Thanks to Franzi Roesner, Dan Boneh, Dieter Gollmann, Dan Halperin, David Kohlbrenner, Yoshi Kohno, Ada Lerner, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...
Admin

• Lab 1a: Oct 15
  • That is, sploits 1-3
  • When you are ‘done,’ stop changing those files.
  • You really want to have started by now!
Another Type of Vulnerability

• Consider this code:

```c
char buf[80];
void vulnerable() {
    int len = read_int_from_network();
    char *p = read_string_from_network();
    if (len > sizeof buf) {
        error("length too large, nice try!");
        return;
    }
    memcpy(buf, p, len);
}

void *memcpy(void *dst, const void * src, size_t n);
typedef unsigned int size_t;
```
Another Type of Vulnerability

• Consider this code:

```c
char buf[80];
void vulnerable() {
    long long len = read_int_from_network();
    char *p = read_string_from_network();
    if (len > sizeof buf) {
        error("length too large, nice try!");
        return;
    }
    memcpy(buf, p, len);
}
```

```c
typedef unsigned int size_t;
```
Timing Attacks

• Assume there are no “typical” bugs in the software
  • No buffer overflow bugs
  • No format string vulnerabilities
  • Good choice of randomness
  • Good design

• The software may still be vulnerable to timing attacks
  • Software exhibits input-dependent timings

• Complex and hard to fully protect against
Hey what about if its over a network?

• “Remote timing attacks are practical” - 2005
  • David Brumley, Dan Boneh
Other Examples

• Plenty of other examples of timings attacks
  • Timing cache misses
    • Extract cryptographic keys...
    • Recent Spectre/Meltdown attacks
  • Duration of a rendering operation
    • Extract webpage information
  • Duration of a failed decryption attempt
    • Different failures mean different thing (e.g., Padding oracles)
Side-channels

• **Timing** is only one possibility

• Consider:
  • Power usage
  • Audio
  • EM Outputs
General Principles

• Check inputs
• Check all return values
• Least privilege
• Securely clear memory (passwords, keys, etc.)
• Failsafe defaults
• Defense in depth
  • Also: prevent, detect, respond
General Principles

• Reduce size of trusted computing base (TCB)
• Simplicity, modularity
  • But: Be careful at interface boundaries!
• Minimize attack surface
• Use vetted components
• Security by design
  • But: tension between security and other goals
• Open design? Open source? Closed source?
  • Different perspectives
Does Open Source Help?

• Different perspectives...

• Positive example?
  • Linux kernel backdoor attempt thwarted (2003)
    (http://www.freedom-to-tinker.com/?p=472)

• Negative example?
  • Heartbleed (2014)
    • Vulnerability in OpenSSL that allowed attackers to read arbitrary memory from vulnerable servers (including private keys)
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?
  • Boeing 787?
  • TSA procedures?

Breakout Groups:
What would you do? What ethical questions come up?
Vulnerability Analysis and Disclosure

• Suppose companies A, B, and C all have a vulnerability, but have not made the existence of that vulnerability public.

• Company A has a software update prepared and ready to go that, once shipped, will fix the vulnerability; but B and C are still working on developing a patch for the vulnerability.

• Company A learns that attackers are exploiting this vulnerability in the wild.

• Should Company A release their patch, even if doing so means that the vulnerability now becomes public and other actors can start exploiting Companies B and C?

• Or should Company A wait until Companies B and C have patches?
Next Major Section of the Course: Cryptography
Terminology Note: "blockchain" and "crypto"

- Rising interest, mostly in the cryptocurrency space

- For this course: crypto means "cryptography"
Common Communication Security Goals

**Privacy of data:**
Prevent exposure of information

**Integrity of data:**
Prevent modification of information
Recall Bigger Picture

- Cryptography only one small piece of a larger system
- Must protect entire system
  - Physical security
  - Operating system security
  - Network security
  - Users
  - Cryptography (following slides)
- Recall the weakest link

- Still, cryptography is a crucial part of our toolbox
XKCD:  http://xkcd.com/538/
History

• Substitution Ciphers
  • Caesar Cipher
• Transposition Ciphers
• Codebooks
• Machines

• Recommended Reading: *The Codebreakers* by David Kahn and *The Code Book* by Simon Singh.
History: Caesar Cipher (Shift Cipher)

- Plaintext letters are replaced with letters fixed shift away in the alphabet.
- Example:
  - Plaintext: The quick brown fox jumps over the lazy dog
  - Key: Shift 3
    
    | A | B | C | D | E | F |
    |---|---|---|---|---|---|
    | G | H | I | J | K | L |
    | M | N | O | P | Q | R |
    | S | T | U | V | W | X |
    | Y | Z | A | B | C | D |

  - Ciphertext: WKHTX LFNEU RZQIR AMXPS VRYHU WKHOD CBGRJ
History: Caesar Cipher (Shift Cipher)

- ROT13: shift 13 (encryption and decryption are symmetric)
- What is the key space?
  - 26 possible shifts.
- How to attack shift ciphers?
  - Brute force.
History: Substitution Cipher

- **Superset of shift ciphers:** each letter is substituted for another one.
- One way to implement: **Add a secret key**
- Example:
  - Plaintext: `ABCDEFGHIJKLMNOPQRSTUVWXYZ`
  - Cipher: `ZEBRAS CDFGHIJKLMNOPQTUVWXY`
- “State of the art” for thousands of years
History: Substitution Cipher

• What is the key space?
• How to attack?
  • Frequency analysis.

26! ≈ 2^88

Bigrams:
- th 1.52%
- he 1.28%
- in 0.94%
- er 0.94%
- an 0.82%
- re 0.68%
- nd 0.63%
- at 0.59%
- on 0.57%
- nt 0.56%
- ha 0.56%
- es 0.56%
- st 0.55%

Trigrams:
1. the
2. and
3. tha
4. ent
5. ing
6. ion
7. tio
8. for
9. nde
10. has
11. nce
12. edt
13. tis
14. oft
15. sth
History: Enigma Machine

Uses rotors (substitution cipher) that change position after each key.

Key = initial setting of rotors

Key space?

26^n for n rotors
How Cryptosystems Work Today

• **Layered approach:** Cryptographic protocols (like “CBC mode encryption”) built on top of cryptographic primitives (like “block ciphers”)

• **Flavors of cryptography:** Symmetric (private key) and asymmetric (public key)

• Public algorithms (*Kerckhoff’s Principle*)

• Security proofs based on assumptions (*not this course*)

• Be careful about inventing your own! (If you just want to use some crypto in your system, use vetted libraries!)
The Cryptosystem Stack

• Primitives:
  • AES / DES / etc
  • RSA / ElGamal / Elliptic Curve (ed25519)

• Modes:
  • Block modes (CBC, ECB, CTR, GCM, ...)
  • Padding structures

• Protocols:
  • TLS / SSL / SSH / etc

• Usage of Protocols:
  • Browser security
  • Secure remote logins
Kerckhoff’s Principle

- Security of a cryptographic object should depend only on the secrecy of the secret (private) key.
- Security should not depend on the secrecy of the algorithm itself.
- Foreshadow: Need for randomness – the key to keep private
Flavors of Cryptography

• Symmetric cryptography
  • Both communicating parties have access to a shared random string $K$, called the key.

• Asymmetric cryptography
  • Each party creates a public key $pk$ and a secret key $sk$.
  • Hard concept to understand, and revolutionary! Inventors won Turing Award 😊