The road to Hell...

... is paved with best practices
Warning

Caution

<RANT>

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

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

Often overlooked:
“...when applied to a particular condition or circumstance.”
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
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”
Firewalls from two different vendors...

Reasoning:
» If one vendor has a serious flaw, there will not be a total compromise.
It's 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...

Like every technology you need to know how to apply it to benefit from it.
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
Hacker ‘handshake’ hole found in common firewalls

In February 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”.

Your votes please...
Cryptography

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.

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

Ian

Frank

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

» Do you use the wireless here?

» What do you prefer, telnet or SSH?

» Do you do any online banking?
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
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.
Your votes please...

Old School Voting. The way it should be. A CC NC image from Just Us 3's Flickr stream http://www.flickr.com/photos/73835037@N00/292239798/
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
Rock, Paper, Scissors

Ian

Frank

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

The reality


» 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.

» 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.

[http://tinyurl.com/RTHpasswd2]
Complex passwords...

Assumption: a ‘complex’ password is harder to crack than 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
No voting necessary...

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/
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
There is strength in numbers...

“Limit the number of system administrators”
Rock, Paper, Scissors

Ian

Frank

Image: sessions beer bottlecaps, a CC NC SA image from C_Knaus' Flickr stream http://www.flickr.com/photos/40732569106@N01/942653401/
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...
What is the right number of administrators...
Does this consider the level of the system administrators?

But, are all animals equal...
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!
Your votes please...

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

Ian

Frank

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

If you are working from home they can make you do stuff at gunpoint...
Teleworking has advantages

Remote system administration =
Faster response time +
More dedicated staff +
Better uptime +
Better maintained system
=
Better security
Your votes please...
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?
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 სათაურო სამყარო computer system. This resource, including all related equipment, networks and network devices, are provided for authorized სამყარო use. სათაურო 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 სამყარო პერსონალ 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 სათაურო computer system, authorized or unauthorized, constitutes consent to this policy and the policies and procedures set forth by სამყარო. Evidence of unauthorized use collected during monitoring may be used for criminal prosecution by სამყარო staff, legal counsel and law enforcement agencies."
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: pong undead!!!, a Creative Commons Attribution Non-Commercial Share-Alike (2.0) image from astio's photostream
Security making life too hard...

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
Don’t take away my tools...

- Removing telnet (client)
- Remove development tools
- Remove security tools
  - Nmap?
  - Ping?
  - Traceroute?
  - OpenSSL?
- Taking SUID from ping
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...
Idle session time out...

It’s just there to piss users off.

Zhorn Software

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)

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.
Single sign on...

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

What is the alternative? Passwords.xls?
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
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)
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.
Using your cell phone in datacenters...

Why?
Interference has happened...
It is because of the cameras...
Let's get serious...

The end is near

</RANT>
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 were added there because something went wrong sometime.
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
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
If all you got is a hammer...

Everything looks like a nail...

Consider what you need to secure, before you decide how to...
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.
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
Questions?

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
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