Reading Discussion

Blown to Bits

Chapter 5

Secret Bits

How Codes Became Unbreakable

Notes for CSC 100 - The Beauty and Joy of Computing
The University of North Carolina at Greensboro

A comment rather than a question...

What is this *book* about?

It's about ***Your Life, Liberty, and Happiness***

If you are focusing on the technology then you're missing the point. It's how technology impacts and interacts with society and the trade-offs that come with new technologies.

With that in mind...

What was the point of the chapter?

Some misconceptions...

Did the 9/11 hijackers use encryption?

Is perfectly secure encryption possible?

Encryption and the US Government

Encryption algorithm development

DES: Data Encryption Standard (1974-1976) [56 bit key]

- Proposals solicited in 1972
- Second call brought in IBM's Lucifer cipher
- NSA made two significant changes
- Result became standard after some review
- Significant paranoia about those two changes

Skipjack: Embedded in the "Clipper Chip" (1993) [80 bit key]

- Secret algorithm! (a bad idea from a security standpoint, so why?)
- Key escrow - government can eavesdrop!

AES: Advanced Encryption Standard (2001) [128-256 bit key]

- Open competition - no "modifications"
- Final winner wasn't even an American submission!
- NSA has approved for secret and top secret information encryption
- 128-bit key brute force using a million fast computers takes 10^{16} years
  (the universe is only about 10^{10} years old...)

Encryption and the US Government

Controlling the technology

Cryptography traditionally seen as a military technology

- Before 1996: Import/export controlled by ITAR (International Traffic in Arms Regulations)
  - Could not export software or hardware for strong (>40-bit) cryptography
  - Browsers used to have "US-only" and "International" versions
  - BUT: Crypto software was always widely available
- In 1996 control transferred to EAR (Export Administration Regulations) - commercial rather than military
- Now controlled by Dept of Commerce, and greatly relaxed rules
  - *Still lots of rules - best to talk to a lawyer if you make a crypto product!*

Some lawsuits:

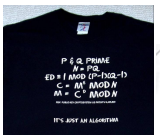
- Phil Zimmerman under investigation after 1991 release of PGP (until 1996)
- Dan Bernstein (crypto researcher) won a lawsuit on free speech grounds
  - Books had been considered "free speech" but not software
  - Odd consequence: "Applied Cryptography" distributed outside US with all source code printed, but not on electronic media

Tales from the Crypto Wars...

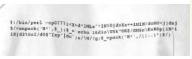
Export restriction silliness...

Can a T-shirt be a munition?

The algorithm...



A program (in perl)...



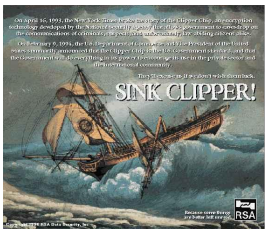
What about a tatoo?

Machine readable...

Tales from the Crypto Wars...

Clipper Chip Protests

Blatant government grab for encryption control incited lots of protest



Should government have access to keys?

England passed law in 2007 making it mandatory to turn over keys when legally requested.

Does our Bill of Rights make this impossible?

- 4th Amendment: Prohibiting unreasonable search and seizure
- 5th Amendment: Protection against self-incrimination

What do ***you*** think?

Public Attitudes Toward Cryptography

Much (like HTTPS) taken for granted

- Transparent, don't need to think about
- A lot of trust is put in browser's CA list
  - And warnings are often just ignored...
- Adds load to server, but most (all?) big sites not offer "https-only" option

Relatively transparent encryption:

- HTTPS and accessing mail server via TLS/IMAP
- Skype (but is that end-to-end secure?)

Requires work, and often people don't bother:

- E-mail
- Chat

Attitude with most people seems to be "I'll use whatever is easiest"