University of Houston

Foundations of Security

COSC 6347

Final Exam Review

Author
K.M. Hourani

Based on Notes By
Dr. Aron Laszka

December 6, 2020

1 Advanced crypto

1.1 Advanced Cryptographic Primitives

- secure multiparty computation
- homomorphic encryption

1.2 Commitment Schemes

Commitment Problem

- Bob "calls" the coin flip (i.e., heads or tails)
- Alice flips the coin
- Bob wins if her call is correct, Alice wins otherwise

Can we prevent Alice from cheating even if the players are not in the same physical location?

Commitment Scheme

- Two phases
  1. commit: A chooses a value V, A sends a **commitment** of V to B
  2. reveal: A reveals the value of V
- Example: coin flipping
  1. commit: A flips a coin, A sends a commitment (i.e., coin is heads or tails) to B
  - B calls the coin flip (i.e., heads or tails)
  2. reveal: A reveals the value of the coin flip
- Requirements for commitment scheme
  - B cannot learn the value of V from the commitment
  - A can reveal only the originally chosen value for a commitment

Naive Attempt Using Hash Function

- H: cryptographic hash function
- If the set of possible values of V are small (e.g., "heads" or "tails"), B can learn V by simply trying all possible values

Secure Commitment Using Hash Function

- Collision-free hash function $\rightarrow$ A cannot cheat by finding V_1 and V_2 such that $H(r_1 \mid r_2 \mid V_1) = H(r_1 \mid r_2 \mid V_2)$
  - r_1 prevents pre-computation of colliding V_1 and V_2

1.3 Secret Sharing

- Problem: distribute a secret among N participants such that
  - any group of at least T participants can reconstruct the secret
  - no group of fewer than T participants can reconstruct any part of it
- Types
  - **unconditionally secure**: information-theoretically secure (unbounded attacker)
  - **conditionally secure**: typically more efficient

Special Case: $T = N$

- Unconditionally secure scheme:
  1. let the secret be a binary number S
  2. pick $N - 1$ random numbers R_1, R_2, ..., R_{N-1} of the same length
  3. give each participant i, $i < N$, the number R_i

4. give the last participant the result of $S \oplus R_1 \oplus R_2 \oplus \ldots \oplus R_{N-1}$

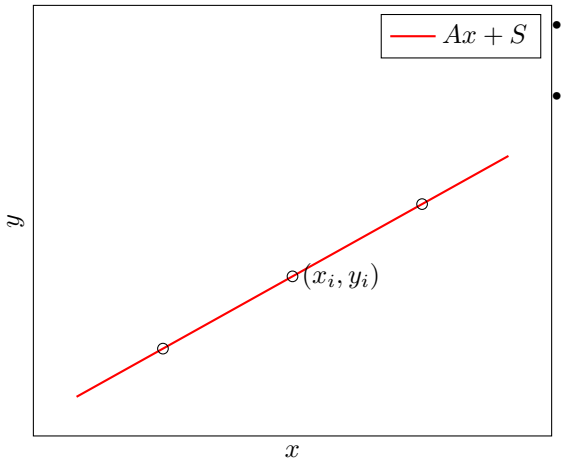
- N participants can reconstruct the secret by XORing their numbers:
  –

$$\begin{aligned} & R_1 \oplus R_2 \oplus \ldots \oplus R_{N-1} \oplus (S \oplus R_1 \oplus R_2 \oplus \ldots \oplus R_{N-1}) \\ & = (R_1 \oplus R_1) \oplus (R_2 \oplus R_2) \oplus \ldots \oplus (R_{N-1} \oplus R_{N-1}) \oplus S \\ & = S \end{aligned}$$

- $N-1$ participants can compute only $S \oplus R_i$, where i is the missing participant (or $R_1 \oplus R_2 \oplus \ldots \oplus R_{N-1}$ if the last participant is missing)

1.4 Shamir's Secret Sharing

- Proposed by Shamir in 1979
- Unconditionally secure
- Special case $T = 2$
  1. let the secret be a number S
  2. pick random number A
  3. let each participant's share be a random point on the line $Ax + S$



- $T = 2$ participants can reconstruct the secret since any two points define a line
- Single participant cannot learn the slope

General Case

- Arbitrary T:
  1. let the secret be a number S
  2. pick random numbers A_1, A_2, …, A_{T-1}
  3. let each participant's share be a random point from the curve

$$y = S + A_1 x + A_2 x^2 + \cdots + A_{T-1} x^{T-1}$$

- At least T points are necessary to define a polynomial of degree $T - 1$
- Example $T = 3$
  – secret is a parabola (i.e., $A_2 x^2 + A1x + S$)
  – there an infinite number of parabolas fitting two points
  – but three point define one uniquely

1.5 Secure Multiparty Computation

- Problem: N participants with private data d_1, d_2, …, d_N
  – participants would like to compute the value $F(d_1, d_2, \ldots, d_N)$ of a public function F over their private data

  - no participant i would like to reveal any information about its data d_i
- Requirements
  - **privacy**: no information is revealed about any private data (other than what is revealed by the public output)
  - **correctness**: public function is correctly computed
- Adversaries may be semi-honest (passive) or malicious (active)

2 WiFi security

2.1 Security Challenge

- Problem: no inherent physical protection
- **joining** a network does not require physical access
- radio transmissions are broadcast → anyone in range can **eavesdrop**
- **injecting** new messages or **replaying** old messages is possible
- **jamming** attacks against availability
- jamming and injecting messages can be combined into **tampering** attacks

2.2 Simple "Solutions" for Access Control

Hidden SSID

- Association request must contain the SSID of the network
  - by default, the AP broadcasts it periodically in the beacon
- AP may be configured to **stop announcing the SSID** → SSID may be be used as a "password"
- However,
  - SSID must be hard to guess
  - every authorized user must know the SSID
  - **SSID can be easily eavesdropped** whenever an authorized station connects to the network → does not provide any security
- Tools are available for eavesdropping (e.g. Aircrack-ng)

MAC Address Based Filtering

- AP may be configured to **allow only devices with certain MAC addresses** to connect
  - MAC addresses of all authorized devices must be registered in advance
- However,
  - **MAC address is sent in plaintext** in every packet
  - many WLAN devices allow their MAC addresses to be changed → attacker can easily impersonate an authorized user

2.3 802.11 Security Standards

WEP

- security is based on a 40 or 104-bit secret key
  - WiFi "password" shared by all users
- confidentiality: RC4 stream cipher
  - key is extended by a 24-bit IV, which is changed for each message → used as nonce to prevent key reuse problems
- integrity: encrypted CRC32 (Cyclic Redundancy Check) checksum
- access control: challenge-response between AP and station

WEP Design Flaws

- Authentication
  - **one-way authentication** (only for station) → AP can be impersonated
- Integrity protection
  - based on **error-detection code** (CRC32) instead of cryptographic hash → forging authentication tags is trivial
  - **no message replay protection**
- Key usage
  - **no session key**: long-term key used for all purposes (authentication, encryption, integrity protection)
  - **short nonce** (i.e., 24-bit IV) → danger of key reuse for stream cipher
    - busy network with 1000 packets per second reuses in less than 5 hours
  - vulnerable to Fluhrer-Mantin-Shamir Attack
    - In practice, WEP keys can be broken in a matter of minutes (or less) → WEP is **not secure**

2.4 WiFi Protected Access (WPA)

WPA

- Standard: 802.11i TKIP (Temporal Key Integrity Protocol
- Design goals: **fix the flaws of WEP** and be **compatible with legacy hardware**
- Overview
  - key usage: session key is established during a secure two-way authentication
  - confidentiality: RC4 encryption, but with **48-bit IV**, which is **mixed thoroughly** with the session key and source MAC address
    - prevents key reuse and the Fluhrer-Mantin-Shamir attack
  - integrity: 64-bit message integrity codes computed using Michael, which is **computationally very efficient** but provides only 20 bits of effective security
    - after wrong code, station is banned for a minute and needs to re-authenticate
  - Deprecated in later revisions of the standard
-

WPA-2

- Standard: **IEEE 802.11i**
- WPA 2 Devices can be certified by the Wi-Fi Alliance

Phases

1. Discovery
   - agree on what authentication method and ciphers to use
2. Authentication
   - may use an authentication server
   - create a master session key
3. Key management
   - derive keys for various purposes
4. Protected data transfer
5. Connection termination

Discovery Phase

- Goal: station and AP may support different sets of authentication methods and ciphers → they need to agree on which ones they will use
- **Authentication and key-management suite**: how to perform mutual authentication and derive fresh keys
  - IEEE 802.1X, pre-shared key (PSK), or vendor-specific
- **Cipher suite**: what ciphers to use for confidentiality and integrity
  - WEP, TKIP, CCMP, or vendor-specific
- Protocol
  1. AP can periodically **broadcast** its security capabilities using a **Beacon** (or station can ask for it using a Probe Request message)
  2. Station **specifies** an authentication and cipher suite in an **Association Request**
  3. if the AP **accepts** the specified suites, it sends an **Association Response**

Authentication Phase

- Goals:
  - mutual authentication:
    1) only authorized stations can use the network
    2) station is assured that it communicates with a legitimate network
  - generate **pairwise master key** (PMK)
- Approaches
  - Pre-shared key (PSK)
    - password is deployed on each station and the AP manually
    - PMK = PSK = generated from the password using a hash function
    - ideal for home and small office networks
  - IEEE 802.1X

Key-Management Phase

- Goals:
  - derive **pairwise transient keys** from the PMK
  - distribute **group keys**
- Pairwise transient key (PTK)
  - protecting data between station and AP
  - generated from PMK and the AP's and station's MAC addresses and nonces
- Group temporal key (GTK)
  - protecting multicast communication
  - group master key (GMK): generated randomly by the AP
  - distributed using the PTK

Protected Data Transfer Phase

- Standard defines two schemes: TKIP and CCMP
- TKIP: see WPA
- CCMP (Counter mode CBC-MAC Protocol)
  - based on the CCM (Counter with CBC-MAC) authenticated encryption mode
  - integrity: CBC-MAC based on AES encryption
  - confidentiality: AES encryption in counter (CTR) mode
  - same 128-bit key for integrity and confidentiality (from PTK)
  - 48-bit packet number to prevent replay attacks

IEEE 802.1X

- Standard for port-based network access control
- Entities
  - supplicant = station
  - authenticator = access point
  - authentication server
- Port-based: supplicant can access only the authentication server until the authentication succeeds
- Authentication server does not have to be implemented on the access point → little overhead for the access point

EAP Authentication Methods

- Extensible framework, not a specific authentication mechanism
- Example methods
  - EAP-TLS: based on public-key certificates
  - EAP-GPSK (Generalized Pre-Shared Key): based on secret keys shared by the client and the server, uses symmetric-key cryptography

3 IPSec

- Collection of protocols and mechanisms, standardized by the Internet Engineering Task Force (IETF) in a series of publications
- Provides
  - data confidentiality and integrity
  - source authentication (prevent address spoofing, i.e., sending from fake address)
  - protection against packet replay
- Below the transport layer (TCP or UDP) → transparent to applications
- End-to-end security between two hosts, a host and a network, or between two networks
- Example Applications of IPSec
  - Secure remote access over the Internet
  - Secure virtual private network

3.1 Transport Mode and Tunnel Mode

- Transport mode
  - protects the payload of the IP packet
  - typically host-to-host communication
- Tunnel mode
  - protects the entire IP packet by encapsulating it in the payload of a new IP packet
  - typically host-to-network or network-to-network communication

	Protocol	
	Authentication Headher (AH)	Encapsulating Security Payloads (ESP)
Modes	both transport and tunnel	
Provides	integrity, replay protection	integrity, confidentiality, replay protection
Protects	payload and IP header	payload

Authentication Header

- Services
  - data and origin integrity
  - replay-prevention
- Message authentication

  - computed from immutable fields of the IP header, AH header (except ICV), and original payload
  - algorithms: HMAC-MD5, HMAC-SHA-1, HMAC-SHA-2, ...

Encapsulating Security Payload

- Services: confidentiality, integrity (optional), replay prevention
- Encryption: AES-CBC, 3DES-CBC, ...
- Message authentication: HMAC-SHA-1, AES-GMAC, ...
- Authenticated encryption: AES-GCM

Combining Modes and Protocols

- Tunnel mode advantage: requires support only at the gateways
- Transport mode advantage: requires support only at the hosts
- AH advantage: authenticates some elements of the original header
- ESP advantage: protects both integrity and confidentiality
- Combining modes
  - IPSec tunnel can carry any IP packet → IPSec transport or tunnel packets can be sent through an IPSec tunnel
  - IPSec transport can protect any IP packet → IPSec transport or tunnel packets can be protected by outer IPSec transport
  - ...
  - can be nested to any depth
- Combination Examples
  1. AH in transport (for integrity) + ESP in transport (for confidentiality)
  2. IPSec packets over tunnel