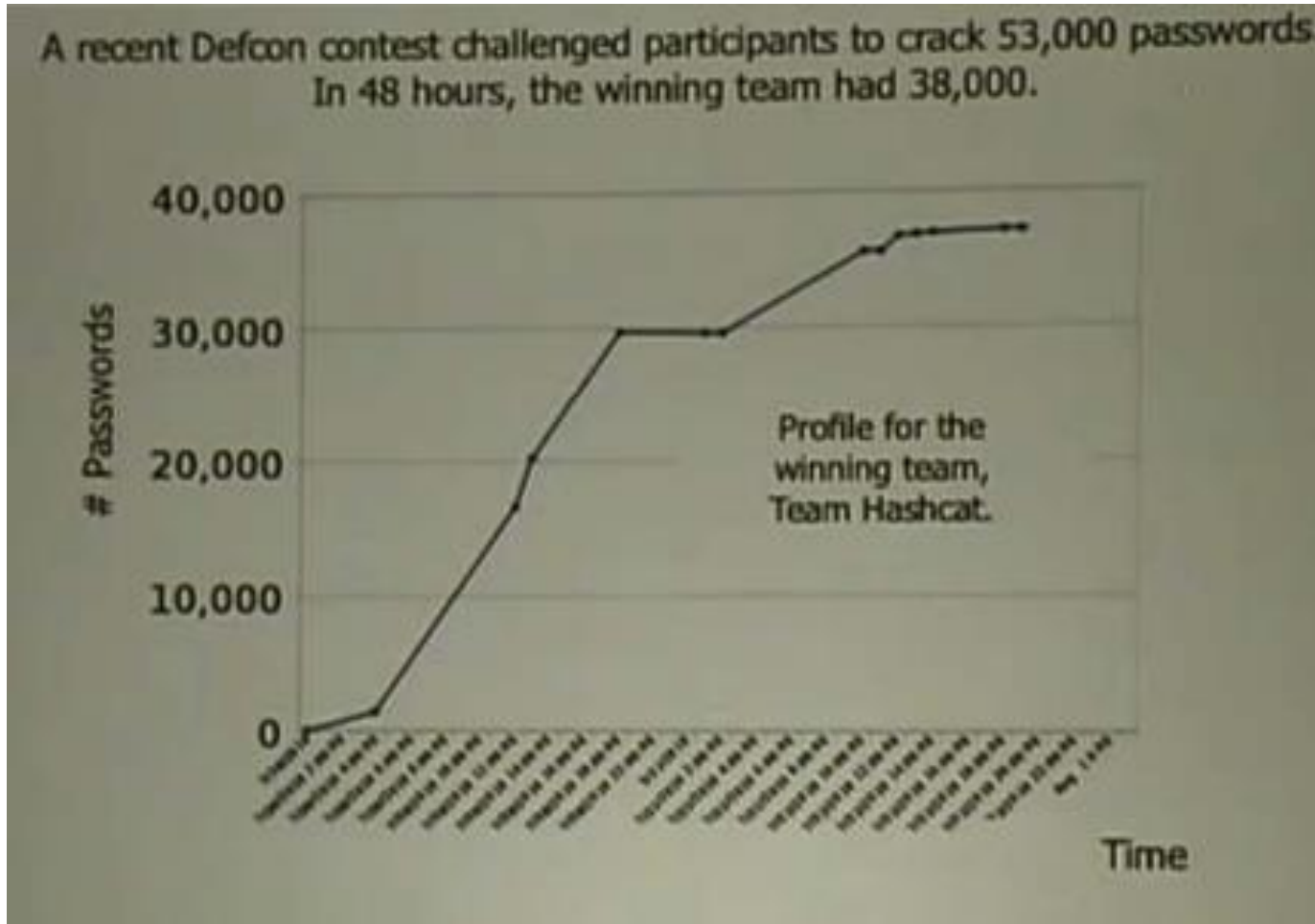
- Exemples de virus difficiles à détecter, pour différentes raisons:
 - Conficker...
 - Zeus, Silentbanker, SpyEye, OddJob, Tatanarg
- Virus avec cibles:
 - Stuxnet (Iran)
 - Ghostnet (Ambassades, Gouvernements)
 - Aurora
 - Agent.btz



Soins intensifs



Deviner les mots de passe



This graph was shown at Schmoocon (2011) by Mudge