Introduction to IT Security

ICCM 2014

June 19, 2014

DEVELOP CENTS

David White

About Me

- Founder of Develop CENTS, an IT consulting company that helps nonprofits & missions organizations.
- Lives in Chattanooga, TN
- Security Nut Case (but no expert)

About Me

- Engaged to the most beautiful girl on earth

Why Have IT Security?

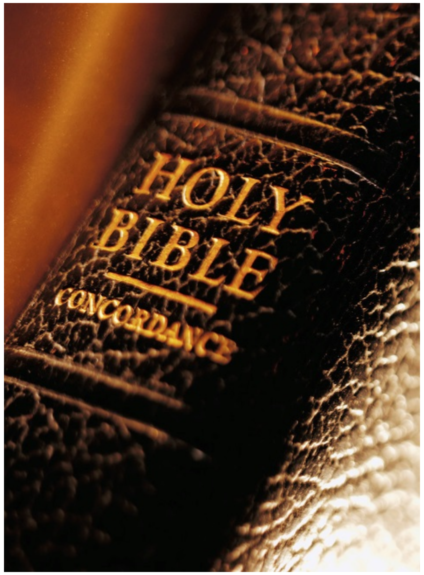
Privacy...

The Naked Private Square by Chris Stamper:
We maintain about our families and goods, and bank statements. We keep the cost of gifts private by removing price tags before wrapping presents.

Why Have IT Security?

Biblical foundation for privacy…

God covered the private parts of the human body.



- Sermon on the Mount (Matthew 6:5-18)

Why Have IT Security?

Physical Security…

- Missionaries working in Creative Access Countries

(Some tax-receiving entities don’t like Missionaries)

Why Not?

Mark Roberts:

- Argues that Early Church shared everything. Very little was private.
- Christians place too much emphasis on Privacy.

The Point?

Responsibility vs. Trusting God…

- Protecting ourselves, our missionaries, our families
- Protecting our identities
- Protecting ourselves physically
-
- ***“We cannot trust our technology. We must trust God.”***

- Pete Holzmann

The Goal…

Visible Ops Security Handbook…

- Security works seamlessly together with other IT departments.
- **Context of Missions**:
- Security for the mission,
  - NOT mission for security.

Important Introductory Concepts

Information Security:

Defending Information (Wikipedia)

Computer Security:

Preserving the integrity, availability, and confidentiality of Information System Resources
- NIST Handbook: Special Publication 800-12

Important Introductory Concepts

A “Secure” Computer…

A secure computer is turned off, unplugged, encased in concrete, buried 5 feet, and guarded 24/7.

Important Introductory Concepts

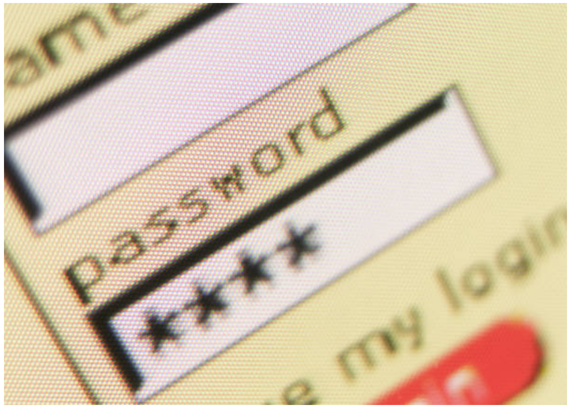
Hackers vs. Crackers

RFC 1983...

A person who delights in having an intimate understanding of the internal workings of a system, computers and computer networks in particular. The term is often misused in a pejorative context, where "cracker" would be the correct term.

Important Introductory Concepts

- **Two-Factor Authentication**
  - Authenticating to a system via two or more of the different means of authentication:
    - What you know
    - What you possess
    - What you are
    - What you do



Encryption

Wikipedia: Encoding messages & information so that only authorized parties can read it.

- The translation of data
- into a secret code.

- 2 Types:
  - Symmetric Key (1 key)
  - Asymmetric Key (2 keys)

Encryption

Encryption != Hashes

- You use hashes to store data that *cannot* be “de-hashed.”
  - Storing passwords, for example

- You use encryption when you or someone else needs to access the data again.

Encryption

Symmetric vs. Asymmetric Encryption...

- Asymmetric Key Encryption
  - Involves a public key and a private key.

Examples:

- HTTPS
- PGP / GnuPG (GPG)
- Key-based SSH Authentication

Encryption

- Encrypted Data at Rest:
  - Data stored on the hard drive that is fully encrypted, even when the machine is off.
  - TrueCrypt, BitLocker, etc…

- Data in Transit
  - Data being sent between server & client
  - HTTPS, SSH, VPN, etc…

Encryption

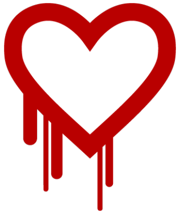
What do you use for data encryption?
Do you trust TrueCrypt? BitLocker?
Built-in Linux Distro tools?

Encryption

The catch?

Encryption is hard to use properly.

Example...



Heartbleed

Any info transmitted between affected machines can be seen by *anyone*.

Heartbleed

So just update the Servers, what’s the big deal?

- Affected code is 2+ years old
- One of *the most critical bugs*
- System Admins aren’t taking it seriously
- Possibly two-thirds of the internet was affected

Heartbleed

Websites weren’t the only thing affected…

Email, Telephone connections (SIP), video conferencing, WiFi hubs, VPN links, instant messaging, were *ALL* affected.

(See ICTA’s article)

Back to Encryption...

The point?

Encryption is hard to use properly.

Another example...

PGP: To Use, or Not To Use

Pretty Good Privacy since 1991…

PGP, when used properly, is secure (according to some)…

- Endorsed by Edward Snowden
- Recommended by “Freedom of the Press” Foundation

PGP: To Use, or Not To Use

The catch?

PGP - and encryption, in general - is hard to use properly.

PGP: To Use, or Not To Use

RFC 4880 (OpenPGP RFC), section 14:

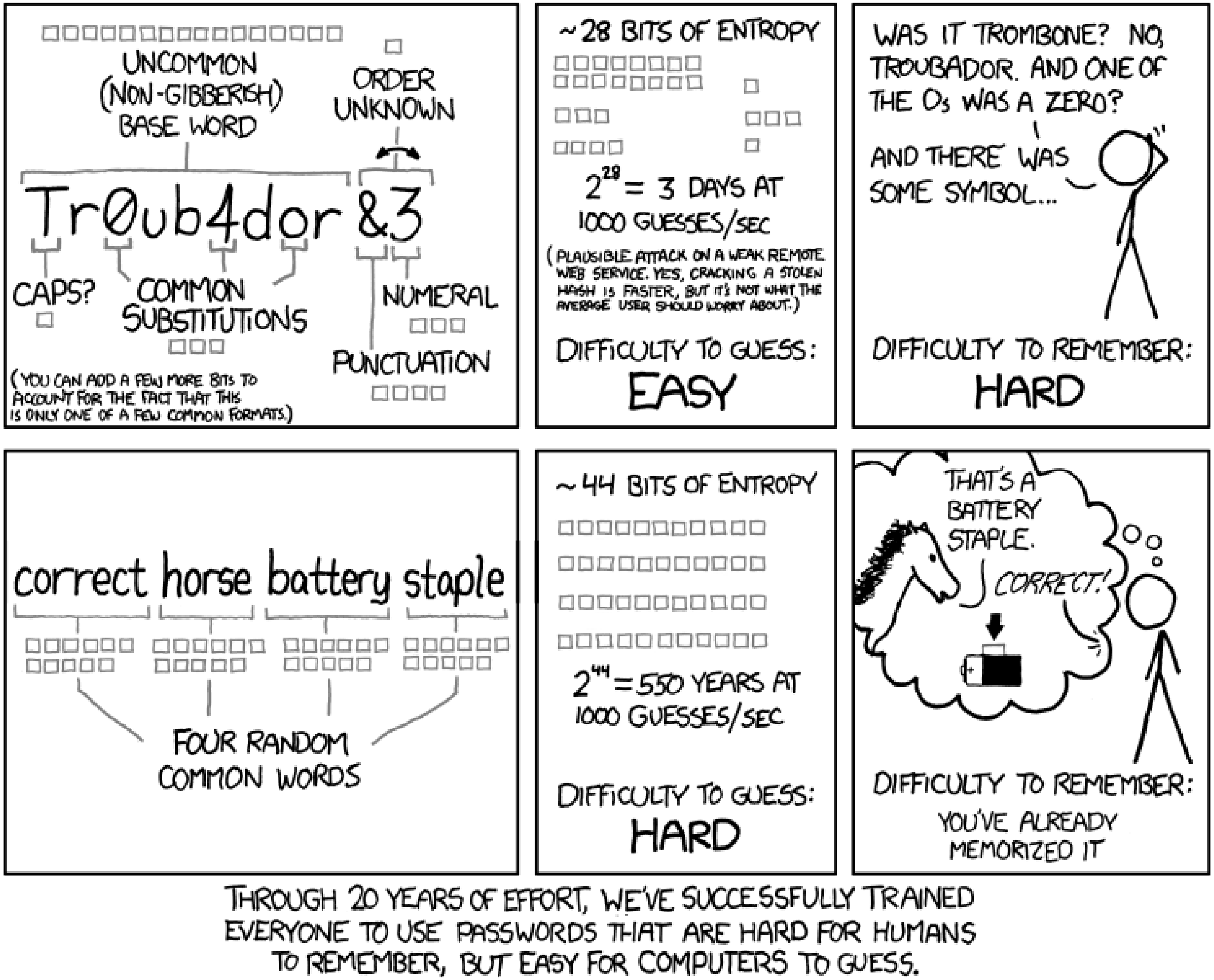
- MD5 Hash algorithm has weaknesses
- Some professionals say you should use a key for encryption, and a different key for signatures.
- The weakest link is enough to make it weak!

PGP Summary

Use at your own risk & at your own discretion

(Do you see a theme here?)

Secure Passwords


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 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 Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 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.

Secure Passwords

So what’s a secure password?

- Combination of memorial phrases and numbers
- At least 15 characters & symbols

(Not your first pet’s name)

Password Management

- LastPass
  - –Cloud Based
  - –Data is encrypted twice
- KeePass
  - –Local Password Manager
  - –My favorite

The End

(Questions & Comments)

DEVELOP
CENTS

David White
http://developcents.com

Online Resources

Security on Stack Exchange:
http://security.stackexchange.com

Internet Storm Center:
https://isc.sans.edu/

US-CERT mailing lists:
http://www.us-cert.gov/mailing-lists-and-feeds

Freedom of the Press Foundation:
“Encryption Works”
https://pressfreedomfoundation.org/encryption-works

Brian Krebs:
http://krebsonsecurity.com/
@briankrebs

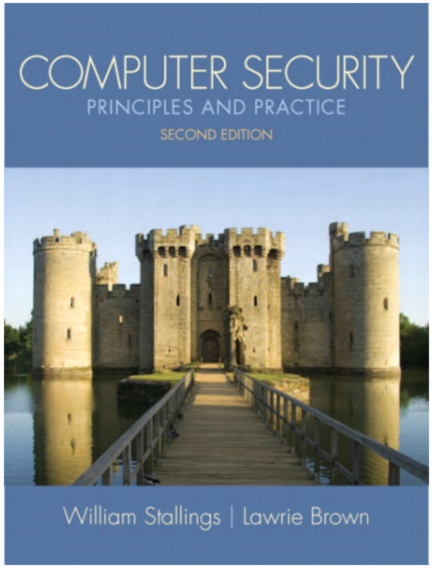
Common Vulnerabilities and Exposures
http://cve.mitre.org/

RFC Database at IETF:
http://www.ietf.org/rfc.html

National Vulnerability Database:
http://nvd.nist.gov/

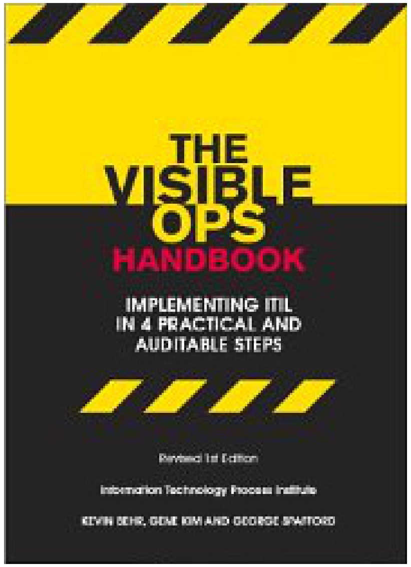
National Institute of Standards & Technology (NIST):
“Computer Security Handbook”
http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/

Books



COMPUTER SECURITY
PRINCIPLES AND PRACTICE
SECOND EDITION

William Stallings | Lawrie Brown



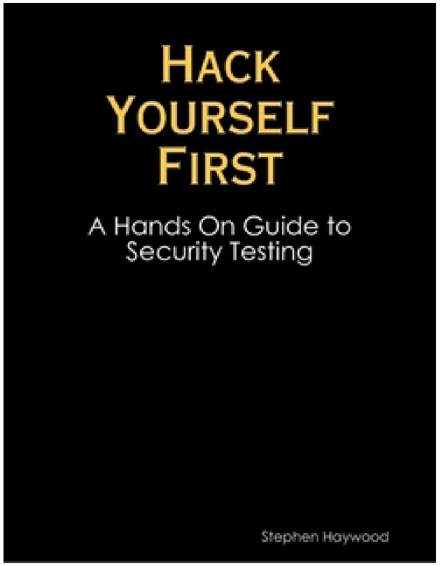
THE VISIBLE OPS HANDBOOK

IMPLEMENTING ITIL
IN 4 PRACTICAL AND
AUDITABLE STEPS

Revised 1st Edition

Information Technology Process Institute

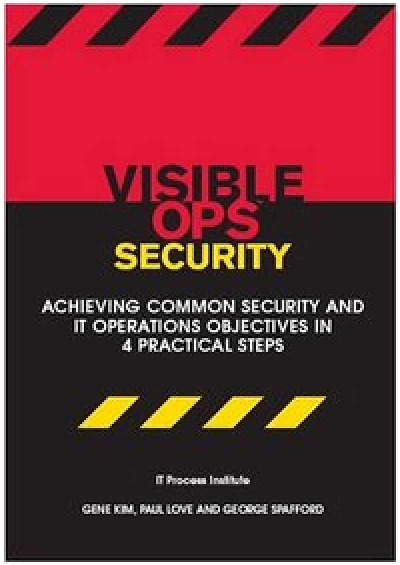
KEVIN BEHR, GENE KIM AND GEORGE SPAFFORD



HACK
YOURSELF
FIRST

A Hands On Guide to
Security Testing

Stephen Haywood



VISIBLE OPS SECURITY

ACHIEVING COMMON SECURITY AND
IT OPERATIONS OBJECTIVES IN
4 PRACTICAL STEPS

IT Process Institute

GENE KIM, PAUL LOVE AND GEORGE SPAFFORD

An eBook By Stephen Haywood, a local Pent Tester & Security Researcher. Available at http://www.Lulu.com.

Other References & Resources

“The Naked Private Square. *Tabletalk Magazine, Forbidden Knowledge: Knowing What We Shouldn’t Know”*, November 2000.

“Privacy and God: From Facebook to a Biblical Theology of Privacy”
http://www.patheos.com/blogs/markdroberts/series/privacy-and-god/

RFC: “Internet User’s Glossary”
http://tools.ietf.org/html/rfc1983

ICTA: “The HeartBleed Bug.”
http://icta.net/HeartBleed/