How to Implement Cryptography for the OWASP Top 10 (Reloaded)

AppSec USA 2011

http://www.appsecusa.org/

Minneapolis Convention Center

Minneapolis, MN, USA

Friday September 23 2011 1:30pm

Anthony J. Stieber

mailto:anthony.j.stieber@gmail.com

How NOT to Implement Cryptography for the OWASP Top 10 (Reloaded)

AppSec USA 2011

http://www.appsecusa.org/

Minneapolis Convention Center

Minneapolis, MN, USA

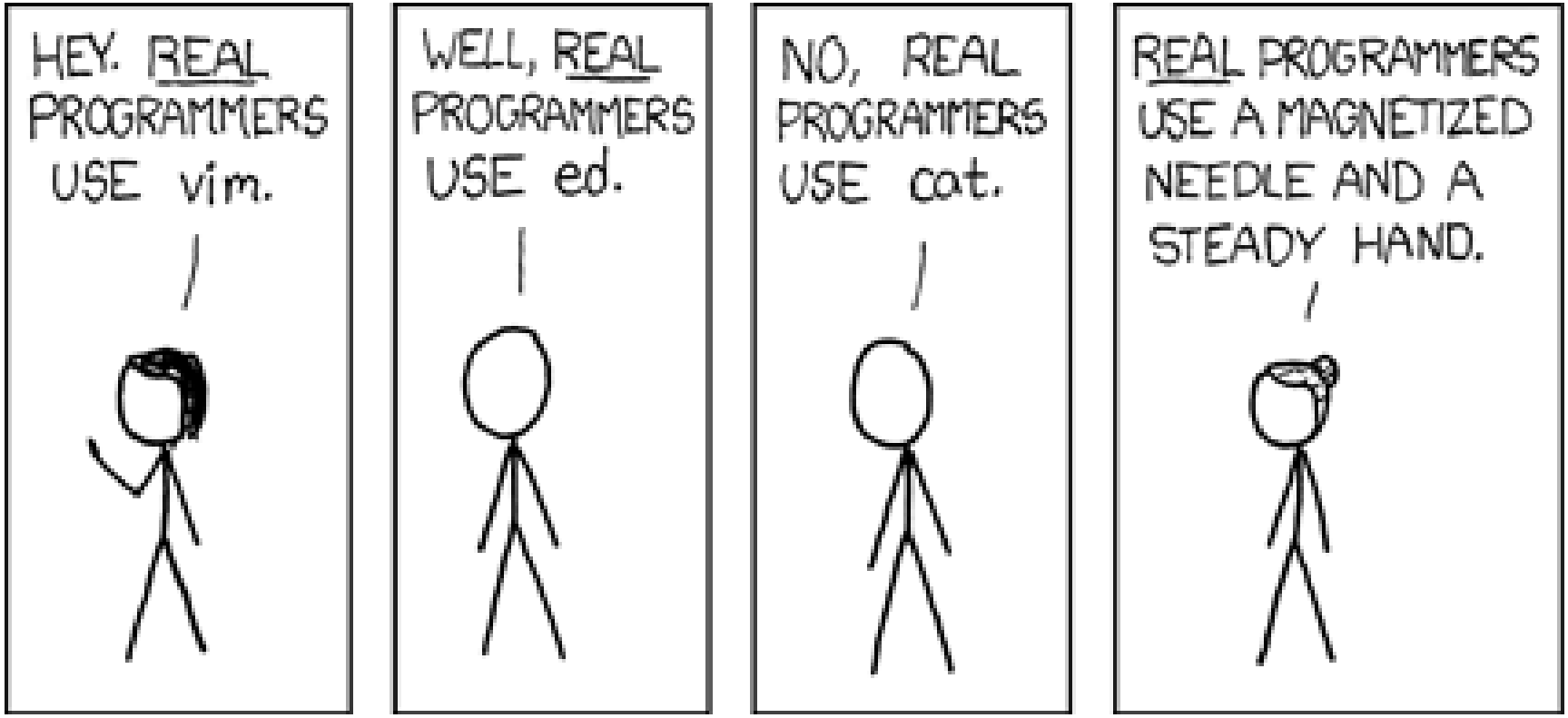
+02011-09-23T1330Z-05

Anthony J. Stieber

mailto:anthony.j.stieber@gmail.com

http://en.wikipedia.org/wiki/ISO_8601#Years http://en.wikipedia.org/wiki/Year_10,000_problem

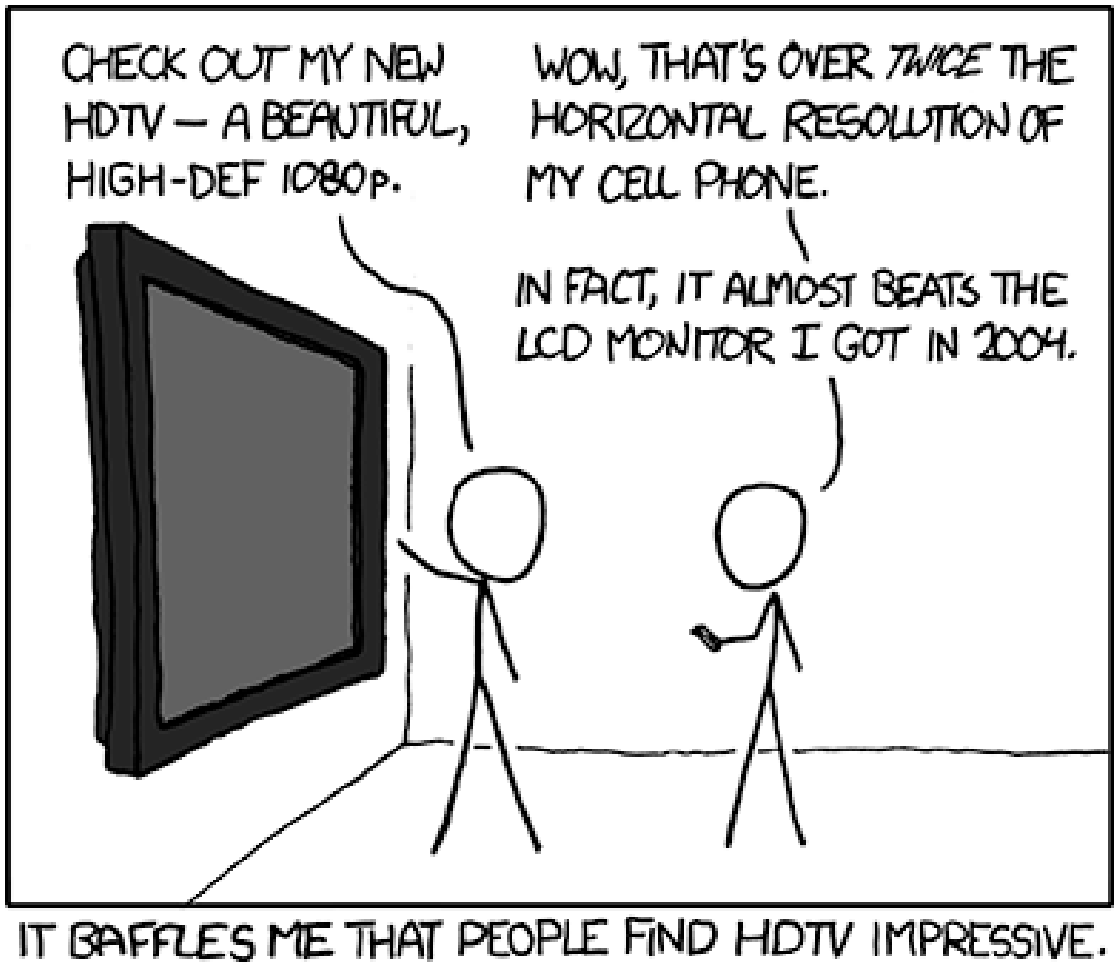
I am not a real programmer



http://xkcd.com/153/

http://en.wikipedia.org/wiki/Real_Programmer
http://en.wikipedia.org/wiki/Editor_war

not even on TV



http://xkcd.com/732/

http://en.wikipedia.org/wiki/High-definition_television#High-definition_display_resolutions

http://www.notepad.org/
http://en.wikipedia.org/wiki/Notepad_%28software%29

ACI Triad

- Availability →not much*
- Confidentiality→ Ciphers!
- Integrity → Digital signatures, HMAC!

ACI Triad

- Availability →not much*
- Confidentiality→ Ciphers!
- Integrity → Digital signatures, HMAC!

* Except for Blakely-Shamir Secret Sharing Schemes

http://en.wikipedia.org/wiki/Secret_sharing

Crypto Terms

- cryptography → making and keeping secrets
- cryptanalysis → breaking secrets
- cryptology → how to make/break secrets
- Kerckhoffs' Principle

Crypto Terms

Kerckhoffs' Principle

"…depend solely on the secrecy of the key…"

http://en.wikipedia.org/wiki/Kerckhoffs%27s_Principle

Crypto Terms

- algorithm
- cipher
- hash function
- random number generator (RNG)

Crypto Terms

- cipher algorithm
  - encrypts plaintext using key into ciphertext
  - decrypts ciphertext using key into plaintext
- hash algorithm
  - variable length input into fixed length hash value
  - no inverse

What's Defense in Depth?

1. Safe protects your stuff
2. Building protects safe
3. Fence protects building
4. Moat protects fence
5. Water protects moat

What's Defense in Depth?

1. Safe protects your stuff
2. Building protects safe
3. Fence protects building
4. Moat protects fence
5. Water protects moat, but what protects water?

What's Defense in Depth?

1. Safe protects your stuff
2. Building protects safe
3. Fence protects building
4. Moat protects fence
5. Water protects moat, but what protects water?
6. Alligators!

OSI Protocol Stack

7. Application
6. Presentation
5. Session
4. Transport
3. Network
2. Link
1. Physical

OSI Protocol Stack Reality

9. Political ← You Are Here
8. Financial
7. Application
6. Presentation
5. Session
4. Transport
3. Network
2. Link
1. Physical

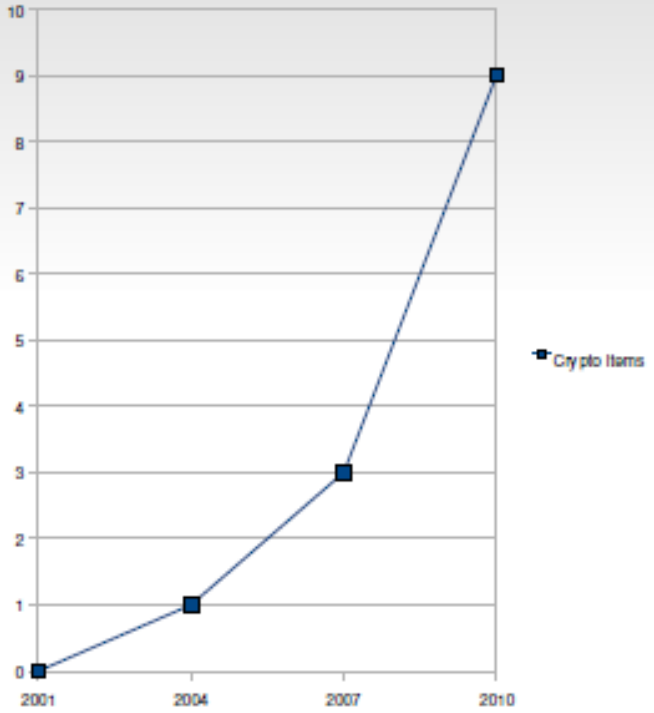
Change is Good

Spare Change is Better

My prediction in 2008

OWASP Crypto Growth

- 2004: A8 Insecure Storage
- 2007: A7, A8, A9 300% growth
- 2010: ???



Crypto in OWASP Top Ten 2010

- A1-Injection
- A2-XSS
- A3-Auth’n
- A4-DOR
- A5-CSRF
- A6-Config
- A7-Crypto
- A8-URL
- A9-Transport
- A10-Redirects

Crypto in OWASP Top Ten 2010

- A1-Injection crypto useless, except…
- A2-XSS crypto useless, except…
- A3-Auth'n **YES!** But...
- A4-DOR crypto useless, except…
- A5-CSRF crypto useless, except…
- A6-Config Maybe, unless…
- A7-Crypto **YES!** Tautological tautology.
- A8-URL Access crypto useless except…
- A9-Transport **YES!**
- A10-Redirects crypto useless except…

OWASP crypto changes since 2008

- A7 Auth’n promoted to A3
- A8 Crypto promoted to A7

OWASP crypto changes since 2008

- A7 Auth’n promoted to A3
- A8 Crypto promoted to A7
- A9 Transport no change
- ESAPI 2.0 crypto

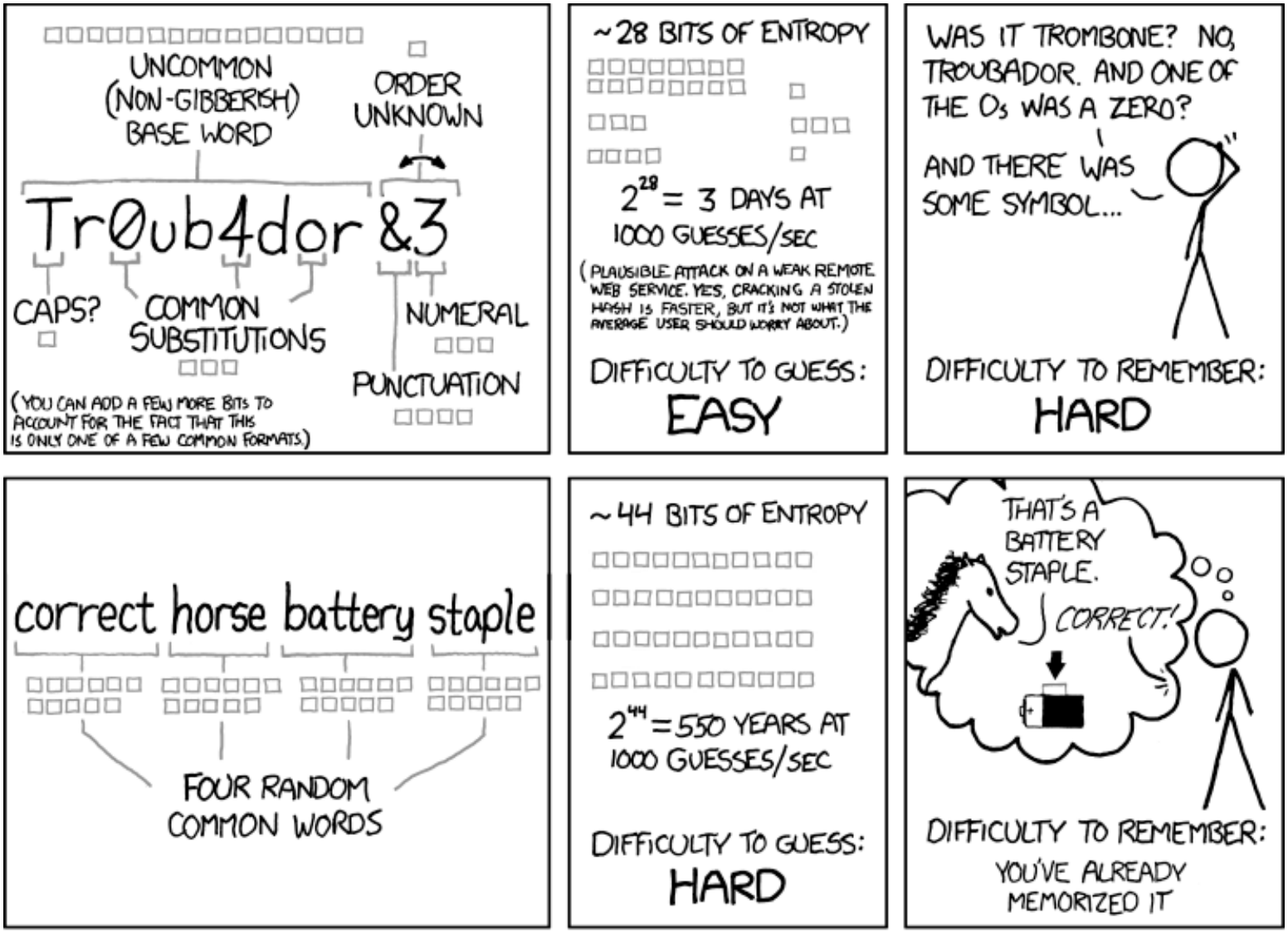
A3-Auth’n Fail

- HTTP
- Password authentication
- Password encryption

A3-Auth’n Fail

- Fast efficient hash
- No, static, small, or non-random salt
- Password “quality”
- Preventing passphrases
- Non-random number generators

https://www.owasp.org/index.php/Authentication_Cheat_Sheet
http://www.cryptosmith.com/password-sanity
http://diceware.com/



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.

http://xkcd.com/936

A7-Crypto Fails

- Default keys (A6 Config)
- MD5 ≈21 bits of security
- SHA1 ≈51 bits of security

https://www.owasp.org/index.php/Cryptographic_Storage_Cheat_Sheet
http://en.wikipedia.org/wiki/MD5
http://en.wikipedia.org/wiki/SHA-1

A7-Crypto Fails

- 2TDES ≈80 bits of security
- RSA-1024 ≈80 bits of security
- Never rekeying

http://csrc.nist.gov/publications/PubsSPs.html#800-131A

A7-Crypto Fails

- Confusing encryption with authentication
- Reuse a stream cipher key

http://en.wikipedia.org/wiki/Padding_oracle_attack
http://en.wikipedia.org/wiki/Authenticated_encryption
http://en.wikipedia.org/wiki/Stream_cipher_attack

A7-Crypto Fails

- Invent a crypto protocol
- FIPS 140 validated products do fail
- Non-random number generators

http://www.cs.auckland.ac.nz/~pgut001/pubs/linux_vpn.txt
https://www.ironkey.com/usb-flash-drive-flaw-exposed
http://csrc.nist.gov/publications/PubsSPs.html#sp800-130

Any one who considers arithmetical methods

Any one who considers arithmetical methods of producing random digits

Any one who considers arithmetical methods of producing random digits is, of course, in a state of sin.

John von Neumann "Various techniques used in connection with random digits", +01951
Applied Mathematics Series, no. 12, 36–38

Random Failures

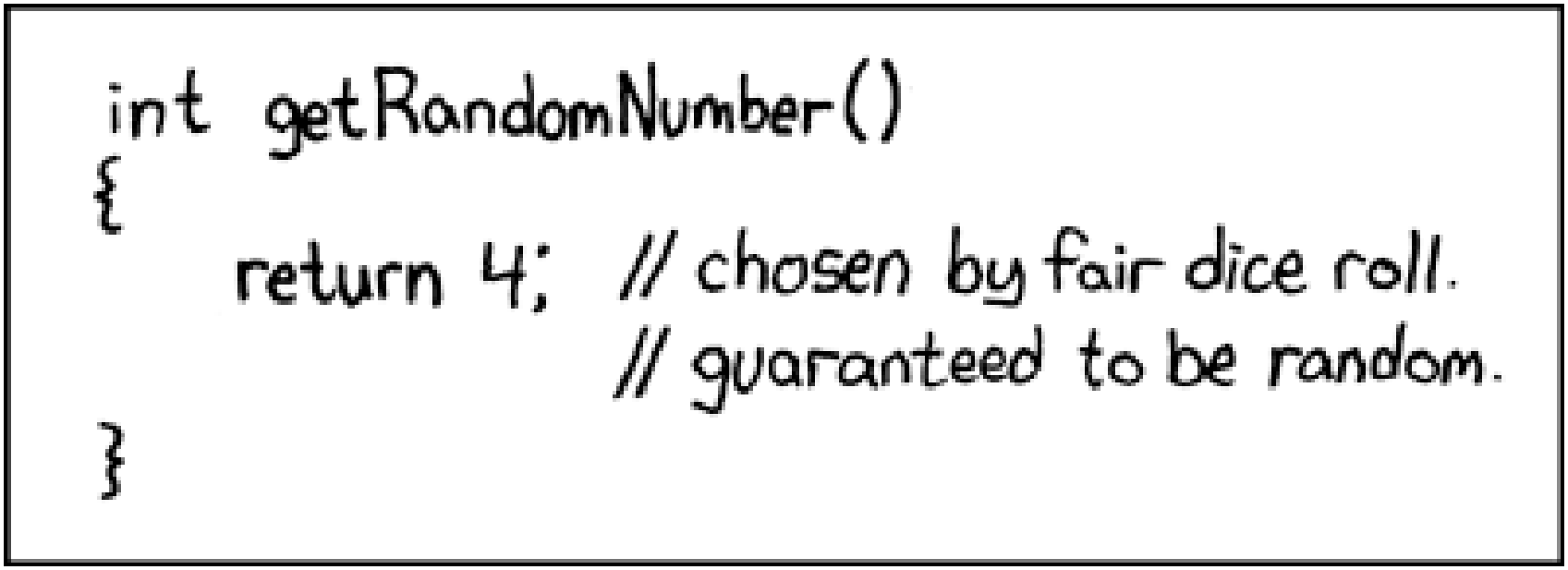
- Time of day RNG seed ≈30 bits
- No/weak seed, all possible keys compromised
- No persistent seed pool
- No NSA Suite B RNG

Randomness and Netscape Browser seed, +01996-01
http://www.cs.berkeley.edu/~daw/papers/ddj-netscape.html

Debian -- Security Information -- DSA-1571-1 openssl, +02008 -05-13
http://www.debian.org/security/2008/dsa-1571

Analysis of the Linux Random Number Generator, Zvi Gutterman and Benny Pinkas and Tzachy Reinman, +02006-03-06
http://eprint.iacr.org/2006/086

NSA Suite B Cryptography - NSA/CSS
http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml



http://xkcd.com/221/

A9-Transport Fail

- HTTP
- Using SSL
- Using TLS 1.1

https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet
http://tools.ietf.org/html/rfc5746

A9-Transport Fail

- Password authentication
- Password authentication over HTTP

https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet

Transport Layer Security (TLS) Renegotiation Indication Extension, February 2010
http://tools.ietf.org/html/rfc5746

A9-Transport Fail

- Exportable CipherSuites
- Weaker CipherSuites

http://csrc.nist.gov/publications/PubsSPs.html#800-131A

Crypto is Hard

- Cryptography is 3,000 years old
- Nearly all crypto prior to 1977 is broken

Crypto is Hard

- Modern cryptology is about 30 years old
- Weak crypto is breakable
- Strong crypto is just not broken yet

Why Cryptography Is Harder Than It Looks
http://www.schneier.com/essay-037.html

Questions?

How NOT to Implement Cryptography for the OWASP Top 10 (Reloaded)
AppSec USA 2011 +02011-09-23T1330Z-05

</body></html>

Connection closed by presenter.

mailto:anthony.j.stieber@gmail.com