



THE SECURITY STANDARD™



Securing the Enterprise from a Dangerous Cyberworld

September 19-20, 2011 • Marriott Brooklyn Bridge, New York City

Produced by
CSO

PCI Zen: How To Be Compliant By Not Being Compliant

Andy Ellis

CSO

Akamai Technologies



THE
SECURITY
STANDARD™

Securing the Enterprise
from a Dangerous Cyberworld

Produced by
CSO

Compliance is painful

- Cost of annual *audits* averages \$225K for Tier 1 merchants¹
- Technology upgrades to achieve “compliance” have opportunity costs
- Documentation against 217 requirements

1: PCI DSS Trends – QSA Insights, Ponemon Institute, 2010



THE
SECURITY
STANDARD™

Securing the Enterprise
from a Dangerous Cyberworld

Produced by

CSO

A look at the requirements

- Reqt 1: Install and maintain a firewall configuration to protect cardholder data
- Reqt 2: Do not use vendor-supplied defaults for system passwords and other security parameters
- Reqt 3: Protect stored cardholder data
- Reqt 4: Encrypt transmission of cardholder data across open, public networks
- Reqt 5: Use and regularly update anti-virus software or programs
- Reqt 6: Develop and maintain secure systems and applications



THE
SECURITY
STANDARD™

Securing the Enterprise
from a Dangerous Cyberworld

Produced by

CSO

A look at the requirements (continued)

- Reqt 7: Restrict access to cardholder data by business need to know
- Reqt 8: Assign a unique ID to each person with computer access
- Reqt 9: Restrict physical access to cardholder data
- Reqt 10: Track and monitor all access to network resources and cardholder data
- Reqt 11: Regularly test security systems and processes
- Reqt 12: Maintain a policy that addresses information security for all personnel
- Reqt A: Shared hosting providers protect cardholder data environment



THE
SECURITY
STANDARD™

Securing the Enterprise
from a Dangerous Cyberworld

Produced by
CSO

My favorite dead horse

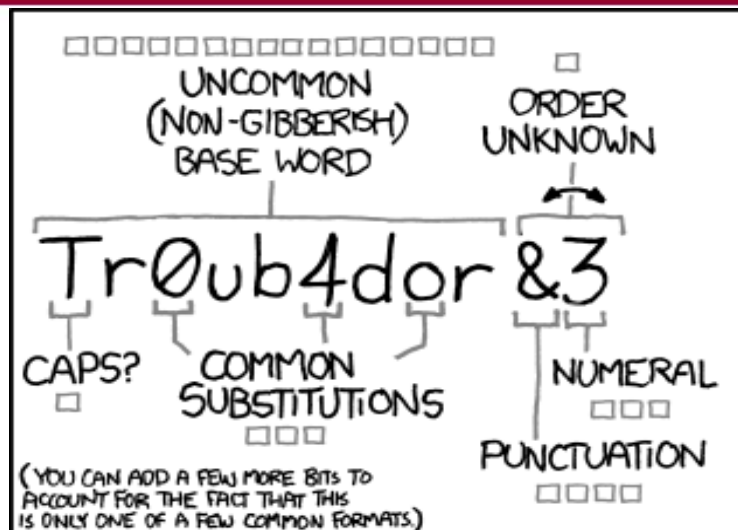
- Implement automated audit trails for all system components to reconstruct the following events:
 - Creation and deletion of system-level objects
- Anything on a system component that is required for its operation, including but not limited to application executable and configuration files, system configuration files, static and shared libraries & DLL's, system executables, device drivers and device configuration files, and added third-party components.



THE
SECURITY
STANDARD™

Securing the Enterprise
from a Dangerous Cyberworld

Produced by
CSO



~28 BITS OF ENTROPY


□□□□□□□
 □□□□□□□
 □□
 □□□

$2^{28} = 3 \text{ DAYS AT}$
 1000 GUESSES/SEC

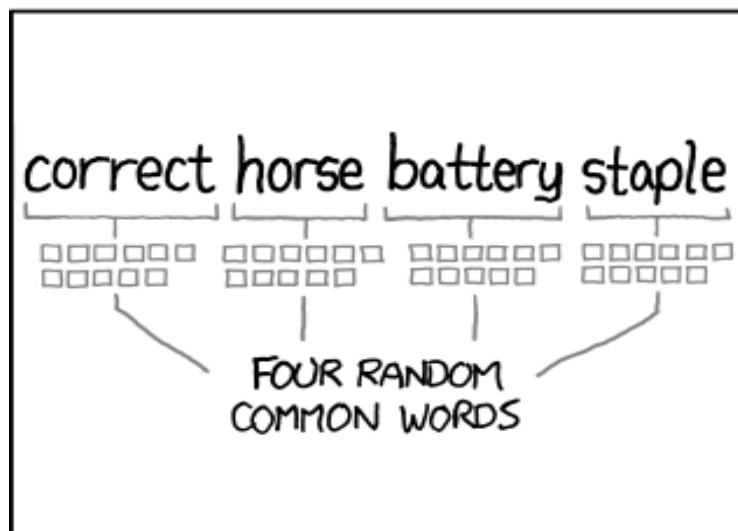
(PLAUSIBLE ATTACK ON A WEAK REMOTE
 WEB SERVICE. YES, CRACKING A STOLEN
 HASH IS FASTER, BUT IT'S NOT WHAT THE
 AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS:
EASY

WAS IT TROMBONE? NO,
 TROUBADOR. AND ONE OF
 THE 0s WAS A ZERO?
 AND THERE WAS
 SOME SYMBOL...



DIFFICULTY TO REMEMBER:
HARD



~44 BITS OF ENTROPY

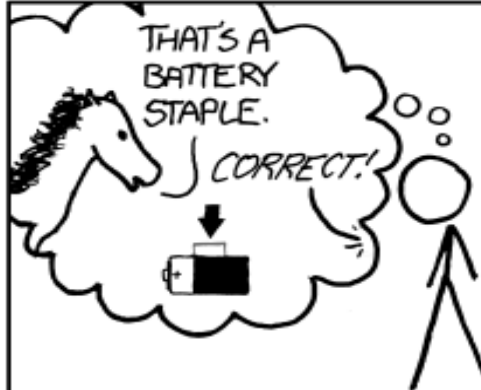
□□□□□□□□□□
 □□□□□□□□□□
 □□□□□□□□□□
 □□□□□□□□□□

$2^{44} = 550 \text{ YEARS AT}$
 1000 GUESSES/SEC

DIFFICULTY TO GUESS:
HARD

THAT'S A
 BATTERY
 STAPLE.

CORRECT!



DIFFICULTY TO REMEMBER:
 YOU'VE ALREADY
 MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED
 EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS
 TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.



THE
 SECURITY
 STANDARD™

Securing the Enterprise
 from a Dangerous Cyberworld

Produced by

CSO

Reboot

- PCI-DSS is primarily a battlefield bandage on a gaping chest wound.
- If system design is the problem, how can we redesign, and obviate the standard?
- *Or, Zen and the Art of PCI Compliance!*



THE
SECURITY
STANDARD™

Securing the Enterprise
from a Dangerous Cyberworld

Produced by

CSO

Out of Control, or Out of Scope?

- Two ways to bypass PCI:
 - Build qualitatively better controls. Use them as “compensating controls”!
 - Remove your systems from scope: Don’t let cardholder data touch them!



THE
SECURITY
STANDARD™

Securing the Enterprise
from a Dangerous Cyberworld

Produced by

CSO

Better Controls: Passwords?

- Eliminate Passwords
 - Switch to cryptographic identities (SSL certificates, SSH keys).
 - Improvements:
 - Removes oracle & gatekeeper attacks
 - Simpler for users in the long run



THE
SECURITY
STANDARD™

Securing the Enterprise
from a Dangerous Cyberworld

Produced by
CSO

Better Controls: WAF

- 6.6 all but requires a WAF...
- ... but it doesn't mandate a box!
- Use a WAF module to your proxy layer
 - Improvements:
 - Easy to maintain
 - No capex overhead!



THE
SECURITY
STANDARD™

Securing the Enterprise
from a Dangerous Cyberworld

Produced by

CSO

Better Controls: Firewalls?

- Bypass your firewalls
 - Utilize IPSEC/VPN technologies for *all* interserver communication
 - Improvements:
 - Better authentication of traffic
 - Simpler firewall management



THE
SECURITY
STANDARD™

Securing the Enterprise
from a Dangerous Cyberworld

Produced by
CSO

Better Controls: Log Watching?

- Shift to real-time monitoring
- Improvements:
 - Better responsiveness to issues
 - No “make-work”



THE
SECURITY
STANDARD™

Securing the Enterprise
from a Dangerous Cyberworld

Produced by
CSO

Out of Scope: Wireless?

- Use wired lines
- Improvements:
 - Low interference
 - With IPSEC or 802.1x, reduced risk of eavesdrop



THE
SECURITY
STANDARD™

Securing the Enterprise
from a Dangerous Cyberworld

Produced by

CSO

Out of Scope: Anti-Virus?

- Antivirus is primarily applicable to Windows (vendors will add Mac to list)
- Switch to Linux for administration
 - Improvements:
 - Develop a Jedi mindset among your admin



THE
SECURITY
STANDARD™

Securing the Enterprise
from a Dangerous Cyberworld

Produced by
CSO

Out of Scope: Tokens

- Cardholder Data is the Problem!
- Eliminate it by using a tokenization solution
 - Improvements:
 - Don't have CC# to be stolen anymore
 - Can use tokens more widely (anti-fraud) as identifier
 - Say goodbye to your auditor!



THE
SECURITY
STANDARD™

Securing the Enterprise
from a Dangerous Cyberworld

Produced by

CSO

Thank You

Andy Ellis
@csoandy



THE
SECURITY
STANDARD™

Securing the Enterprise
from a Dangerous Cyberworld

Produced by

CSO