Announcement

ITIS 6200 / 8200

- Course Evaluation! (Canvas)
  - Extra 1%
- Project #3 due today
- Final Exam (schedule)
  - Dec.14 8-11:30 am
  - About 9-10 Questions
- 4 Quizzes
  - Single-choice questions; about 10 questions each
  - To be release between Dec.6 and Dec.10
- Class Participation Credits (extra 5% max)
  - Baseline: 1%
  - If you want more than 1%, come to any of my office hours starting today (Dec.5)

Today’s plan: Final Review

- Brief Review of Key Concepts
- Q & A

Security Principles

- What are the security principles?
- Identify security examples being used
- Give real life examples of security principles

Cryptography Roadmap

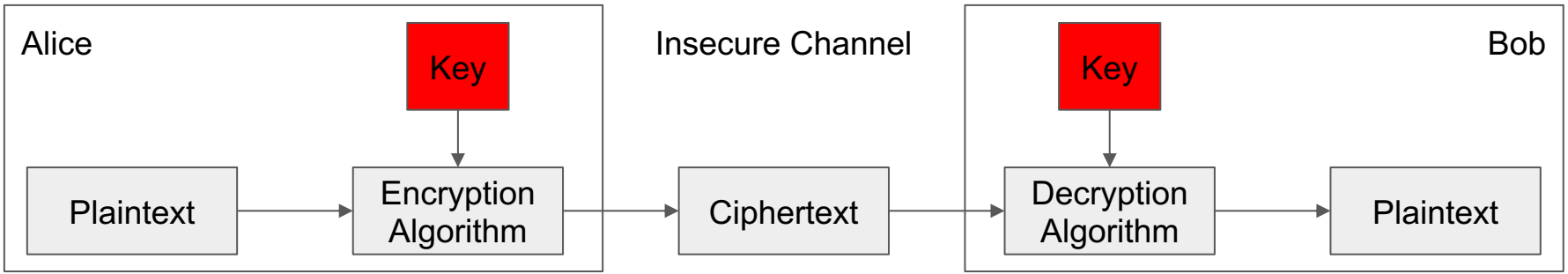
ITIS 6200 / 8200

	Symmetric-key	Asymmetric-key
Confidentiality	• One-time pads • Block ciphers with chaining modes (e.g. AES-CBC) • Stream ciphers	• RSA encryption
Integrity, Authentication	• MACs (e.g. HMAC)	• Digital signatures (e.g. RSA signatures)

- Hash functions
- Pseudorandom number generators
- Public key exchange (e.g. Diffie-Hellman)
- Key management (certificates)
- Password management

Symmetric-Key Encryption: Definition

- A symmetric-key encryption scheme has three algorithms:
  - KeyGen() → *K*: Generate a key *K*
  - Enc(*K*, *M*) → *C*: Encrypt a **plaintext** *M* using the key *K* to produce **ciphertext** *C*
  - Dec(*K*, *C*) → *M*: Decrypt a ciphertext *C* using the key *K*



One-Time Pad

- How does it work?
  - How does encryption work? Formula?
  - How does decryption work? Formula?

- Why is it called One-Time Pad?

- Security
  - What is IND-CPA secure? What is the IND-CPA game?
  - Does One-Time Pad have IND-CPA?
  - What if we reuse the same key for different messages? Do we still have IND-CPA?

Block Cipher

ITIS 6200 / 8200

- How does block ciphers work?
  - Why it is called block ciphers?
  - Why do we need operating modes?
  - Where do we use the key?
- Analyzing Modes
  - Giving a new operating mode, analyzing the formulas used for encryption and description
  - Analyze the performance implication
  - Analyze if the mode is IND-CPA secure: why some modes are secure and others are not
- Security
  - What are IV and nonce?
  - Where do we use them?
  - Why do we need them?
  - Does block cipher provide integrity?

Hash

ITIS 6200 / 8200

- What are the basic properties of hash functions?
  - What is one way function?
  - What is collision resistant?
- What can length extension attacks do?
- Security
  - Do hash provide integrity?
  - How can we use hash for integrity?

MAC

- Why do we want MAC?
  - Why is it different from hash?
- How does HMAC work?
  - What are the inputs?
- Security
  - Do MACs provide integrity?
  - Do MACs provide confidentiality?
  - How do we get both confidentiality and integrity?
    - What is Encrypt-then-MAC?
    - What is MAC-then-encrypt?

PRNG

- Where do we need random numbers?

- PRNG
  - Why is it called Pseudorandom?
  - What is rollback resistance?
  - What can the attacker do if the PRNG is not rollback resistant?

Diffie-Hellman Key Exchange

- Why do we want it?
- How does it work?
  - What variables are public? What variables are private?
  - What is the information being sent between Alice and Bob? Formula?
  - What is the secret being shared? Formula?
- Security
  - What’s the security issue with it?

Public-Key Encryption

- Why do we want Asymmetric-key encryption?
  - What are the major benefits?
  - What is the major issue?

- How does RSA encryption work?
  - What variables are the public key?
  - What variables are the private key?
  - How do we do encryption? Formula?
  - How do we do decryption? Formula?

- Security
  - Can it defend against MITM attack?

Digital Signature

- Why do we need signature?
  - What key is used for digital signature?
  - Why do we sign the hash instead of the plaintext?
- How does RSA signature work?
  - How do we sign a message? Formula?
  - How do we verify a signature? Formula?
- Security
  - How can we combine public-key encryption and digital signature?
  - Can we provide confidentiality and integrity together?

Access Control

ITIS 6200 / 8200

- What is Discretionary Access Control?
  - What is Access Matrix?
  - ACL vs. Capabilities
  - How does Trojan Horse attack work?

- What is Mandatory Access Control?
  - Multi-level security (MLS)
    - Bell-LaPadula (BLP)
    - Biba Model
  - Chinese Wall

Web Security (Basics)

ITIS 6200 / 8200

- The basics (syntax and semantics)
  - HTML
  - HTTP
  - URL
  - JavaScript (security problems)

- What is the same origin policy?
  - How to tell if two websites have the same origin?

Web Security (Cookies)

ITIS 6200 / 8200

- Basics of Cookies
  - Fields of cookies
  - Cookie Policy: when to allow cookie creation? What cookies to send for a request?
- Session Authentication
  - How do session tokens work?
- Cross-Site Request Forgery (CSRF)
  - How does CSRF work?
- CSRF Defenses
  - How does CSRF token work? How does Referer header work?

Web Security (XSS)

ITIS 6200 / 8200

- Cross-Site Scripting (XSS)
  - How to design a XSS attack?
  - What are Stored and Reflected XSS?
  - What is difference between CSRF and reflected XSS?
  - Defense
    - HTML sanitization
    - Content Security Policy (CSP)

Web Security (SQL injection)

ITIS 6200 / 8200

- SQL Injection
  - SQL basics
  - Design SQL scripts to compromise a system

- SQL Defense
  - Pros and Cons of
    - Input sanitization
    - Prepared statements

Network Security (Basics)

ITIS 6200 / 8200

- Network layers
  - Basics of the five layers
  - what does each layer provide?
    - e.g., MAC address versus IP address
    - e.g., how does routing work?

- Threat Models
  - What are the assumptions for
    - On-path attacker
    - Off-path attacker
    - Man-in-the-middle

Network Security (ARP and TCP)

ITIS 6200 / 8200

- Basics of ARP
  - Why do we need ARP? How does ARP use?
- ARP security
  - How does ARP spoofing work?
- Basics of TCP
  - What is 3-way handshake?
  - How does TCP provide reliability?
- TCP Security
  - What can TCP data injection do?
  - How does TCP spoofing work?
  - What can the attackers achieve with different threat models?
  - What does the attacker need for launching attacks?

Network Security (DoS)

ITIS 6200 / 8200

- What property does DoS break?
- Application-level DoS defenses
  - Identify the resources being attacked / consumed
- Network-level DoS
  - What is DDoS? How to launch DDoS?
  - What is amplified DoS?
  - How does SYN flooding work?
  - What are SYN cookies? How can they prevent SYN flooding?

Network Security (Firewall)

ITIS 6200 / 8200

- Basics of Firewall
  - Benefits of using firewall
  - What are inbound/outbound policies?

- Packet filters:
  - Stateless
    - How do we implement filtering with TCP flags?
  - Stateful
    - What rules can be defined?
  - How can the packet filters fail?
  - How to design the packets to bypass filters?
  - Pros and Cons

Network Security (Intrusion Detection)

ITIS 6200 / 8200

- Path Traversal Attacks
- Types of detectors
  - Network intrusion detection system (NIDS)
    - What are evasion attacks?
    - Why do they succeed?
    - What cause inconsistent interpretations?
  - Host-based intrusion detection system (HIDS)
  - NIDS versus HIDS
- Detection Accuracy
  - What false positives and false negatives?
  - When do they matter?
- Four Styles of Detection

System Security

ITIS 6200 / 8200

- x86 Assembly and Call Stack
  - Memory layout
  - Assembly basics
  - How do function calls work? How do ESP EIP EBP move?

- Buffer overflows
  - Stack smashing
  - How to design and construct an exploit?
  - What do we need to execute our shellcode?

Q & A