Admin

• Lab 1
  • **Checkpoint due today (11:59pm)**
  • Sploits 4-7 due 02/01 (11:59pm)
  • Reminder that you have **5 late days** you can use throughout the quarter
    • Up to 3 at a time
    • Everyone in a group uses them simultaneously
    • You must indicate on the assignment how many late days you are taking!
Software Security: So what do we do?
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?
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?
Realistic Security
How do we make everything secure?

• “Educate users!”
  • Then they can’t make mistakes!
• “Educate developers!”
  • Then they can’t make mistakes!
• Or…
  - phished / good / no buffer overflow
  - build tools that just work
  - users applications that are secure by default
Next Major Section of the Course: Cryptography
Aside: “blockchain” and “crypto”

• Rising interest, mostly in the cryptocurrency space

• Crypto will, for this course, exclusively mean “cryptography”

• While blockchain sometimes has neat crypto ideas, its not going to come up here
Next Major Section of the Course: 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

**A CRYPTO NERD’S IMAGINATION:**

- His laptop’s encrypted.
- Let’s build a million-dollar cluster to crack it.

**WHAT WOULD ACTUALLY HAPPEN:**

- His laptop’s encrypted.
- Drug him and hit him with this $5 wrench until he tells us the password.

Blast! Our evil plan is foiled!

GOT IT.
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 a fixed shift away in the alphabet.

- Example:
  - Plaintext: The quick brown fox jumps over the lazy dog
  - Key: Shift 3
    
    | ABCDEFGHIJKLMNOPQRSTUVWXYZ |
    | DEFHIJKLMNOPQRSTUVWXYZABC |
  
  - 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.

\[
26! \approx 2^{88}
\]

**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 6. ion 11. nce
2. and 7. tio 12. edt
3. tha 8. for 13. tis
4. ent 9. nde 14. oft
5. ing 10. has 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!)
Cryptographic tools, primitives, and more

- **Primitives**
  - RSA
  - SHA

- **Conceptual Tools**
  - E2E

- **Tools**
  - SSH
The Cryptosystem Stack

• Primitives:
  • AES / DES / etc
  • RSA / ElGamal / Elliptic Curve (ed25519)
• Modes:
  • Block modes (CBC, ECB, CTR, GCM, ...)
  • Padding structures
• Protocols:
  • TLS / SSL / etc
• Usage of Protocols:
  • Browser security
  • SSH connections

Hashing: SHA, MD5, etc
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.
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 😊*

- AES, DES, RSA, ECC
Received April 4, 1977

A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

R.L. Rivest, A. Shamir, and L. Adleman∗

Abstract

An encryption method is presented with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key. This has two important consequences:

1. Couriers or other secure means are not needed to transmit keys, since a message can be encrypted using an encryption key publicly revealed by the intended recipient. Only he can decipher the message, since only he knows the corresponding decryption key.

2. A message can be “signed” using a privately held decryption key. Anyone can verify this signature using the corresponding publicly revealed encryption key. Signatures cannot be forged, and a signer cannot later deny the validity of his signature. This has obvious applications in “electronic mail” and “electronic funds transfer” systems.
Both communicating parties have access to a shared random string $K$, called the key.
Each party creates a public key $pk$ and a secret key $sk$. 
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 $sk$. 
Flavors of Cryptography

• Symmetric cryptography
  • Both communicating parties have access to a shared random string $K$, called the key.
  • Challenge: How do you privately share a key?

• Asymmetric cryptography
  • Each party creates a public key $pk$ and a secret key $sk$.
  • Challenge: How do you validate a public key?