"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
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
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

Security Via Obscurity Is A Bad Idea!

http://goo.gl/b03ncJ
Use Strong Cryptography & Keys

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
Researchers hack a pacemaker, kill a man(nequin)

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.

Reaver Used To Break WPA WiFi Protected Setup PIN

Obscurity and Weak Passwords Are Bad!

DVD Decrypt in C (ASCII Art Version)

Only a 40-bit key

POLISH TEEN HACKS HIS CITY’S TRAMS, CHAOS ENSUES

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.

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

- 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

[Image of a bike rack]

[Image of a document with text: Davis Besse Nuclear Power Plant]

[Image of a document with text: Homeland Security]

Security Testing Isn’t Enough

- Security testing typically finds currently known problems
  - Some problems known but not publicly announced
  - More problems will be discovered after you ship

- 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

<table>
<thead>
<tr>
<th>Software</th>
<th>Price Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADOBE READER</td>
<td>$5,000-$30,000</td>
</tr>
<tr>
<td>MAC OSX</td>
<td>$20,000-$50,000</td>
</tr>
<tr>
<td>ANDROID</td>
<td>$30,000-$60,000</td>
</tr>
<tr>
<td>FLASH OR JAVA BROWSER PLUG-INS</td>
<td>$40,000-$100,000</td>
</tr>
<tr>
<td>MICROSOFT WORD</td>
<td>$50,000-$100,000</td>
</tr>
<tr>
<td>WINDOWS</td>
<td>$60,000-$120,000</td>
</tr>
<tr>
<td>FIREFOX OR SAFARI</td>
<td>$60,000-$150,000</td>
</tr>
<tr>
<td>CHROME OR INTERNET EXPLORER</td>
<td>$80,000-$200,000</td>
</tr>
<tr>
<td>IOS</td>
<td>$100,000-$250,000</td>
</tr>
</tbody>
</table>

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://en.wikipedia.org/wiki/Snake_oil_(cryptography)
© 2017 Philip Koopman
Most embedded networks are not secure
- No encryption
- No authentication
- Non-secure integrity checks (CRC, checksum)

Possible approaches
- Insert a firewall (helps, but has limitations)
- Add integrity checks in data field
- Encrypt (but, this might not help with integrity)

Many pitfalls here – tricky area
- Usually “air gap” is infeasible due to functionality
- Avoid permitting general purpose/risky packets through firewall
Aircraft Flight Controls ⇔ Seatbacks?

A-330 Running Internet Explorer

- Altitude: 32956 ft
- Ground Speed: 477 mph
- Outside Air Temperature: -72 °F
- Head Wind: 50 mph

Internet Explorer Script Error:
An error has occurred in the script on this page.

- Line: 3235
- Char: 6
- Error: Subscript out of range: 'CurrentAd'
- Code: 0

Do you want to continue running scripts on this page?

Yes  No
Best Practices For Avoiding Security Pitfalls

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!