CSE 484 / CSE M 584 (Autumn 2011)

# Software Security (Day 3) & Introduction to Cryptography

Daniel Halperin
Tadayoshi Kohno

Thanks to Dan Boneh, Dieter Gollmann, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...

# Updates Oct. 10th

- Coffee/tea signup sheet posted (optional)
  - First is tomorrow @2 pm. Meet in CSE Atrium
- Security reviews & Current events
  - Instructions on Catalyst; one each due 11/4 and 12/2
- **Reading:** over the next few days, Crypto chapters (Ch. 12--15, ~50 pages) in Daswani et al.
  - Chapter 12 by Wednesday

# Today

- Principles for Software Design
- Introduction to Cryptography

# Fuzz Testing

- Generate "random" inputs to program
  - Sometimes conforming to input structures (file formats, etc)
- See if program crashes
  - If crashes, found a bug
  - Bug may be exploitable
- Surprisingly effective

- Now standard part of development lifecycle

# Genetic Diversity

# Genetic Diversity

- Problems with Monoculture

# Genetic Diversity

- Problems with Monoculture

# Genetic Diversity

- Problems with Monoculture
- Steps toward diversity
  - Automatic diversification of compiled code
  - Address Space Randomization

# Genetic Diversity

- Problems with Monoculture
- Steps toward diversity
  - Automatic diversification of compiled code
  - Address Space Randomization
- Example in Tor:
  - users get lists of relays from "directory authorities"
  - require signatures from 4/7 authorities to accept
  - variety of OS'es, crypto libs, etc.
  - Works: only 3 servers compromised by Debian SSL bug

# Principles

- Open design?  Open source?
- Maybe...

- Linux Kernel Backdoor Attempt:  http://www.freedom-to-tinker.com/?p=472

- PGP Corporation:  http://www.pgp.com/developers/sourcecode/index.html

# Principles

- Check inputs

# Principles

- Least privilege

# Principles

- Check all return values

# Principles

- Securely clear memory (passwords, keys, etc)

# Principles

- Failsafe defaults

# Principles

- Defense in Depth

- Also
  - Prevent
  - Detect
  - Deter

# Schneier on Security

A blog covering security and security technology.

« Pork-Filled Counter-Islamic Bomb Device | Main | Security Vulnerabilities of Smart Electricity Meters »

## July 28, 2010

### DNSSEC Root Key Split Among Seven People

The DNSSEC root key has been divided among seven people:

> Part of ICANN's security scheme is the Domain Name System Security, a security protocol that ensures Web sites are registered and "signed" (this is the security measure built into the Web that ensures when you go to a URL you arrive at a real site and not an identical pirate site). Most major servers are a part of DNSSEC, as it's known, and during a major international attack, the system might sever connections between important servers to contain the damage.
>
> A minimum of five of the seven keyholders -- one each from Britain, the U.S., Burkina Faso, Trinidad and Tobago, Canada, China, and the Czech Republic -- would have to converge at a U.S. base with their keys to restart the system and connect everything once again.

That's a secret sharing scheme they're using, most likely Shamir's Secret Sharing.
We know the names of some of them.

> Paul Kane -- who lives in the Bradford-on-Avon area -- has been chosen to look after one of seven keys, which will 'restart the world wide web' in the event of a catastrophic event.

Dan Kaminsky is another.

I don't know how they picked those countries.

# Principles

- Reduce size of TCB
- Simplicity
- Modularity

# Vulnerability Analysis and Disclosure

- What do you do if you've found a security problem in a real system?
- Say
  - A commercial website?
  - UW grade database?
  - iPhone?
  - Boeing 787?