

## Security in Wireless LANs and Mobile Networks

---

---

---

---

---

---

---

---

### Wireless Magnifies Exposure Vulnerability

- Information going across the wireless link is exposed to anyone within radio range
  - RF may extend beyond a room or a building
  - Infrared limited to a room
- Traditional wireline networks benefit from physical security
  - Access to the wire is required to gain information
  - Switched networks further reduce exposure



---

---

---

---

---

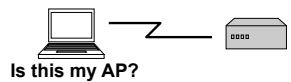
---

---

---

### Mobility Makes it Difficult to Establish Trust

- A mobile user must connect to a network component (e.g., an access point) that is physically hidden
  - Problem on both home and foreign networks
- Mobility on foreign networks -- service providers are unknown and, perhaps, not trusted
  - Access points
  - Foreign agents
  - DHCP servers



---

---

---

---

---

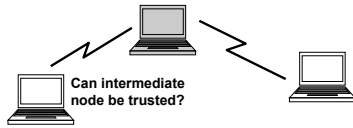
---

---

---

### Lack of Infrastructure

- Lack of security infrastructure
  - Authentication servers
  - Certificate authorities
- Unknown nodes providing service
  - Intermediate nodes for ad hoc routing



---

---

---

---

---

---

---

---

### System Design Issues

- Mobile form factor
  - Desire low power consumption
    - Minimize computation
    - Minimize network communication
  - Constrained by low processing capabilities
  - Constrained by limited link capacity
- Need cryptographic and other security-related algorithms to be simple
- Need to minimize communications overhead for security protocols

---

---

---

---

---

---

---

---

### Secure Communications (1)

- Privacy or confidentiality
  - The intended recipients know what was being sent but unintended parties cannot determine what was sent
  - Requires some form of encryption and decryption
    - Encryption at the sender
    - Decryption at the receiver using a public or private (secret) key to decode the encrypted information
- Authentication
  - Confirms the identity of the other party in the communication
  - Assures that
    - The claimed sender is the actual sender
    - The claimed receiver is the actual receiver

---

---

---

---

---

---

---

---

## Secure Communications (2)

- Message integrity and non-repudiation
  - Data integrity – data is transmitted from source to destination without undetected alteration
  - Non-repudiation – prove that a received message came from a claimed sender
- Availability and access control
  - Ensures availability of resources for the intended users
  - Controls access to resource

---

---

---

---

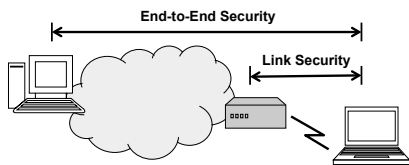
---

---

---

---

## Link Versus End-to-End Security



- End-to-end security
  - Provided by network (e.g., IPsec), transport (e.g., SSL), and/or application layer (e.g., application-specific)
- Link security
  - Provided by link layer (e.g., IEEE 802.11 WEP, WPA, or IEEE 802.11i)

---

---

---

---

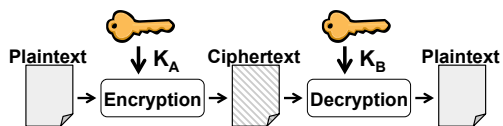
---

---

---

---

## Cryptography



- Symmetric (private) key cryptography
  - Sender and receiver keys are identical ( $K_A = K_B$ )
- Asymmetric (public) key cryptography
  - Sender (encryption) key ( $K_A$ ) is public
  - Receiver (decryption) key ( $K_B \neq K_A$ ) is private

---

---

---

---

---

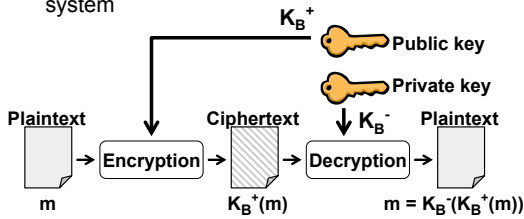
---

---

---

### Public Key Cryptography

- Unlike a private key system, one can publish the key for encryption in a public key encryption system




---

---

---

---

---

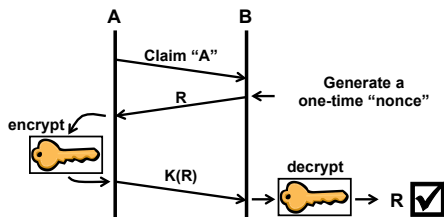
---

---

---

### Authentication with Private Key Cryptography

- Authentication can be implemented with symmetric (private) key cryptography




---

---

---

---

---

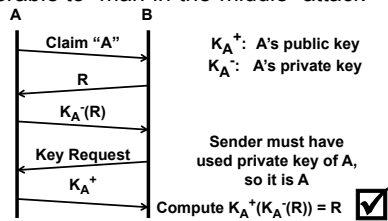
---

---

---

### Authentication with Public Key Cryptography

- Use of public key avoids shared key problem
- Vulnerable to "man-in-the-middle" attack




---

---

---

---

---

---

---

---

### IEEE 802.11 Security

- Security was not thoroughly addressed in the original IEEE 802.11 standard
  - Based on Wired Equivalent Privacy (WEP)
  - Objective is to not compromise security when compared to a standard wired LAN (e.g., Ethernet)
- Evolution
  - Long-term: IEEE 802.11i
  - Short-term: WiFi Protected Access (WPA)

---

---

---

---

---

---

---

---

### IEEE 802.11: Authentication (1)

- IEEE 802.11 supports two authentication schemes
  - Open system "authentication"
  - Shared key authentication
- Authentication management frames used in a transaction to establish authentication
  - Authentication algorithm number
  - Authentication transaction sequence number
  - Status code
- Deauthentication management frame sent to terminate an association
  - Reason code

---

---

---

---

---

---

---

---

### IEEE 802.11: Authentication (2)

- Open system "authentication" is really just a placeholder for systems that do not wish to implement true authentication
  - One station asserts its identity
  - The other station responds with success
- Shared key authentication
  - Both stations must have a copy of a WEP key
  - Station proves identity by encrypting and returning challenge text
  - 128-bit challenge text based on RC4 stream cipher
- Shared key authentication only authenticates the station to the AP, not the AP to the station!

---

---

---

---

---

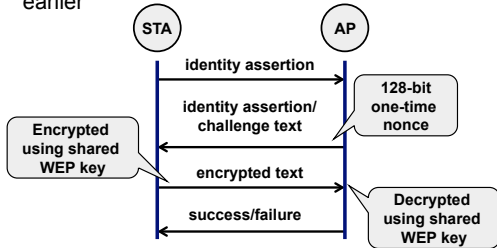
---

---

---

### IEEE 802.11: Shared Key Authentication

- Uses private key authentication scheme shown earlier



---

---

---

---

---

---

---

---

### IEEE 802.11: Deauthentication

- A station can terminate an authentication association with another station by sending that station a deauthentication frame
  - Contains just a reason code, e.g., sending station is leaving the BSS or ESS

---

---

---

---

---

---

---

---

### IEEE 802.11: Privacy

- Based on Wired Equivalent Privacy (WEP)
- MAC at sender encrypts frame body of data frames
  - Headers and non-data frames are not encrypted
  - Does not protect against data analysis attacks
- MAC at receiver decrypts and passes data to higher level protocol
- Uses RC4 symmetric stream cipher
  - Same key at sender and receiver
  - Can be applied to variable length data
- Key distribution not addressed in standard

---

---

---

---

---

---

---

---

## WEP Data Encryption

- Host/AP share 40-bit symmetric key
  - Semi-permanent WEP key
  - May be longer (e.g., 128 bits)
- Host appends 24-bit initialization vector (IV) for each frame to create a 64-bit key
  - 152-bit key with 128-bit WEP key
- The 64-bit key is used to generate a stream of keys,  $k_i^{IV}$ , using RC4 private key stream cipher algorithm
  - Key  $k_i^{IV}$  is used to encrypt byte  $d_i$  in the frame
    - $c_i = d_i \text{ XOR } k_i^{IV}$  (XOR is exclusive-or)
  - Initialization vector (IV) and the encrypted bytes,  $c_i$ , are sent in the frame

---

---

---

---

---

---

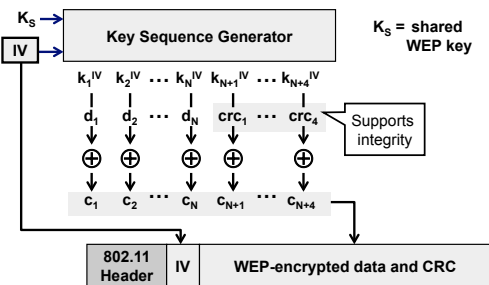
---

---

---

---

## WEP Encryption at the Sender




---

---

---

---

---

---

---

---

---

---

## WEP Encryption Vulnerability

- Initialization vectors are 24 bits in length and a new one is used for each frame, so IVs are eventually reused
- IVs are transmitted in plaintext, so IV reuse can be detected just by packet sniffing
- Attack
  - An intruder causes a host to encrypt known plaintext,  $d_1, d_2, d_3, \dots$
  - The intruder sees  $c_i = d_i \text{ XOR } k_i^{IV}$
  - The intruder knows  $c_i$  and  $d_i$ , so it can compute  $k_i^{IV}$
  - The intruder knows encrypting key sequence  $k_1^{IV}, k_2^{IV}, k_3^{IV}, k_4^{IV}, \dots$
  - The next time that the same IV is used, the intruder can decrypt

---

---

---

---

---

---

---

---

---

---

IEEE 802.11: Security Weaknesses (1)

- WEP encryption is flawed, affecting privacy and authentication
  - Static WEP keys leave encryption vulnerable
  - Initialization vectors sent in the clear
  - Generation of IVs may be weak
    - Not specified in the standard
    - All NICs from a vendor may generate the same sequence of IVs or the IV may be a fixed value
  - Exposed IV (revealing part of key) plus weakness of RC4 make WEP vulnerable to analysis
  - Can be broken for a busy network by a contemporary personal computer – about 10 hours for sniffing and a few seconds to “guess” the key

---

---

---

---

---

---

---

---

IEEE 802.11: Security Weaknesses (2)

- Integrity check based on CRC
  - Relatively weak compared to a hash or message authentication scheme
  - Introduces vulnerabilities for certain kinds of attacks
- Unilateral challenge-response used for authentication vulnerable to “man-in-the-middle” attack
- Asymmetric authentication
  - Station cannot authenticate AP
  - Key management is not addressed by the standard
    - Very complex task, especially for a large network

---

---

---

---

---

---

---

---

IEEE 802.11: Security Weaknesses (3)

- “Out-of-the-box” default is usually no security
  - Ease of deployment and ease of operation for users
  - Lots of WLANs with no security configured!

---

---

---

---

---

---

---

---

### Improving IEEE 802.11 Security

- RSA Security's Fast Packet Rekeying
- WiFi Alliance's WiFi Protected Access (WPA)
- IEEE 802.11 Technical Group i (IEEE 802.11i)

---

---

---

---

---

---

---

---

### Fast Packet Rekeying

- Message Integrity Check function on all WEP-encrypted data frames
- Generates a unique key to encrypt each network packet on the WLAN
  - Hashing technique (known by sender and receiver) used to rapidly generate per packet keys
  - Per-packet key is based on fixed WEP key
- The IEEE 802.11 group has approved fast packet rekeying as a fix for some WEP security weaknesses

---

---

---

---

---

---

---

---

### WiFi Protected Access

- WiFi Protected Access (WPA) is intended as a near-term solution to the IEEE 802.11 security problem
  - Software-only updates – requires update to AP firmware and NIC driver
  - A subset of the more extensive IEEE 802.11i techniques
- Based on two main functions
  - 802.1x port-based access control
  - Temporal Key Integrity Protocol (TKIP)

---

---

---

---

---

---

---

---

### IEEE 802.1x Port-Based Access Control

- Allows use of upper-layer authentication protocols
  - AP and station can authenticate each other
  - Integrates with IETF's Extensible Authentication Protocol (EAP)
    - See RFC 2284
  - Authentication can be...
    - On the AP
    - Use a backend server, e.g., with RADIUS
- Allows use of session keys
  - 802.1x keys can be changed each session
  - Standard WEP keys are semi-permanent

---

---

---

---

---

---

---

---

### Temporal Key Integrity Protocol

- Extends the initialization vector (IV) space beyond 24 bits
- Uses key construction for each packet
- Improves cryptographic integrity check beyond CRC used in WEP
- Supports key derivation and distribution

---

---

---

---

---

---

---

---

### IEEE 802.11i

- IEEE 802.11i also known as Robust Security Network (RSN)
  - Longer-term solution (but should be available very soon)
  - Requires hardware *replacements* for APs and NICs
- Superset of WPA – includes...
  - IEEE 802.1x port-based access control
  - Temporal Key Integrity Protocol (TKIP)
- Includes support for Advanced Encryption Standard (AES) for confidentiality and integrity

---

---

---

---

---

---

---

---

### Advanced Encryption Standard

- The Advanced Encryption Standard (AES) is published by NIST as the successor to Data Encryption Standard (DES)
- Operation
  - 128-byte blocks of data (cleartext)
  - 128-, 192-, or 256-bit symmetric keys
- NIST estimates that a machine that can break 56-bit DES key in 1 second would take about 149 trillion years to crack a 128-bit AES key (unless someone is very lucky)

---

---

---

---

---

---

---

---

### Mitigating Risk

- Management countermeasures
  - For example, standardizing AP settings and controlling use of WLANs within an organization
- Operational countermeasures
  - For example, controlling coverage area of APs
- Technical countermeasures
  - Access point configuration
  - Firmware and software updates
  - Personal firewalls
  - Intrusion detection systems (IDS)
  - Maximizing WEP key length
  - Security audits
  - Virtual private networks

---

---

---

---

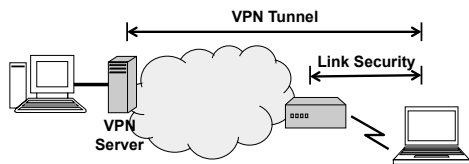
---

---

---

---

### Virtual Private Networks



- Using a VPN (e.g., based on IPsec) above the WLAN provides the security present in the environment of the VPN server

---

---

---

---

---

---

---

---

## Mobile Networks

- Security vulnerabilities in Mobile IP
  - Rogue Foreign Agents
  - Impersonating a Home Agent
  - Impersonating a Mobile Host to redirect traffic
  - Reducing security to enable Mobile IP – router at foreign network
- Security vulnerabilities in mobile ad hoc networks (MANETs)
  - Generating faulty routing information
  - Snooping on relayed traffic
  - Refusing to route
  - Power-oriented attacks

---

---

---

---

---

---

---

---

## Summary

- Examined the basic objectives of security and fundamental approaches to cryptography and authentication
- IEEE 802.11 security features (which are flawed)
  - Authentication
  - Privacy and integrity
- Solutions to IEEE 802.11's security problems
  - WiFi Protected Access (WPA)
  - IEEE 802.11i – Robust Security Network (RSN)
- Higher layer security methods can also address WLAN security problems
- Other security issues in wireless and mobile systems

---

---

---

---

---

---

---

---