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

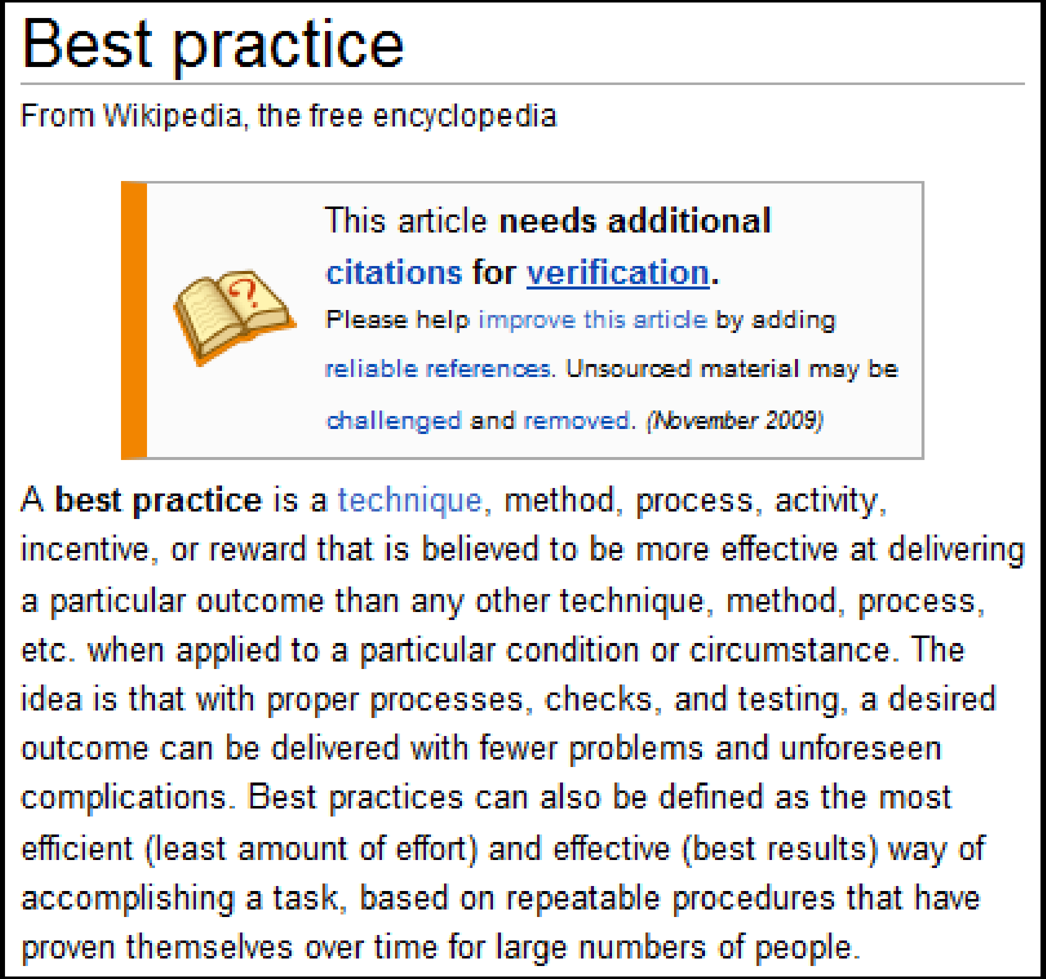
<RANT>

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 am I?

Frank Breedijk

- Security Engineer 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

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 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:

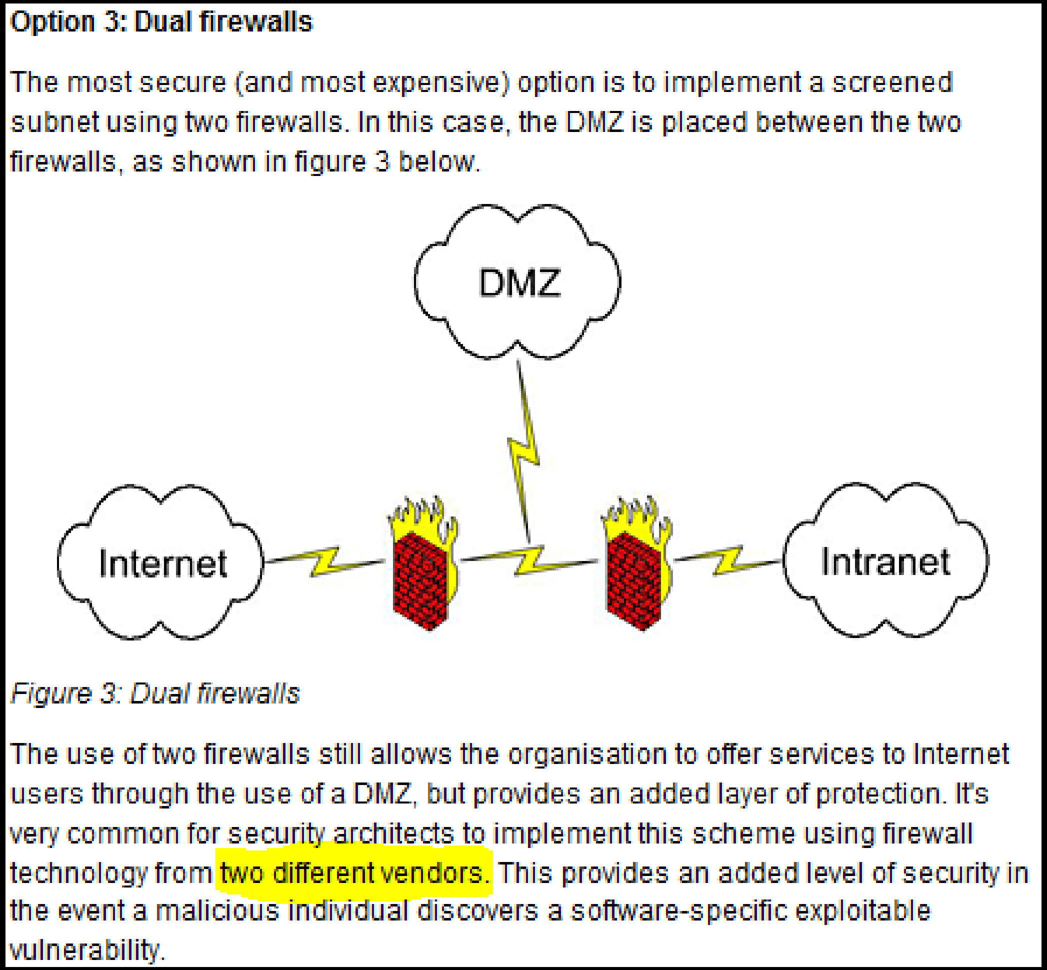
» Firewall bypass bugs are rare

» 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.

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

Its like two locks on a bicycle

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

But just two locks isn’t enough…

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

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

Image: conjoined twin roundabouts, a Creative Commons Attribution Non-Commercial (2.0) image from duncan's photostream

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

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

Image: Security, cartoon #538 from xkcd.com

What about encryption…

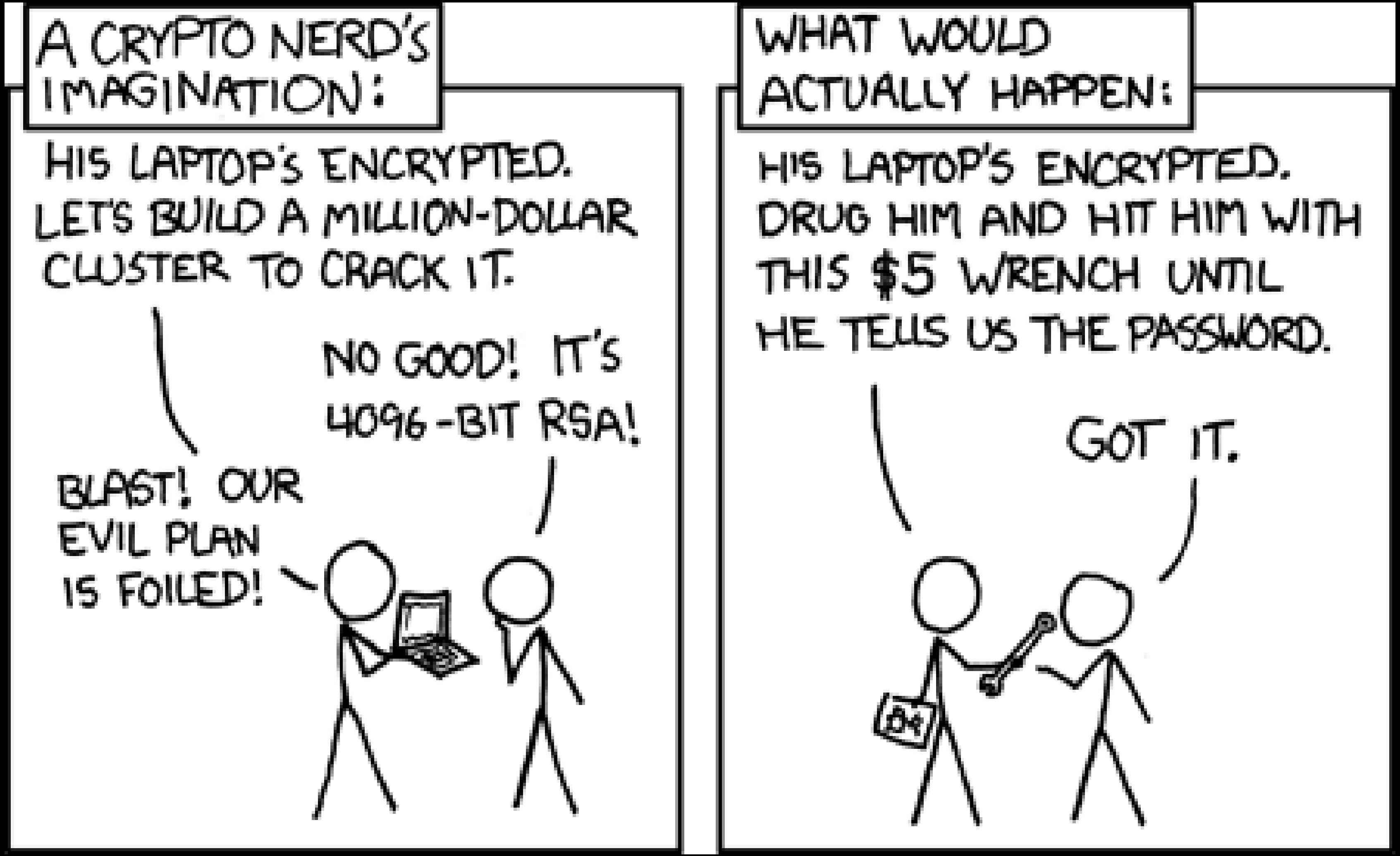

A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.
D4

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

Encryption is not a silver bullet…

Many attacks:

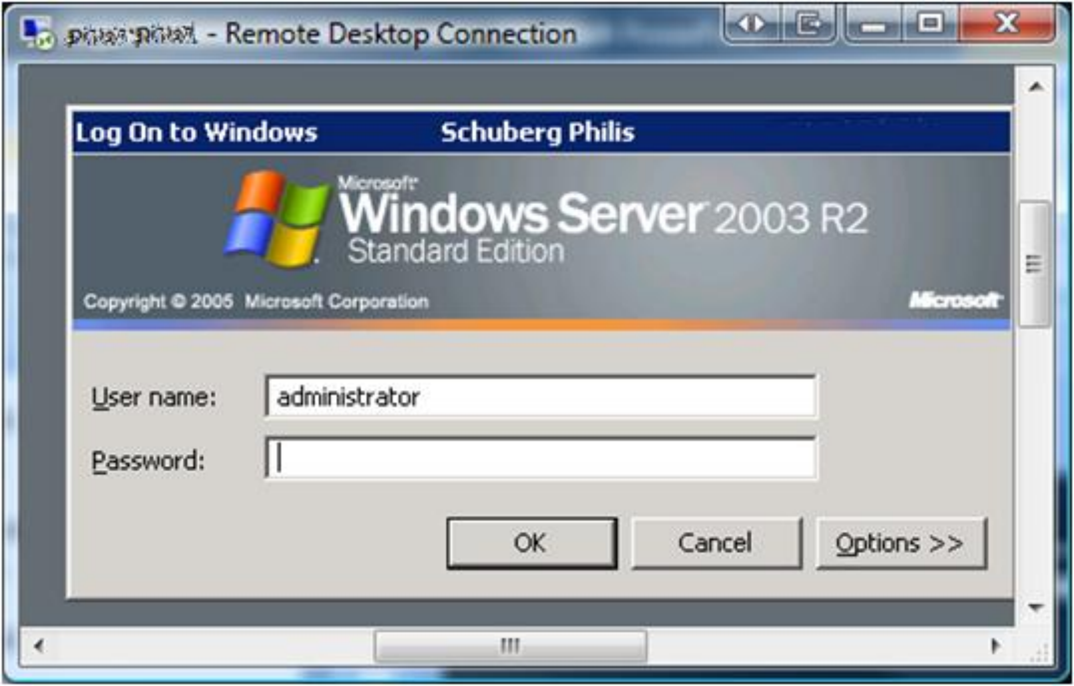
- Key theft
- Brute force
- Social engineering
- End point compromise
- Man in the browser attack
- Man in the Middle attack
- Downgrade attack
- Rubber hose cryptology
- Side channel attack
- Cache timing attack
- Replay attacks

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

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:

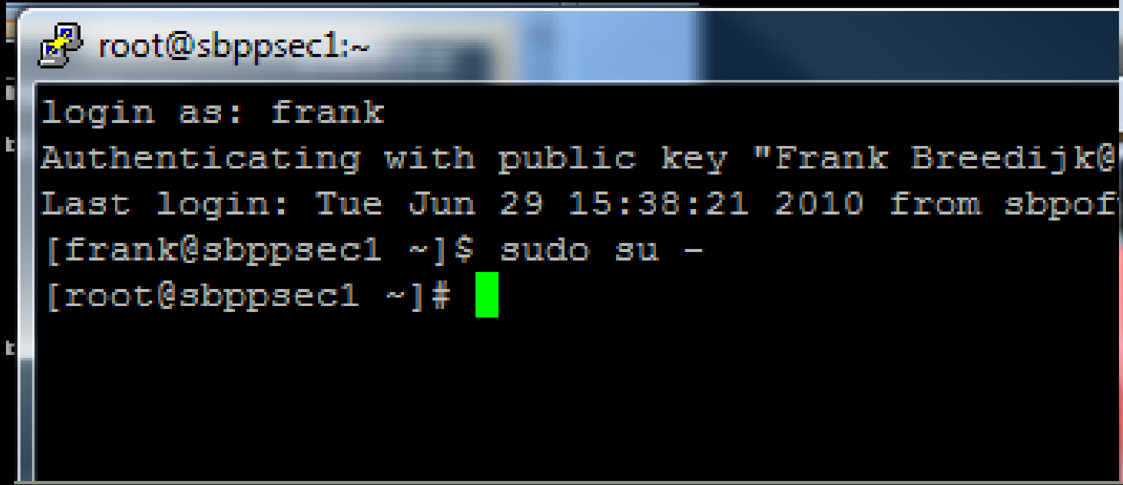
- I set up a really hard adminstrator password
- I put it in the password vault
- I now have to type 15 random characters to gain access
- I may start to remember this password
- I may start to use weaker passwords
- Maybe I will write the password down

Image: 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 ~]# 
```

Image by Frank Breedijk

There is strength in numbers…

"Limit the number of system administrators"

Images by Frank Breedijk

Does this consider the level of the system administrators?

Or are all animals equal…

What is the right number of administrators…

5 20 25 47

50 35

18

17 53 6 42 35 15

120 33 19

28 11

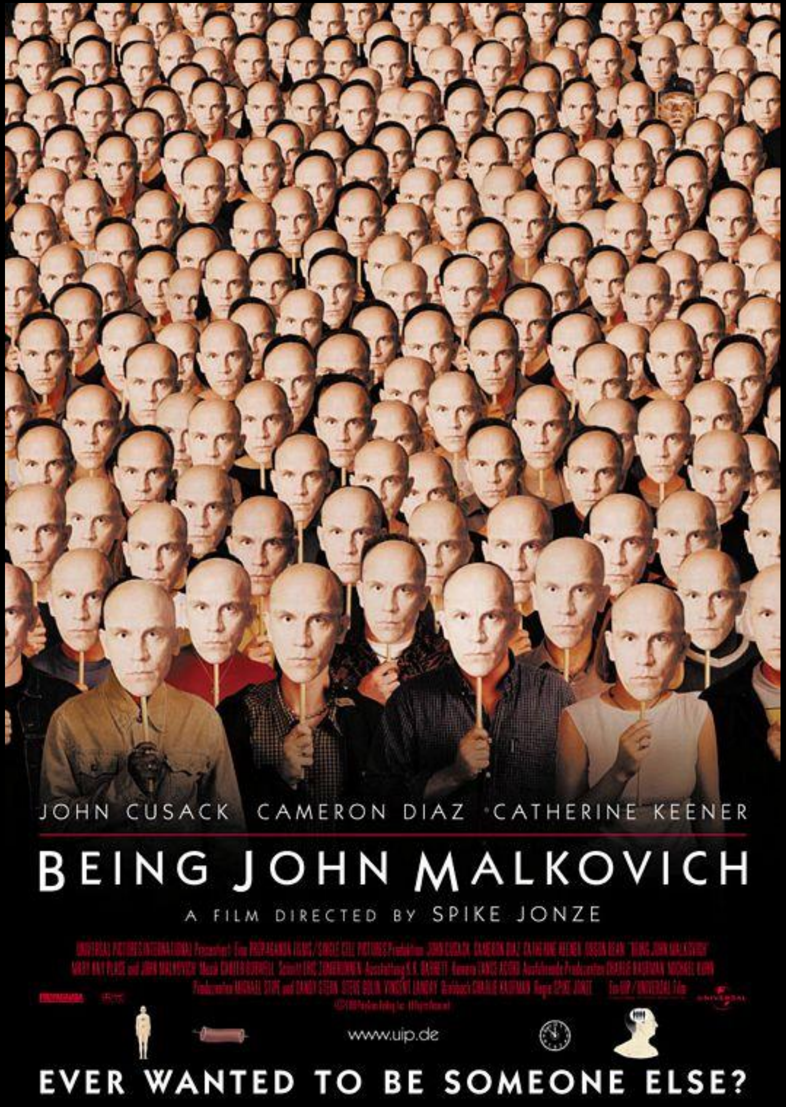
Please don’t force me to…

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?

Image: Being John Malcovich movie poster

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."

Why?

- Stop data leaving the premises?
- Reduce risk of duress?
- Keep an eye on your actions?

- That warm and fuzzy feeling?

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

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

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

Duress

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

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: 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

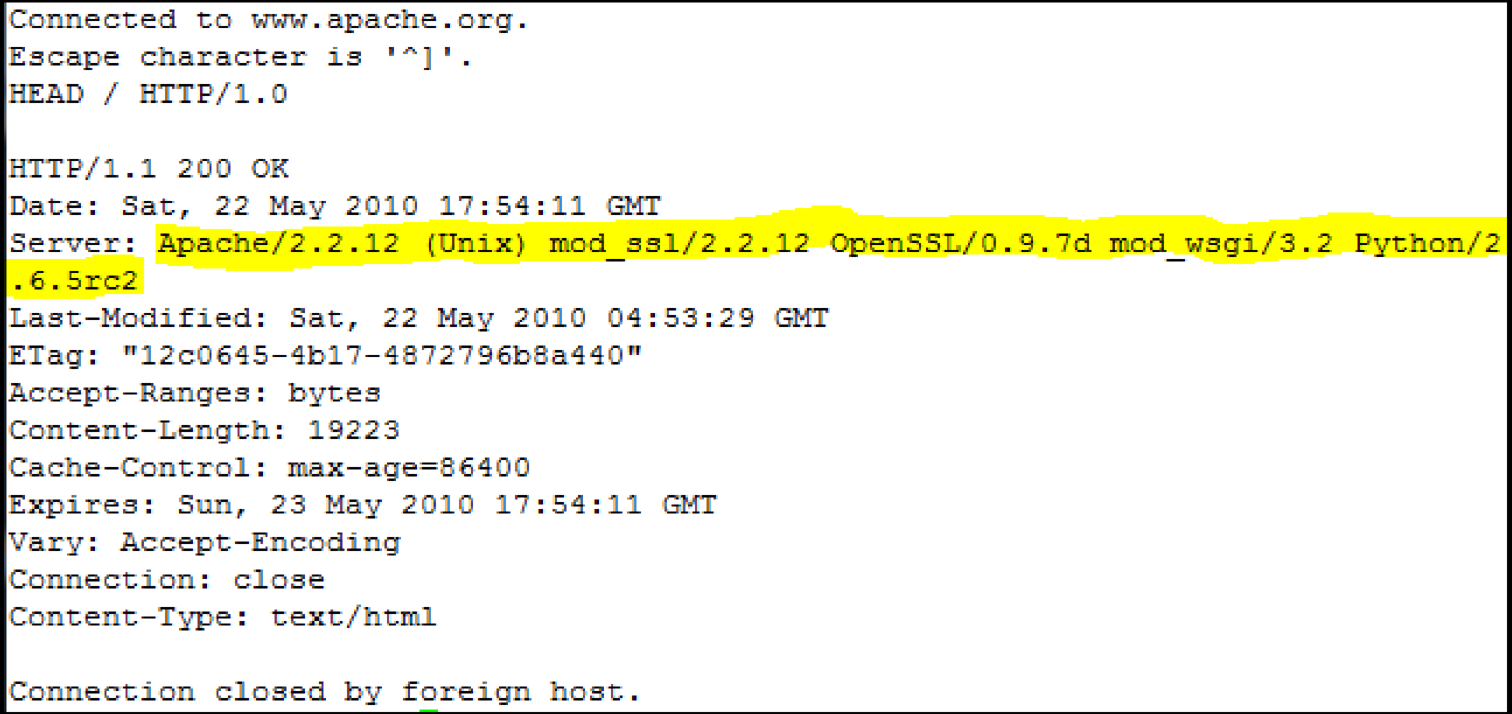
Remove all identifying banners

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?

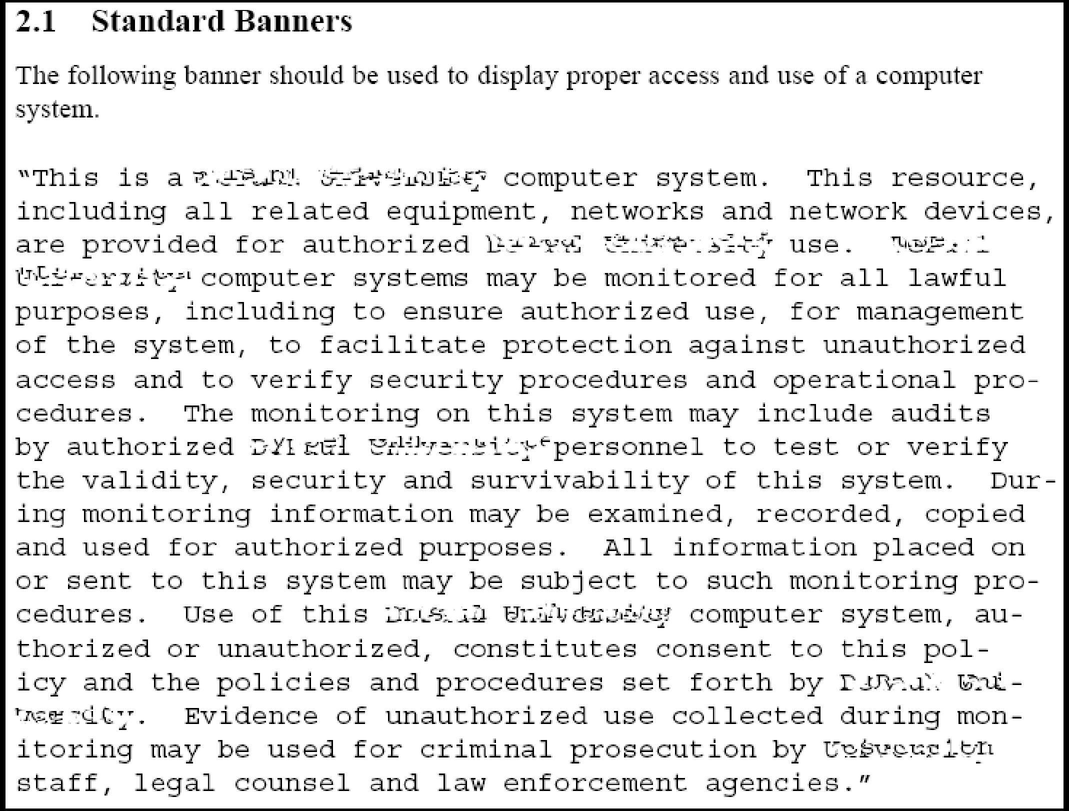


```
Connected to www.apache.org.
Escape character is '^]'.
HEAD / HTTP/1.0

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 [redacted] computer system. This resource, including all related equipment, networks and network devices, are provided for authorized [redacted] use. [redacted] 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 [redacted] 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 [redacted] computer system, authorized or unauthorized, constitutes consent to this policy and the policies and procedures set forth by [redacted]. Evidence of unauthorized use collected during monitoring may be used for criminal prosecution by [redacted] 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?

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?

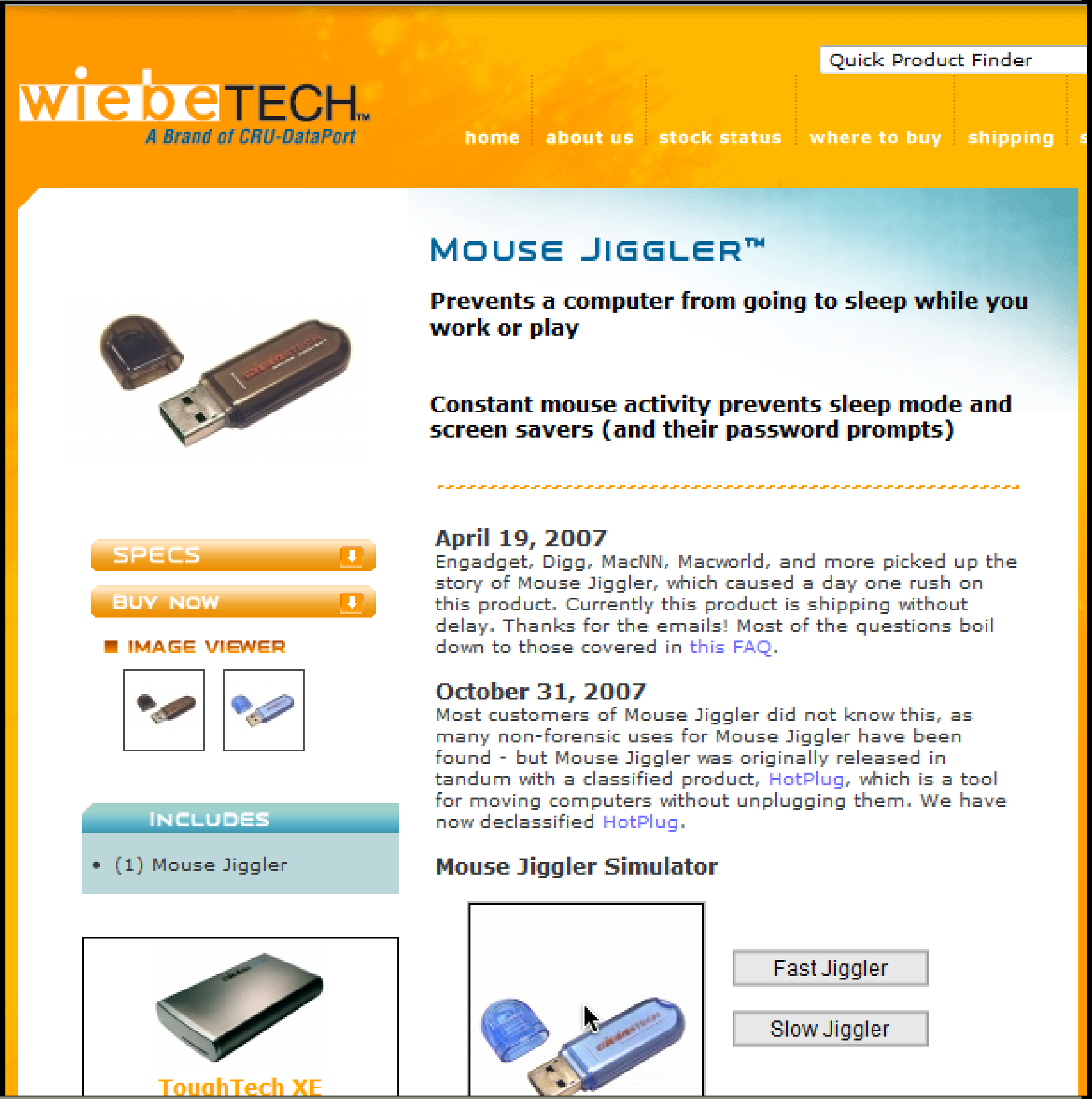
There is no “evil bit” (except in RFC 3514)

EVIL

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

Idle session time out…

Its just there to piss users off



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)

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 tandem with a classified product, HotPlug, which is a tool for moving computers without unplugging them. We have now declassified HotPlug.

Mouse Jiggler Simulator

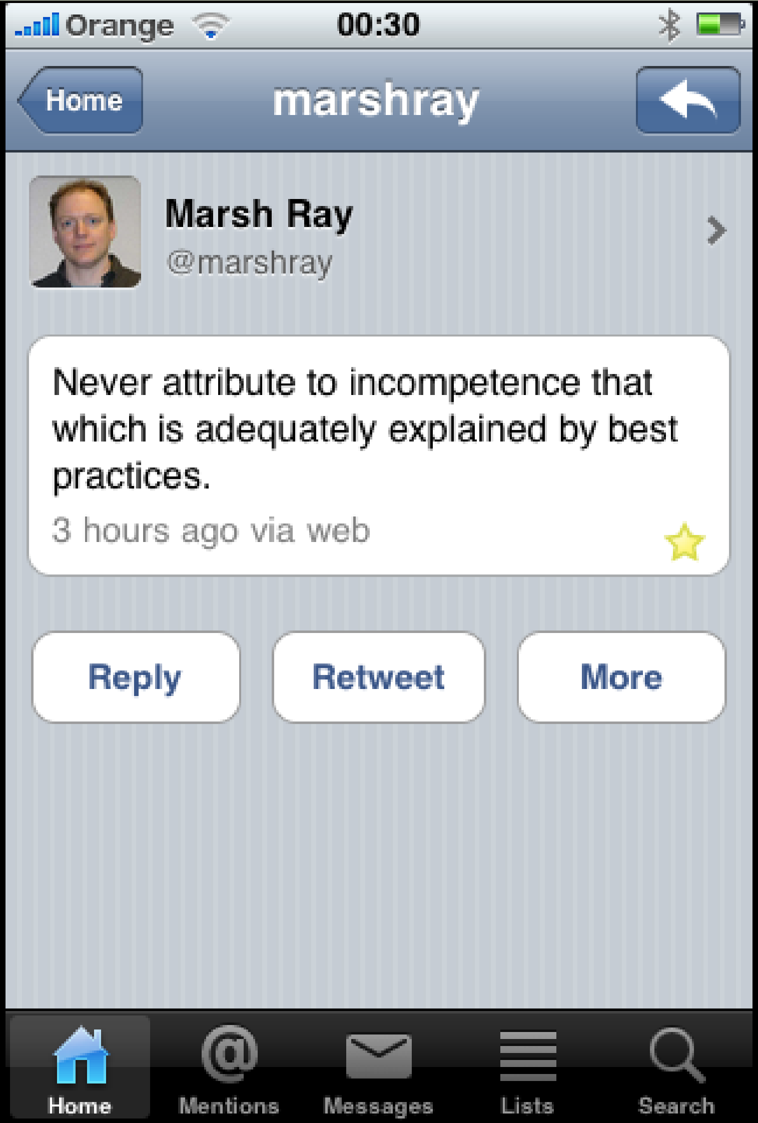
- (1) Mouse Jiggler

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

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

Don’t take away my tools…

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

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

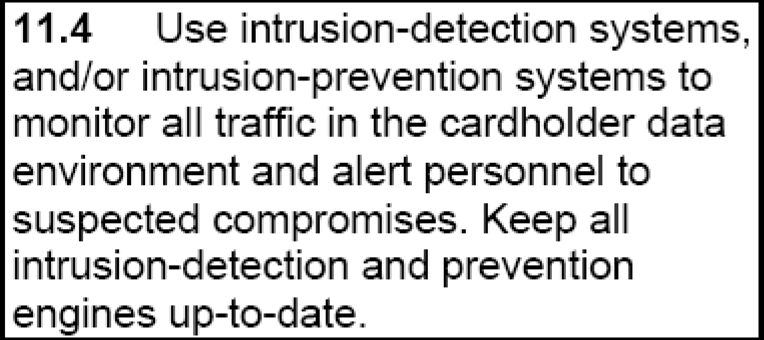
Intrusion Detection System (IDS)

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.

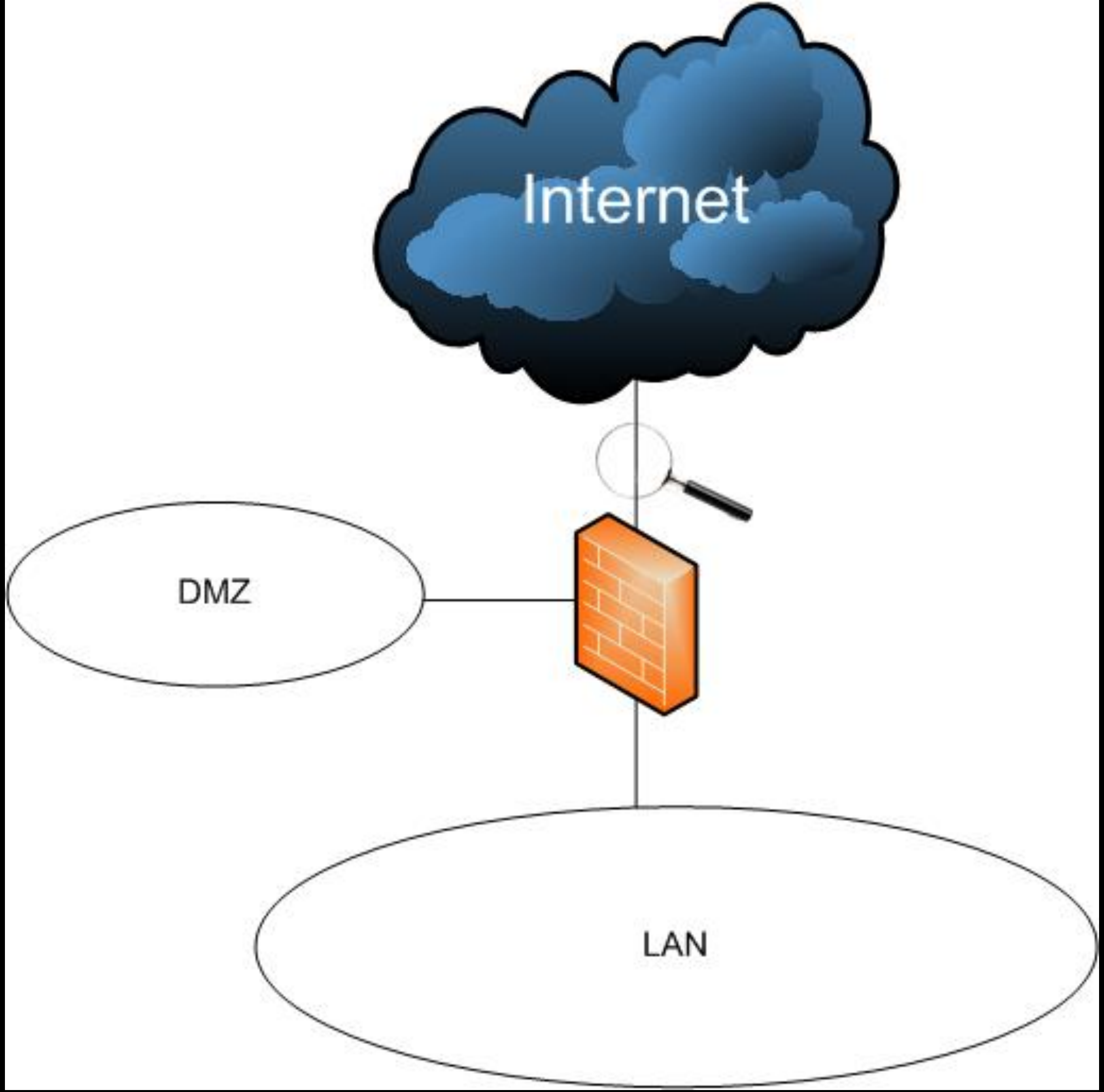


Image: Thanks Dan, your gifts from Shanghai are always a treat, a Creative Commons Attribution Non-Commercial No-Derivative-Works (2.0) image from joepemberton's photostream

Using your cell phone in datacenters…

Why?

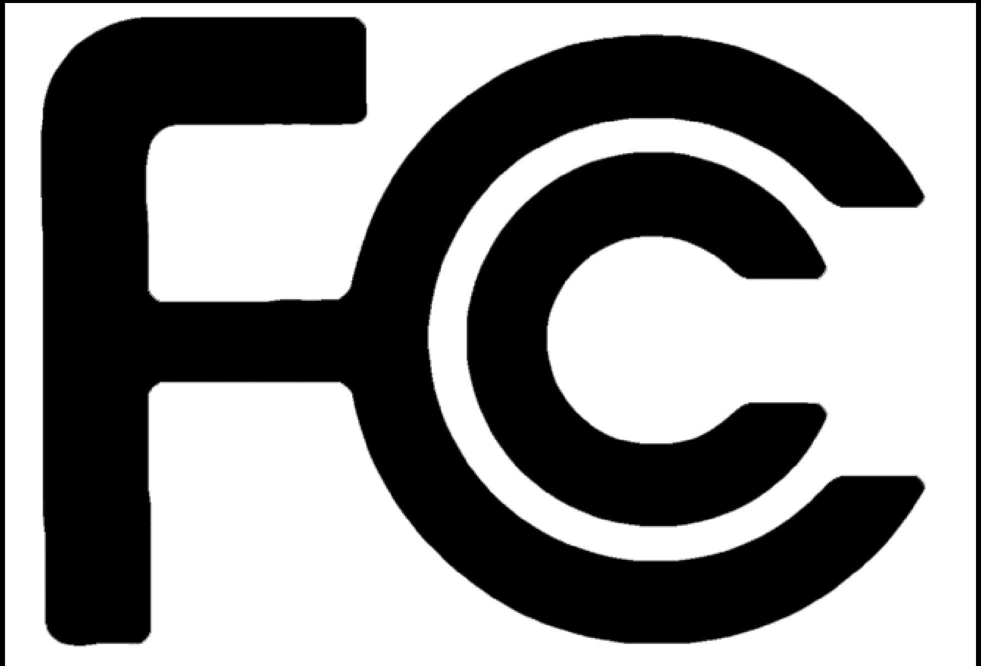


Image taken from www.muscom.nl

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

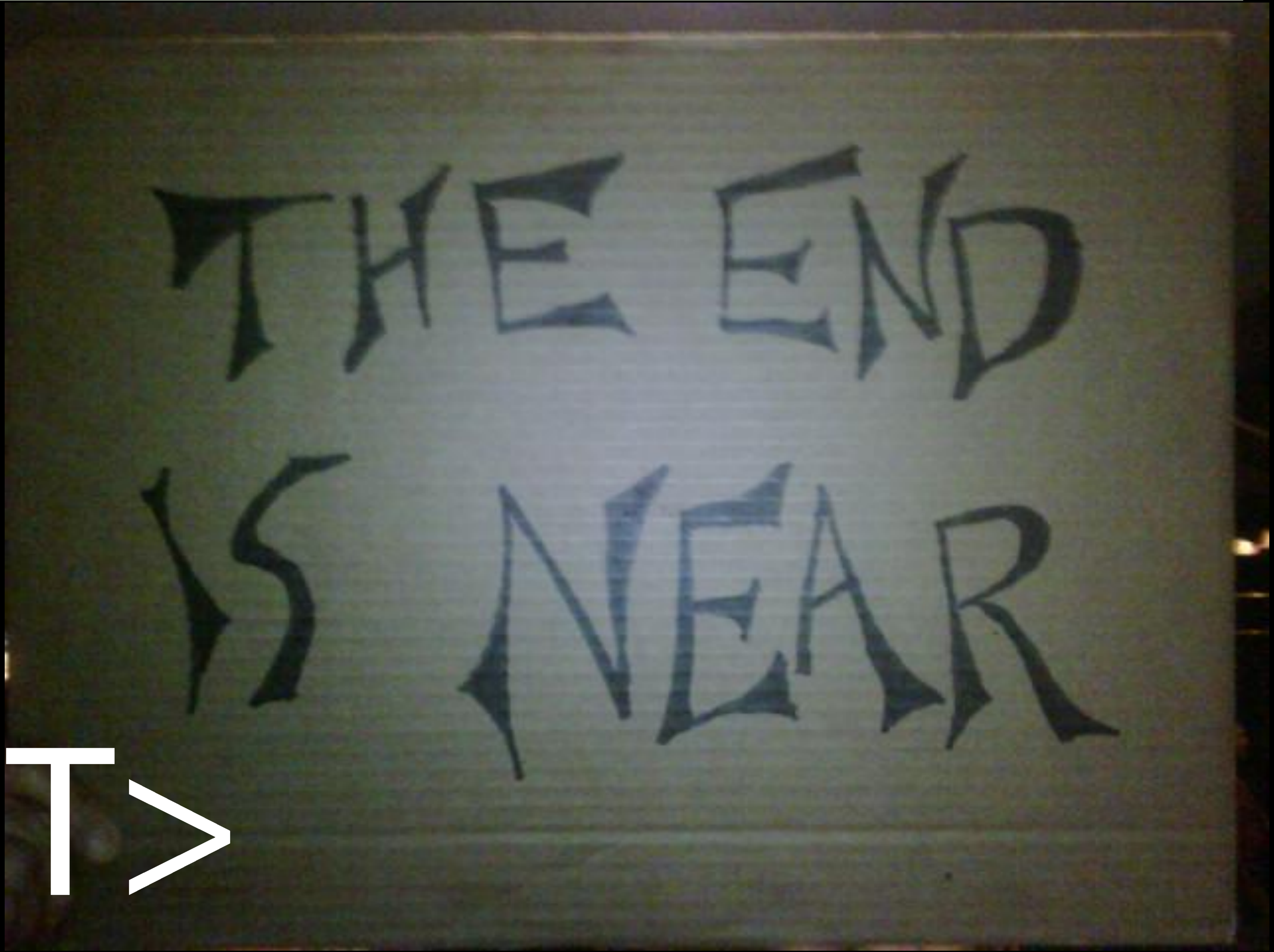
Interference has happened…

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

Its because of the cameras…

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

Lets get serious…



</RANT>

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

Do not disengage your brain…

What is the risk?

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 me your examples of non-security through stupidity

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