Prof. Philip Koopman

Carnegie Mellon University

Electrical & Computer ENGINEERING

Security Pitfalls

"On two occasions I have been asked [by members of Parliament]: 'Pray, Mr. Babbage, if you put into the machine wrong figures, will the right answers come out?' I am not able rightly to apprehend the kind of confusion of ideas that could provoke such a question."

– Charles Babbage

Security Pitfalls

Carnegie Mellon University

- Anti-Patterns:
  - Master password
  - Home-made cryptography
  - Encryption used for integrity
  - Unrealistic security assumptions
  - Security via obscurity
- Security can be counter-intuitive
  - Attacks are easier than you might think
    - You must defend everywhere
    - The attacker need only succeed one time

The Konami Code

Security Via Obscurity Is A Bad Idea!

Carnegie Mellon University

- Leaving a key under your doormat…

… is not secure

- Attackers are clever & resourceful
  - They know all the “tricks”
  - They have lots of time to figure things out
  - Networks make systems more accessible

JUL 23, 2012 @ 12:17 PM **Andy Greenberg,** FORBES STAFF

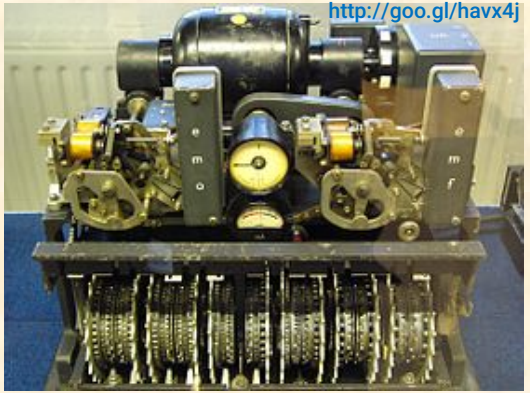
Hacker Will Expose Potential Security Flaw In Four Million Hotel Room Keycard Locks

The system’s vulnerability arises, Brocious says, from the fact that every lock’s memory is entirely exposed to whatever device attempts to read it through that port. Though each lock has a cryptographic key that’s required to trigger its “open” mechanism, that string of data is also stored in the lock’s memory, like a spare key hidden under the welcome mat.

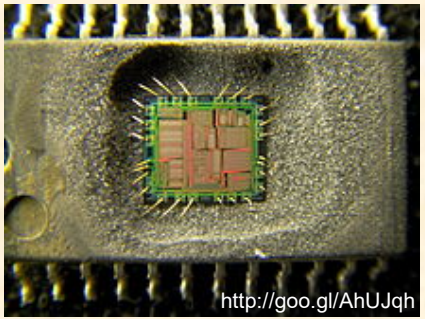
Use Strong Cryptography & Keys

Carnegie Mellon University

- Kerckhoff's Principle (from 1883!)
  - Secrecy should entirely rest on the secret encryption key
  - Assume public encryption algorithm
- Almost always, home-made crypto is breakable
  - Use only public, vetted cryptography & security protocols
  - Use vetted implementations (not the book versions)
- Widely shared "secrets" will be revealed
  - Master passwords will leak out
  - Someone will reverse-engineer a unit
- Strong, unique secret key for each item
  - No record kept at factory (database theft)
  - This pushes systems toward public key cryptography for initial information exchange



Lorenz Cipher Machine: Tunny
(Broken without seeing the machine)



A Chip Peel

Obscurity and Weak Passwords Are Bad!

Carnegie Mellon University

Researchers hack a pacemaker, kill a man(nequin)

Computerworld | Sep 8, 2015 8:08 AM PT

Credit: CAE Healthcare

While killing a simulated human via hacking is less dramatic than wirelessly murdering a real human via a keyboard, researchers said it can be done by "a student with basic information technology and computer science background," the medical mannequin attackers had no penetration testing skills, but successfully launched brute force and denial of service attacks as well as attacks on security controls.

https://goo.gl/Y0zwz0

Reaver Used To Break WPA WiFi Protected Setup PIN

```
/*      efdtt.c      Author:  Charles M. Hannum <root@ihack.net>                */
/*      Thanks to Phil Carmody <fatphil@asdf.org> for additional tweaks.        */
/*      DVD-logo shaped version by Alex Bowley <alex@hyperspeed.org>            */
/*      Usage is:  cat title-key scrambled.vob | efdtt >clear.vob               */
#define m(i)(x[i]^s[i+84])<<

                  unsigned char x[5]      ,y,s[2048];main(
                  n){for( read(0,x,5     );read(0,s ,n=2048
                              write(1    ,s,n)          )if(s
                [y=s      [13]%8+20]  /16%4  ==1       ){int
                i=m(      1)17  ^256 +m(0)   8,k       =m(2)
                0,j=      m(4)   17^ m(3)   9^k*      2-k%8
                ^8,a      =0,c    =26;for   (s[y]     -=16;
               --c;j  *=2)a=      a*2^i&    1,i=i /2^j&1
               <<24;for(j=         127;     ++j<n;c=c>
```

https://goo.gl/PvzgQy

DVD Decrypt in C (ASCII Art Version)

Only a 40-bit key

POLISH TEEN HACKS HIS CITY'S TRAMS, CHAOS ENSUES

CHUCK SQUATRIGLIA AUTOPIA 01.11.08 1:29 PM

A teenager in Lodz, Poland hacked the city's tram system with a homemade transmitter that tripped rail switches and redirected trains, a prank that derailed four trams and injured a dozen people.

https://goo.gl/LS0VD9

According to reports in the Register and the Telegraph, the 14-year-old boy – described by his teachers as an electronics genius (Gee- you think?) – spent months studying the city's rail lines to determine the best places to redirect trains and cause the most havoc, then converted an old TV remote into an infrared transmitter capable for tripping the switches.

How You Use Cryptography Matters

Carnegie Mellon University

- Use the right mechanism for the job
  - Encryption for secrecy, not for authentication
  - Use secure hash/digital signature for integrity
- Don't forget about export restrictions
  - Encryption might be weakened by short keys
  - Typically no strength limits on hash/signatures
- Consider your assumptions
  - Proprietary protocols are obscurity, not security
  - Firewalls are often permeable
  - Customers will leave default configuration
- Make the system usable
  - People prefer weak passwords (1234, 777)
  - Complex passwords get written on sticky notes

Davis Besse Nuclear Power Plant

Event: Aug 20, 2003 Slammer worm infects plant

Impact: Complete shutdown of digital portion of Safety Parameter Display System (SPDS) and Plant Process Computer (PPC)

Specifics: Worm started at contractors site

- Worm jumped from corporate to plant network and found an unpatched server
- Patch had been available for 6 months

Homeland Security

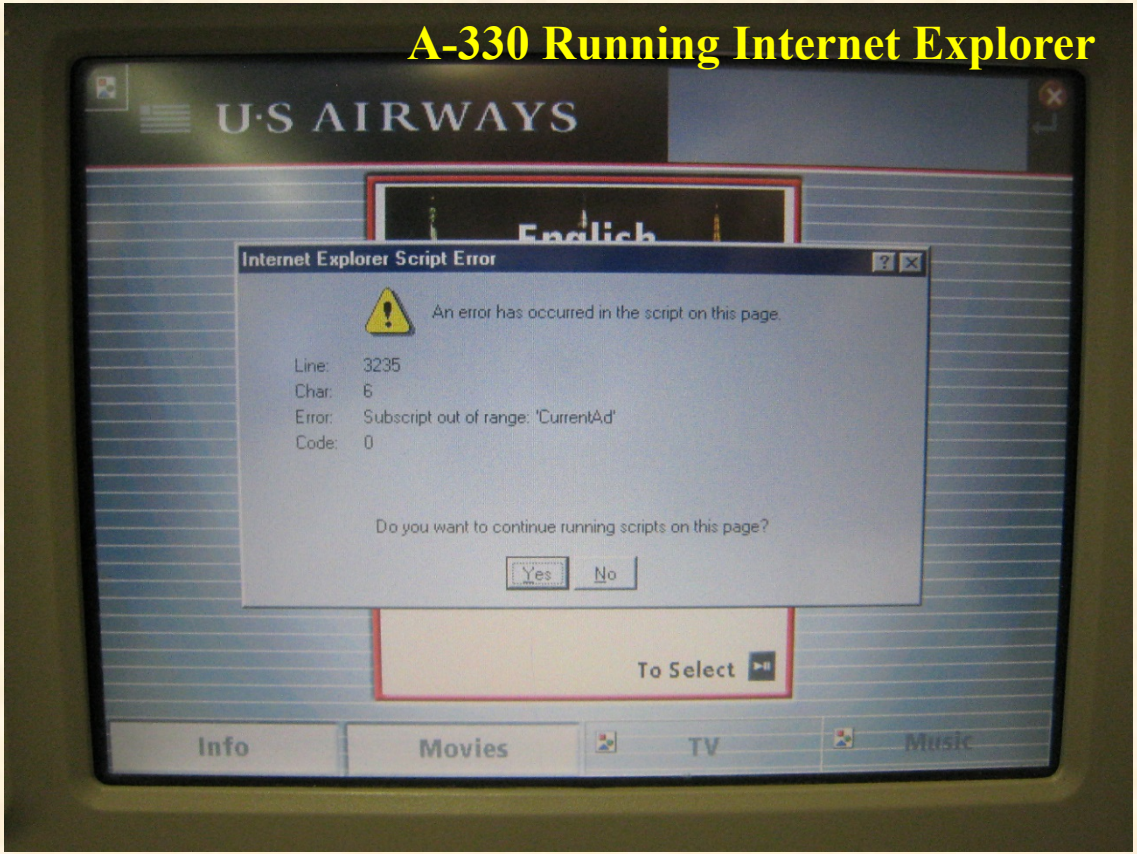
Lessons learned:

- Secure remote (trusted) access channels
- Ensure Defense-in-depth strategies with appropriate procurement requirements
- Critical patches need to be applied

https://goo.gl/1opMJP

Aircraft Flight Controls ⇔ Seatbacks?

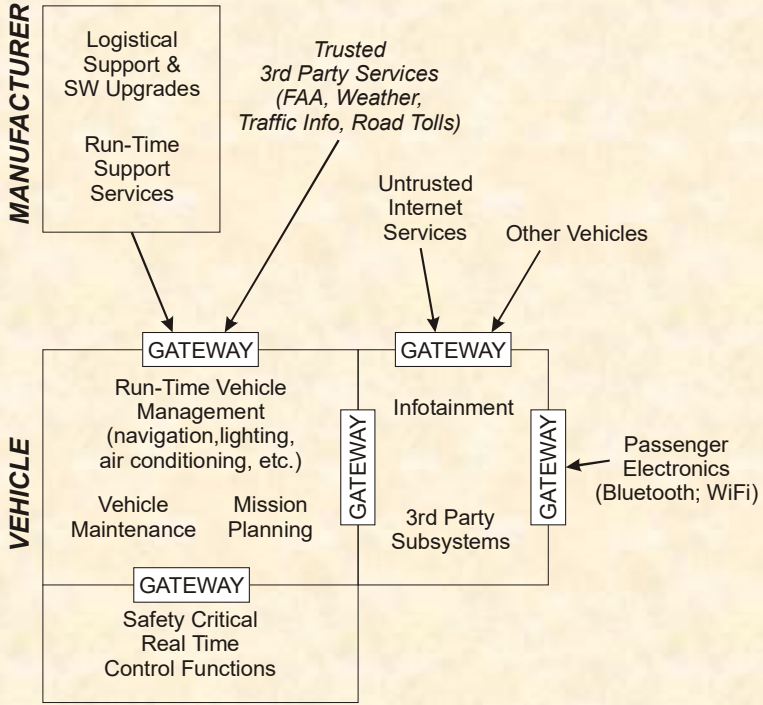
Carnegie Mellon University



Secure Communications & Firewalls

Carnegie Mellon University

- Securing safety critical + infotainment
  - Insert a firewall (helps, but has limitations)
  - Add integrity checks in data field
  - Encrypt (but, this might not help with integrity)
- Most legacy embedded networks insecure
  - No encryption
  - No authentication
  - Non-secure integrity checks (CRC, checksum)
- Many pitfalls here – tricky area
  - Usually "air gap" is infeasible due to functionality
  - Avoid permitting general purpose/risky packets through firewall



Security Testing Isn't Enough

Carnegie Mellon University

- **Security testing typically finds currently known problems**
  - Some problems known but not publicly announced
    - "Zero Day" vulnerabilities
  - More problems will be discovered after you ship ➔ patches
- **Attacks will likely increase over time**
  - How will you respond to emergent threats?
- **Use lists of common weaknesses to avoid making mistakes**
  - https://cwe.mitre.org/index.html

Forbes / Security MAR 23, 2012 @ 09:43 AM

Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits

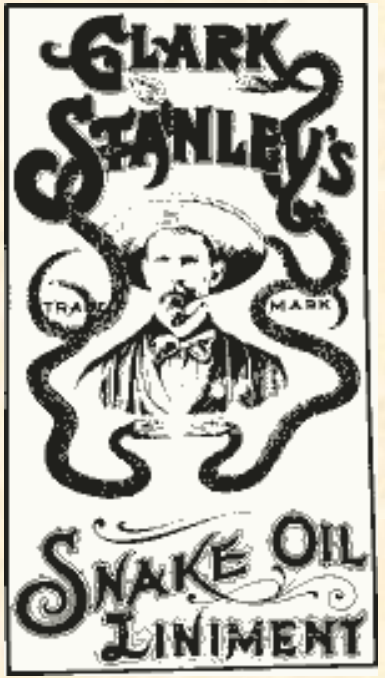
Andy Greenberg
FORBES STAFF

ADOBE READER	$5,000-$30,000
MAC OSX	$20,000-$50,000
ANDROID	$30,000-$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000-$100,000
MICROSOFT WORD	$50,000-$100,000
WINDOWS	$60,000-$120,000
FIREFOX OR SAFARI	$60,000-$150,000
CHROME OR INTERNET EXPLORER	$80,000-$200,000
IOS	$100,000-$250,000

http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/

Security Snake Oil (avoid these!)

- Secret system
  - Security claims rest even in part on "we won't tell you how we do it" or "we have a proprietary algorithm"
  - Good systems are secure even against the actual system designer
  - Security should be based on the secret key (which means the actual system designer can't know the secret key in all devices)
- Technobabble
  - Buzzwords don't make you secure
- We're "unbreakable"
  - No, they're not. Best you can do is a sufficiently high cost to break
- Strong claims about weak systems
  - 2008 hard drive used AES for encrypting the key – but only XORd the key with the data
  - Are secret keys sent in unencrypted?
  - Does the manufacturer have a back door device key?



http://www.h-online.com/security/features/Enclosed-but-not-encrypted-746199.html

http://en.wikipedia.org/wiki/Snake_oil_(cryptography)

Best Practices For Avoiding Security Pitfalls

Carnegie Mellon University

- Avoid Common Pitfalls:
  - Security via obscurity
  - Master password
  - Home-made cryptography
  - Encryption used for integrity
  - Unrealistic security assumptions
- Consult a specialist
  - Security is complex & often counter-intuitive; get some help!

How To Hack An Electronic Road Sign

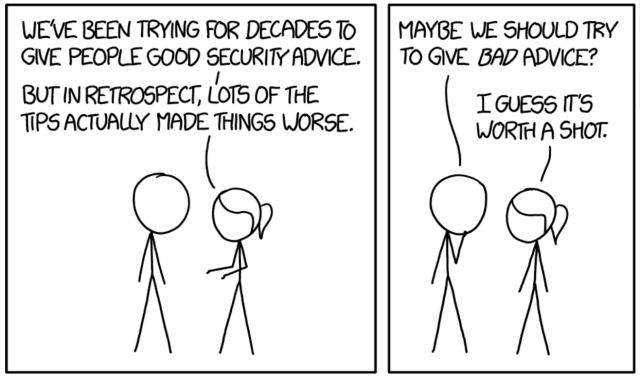
Ben Wojdyla
1/28/09 5:00pm · Filed to: NOVELTIES

JALOPNIK

http://jalopnik.com/[redacted]

DO NOT under any circumstances run around hacking into electronic road signs using the information contained in this step-by-step guide of how to transmit hilarious messages to passing motorists.

** HACKER TIPS ** Should it will ask you for a password. Try "[redacted]", the default password.
In all likelihood, the crew will not have changed it. Howeve they did, never fear. Hold "Control" and "Shift" and while holding, enter "[redacted]". This will reset the sign and reset the password to "[redacted]" in the process. You're in!



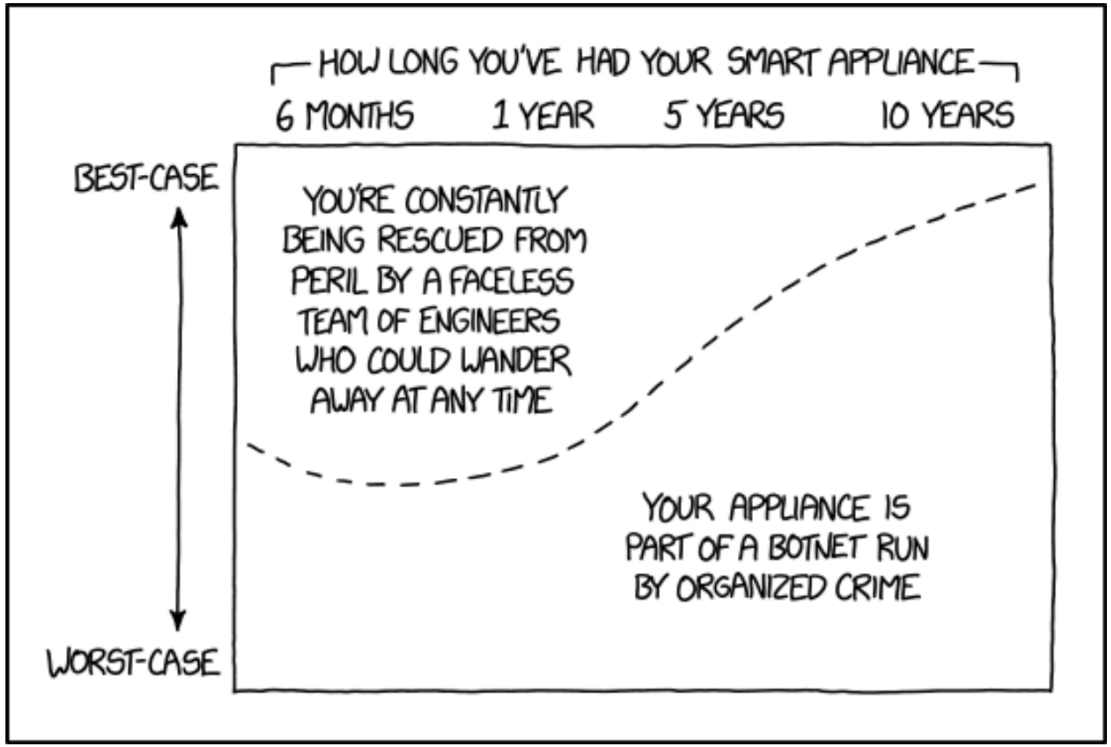
SECURITY TIPS

(PRINT OUT THIS LIST AND KEEP IT IN YOUR BANK SAFE DEPOSIT BOX.)

- DON'T CLICK LINKS TO WEBSITES
- USE PRIME NUMBERS IN YOUR PASSWORD
- CHANGE YOUR PASSWORD MANAGER MONTHLY
- HOLD YOUR BREATH WHILE CROSSING THE BORDER
- INSTALL A SECURE FONT
- USE A 2-FACTOR SMOKE DETECTOR
- CHANGE YOUR MAIDEN NAME REGULARLY
- PUT STRANGE USB DRIVES IN A BAG OF RICE OVERNIGHT
- USE SPECIAL CHARACTERS LIKE & AND %
- ONLY READ CONTENT PUBLISHED THROUGH TOR.COM
- USE A BURNER'S PHONE
- GET AN SSL CERTIFICATE AND STORE IT IN A SAFE PLACE
- IF A BORDER GUARD ASKS TO EXAMINE YOUR LAPTOP, YOU HAVE A LEGAL RIGHT TO CHALLENGE THEM TO A CHESS GAME FOR YOUR SOUL.

https://xkcd.com/1820/

Smart Home Security



If they're getting valuable enough stuff from you, at least the organized crime folks have an incentive to issue regular updates to keep the appliance working after the manufacturer discontinues support.

https://www.xkcd.com/1966/