The road to Hell…

…is paved with best practices

SCHUBERG PHILIS

Image: Caution, a Creative Commons Attribution Non-Commercial Share-Alike (2.0) image from zippy's photostream

Warning

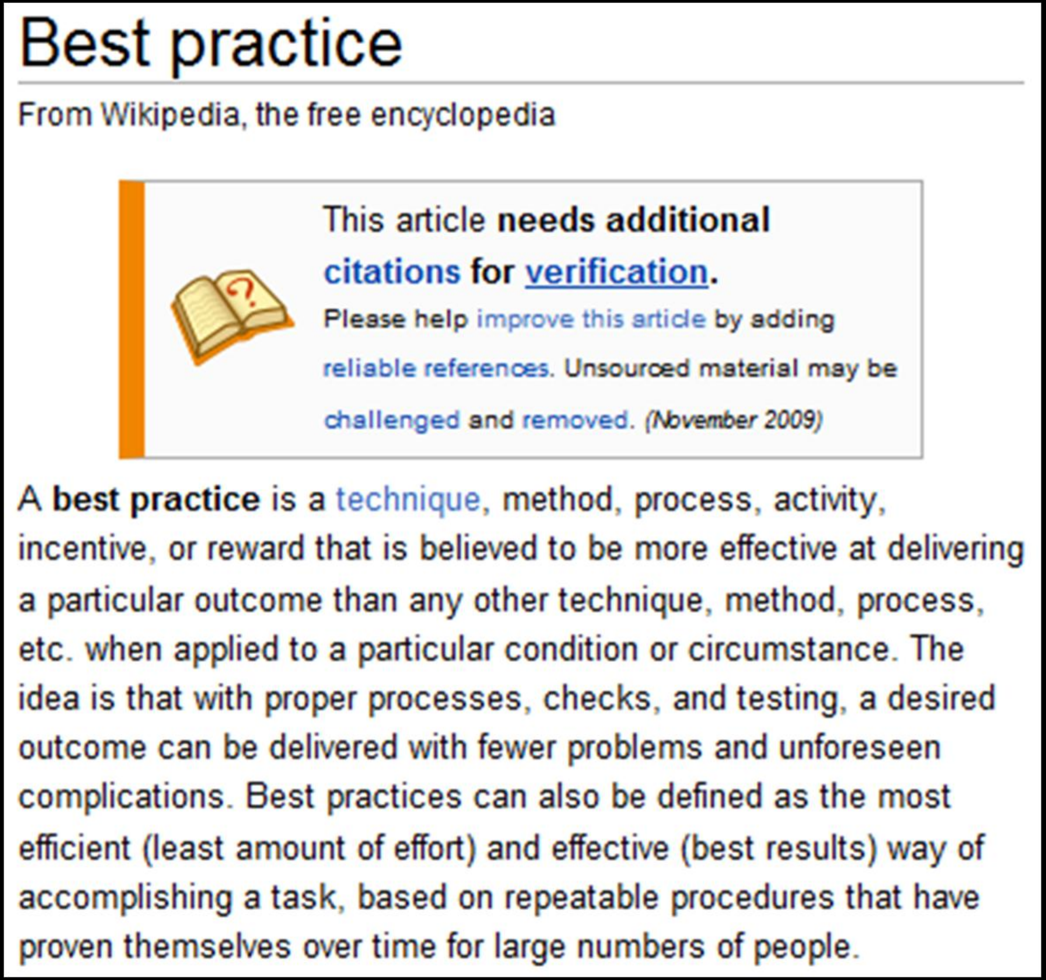
<RANT>

Why…

Not all “best practices” seem to make us more secure.

Often overlooked:

“…when applied to a particular condition or circumstance.”



Best practice

From Wikipedia, the free encyclopedia

This article **needs additional citations for verification.**
Please help improve this article by adding reliable references. Unsourced material may be challenged and removed. *(November 2009)*

A **best practice** is a technique, method, process, activity, incentive, or reward that is believed to be more effective at delivering a particular outcome than any other technique, method, process, etc. when applied to a particular condition or circumstance. The idea is that with proper processes, checks, and testing, a desired outcome can be delivered with fewer problems and unforeseen complications. Best practices can also be defined as the most efficient (least amount of effort) and effective (best results) way of accomplishing a task, based on repeatable procedures that have proven themselves over time for large numbers of people.

Who are we?

Frank Breedijk

- Security Officer at Schuberg Philis
- Author of Seccubus
- Blogging for CupFighter.net

Email:	fbreedijk@schubergphilis.com
Twitter:	@seccubus
Blog:	http://www.cupfighter.net
Project:	http://www.seccubus.com
Company:	http://www.schubergphilis.com

Who are we?

Ian Southam

- » Mission Critical Engineer at Schuberg Philis

Email: isoutham@schubergphilis.com

Company: http://www.schubergphilis.com

We look after the systems that matter…

» Online banking
» Public websites
» Energy Trading
» Portfolio and Risk management
» Mobility Banking
» Online retail
» Enterprise Risk services
» Asset management

Rabobank
moneyou
Deloitte.
ROBECO
ING
ASR nederland
LeasePlan Bank
AIR FRANCE KLM
Eneco
bol.com
NUON VATTENFALL
syntrus achmea

Image: Vicious Circle, a CC NC SA image from metamerist's Flickr stream http://www.flickr.com/photos/94494883@N00/974742/

The rules…

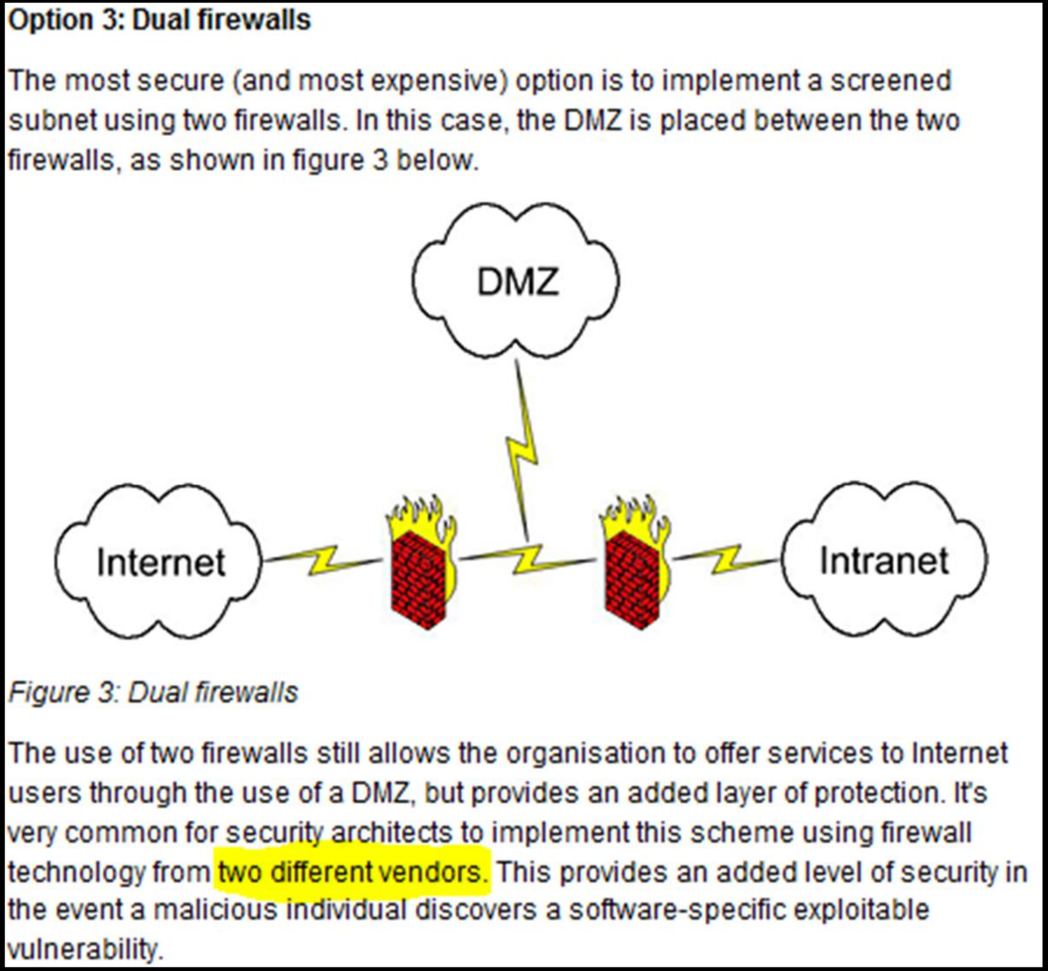
- We will pick a “best practice”
- One of will argue “Pro” the other will argue “Con”
- A game of Rock, Paper, Scissors will determine who gets to choose
- A raise of hands will determine the “winner”

Image from: http://searchnetworking.techtarget.com.au/articles/16554-Choosing-the-right-firewall-topology?topic_id=891

Firewalls from two different vendors…

Reasoning:

» If one vendor has a serious flaw, there will not be a total compromise.



Option 3: Dual firewalls

The most secure (and most expensive) option is to implement a screened subnet using two firewalls. In this case, the DMZ is placed between the two firewalls, as shown in figure 3 below.

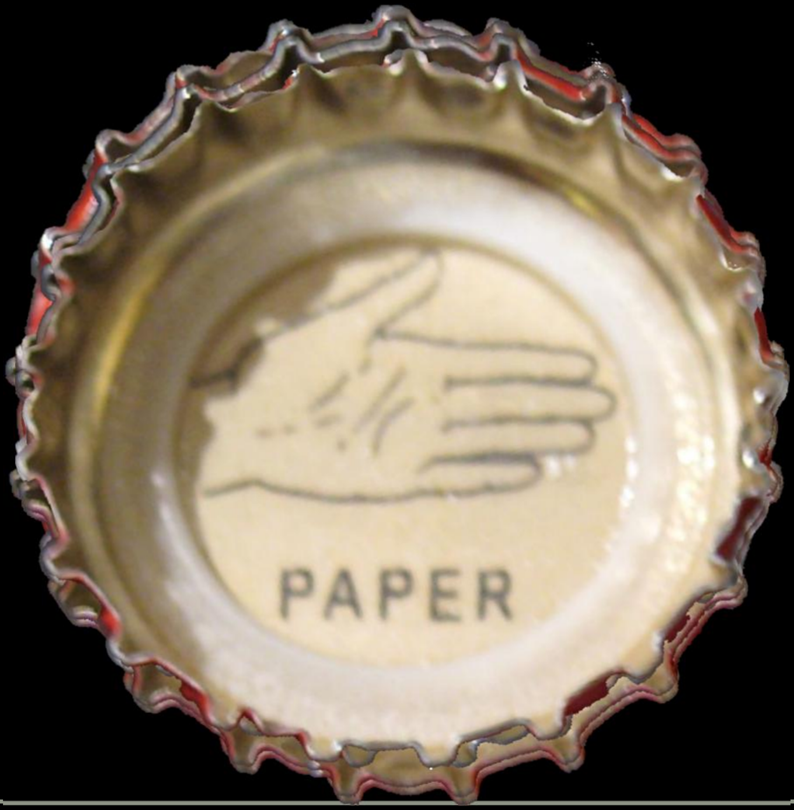
Figure 3: Dual firewalls

The use of two firewalls still allows the organisation to offer services to Internet users through the use of a DMZ, but provides an added layer of protection. It's very common for security architects to implement this scheme using firewall technology from two different vendors. This provides an added level of security in the event a malicious individual discovers a software-specific exploitable vulnerability.

Image: sessions beer bottlecaps, a CC NC SA image from C_Knaus' Flickr stream http://www.flickr.com/photos/40732569106@N01/942653401/

Rock, Paper, Scissors

Ian



Frank

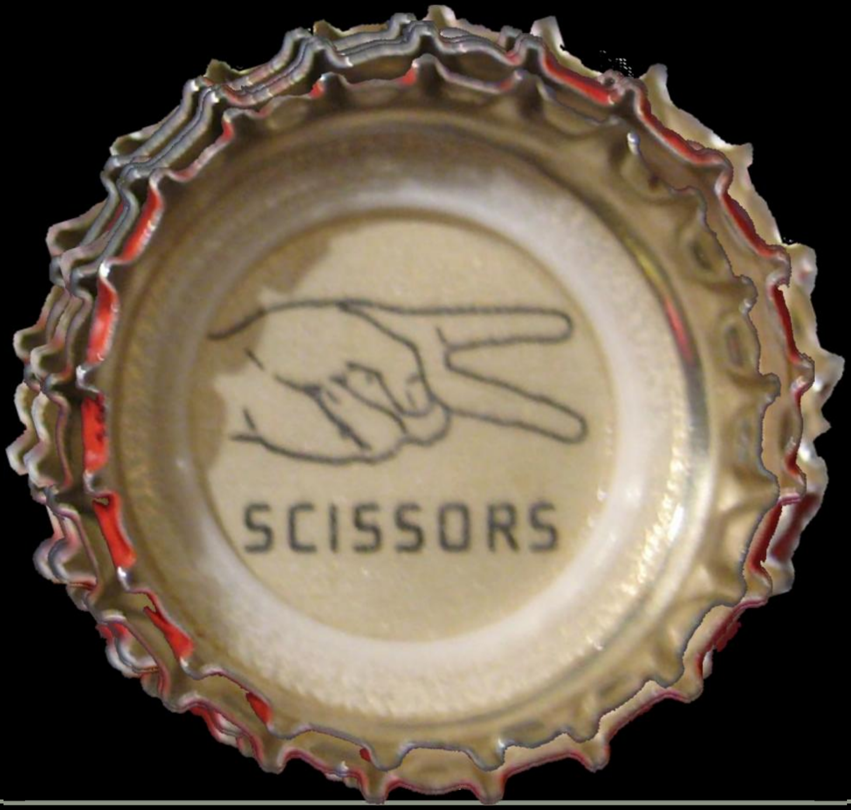


Image: safe safer safest, a Creative Commons Attribution (2.0) image from 20918261@N00's photostream

It’s like two locks on a bicycle

Most bicycle thieves in Amsterdam only know how to quickly open one type of lock

Image: history of missing circles, a Creative Commons Attribution Non-Commercial Share-Alike (2.0) image from camil_t's photostream

But just two locks isn't enough…

Like every technology you need to know how to apply it to benefit from it.

Image from: http://searchnetworking.techtarget.com.au/articles/16554-Choosing-the-right-firewall-topology?topic_id=891

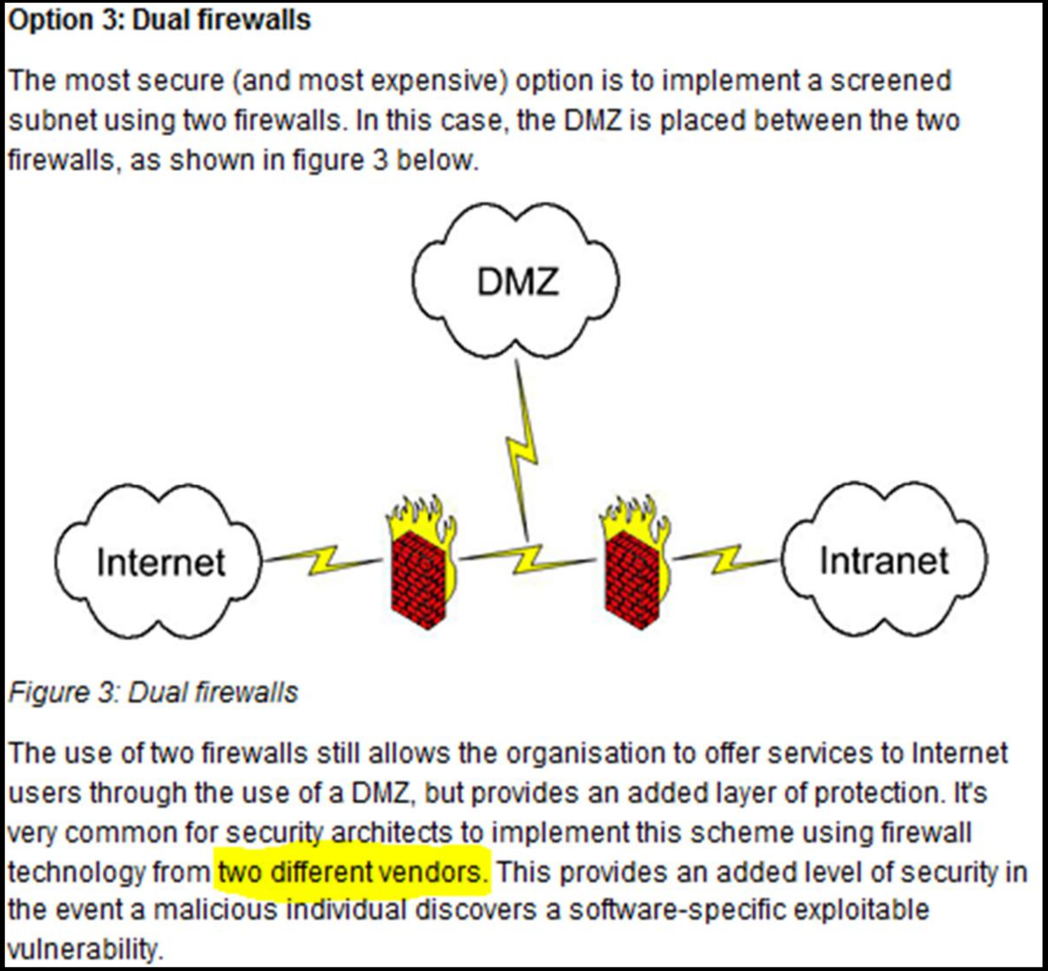
Firewalls from two different vendors…

Reasoning:

- If one vendor has a serious flaw, there will not be a total compromise.

Reality:

- Firewall bypass bugs are rare
- Two rule bases
- Two different technologies
- Most likely outside firewall will pass anything nat-ed behind inside firewall
- Most firewall brand use the same IP stack anyway



Option 3: Dual firewalls

The most secure (and most expensive) option is to implement a screened subnet using two firewalls. In this case, the DMZ is placed between the two firewalls, as shown in figure 3 below.

Figure 3: Dual firewalls

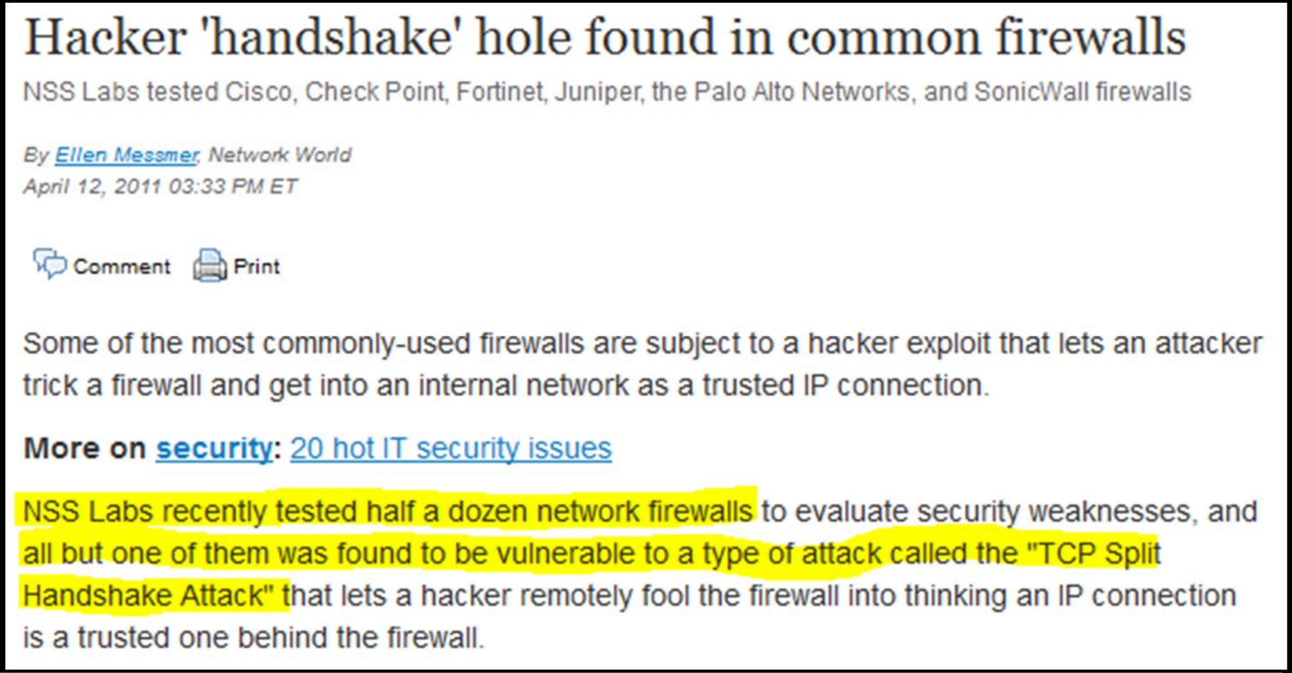
The use of two firewalls still allows the organisation to offer services to Internet users through the use of a DMZ, but provides an added layer of protection. It's very common for security architects to implement this scheme using firewall technology from two different vendors. This provides an added level of security in the event a malicious individual discovers a software-specific exploitable vulnerability.

Source: http://www.networkworld.com/news/2011/041211-hacker-exploit-firewalls.html

Hacker ‘handshake’ hole found in common firewalls

In Februari 2011 NSS Labs tested 6 high end firewalls of 6 different brands

5 out of 6 did not correctly handle the “TCP Split Handshake Attack”



Hacker 'handshake' hole found in common firewalls

NSS Labs tested Cisco, Check Point, Fortinet, Juniper, the Palo Alto Networks, and SonicWall firewalls

By Ellen Messmer, Network World
April 12, 2011 03:33 PM ET

Some of the most commonly-used firewalls are subject to a hacker exploit that lets an attacker trick a firewall and get into an internal network as a trusted IP connection.

More on security: 20 hot IT security issues

NSS Labs recently tested half a dozen network firewalls to evaluate security weaknesses, and all but one of them was found to be vulnerable to a type of attack called the "TCP Split Handshake Attack" that lets a hacker remotely fool the firewall into thinking an IP connection is a trusted one behind the firewall.

Polling Station a CC iamge from James Cridland's Flickr stream
http://www.flickr.com/photos/18378655@N00/4567600547/

Your votes please…

Image: Cypher Disk, a CC NC ND image from Goodimages' Flickr stream
http://www.flickr.com/photos/48734911@N00/798553392/

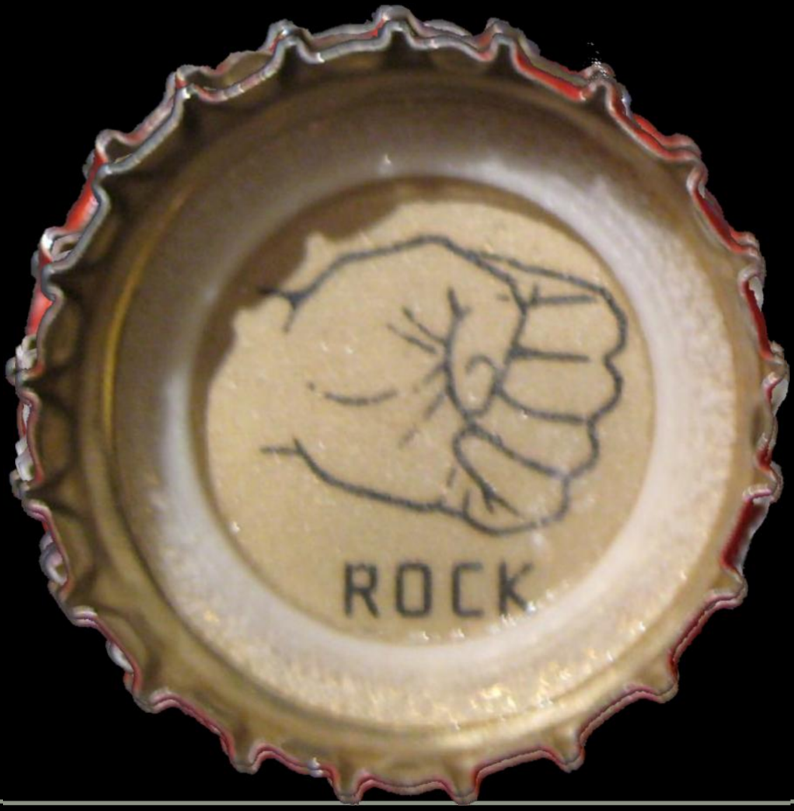
Cryptography

Cypher Disk
2007
A commonly found device, often made of card, wood, plastic or metal. This nice example was made recently with multiple alphabets included - some ancient. I bought this via ebay, April 2007 from the USA. JA

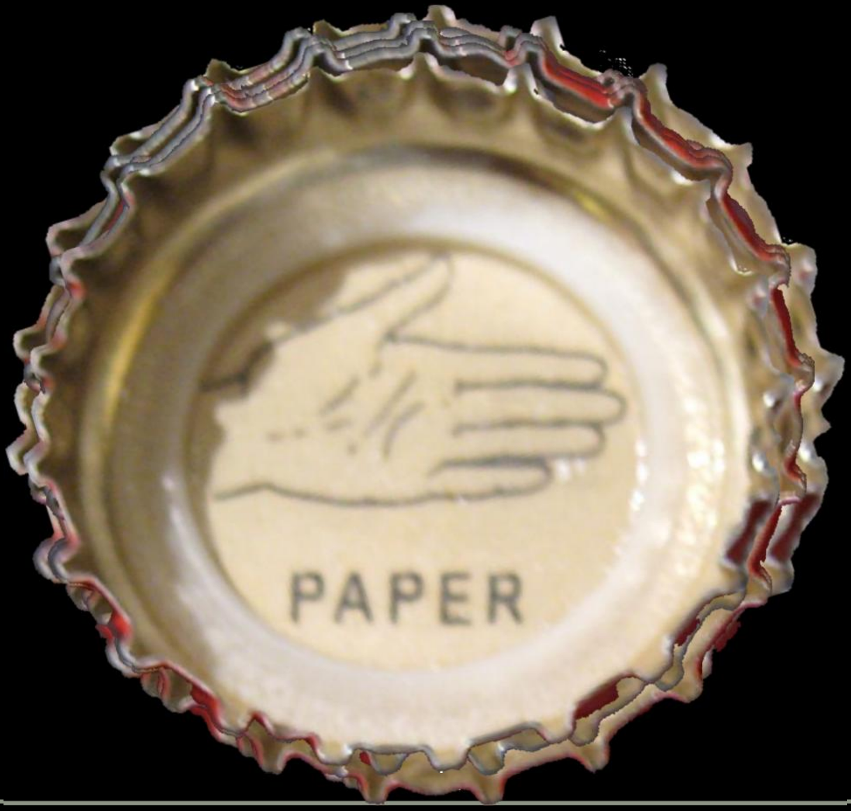
Image: sessions beer bottlecaps, a CC NC SA image from C_Knaus' Flickr stream http://www.flickr.com/photos/40732569106@N01/942653401/

Rock, Paper, Scissors

Ian



Frank

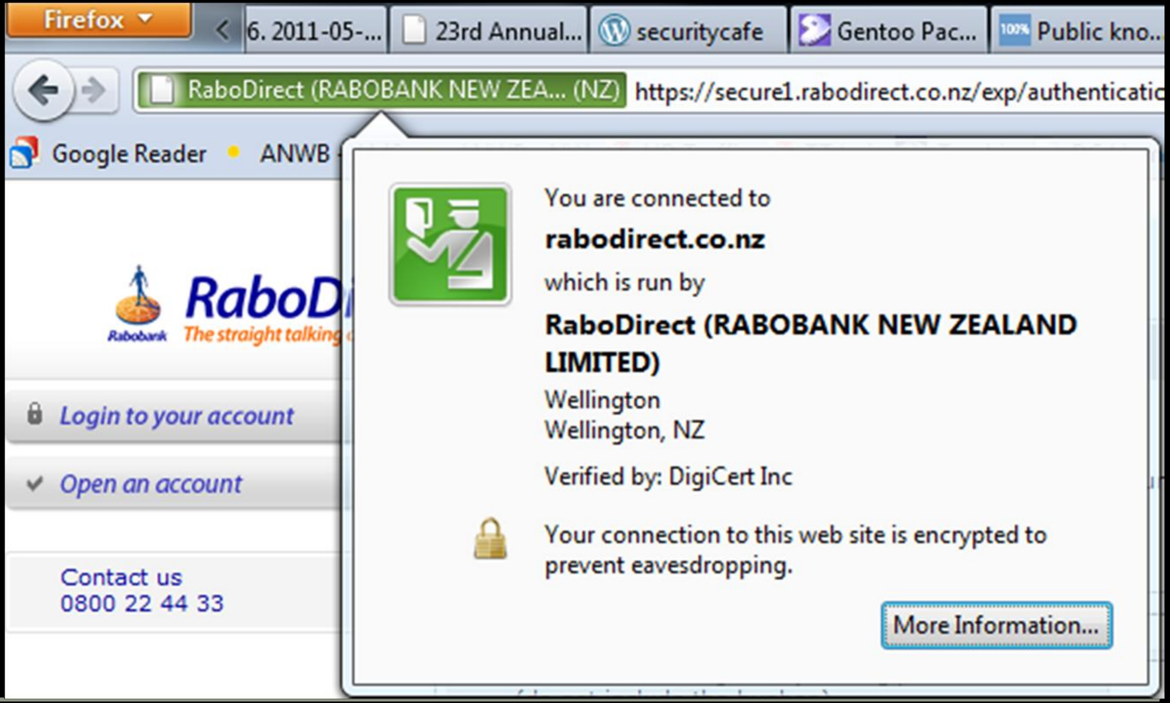


Cryptography just works…

» Do you use the wireless here?

» What do you prefer, telnet or SSH?

» Do you do any online banking?



You are connected to

rabodirect.co.nz

which is run by

RaboDirect (RABOBANK NEW ZEALAND LIMITED)

Wellington
Wellington, NZ

Verified by: DigiCert Inc

Your connection to this web site is encrypted to prevent eavesdropping.

Image: silver bullet, a Creative Commons Attribution Share-Alike (2.0) image from eschipul's photostream

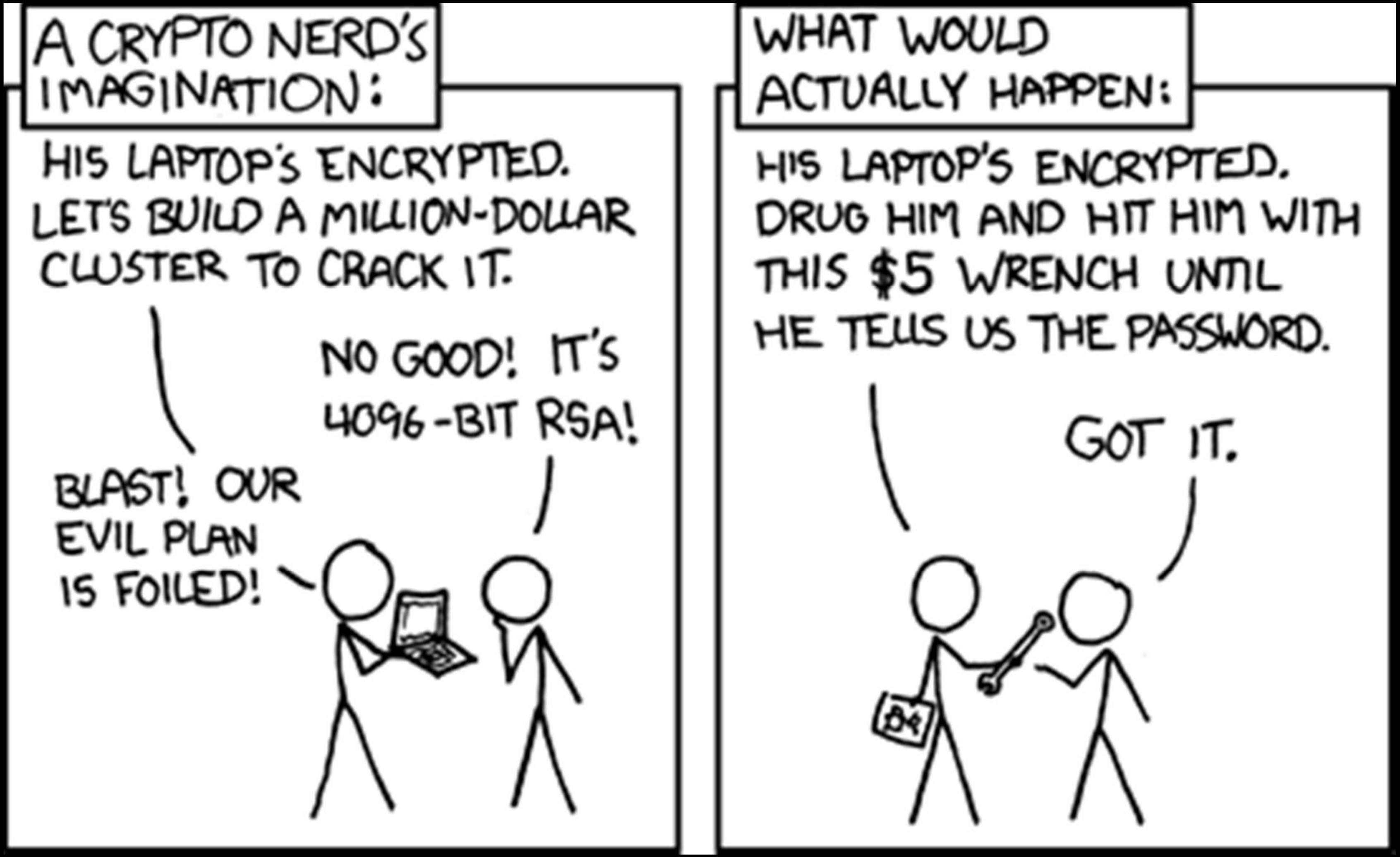
Encryption is not a silver bullet…

Many attacks:

- Key theft
- Brute force
- Social engineering
- End point compromise
- Man in the browser attack
- Man in the Middle attack
- Downgrade attack
- Rubber hose cryptology
- Side channel attack
- Cache timing attack
- Replay attacks

Image: Security, cartoon #538 from xkcd.com

What about encryption…


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Old School Voting. The way it should be. a CC NC imsge from Just Us 3's Flickr stream http://www.flickr.com/photos/73835037@N00/292239798/

Your votes please…

A password key? A CC ND image from Dev.Arka's Flickr stream
http://www.flickr.com/photos/70417422@N00/808187848/

Passwords

A password must have:

- A least 8 characters
- At least three of the following:
  - Uppercase
  - Lowercase
  - Numeral
  - Special character
- Expire every 90 days
- Not be equal to the last 12 passwords

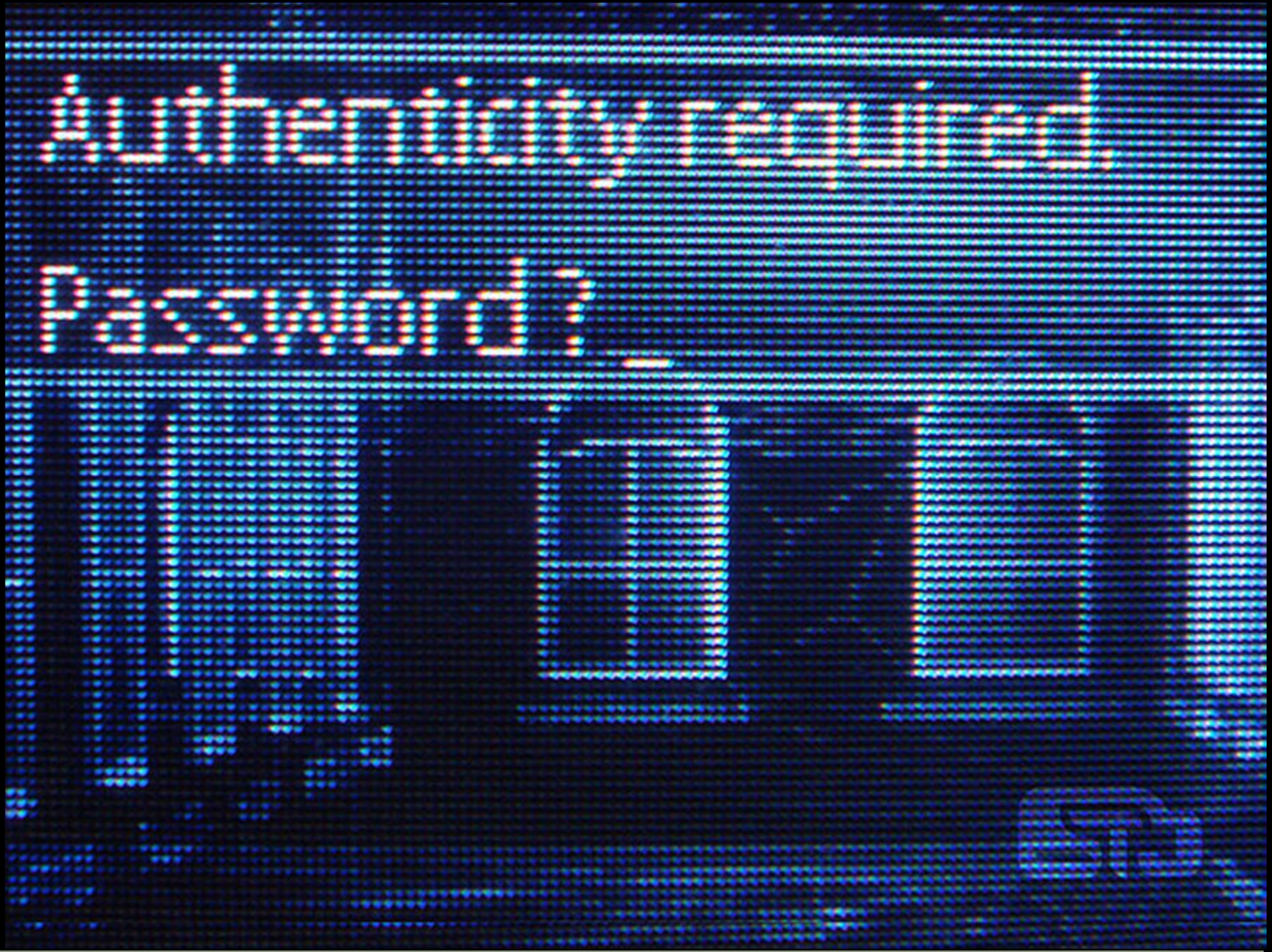
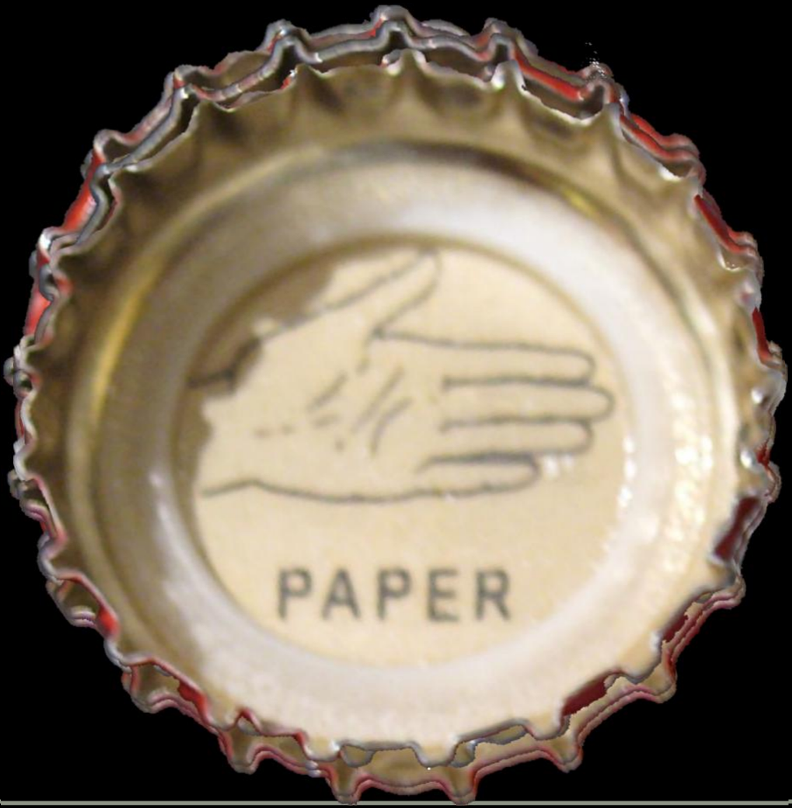


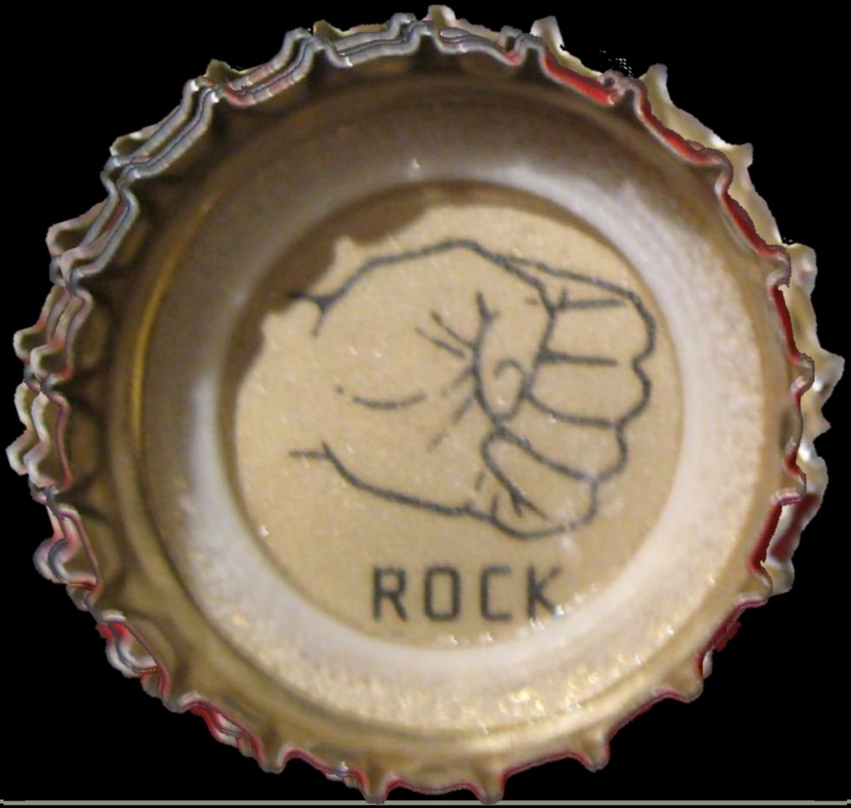
Image: sessions beer bottlecaps, a CC NC SA image from C_Knaus' Flickr stream http://www.flickr.com/photos/40732569106@N01/942653401/

Rock, Paper, Scissors

Ian

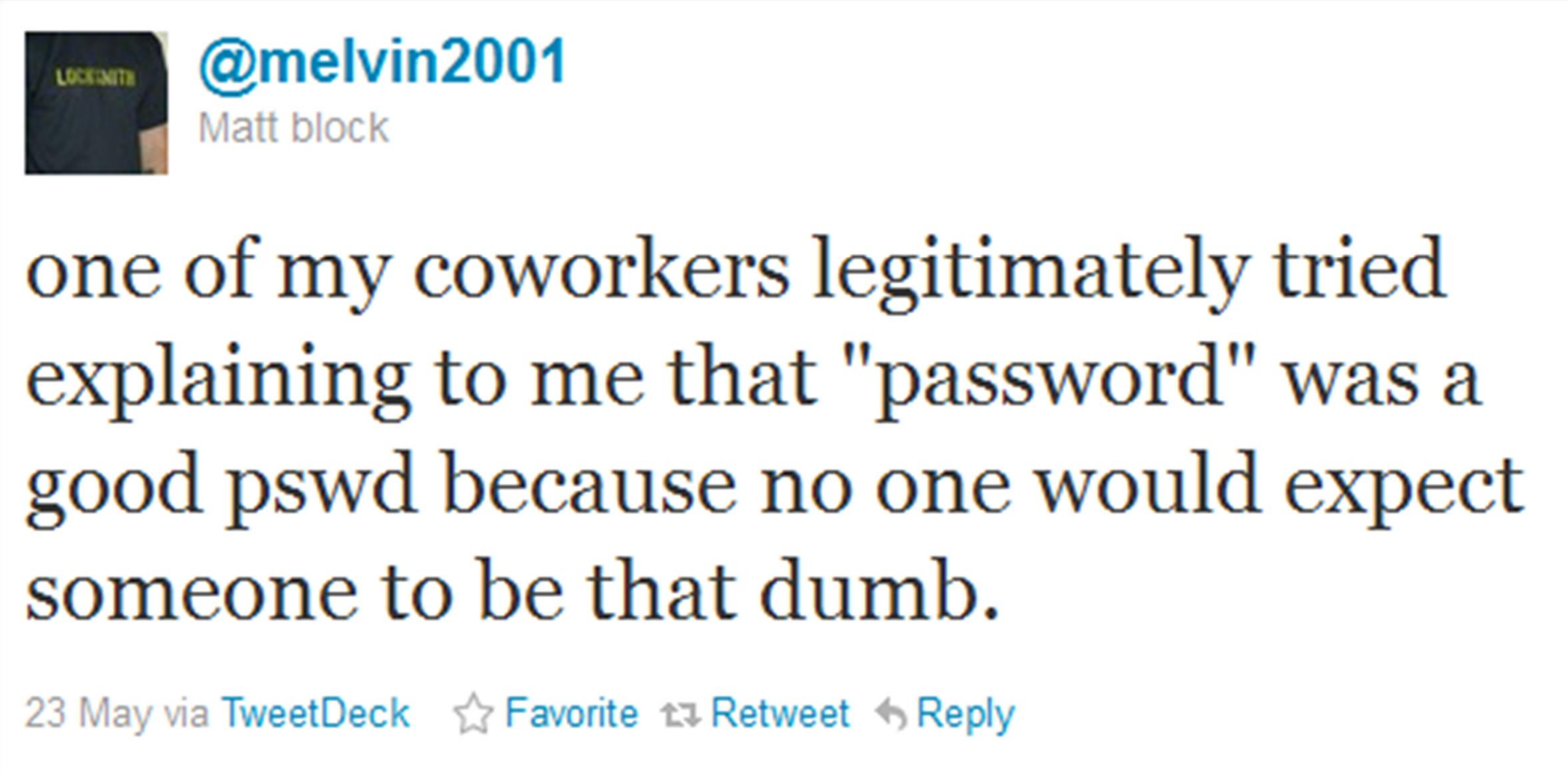


Frank



http://twitter.com/#!/melvin2001/status/72648791949443073

They prevent this...



@melvin2001

Matt block

one of my coworkers legitimately tried explaining to me that "password" was a good pswd because no one would expect someone to be that dumb.

23 May via TweetDeck

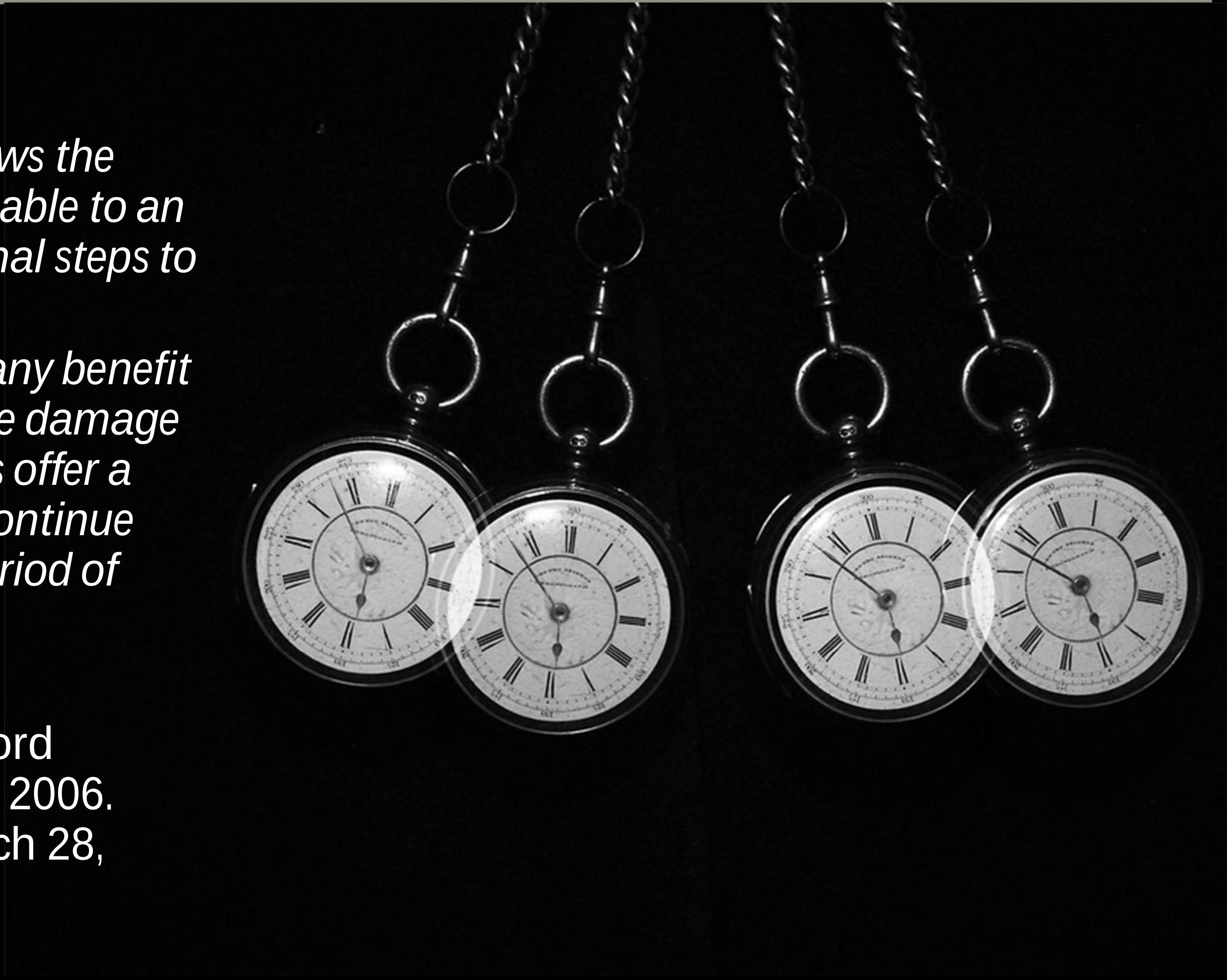
If a “security measure” is too hard… it will more likely hurt

Password requirements:	Likely password:
7 characters	welcome
1 capital	Welcome
1 numeral	W3lc0m3
1 special	W3lc0m3!
10 characters	W3lc0m3!!!
30 days max – cannot use last 12	Welcome01!

The predictability of human behavior can aid in password cracking attempts.
See the work of Matt Weir:
"Using Probabilistic Techniques to Aid in Password Cracking Attacks“
http://tinyurl.com/RTHpasswd

Image: Swing time, a Creative Commons Attribution (2.0) image from Dave-F's photostream

Password expiration…



Changing passwords frequently narrows the window within which an account is usable to an attacker before he has to take additional steps to maintain access.

... Password expiration does not offer any benefit when an attacker wants to do all of the damage that he's going to do right now. It does offer a benefit when the attacker intends to continue accessing a system for an extended period of time.

S. Alexander, Jr. In defense of password expiration. Post to LOPSA blog, April 2006. http://lopsa.org/node/295 as of March 28, 2010.

The reality

The Security of Modern Password Expiration: An Algorithmic Framework en Empirical Analysis. Y Zhang, F. Monrose and M. K. Reiter, University of North Carolina at Chapel Hill

- » Using a dataset of over 7700 accounts, we assess the extent to which passwords that users choose to replace expired ones pose an obstacle to the attacker's continued access.
- » … framework by which an attacker can search for a user's new password from an old one.

[http://tinyurl.com/RTHpasswd2]

- » Using this framework, we confirm previous conjectures that the effectiveness of expiration in meeting its intended goal is weak.
- » …susceptibility of accounts to our search techniques even when passwords in those accounts are individually strong,
- » and the extent to which use of particular types of transforms predicts the transforms the same user might employ in the future.
- » We believe our study calls into question the continued use of expiration and, in the longer term, provides one more piece of evidence to facilitate a move away from passwords altogether.

Image: Hangmand, A Creative Commons, Attribution, Non-Commercial, Share-Alike images from iwinatcookie's photostream

Complex passwords…

Assumption: a 'complex' password is harder to crack then a 'simple' one…

Objectif Sécurité offers online password cracking demo based on rainbow tables and SSD…

- Empty password – 2 seconds
- 72@Fee4S@mura! – 5 seconds
- (689!!!<>"QTHp – 8 seconds
- *mZ?9%^jS743:! – 5 seconds
- T&p/E$v-O6,1@} – 11 seconds

http://tinyurl.com/RTHpasswd3
http://tinyurl.com/RTHpasswd4

a tribute to all who helped make this day wonderful! A CC NC ND image from nathij's Flickr stream http://www.flickr.com/photos/8458705@N04/2983707616/

No voting necessary…

Image: Never use easy –to-guess PINs a Creative Commons, Attribution, Non-commercial No Derivative Works image from kioan's photostream

Our (personal/honest) opinion about passwords…

- Should not be able to predictable
  - Birthday
  - Mothers maiden name
  - Name of you cat
- Expiring a password regularly does not add much
- You account should be blocked if somebody is guessing you password
- If 'they' have the hashes you are toast
- PIN numbers:
  - 4 digits
  - Non-complex
  - Never expire

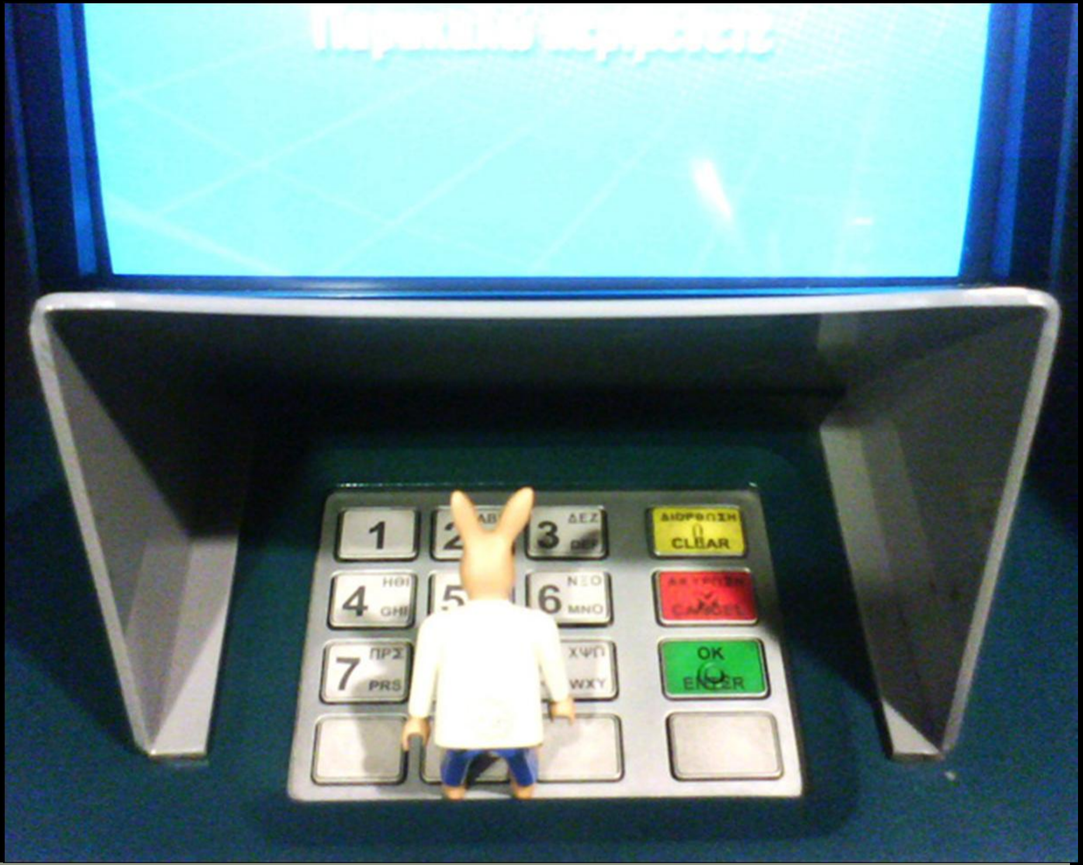


Image by Frank Breedijk

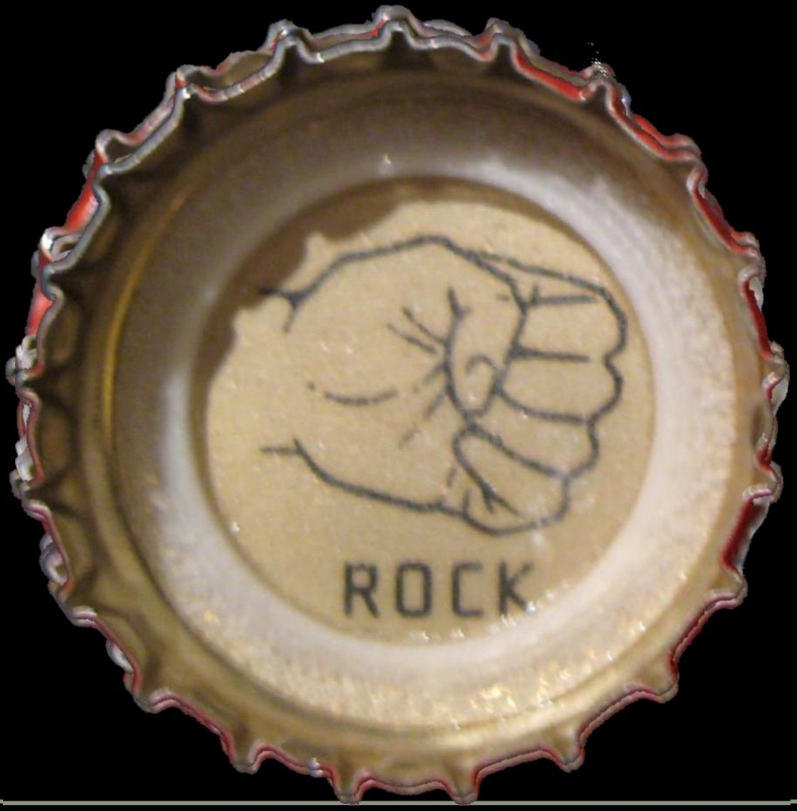
There is strength in numbers…

“Limit the number of system administrators”

Image: sessions beer bottlecaps, a CC NC SA image from C_Knaus' Flickr stream http://www.flickr.com/photos/40732569106@N01/942653401/

Rock, Paper, Scissors

Ian



Frank

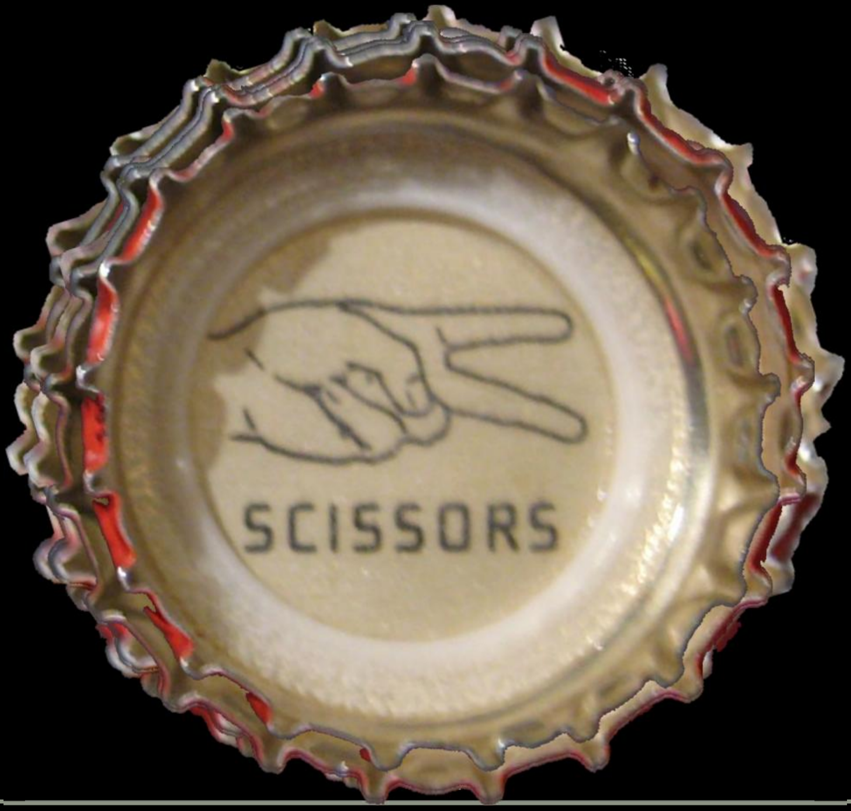


Image by Frank Breedijk

There is strength in numbers…

“Limit the number of system administrators”

- You can prove a computer system is secure
- You cannot prove a human is secure
- Ergo: The less ‘insecure’ super users have, the more secure my system is…

SCHUBERG PHILIS

What is the right number of administrators…

5

20

25

47

35

50

18

17

53

6

42

35

15

120

19

33

11

28

Images by Frank Breedijk

Does this consider the level of the system administrators?

But, are all animals equal…

Image: Being John Malcovich movie poster

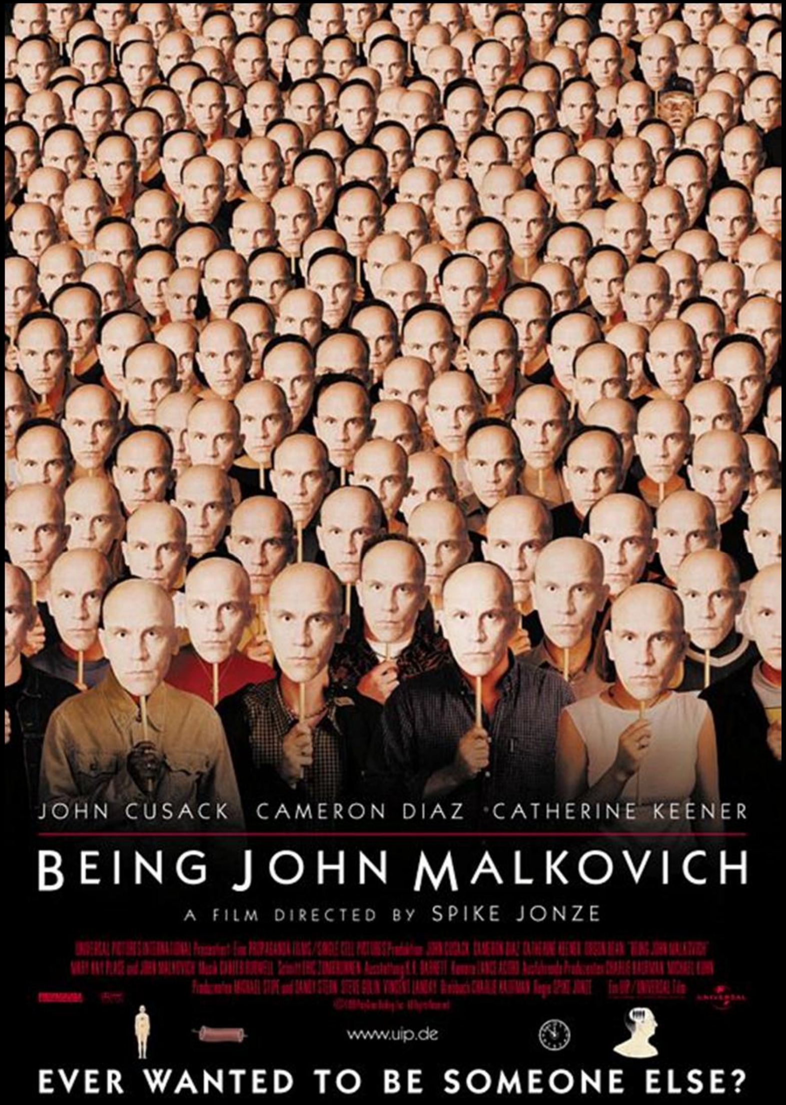
Please don’t force me to…

It would be easy…

The auditors would be happy…

I could do my job…

…it would be so wrong!


JOHN CUSACK CAMERON DIAZ CATHERINE KEENER
BEING JOHN MALKOVICH
A FILM DIRECTED BY SPIKE JONZE
www.uip.de
EVER WANTED TO BE SOMEONE ELSE?

Thumbs-down a CC image from the Italian voice's Flickr stream
http://www.flickr.com/photos/77476789@N00/2059598643/

Your votes please…

Image: Perita, a Creative Commons Attribution Non-Commercial Share-Alike (2.0) image from ournew's photostream

What’s the solution?

Know your administrators…

Set clear rules

Make it obvious when rules are about to be broken

Monitor

Use system logging

Log Changes

Log in multiple places

Keep you admin happy

Peer review

Image: Threads 140.365, a Creative Commons Attribution Non-Commercial No-Derivative-Works (2.0) image from stephangeyer's photostream

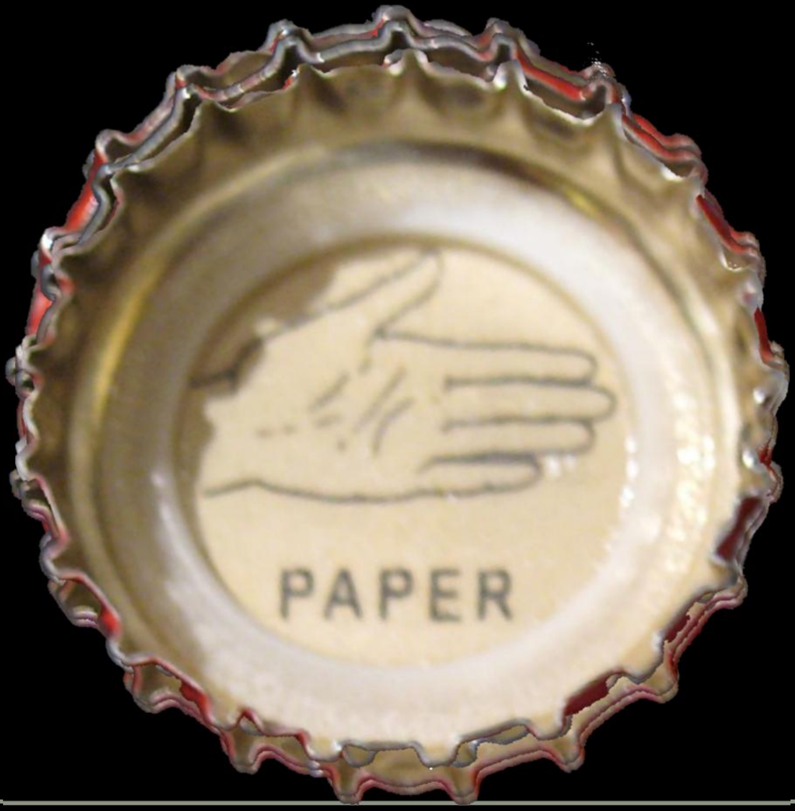
Limit remote access…

“Permission for remote access to **** must be strictly limited to those specific employees who have a strong business need for the access.”

Image: sessions beer bottlecaps, a CC NC SA image from C_Knaus' Flickr stream http://www.flickr.com/photos/40732569106@N01/942653401/

Rock, Paper, Scissors

Ian



Frank

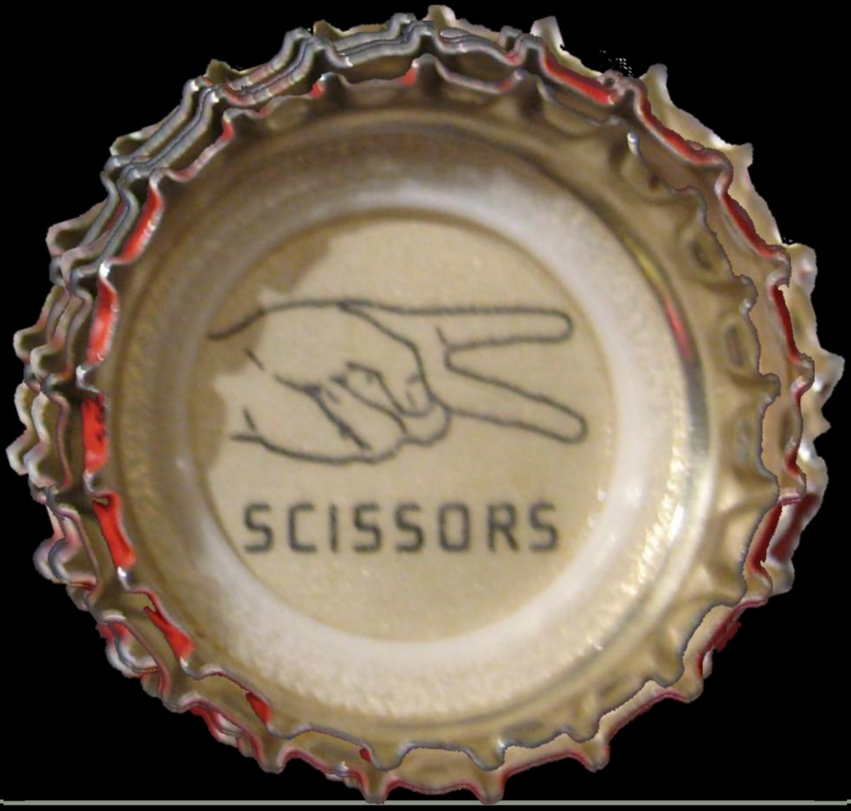


Image: Threads 140.365, a Creative Commons Attribution Non-Commercial No-Derivative-Works (2.0) image from stephangeyer's photostream

Limit remote access…

“Permission for remote access to **** must be strictly limited to those specific employees who have a strong business need for the access.”

Why:

- Prevent data loss
- You have to come in to commit fraud…
- Duress

Can you really stop data “leaks”?

People will try to work from home anyway.

CD-R, USB, MicroSD, SmartPhone, PDA, Portable Harddisk, Printout or simply mail it home.

Memories, PenDrives...., a Creative Commons Attribution Non-Commercial No-Derivative-Works (2.0) image from kikiprinci's photostream

Photo-A-Day #982f 12/16/07, a Creative Commons Attribution Non-Commercial Share-Alike (2.0) image from abennett96's photostream

Keeping an eye on you…

How would you make sure that the person watching me understands what I'm doing?

Would it be impossible to backdoor a system while somebody is watching you?

What is the chance an administrator backdoors a system just so he "can do his job" ?

Image: South Beach Sisters, a Creative Commons Attribution Non-Commercial (2.0) image from adwriter's photostream

Duress

If you are working from home they can make you do stuff at gunpoint…

Image: Old Modem Front, a Creative Commons Attribution (2.0) image from rexroof's photostream

Teleworking has advantages

Remote system administration =

Faster response time +

More dedicated staff +

Better uptime +

Better maintained system

=

Better security

Election Knight a CC NC ND image from Jonathan_W's Flickr stream
http://www.flickr.com/photos/30072283@N00/4585529054/

Your votes please…

Two Brave English Seagulls on Holiday a CC BY NC ND image from aurelio.asiain's Flick stream http://www.flickr.com/photos/75008966@N00/1250799618/

No more good cop, bad cop…

We could not find any Pro arguments for the following best practices…

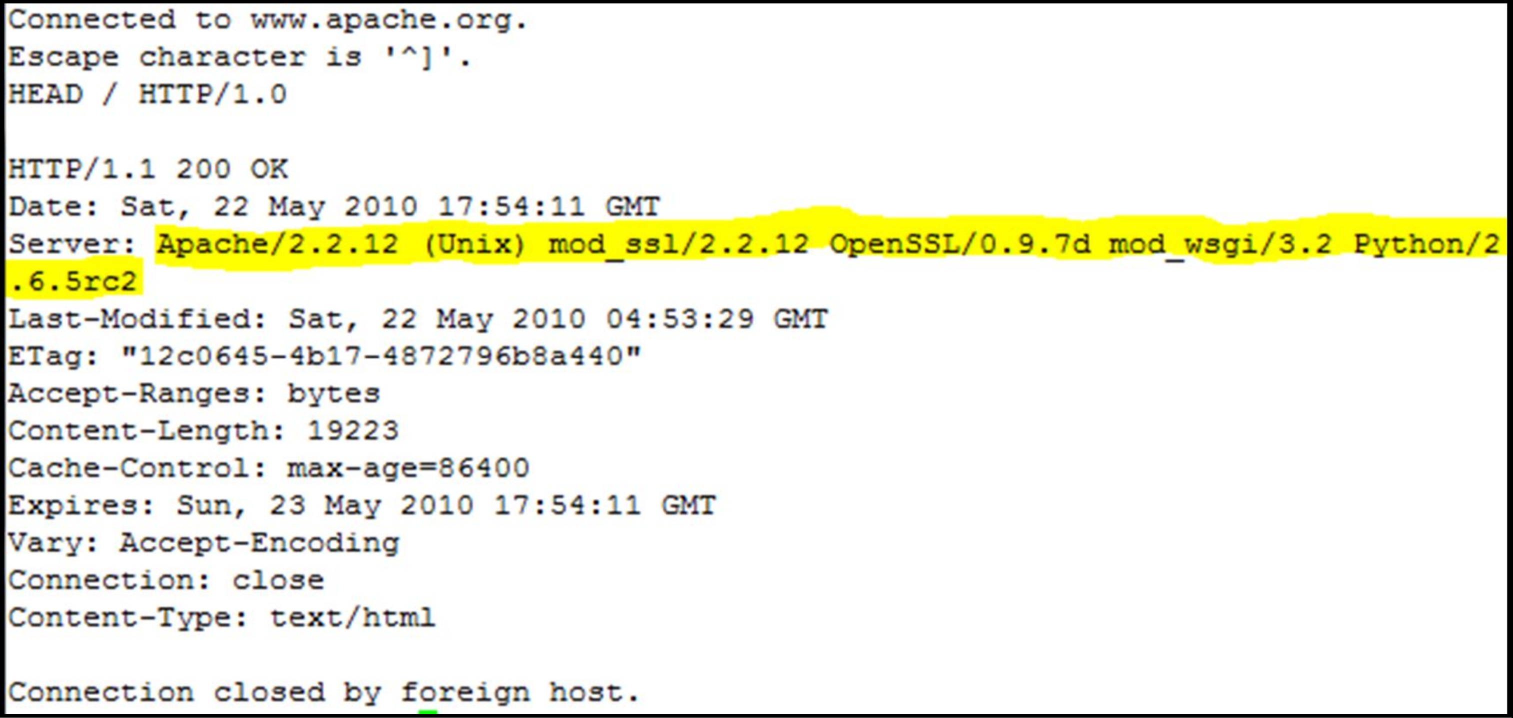
Remove all identifying banners

O.K. disclosing exact versions is bad…

But what about just displaying the products:

- Apache
- X-powered-by: ASP.NET
- OpenSSH

Won’t they just try all?

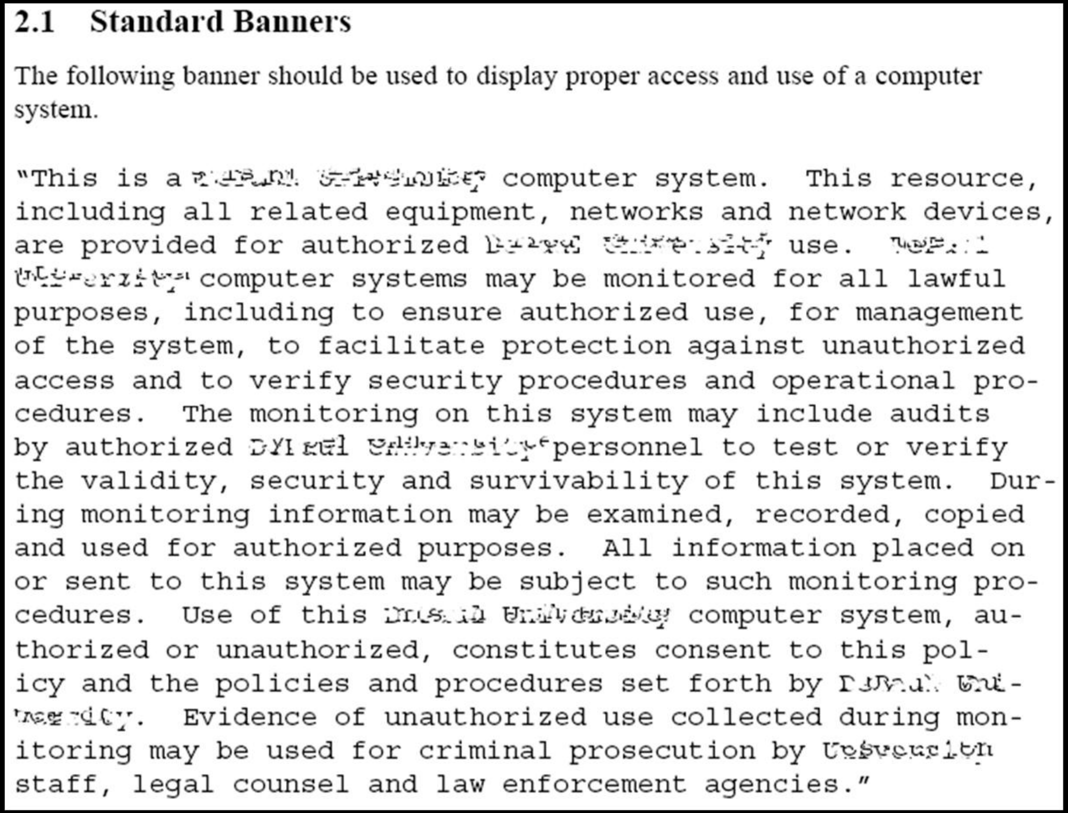


```
Connected to www.apache.org.
Escape character is '^]'.
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Date: Sat, 22 May 2010 17:54:11 GMT
Server: Apache/2.2.12 (Unix) mod_ssl/2.2.12 OpenSSL/0.9.7d mod_wsgi/3.2 Python/2
.6.5rc2
Last-Modified: Sat, 22 May 2010 04:53:29 GMT
ETag: "12c0645-4b17-4872796b8a440"
Accept-Ranges: bytes
Content-Length: 19223
Cache-Control: max-age=86400
Expires: Sun, 23 May 2010 17:54:11 GMT
Vary: Accept-Encoding
Connection: close
Content-Type: text/html

Connection closed by foreign host.
```

What about warning banners?

You must annoy user and administrators by displaying a large annoying legal banner prior to login.

And it tells me its an interesting system, and who owns it even before I have logged in.



2.1 Standard Banners

The following banner should be used to display proper access and use of a computer system.

"This is a [illegible] computer system. This resource, including all related equipment, networks and network devices, are provided for authorized [illegible] use. [illegible] computer systems may be monitored for all lawful purposes, including to ensure authorized use, for management of the system, to facilitate protection against unauthorized access and to verify security procedures and operational procedures. The monitoring on this system may include audits by authorized [illegible] personnel to test or verify the validity, security and survivability of this system. During monitoring information may be examined, recorded, copied and used for authorized purposes. All information placed on or sent to this system may be subject to such monitoring procedures. Use of this [illegible] computer system, authorized or unauthorized, constitutes consent to this policy and the policies and procedures set forth by [illegible]. Evidence of unauthorized use collected during monitoring may be used for criminal prosecution by [illegible] staff, legal counsel and law enforcement agencies."

Image: pong undead!!!, a Creative Commons Attribution Non-Commercial Share-Alike (2.0) image from astio's photostream

Ping

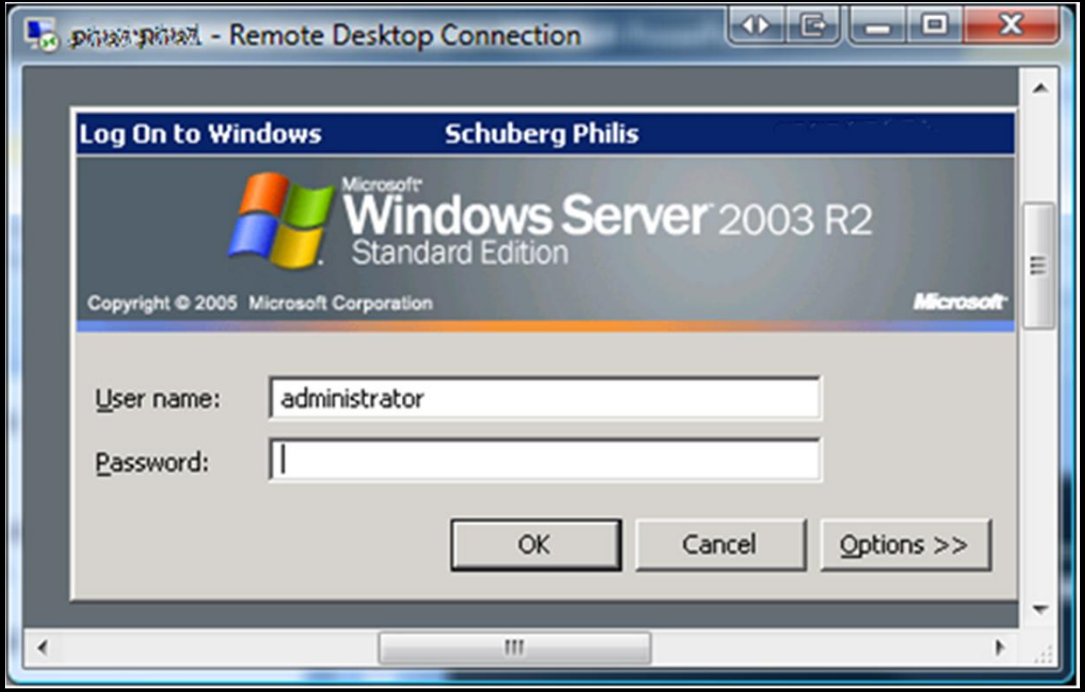
A lot of systems on the internet cannot be pinged anymore…

Great:

- I know the systems IP
- I know its not working
- I cannot ping it
- I can still do a tcptraceroute

Why?

Security making life too hard…



[redacted] - Remote Desktop Connection

Log On to Windows Schuberg Philis

User name: administrator

Password:

You cannot paste a password into an RDP login box

Consequences:

- » I set up a really hard administrator password
- » I put it in the password vault
- » I now have to type 15 random characters to gain access
- » I may start to remember this password
- » I may start to use weaker passwords
- » Maybe I will write the password down

Image: 105. 283, a Creative Commons Attribution Non-Commercial (2.0) image from pwn's photostream

Don’t take away my tools…

- » Removing telnet (client)
- » Remove development tools
- » Remove security tools
  - Nmap?
  - Ping?
  - Traceroute?
  - OpenSSL?
- » Taking SUID from ping

Image: lubbock_track_regionals_2010147, a Creative Commons Attribution Non-Commercial Share-Alike (2.0) image from jduty's photostream

Don’t turn system administration into an obstacle race…

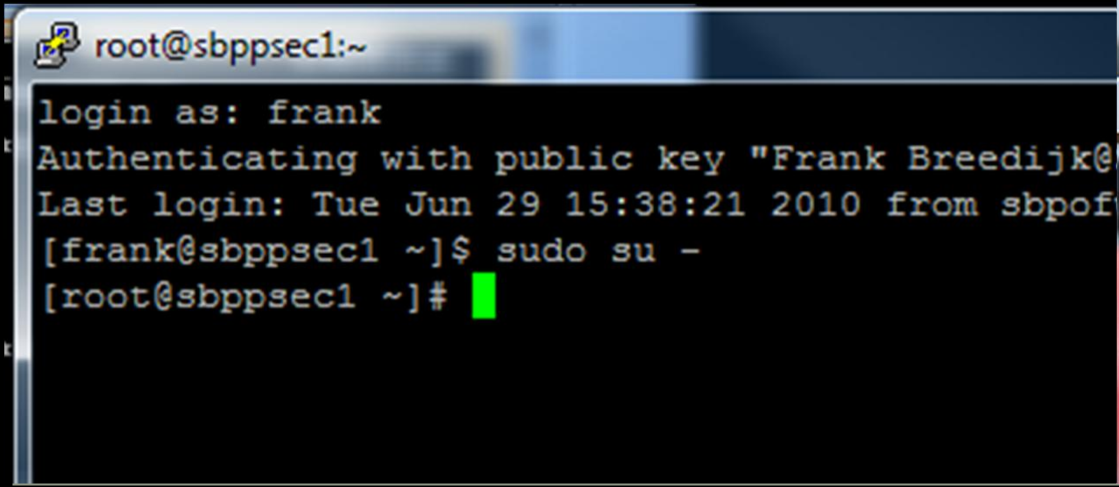
If your only users are system administrators why would you:

» Make home directory 600

» Make roots home directory 100

» Restrict access to /var/log

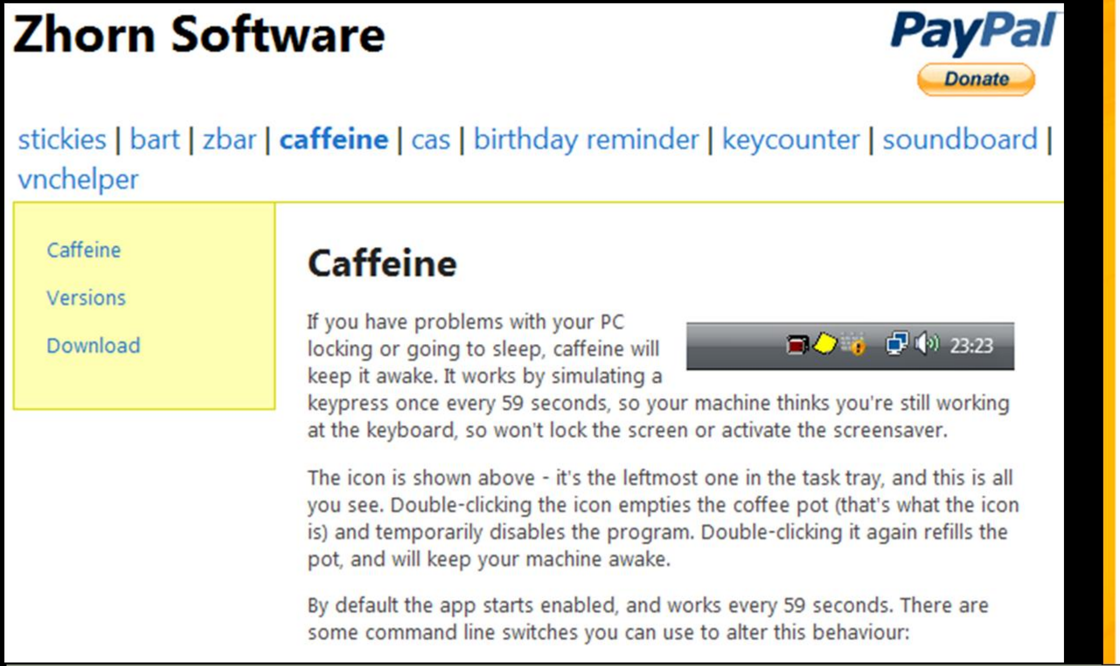
» Etc…



```
login as: frank
Authenticating with public key "Frank Breedijk@
Last login: Tue Jun 29 15:38:21 2010 from sbpof
[frank@sbppsec1 ~]$ sudo su -
[root@sbppsec1 ~]#
```

Idle session time out…

It’s just there to piss users off.



Zhorn Software

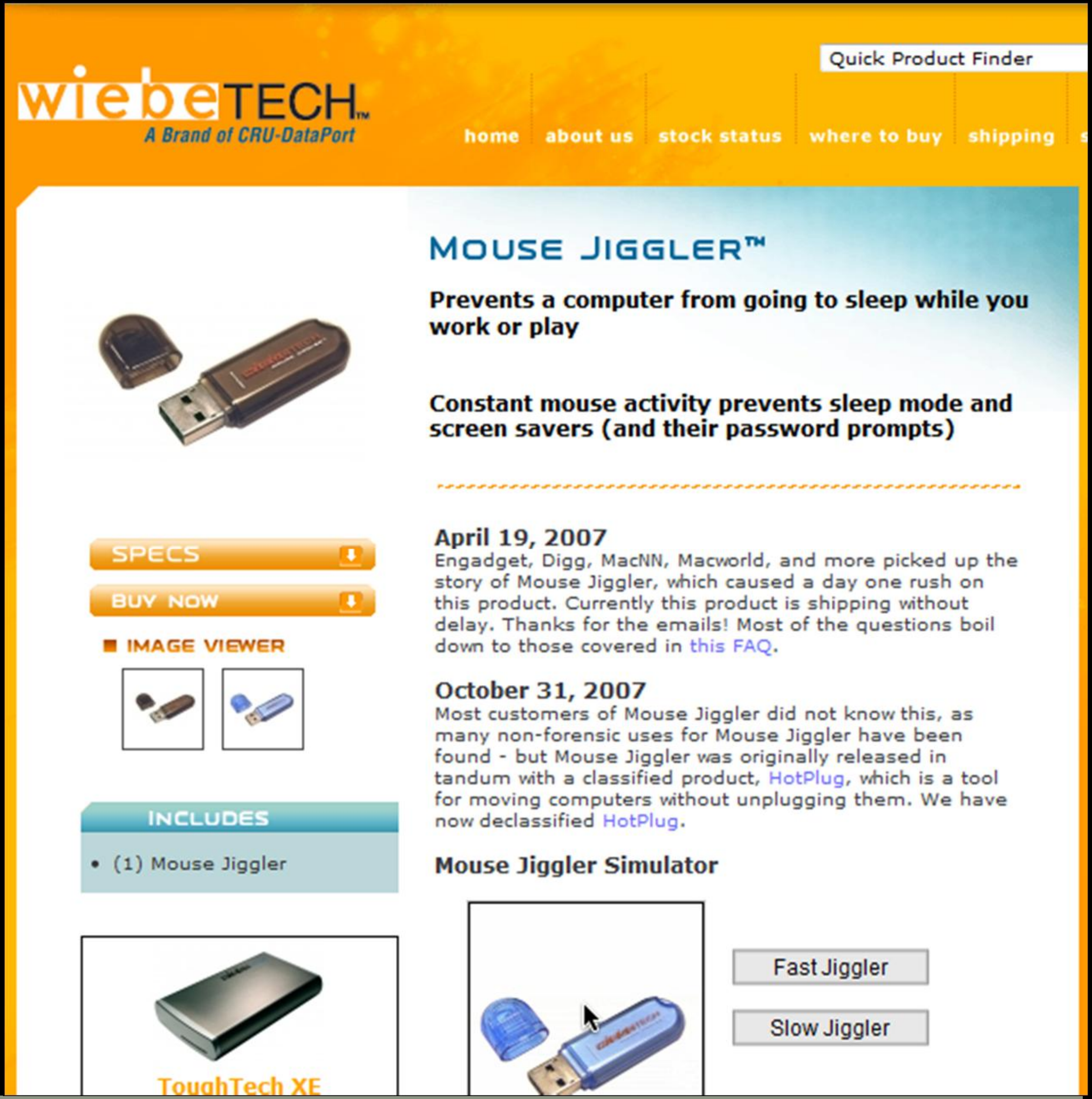
stickies | bart | zbar | **caffeine** | cas | birthday reminder | keycounter | soundboard | vnchelper

Caffeine

If you have problems with your PC locking or going to sleep, caffeine will keep it awake. It works by simulating a keypress once every 59 seconds, so your machine thinks you're still working at the keyboard, so won't lock the screen or activate the screensaver.

The icon is shown above - it's the leftmost one in the task tray, and this is all you see. Double-clicking the icon empties the coffee pot (that's what the icon is) and temporarily disables the program. Double-clicking it again refills the pot, and will keep your machine awake.

By default the app starts enabled, and works every 59 seconds. There are some command line switches you can use to alter this behaviour:



MOUSE JIGGLER™

Prevents a computer from going to sleep while you work or play

Constant mouse activity prevents sleep mode and screen savers (and their password prompts)

- (1) Mouse Jiggler

April 19, 2007
Engadget, Digg, MacNN, Macworld, and more picked up the story of Mouse Jiggler, which caused a day one rush on this product. Currently this product is shipping without delay. Thanks for the emails! Most of the questions boil down to those covered in this FAQ.

October 31, 2007
Most customers of Mouse Jiggler did not know this, as many non-forensic uses for Mouse Jiggler have been found - but Mouse Jiggler was originally released in tandum with a classified product, HotPlug, which is a tool for moving computers without unplugging them. We have now declassified HotPlug.

Mouse Jiggler Simulator

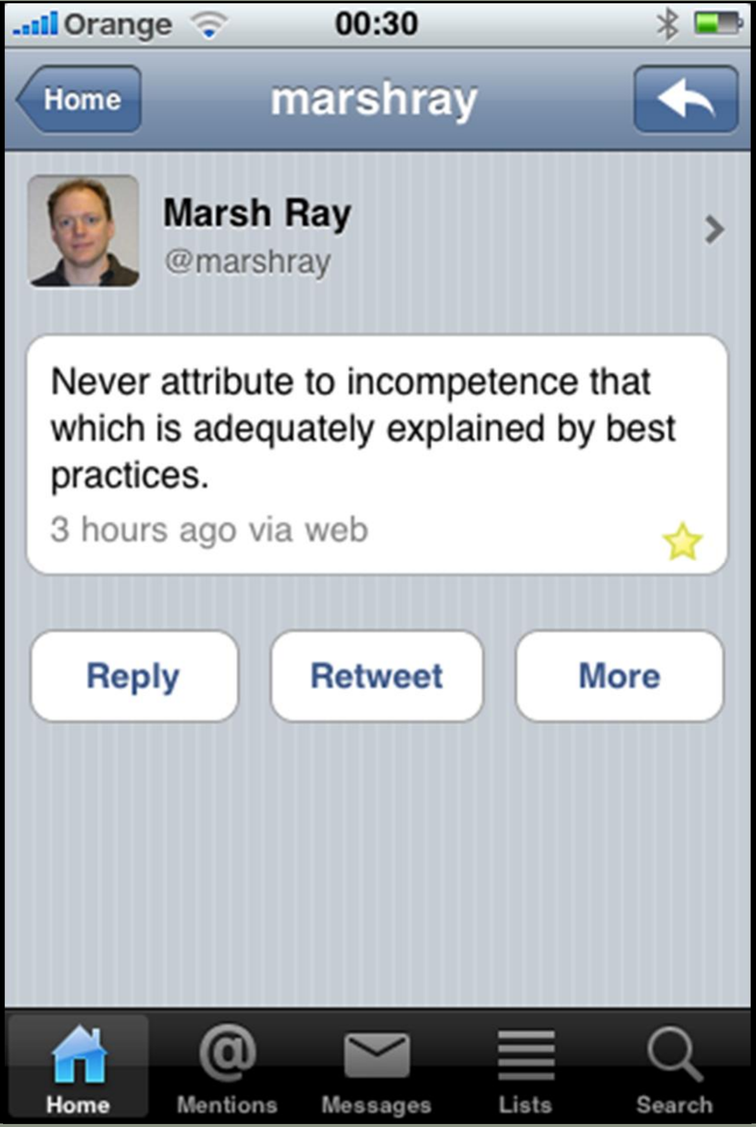
Picture by Frank. Tweet by @marshray: http://twitter.com/#!/marshray/status/14780585932

Single sign on…

It is bad because: One credential will give you access to everything…

What is the alternative?

Passwords.xls?



Never attribute to incompetence that which is adequately explained by best practices.

3 hours ago via web

Creative Commons Attribution Non-Commercial No-Derivative-Works (2.0) image from _brilho-de-conta's photostream

No access to social media…

URL filtering:

- Twitter, FaceBook, Craigslist, WordPress
- Webmail, Hotmail, GMail
- YouTube, Break.com, Failblog
- Google Cache

I'm so glad I have UMTS

Image: EVIL a Creative Commons Attribution Non-Commercial Share-Alike (2.0) image from krazydad's photostream

Firewall log monitoring

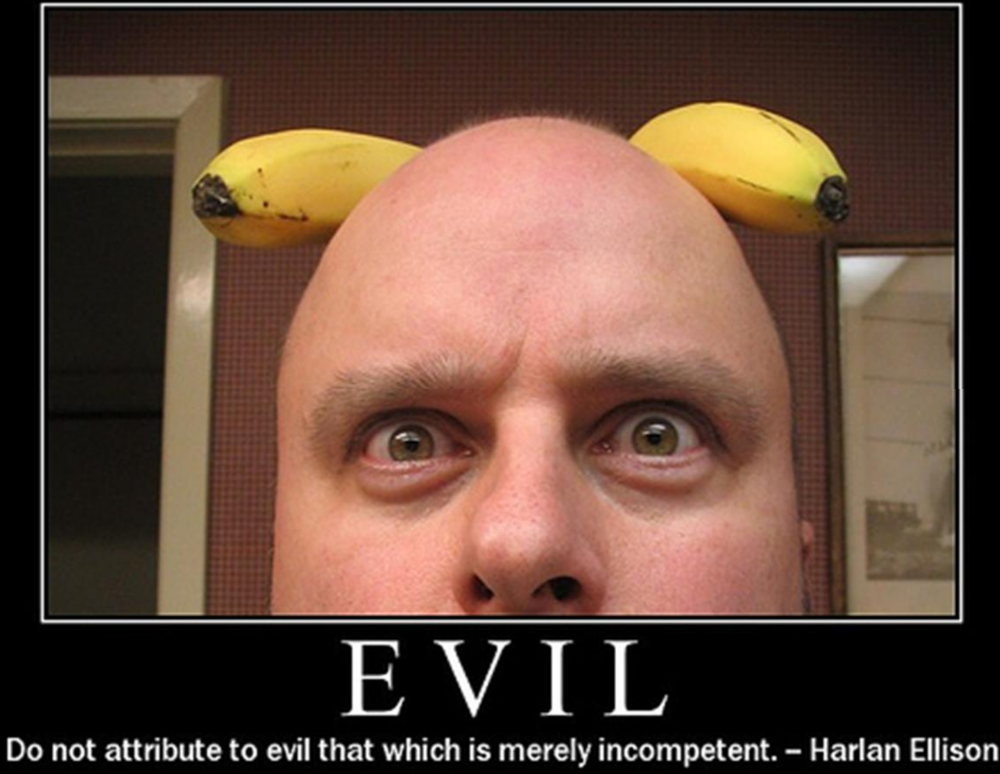
You must monitor your firewall traffic logs…

Why?

If it is passed by firewall it was allowed in the first place…

If it got rejected, it got rejected, why worry about it?

There is no “evil bit” (except in RFC 3514)


EVIL
Do not attribute to evil that which is merely incompetent. – Harlan Ellison

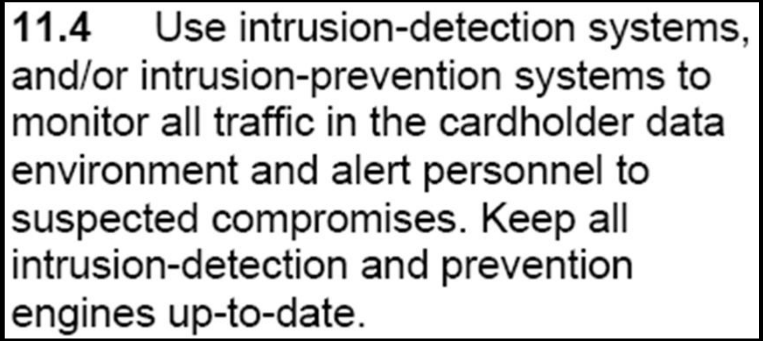
Intrusion Detection System (IDS)

Proving the Internet is evil™

Protecting the network by blacklisting all evil…

IDS/IPS is not all bad:

» It is very good for detection anomalies



11.4 Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic in the cardholder data environment and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines up-to-date.

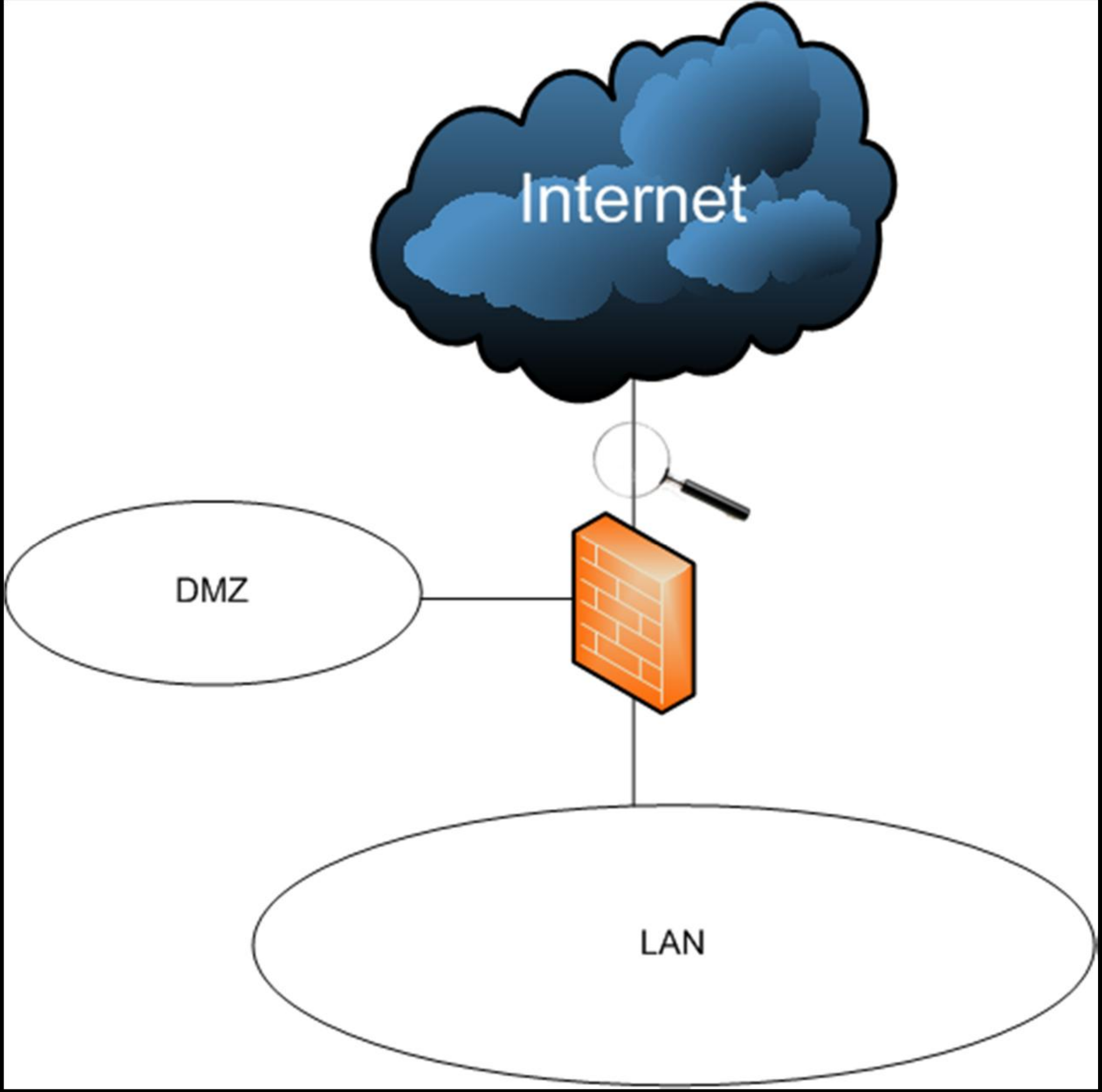


Image: Thanks Dan, your gifts from Shanghai are always a treat, a Creative Commons Attribution Non-Commercial No-Derivative-Works (2.0) image from joepemberton's photostream

Using your cell phone in datacenters…

Why?

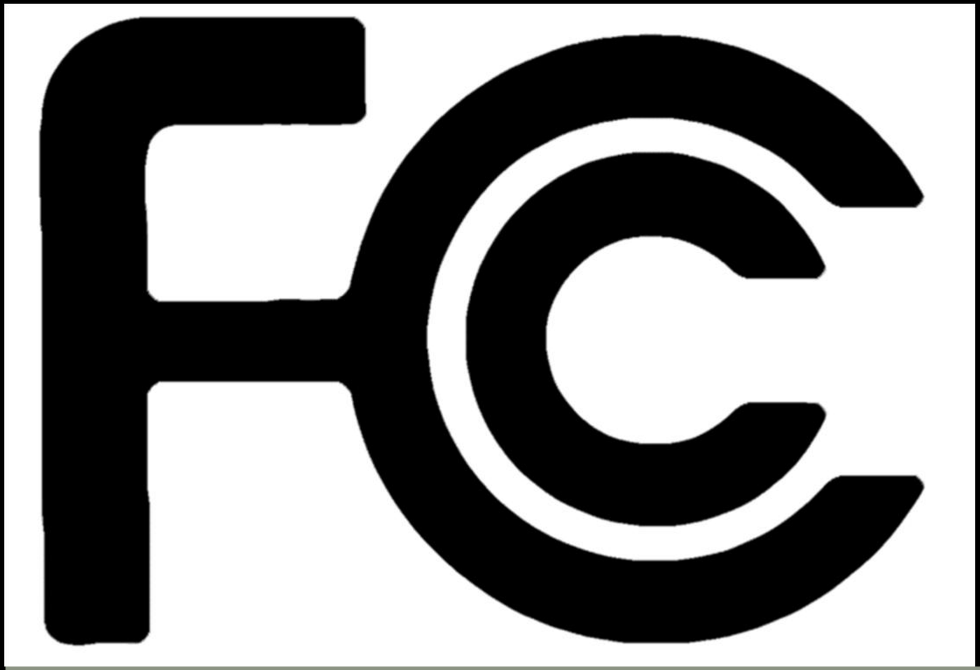
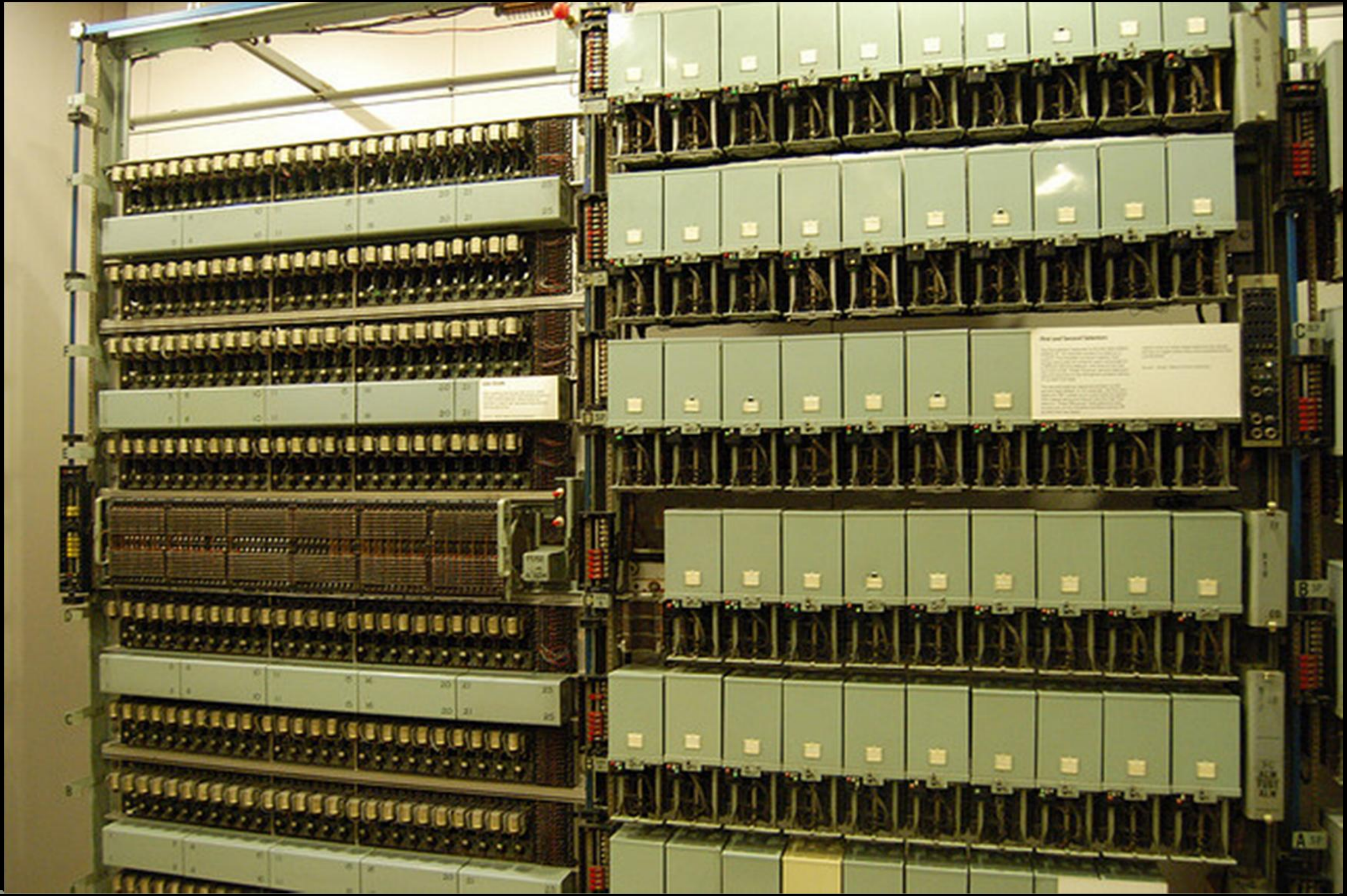


Image taken from www.muscom.nl

Image: Strowger, a Creative Commons Attribution Non-Commercial Share-Alike (2.0) image from pritch's photostream

Interference has happened…



SCHUBERG PHILIS

Image: Don't Mind If I Do a Creative Commons Attribution Non-Commercial (2.0) image from jeremybrooks's photostream

It is because of the cameras…

Image: Taken with Frank Breedijk's BlackBerry at DefCon 17

Let's get serious…

</RANT>

Image: Magic Roundabout Schild db a public domain image by Dickbauch from Wikimedia Commons and Map of Magic Roundabout in Swindon, CC BY SA also from Wikimedia Commons

Is complexity bad?

There are about 25,000 parts in a commercial jet engine.

In order to make a working jet engine you need at a maximum 1,000 parts

The other 24,000 parts where added there because something went wrong sometime

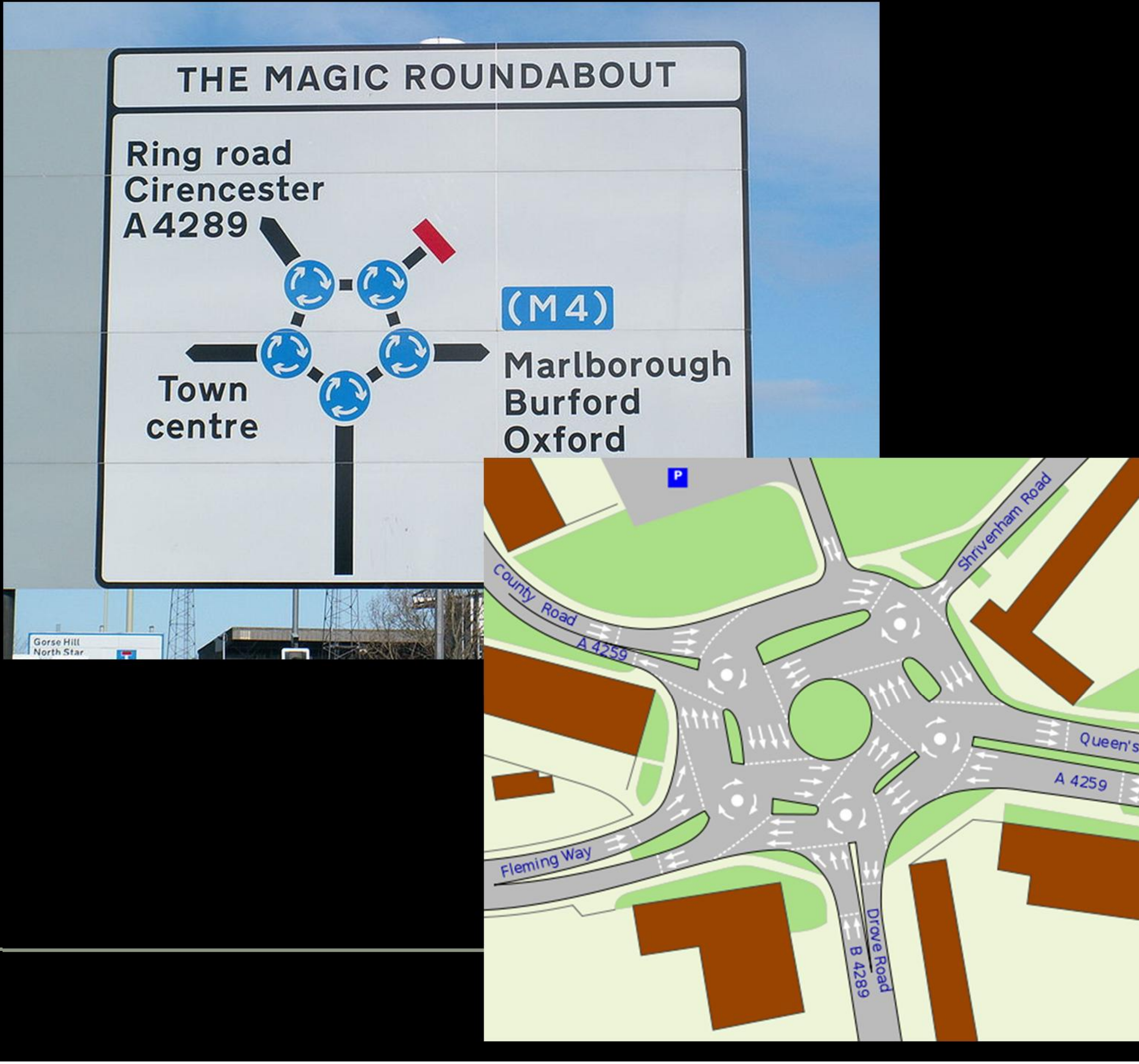


Image: Maze Lock Guarantees You'll Perish In A Fire, a Creative Commons Attribution Share-Alike (2.0) image from billypalooza's photostream

Is complexity bad?

Complexity can also aid security…

It should never be the basis of your security

Never underestimate the power of security by obscurity

Obscurity can defeat plausible deniability

Encryption is a classical example of security by obscurity

The Lure Of Gold, a Creative Commons Attribution Share-Alike (2.0) image from bogenfreund's photostream

Compliance…

Compliance (e.g. PCI compliance) put a business driver into security.

If you implement these security measures you will get a discount

- Firewalls
- IDS
- Regular vulnerability scan
- Physical security

Expect a business decision

Image: Glass smash with liquid, a Creative Commons Attribution Non-Commercial (2.0) image from whisperwolf's photostream

If all you got is a hammer…

Everything looks like a nail…

Consider what you need to secure, before you decide how to…

Image: Bureaucracy illustration, a Creative Commons Attribution Share-Alike (2.0) image from kongharald's photostream

The burden of administration…

“Adding more security” to a system often means more administration and bureaucracy.

It often also means less time to do actual system administration.

Image: homer's minibrain, a Creative Commons Attribution Share-Alike (2.0) image from mabi's photostream

Do not disengage your brain…

What’s the risk?

So how did we do???

☑ Discussed some (so called) best practices

☑ Raised reasonable doubt

☑ At least provided marginal entertainment

☒ Did not mention Sony

☒ Did not mention RSA

Image: "1 more minute?" Richie Hawtin asks Rocco // Awakenings Festival 2007, a Creative Commons Attribution Non-Commercial No-Derivative-Works (2.0) image from merlijnhoek's photostream

Questions?

?

Feedback...

Please send/tell us your examples of non-security through stupidity

Email:	fbreedijk@schubergphilis.com isoutham@schubergphilis.com
Twitter:	@seccubus
Blog:	http://cupfighter.net
Company:	http://schubergphilis.com