Stockholm University

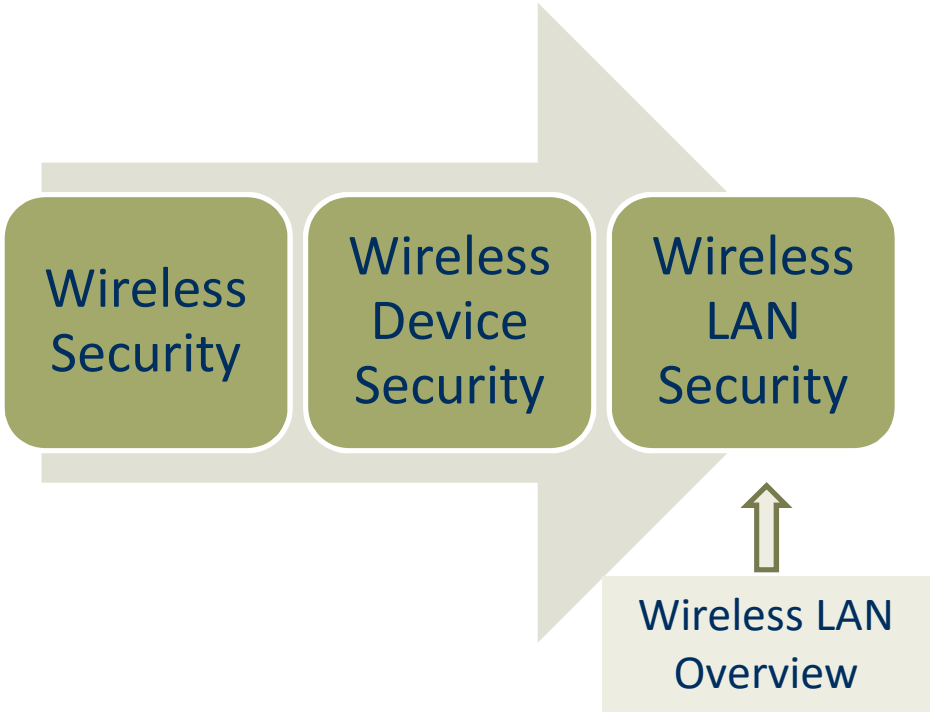
Wireless Network Security

Network Security (NETSEC)

Yuhong Li

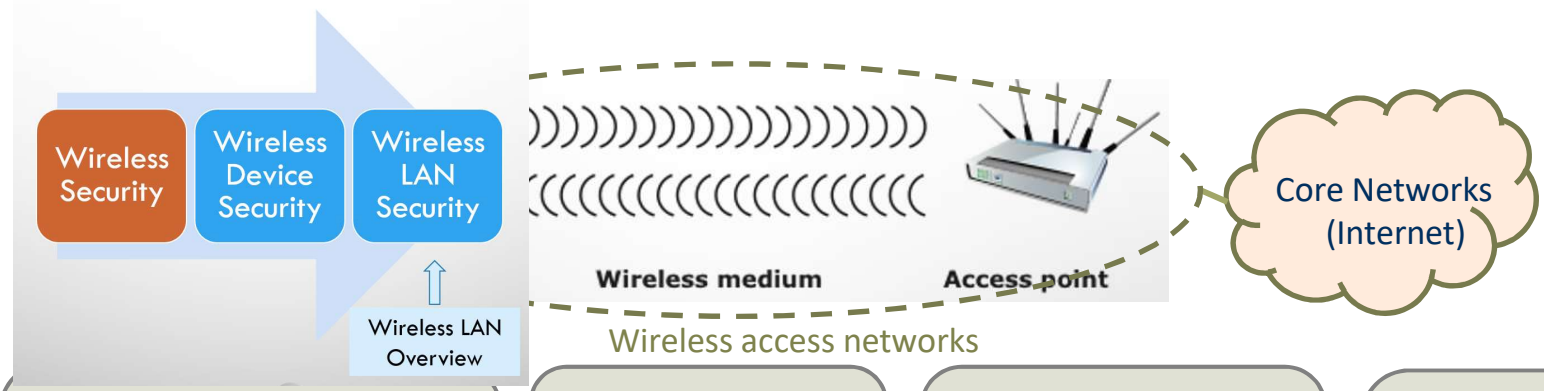
Outline

Stockholm University



Characteristics of Wireless Network and Security Risks

Stockholm University



Channel

Open “medium”(through the air)

Susceptible to eavesdropping and jamming;

More vulnerable to active attacks in communications protocols

Mobility

Portable and mobile

This mobility results in a number of risks

Resources

Sophisticated operating systems but limited memory and processing resources

Counter threats, including denial of service and malware

Accessibility

Some wireless devices, such as sensors and robots left unattended in remote and/or hostile locations

Increases their vulnerability to physical attacks

Wireless Network Threats

Stockholm University

Accidental association

- Company wireless LANs in close proximity may create overlapping transmission ranges
- A user intending to connect to one LAN may unintentionally lock on to a wireless access point from a neighboring network

Malicious association

- A wireless device is configured to appear to be a legitimate access point, enabling the operator to steal passwords from legitimate users and then penetrate a wired network through a legitimate wireless access point

Ad hoc networks

- These are peer-to-peer networks between wireless computers with no access point between them
- Such networks can pose a security threat due to a lack of a central point of control

Nontraditional networks

- Personal network, Bluetooth devices, barcode readers, and handheld PDAs pose a security risk in terms of both eavesdropping and spoofing

Identity theft (MAC spoofing)

- An attacker is able to eavesdrop on network traffic and identify the MAC address of a computer with network privileges

Man-in-the-middle attacks

- Persuading a user and an access point to believe that they are talking to each other when in fact the communication is going through an intermediate attacking device
- Wireless networks are particularly vulnerable to such attacks

Denial of service (DoS)

- An attacker continually bombards a wireless access point or some other accessible wireless port with various protocol messages designed to consume system resources
- The wireless environment lends itself to this type of attack because it is so easy for the attacker to direct multiple wireless messages at the target

Network injection

- This attack targets wireless access points that are exposed to nonfiltered network traffic, such as routing protocol messages or network management messages

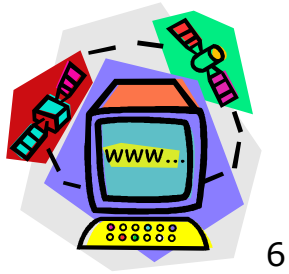
Wireless Security Measures

Stockholm University

Securing Wireless Transmissions

Stockholm University

- The principal threats: eavesdropping, altering or inserting messages, disruption
- To deal with eavesdropping, two types of countermeasures are appropriate:
  - Signal-hiding techniques
    - Turn off SSID broadcasting by wireless access points
    - Assign cryptic names to SSIDs
    - Reduce signal strength to the lowest level that still provides requisite coverage
    - Locate wireless access points in the interior of the building, away from windows and exterior walls
  - Encryption
    - Effective when the encryption keys are secured



Securing Wireless Access Points

Stockholm University

- The main threat: unauthorized access to the network
- The principal approach for preventing such access is the IEEE 802.1x standard for port-based network access control
  - The standard provides an authentication mechanism for devices wishing to attach to a LAN or wireless network
  - The use of 802.1x can prevent rogue access points and other unauthorized devices from becoming insecure backdoors

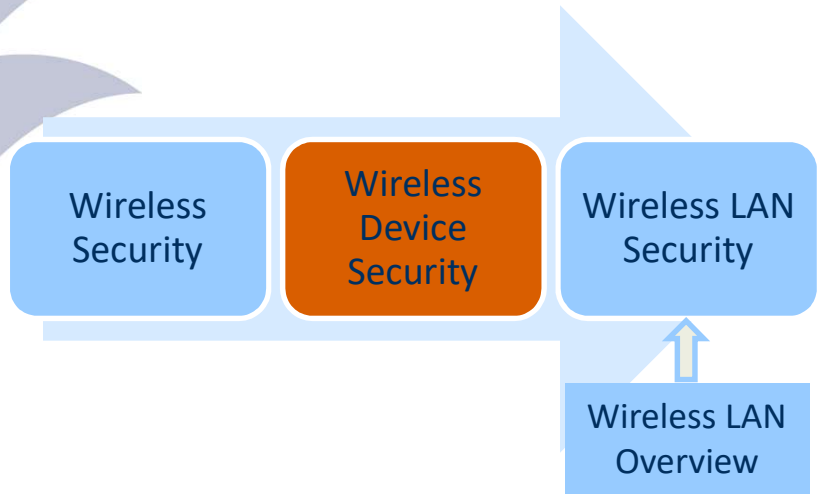
Securing Wireless Networks

Stockholm University

- Use encryption
- Use antivirus, antispyware software and a firewall
- Turn off identifier broadcasting
- Change the identifier on your router from the default
- Change your router’s pre-set password for administration
- Allow only specific computers to access your wireless network

Stockholm University

Wireless Device Security



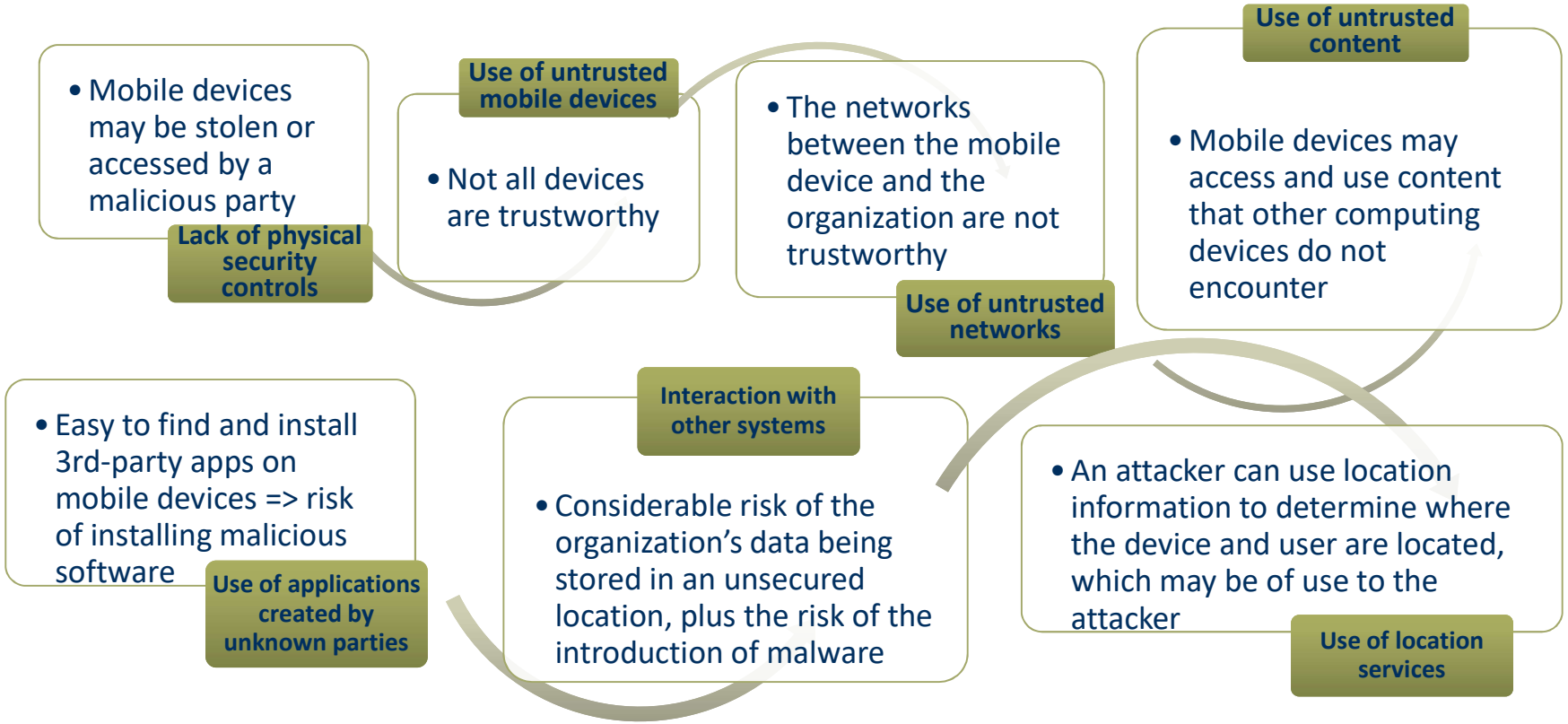
Mobile Device Security Considerations

Stockholm University

- Prior to the widespread use of mobile devices, network security was based upon clearly defined perimeters that separated trusted internal networks from the untrusted Internet
- Mobile devices: an essential element for organizations as part of the overall network infrastructure
- Due to massive changes, an organization's networks must now accommodate:
  - Growing use of new devices
  - Cloud-based applications
  - De-perimeterization
  - External business requirements

Security Threats

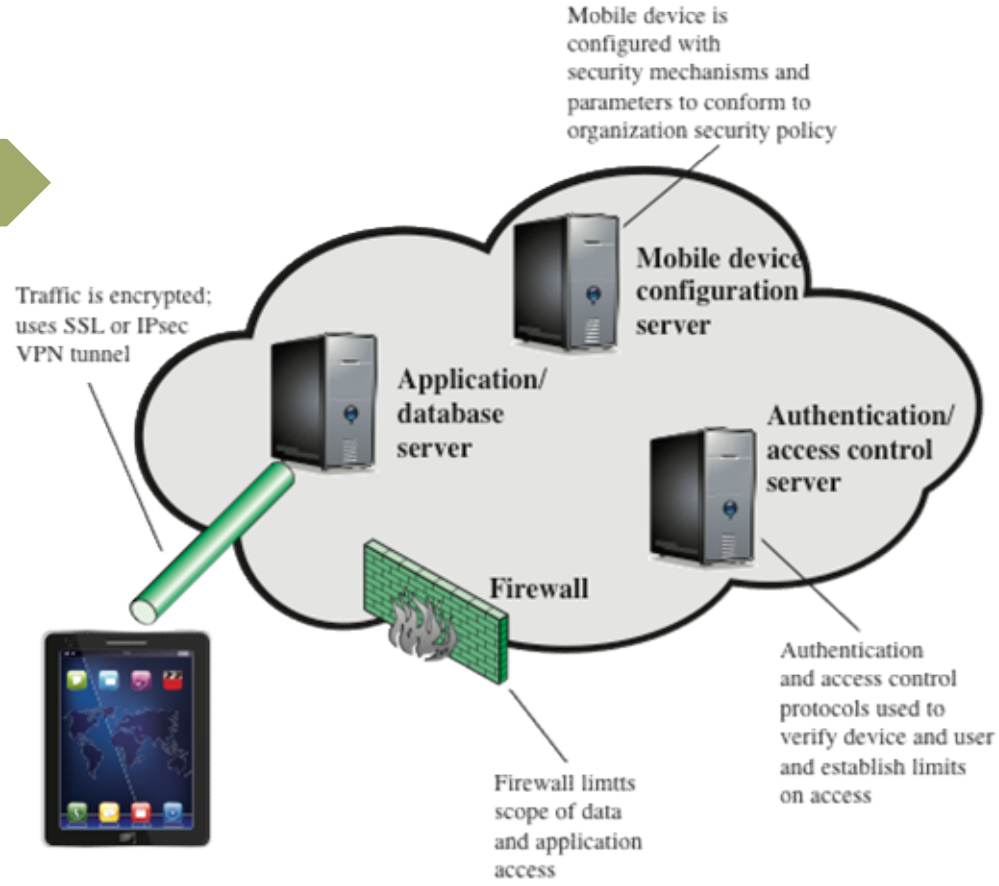
Stockholm University



Mobile Device Security Strategies

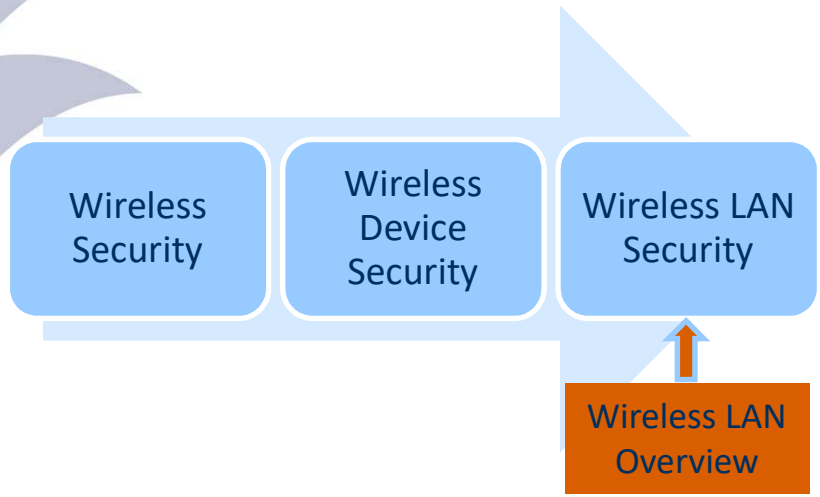
Stockholm University

Device security → Client/sever traffic security → Barrier security



Stockholm University

Overview of Wireless LAN



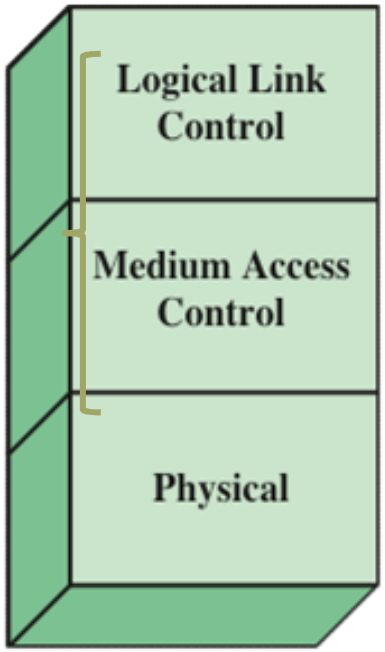
IEEE 802.11Wireless LAN

Stockholm University

- IEEE 802 is a committee that has developed standards for a wide range of local area networks (LANs)
- In 1990 the IEEE 802 Committee formed a new working group, IEEE 802.11, with a charter to develop a protocol and transmission specifications for wireless LANs (WLANs)
- Since that time, the demand for WLANs at different frequencies and data rates has exploded

IEEE 802.11 Protocol Stack

Application Layer	Web services, remote login, multimedia streaming …
Transport Layer	Congestion control, flow control, quality of service
Network Layer	Addressing, routing, device location, hand-over
Data link Layer	Authentication, media access, multiplexing, media access control
Physical Layer	Encryption, modulation, interference, attenuation, frequency



General IEEE 802 functions

Specific IEEE 802.11 functions

Logical Link Control

- Flow control
- Error control

Medium Access Control

- Assemble data into frame
- Addressing
- Error detection
- Medium access

- Reliable data delivery
- Wireless access control protocols

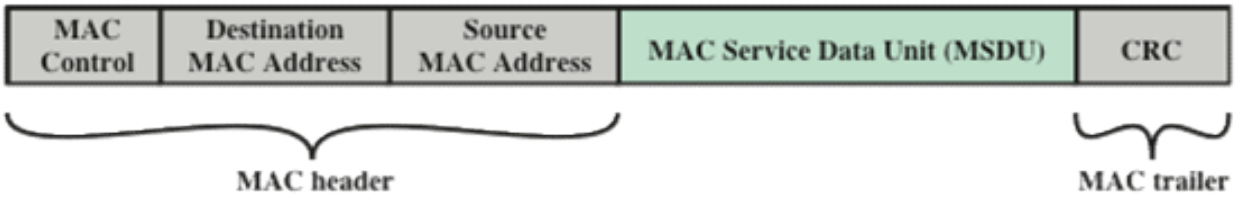
Physical

- Encoding/decoding of signals
- Bit transmission/ reception
- Transmission medium

- Frequency band definition
- Wireless signal encoding

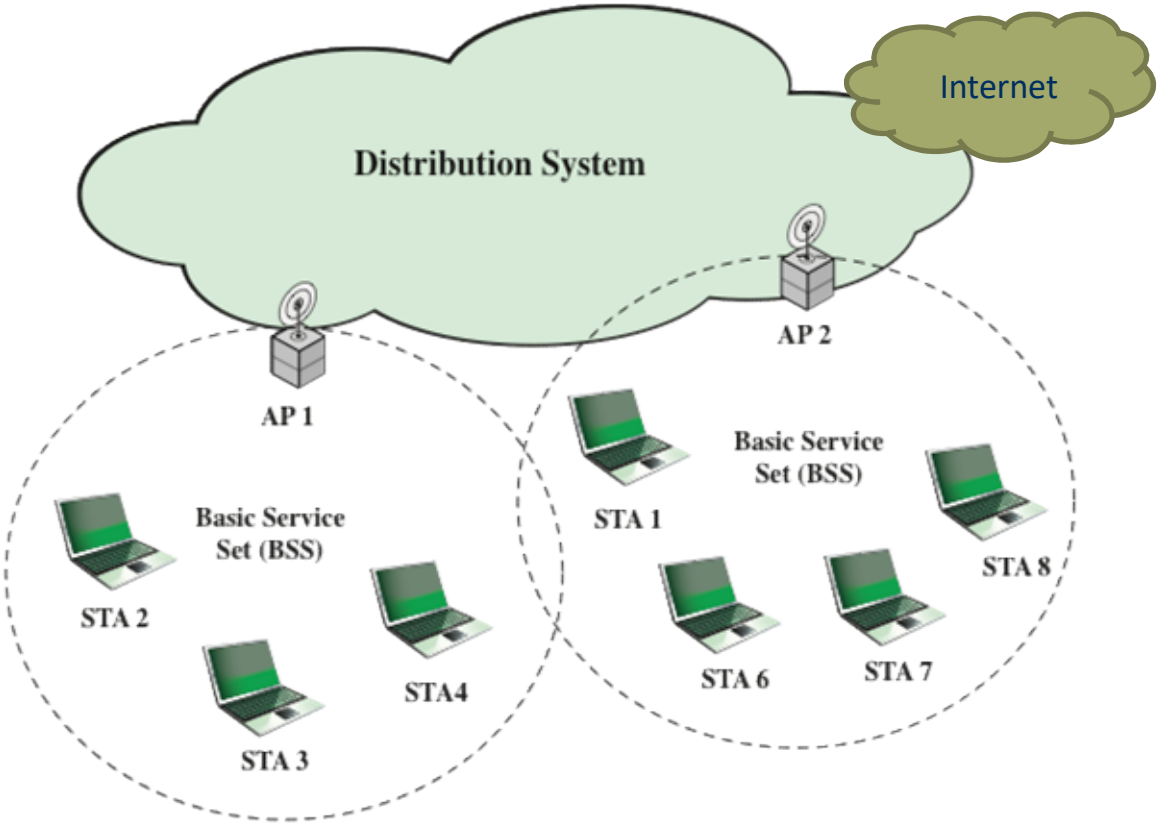
General IEEE 802 MPDU Format

Stockholm University



MPDU: MAC protocol data unit
CRC: The cyclic redundancy check field
MAC: Media Access Control

IEEE 802.11 Network Architecture & Extended Service Set



IEEE 802.11 Terminology

Stockholm University

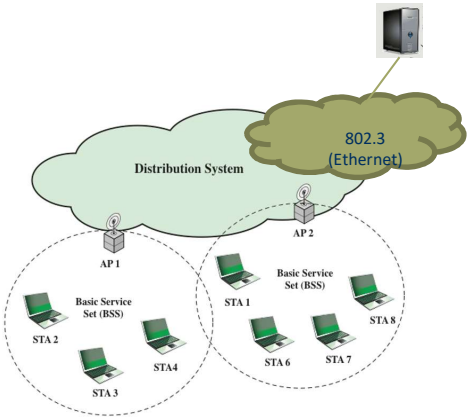
Access point (AP)	Any entity that has station functionality and provides access to the distribution system via the wireless medium for associated stations.
Basic service set (BSS)	A set of stations controlled by a single coordination function.
Coordination function	The logical function that determines when a station operating within a BSS is permitted to transmit and may be able to receive PDUs.
Distribution system (DS)	A system used to interconnect a set of BSSs and integrated LANs to create an ESS.
Extended service set (ESS)	A set of one or more interconnected BSSs and integrated LANs that appear as a single BSS to the LLC layer at any station associated with one of these BSSs.
MAC protocol data unit (MPDU)	The unit of data exchanged between two peer MAC entities using the services of the physical layer.
MAC service data unit (MSDU)	Information that is delivered as a unit between MAC users.
Station	Any device that contains an IEEE 802.11 conformant MAC and physical layer.

IEEE 802.11 Services

Service	Provider	Used to support
Association	Distribution system	MSDU delivery
Authentication	Station	LAN access and security
Deauthentication	Station	LAN access and security
Disassociation	Distribution system	MSDU delivery
Distribution	Distribution system	MSDU delivery
Integration	Distribution system	MSDU delivery
MSDU delivery	Station	MSDU delivery
Privacy	Station	LAN access and security
Reassociation	Distribution system	MSDU delivery

Distribution of Messages Within a DS

The two services involved with the distribution of messages within a DS are:



Integration

- Enables transfer of data between a station on an IEEE 802.11 LAN and a station on an integrated IEEE 802.x LAN
- Takes care of any address translation and media conversion logic required for the exchange of data

Distribution

- The primary service used by stations to exchange MPDUs when the MPDUs must traverse the DS to get from a station in one BSS to a station in another BSS

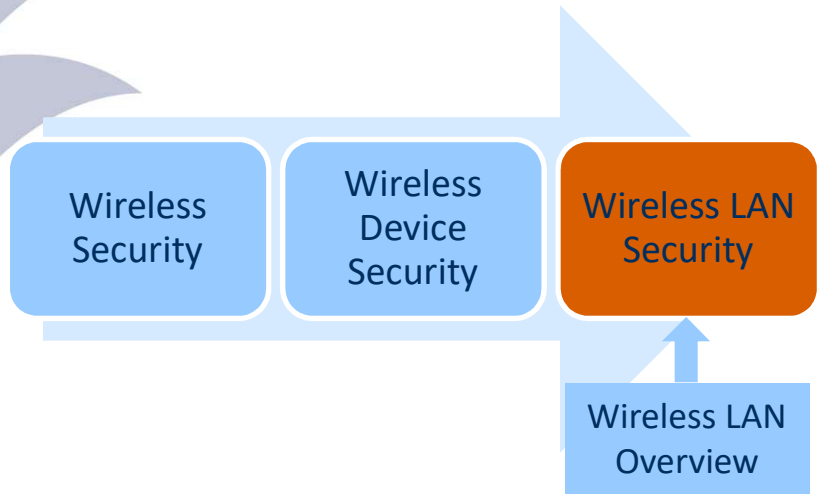
Association-Related Services

Stockholm University

- To deliver a message within a DS, the distribution service needs to know the identity of the AP to which the message should be delivered in order for that message to reach the destination station
- Three services relate to a station maintaining an association with the AP within its current BSS:
  - Association
    - Establishes an initial association between a station and an AP
  - Reassociation
    - Enables an established association to be transferred from one AP to another, allowing a mobile station to move from one BSS to another
  - Disassociation
    - A notification from either a station or an AP that an existing association is terminated

Stockholm University

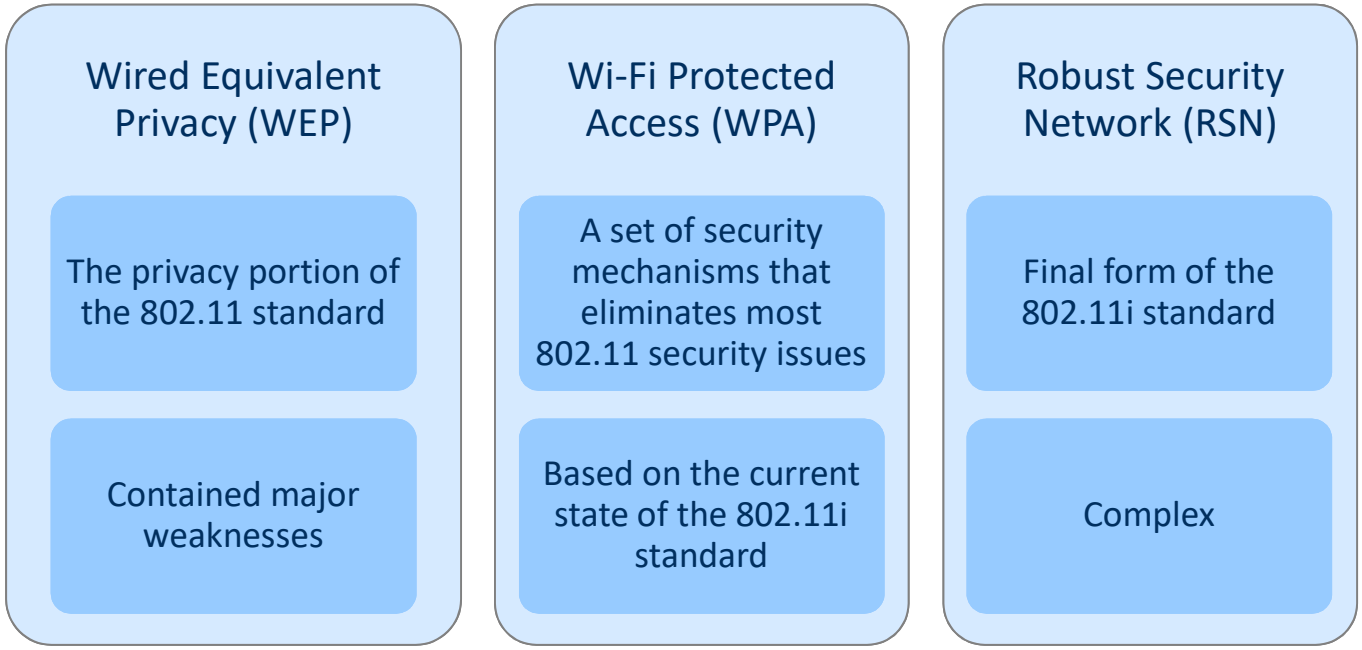
Wireless LAN Security



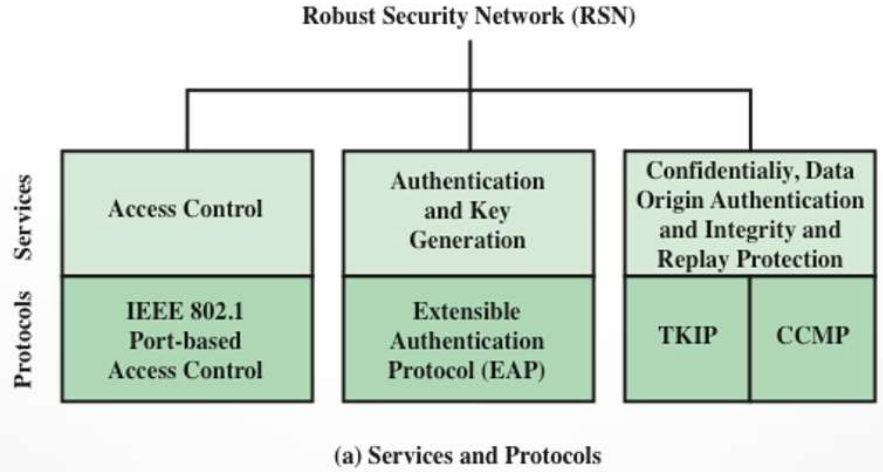
IEEE 802.11i Wireless LAN Security

Stockholm University

There is an increased need for robust security services and mechanisms for wireless LANs



Elements of IEEE 802.11i



IEEE 802.11i defined services:

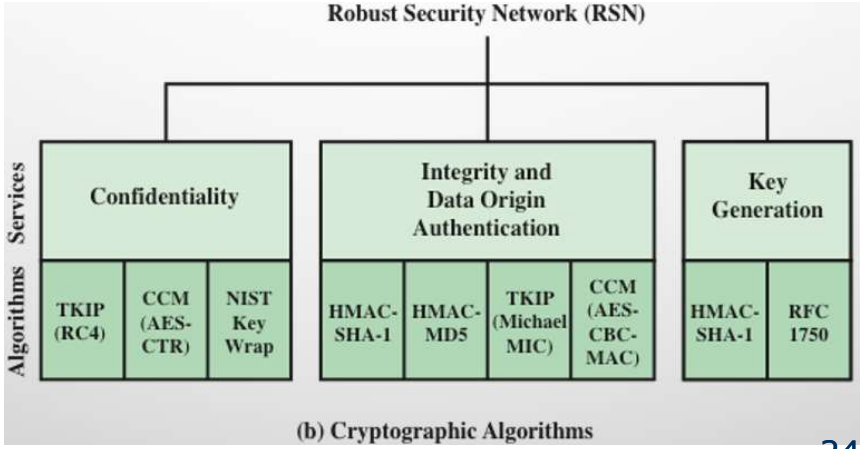
- Authentication
- Access control
- Privacy with message integrity

CBC-MAC: Cipher Block Chaining Message authentication code (MAC)

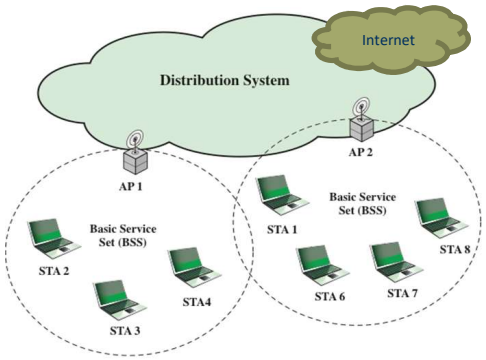
CCM: Counter Mode with Cipher Block Chaining MAC

CCMP: Counter mode with Cipher block chaining MAC Protocol

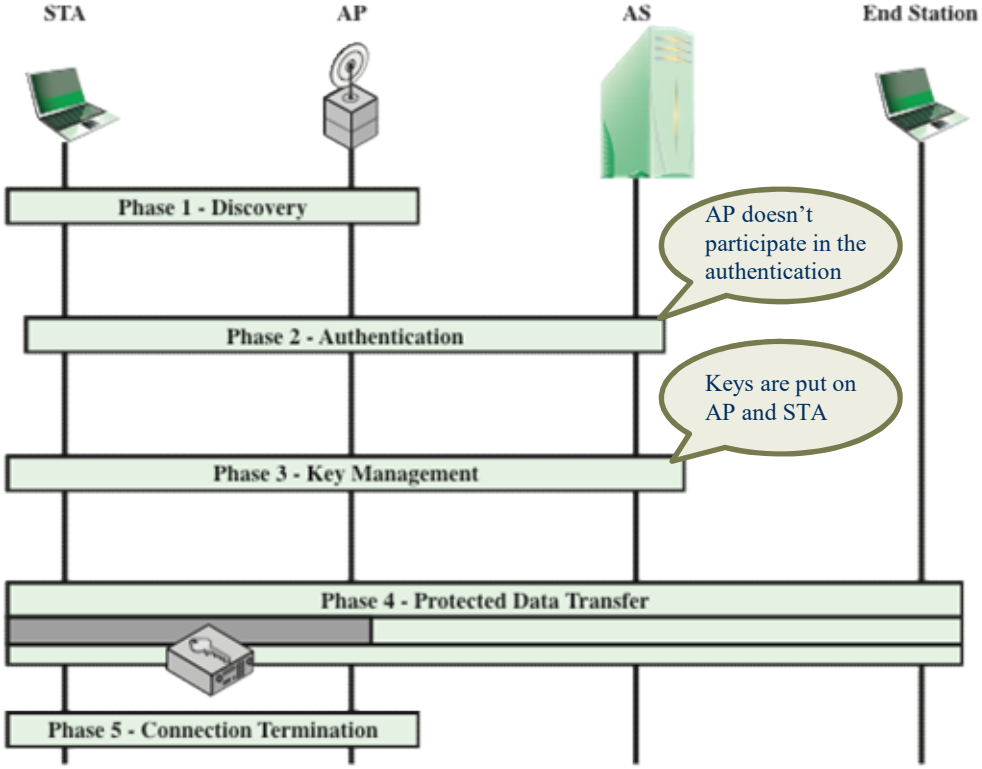
TKIP: Temporal Key Integrity Protocol



IEEE 802.11i Phases of Operation



IEEE 802.11i security is concerned only with secure communication between the STA and its AP.

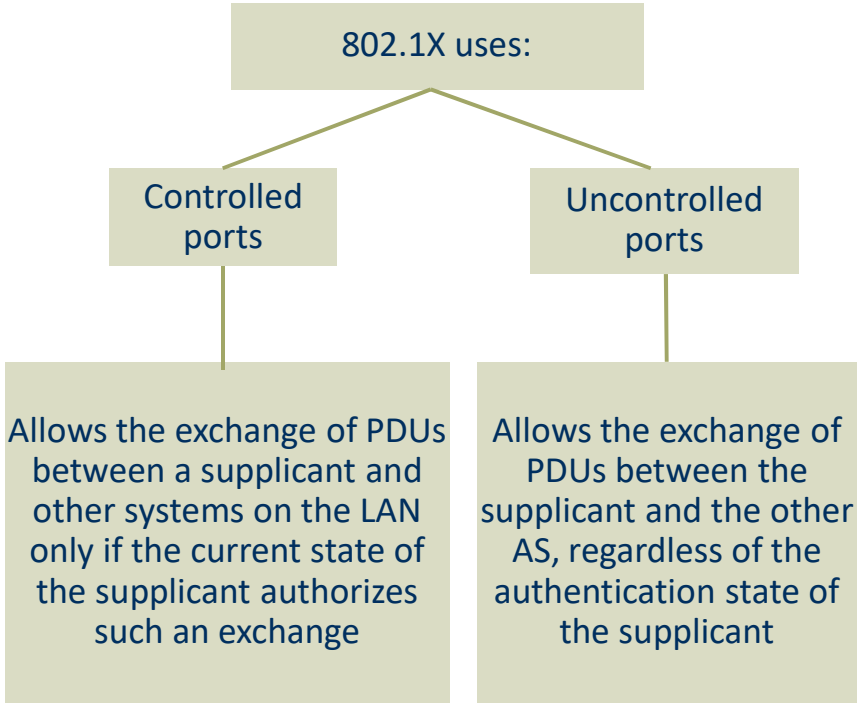


Only the wireless section is encrypted!

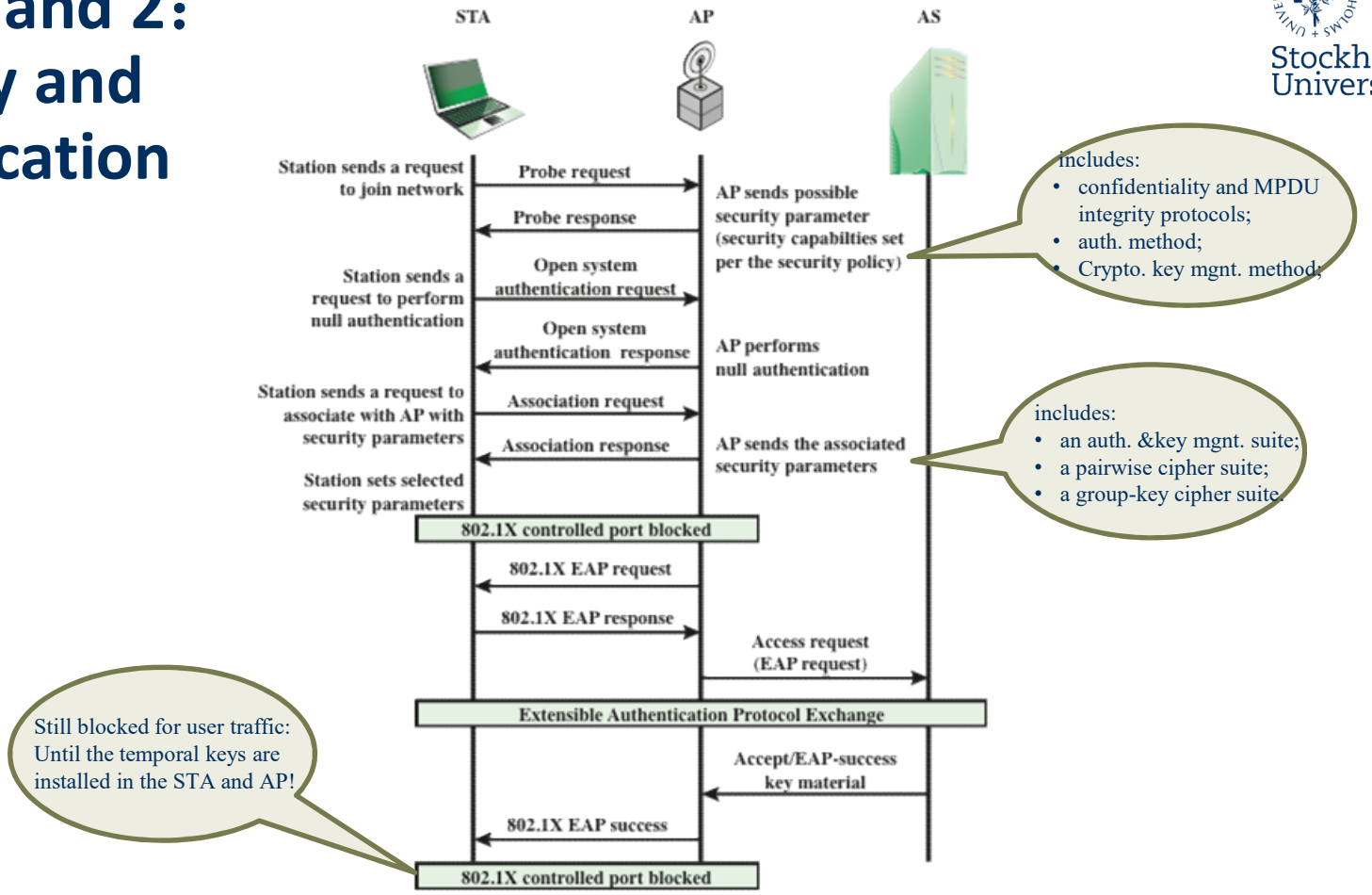
IEEE 802.1X Access Control Approach

Stockholm University

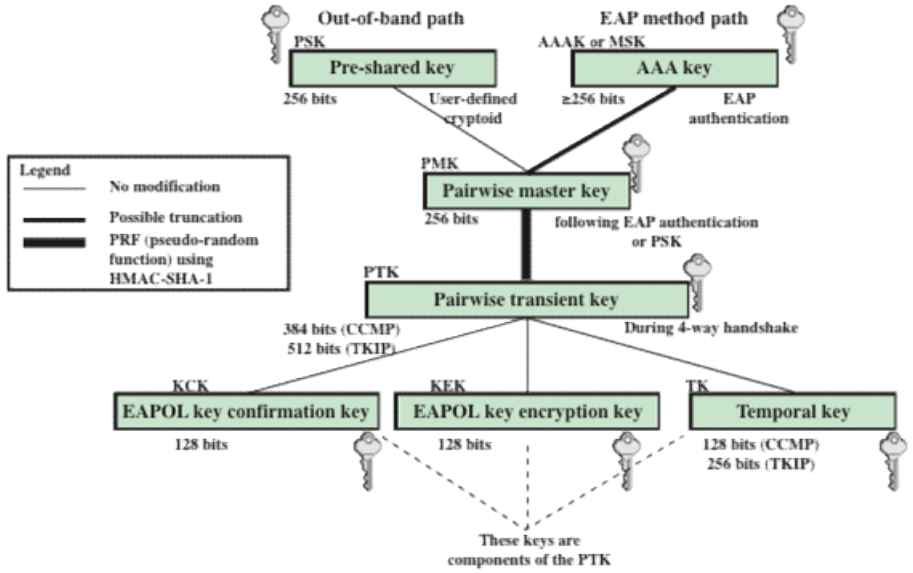
- IEEE 802.1X: Port-Based Network Access Control, used by IEEE 802.11i
  - Port: logical entities used by authenticator (AP); connections/channel
- Terms:
  - Supplicant (e.g., STA)
  - Authenticator (e.g., AP)
  - Authentication server
    - AAA server, support RADIUS
- EAP: Extensible Authentication Protocol, defined in the IEEE 802.1X standard
  - Run on top of PPP or IEEE 802 (EAP over LAN), not dependent on IP



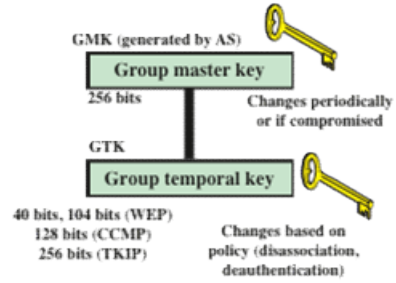
Phases 1 and 2: Discovery and Authentication



Relationship of IEEE 802.11i
Keys for Data Confidentiality and Integrity Protocols



(a) Pairwise key hierarchy



(b) Group key hierarchy

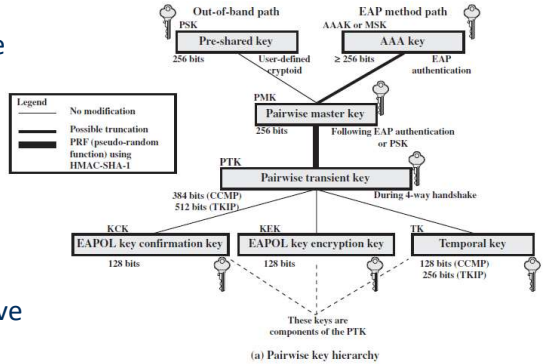
IEEE 802.11i Keys for Data Confidentiality and Integrity Protocols

Abbrev-iation	Name	Description / Purpose	Size (bits)	Type
AAA Key	Authentication, Accounting, and Authorization Key	Used to derive the PMK. Used with the IEEE 802.1X authentication and key management approach. Same as MMSK.	≥ 256	Key generation key, root key
PSK	Pre-shared Key	Becomes the PMK in pre-shared key environments.	256	Key generation key, root key
PMK	Pairwise Master Key	Used with other inputs to derive the PTK.	256	Key generation key
GMK	Group Master Key	Used with other inputs to derive the GTK.	128	Key generation key
PTK	Pair-wise Transient Key	Derived from the PMK. Comprises the EAPOL-KCK, EAPOL-KEK, and TK and (for TKIP) the MIC key.	512 (TKIP) 384 (CCMP)	Composite key
TK	Temporal Key	Used with TKIP or CCMP to provide confidentiality and integrity protection for unicast user traffic.	256 (TKIP) 128 (CCMP)	Traffic key
GTK	Group Temporal Key	Derived from the GMK. Used to provide confidentiality and integrity protection for multicast/broadcast user traffic.	256 (TKIP) 128 (CCMP) 40, 104 (WEP)	Traffic key
MIC Key	Message Integrity Code Key	Used by TKIP's Michael MIC to provide integrity protection of messages.	64	Message integrity key
EAPOL-KCK	EAPOL-Key Confirmation Key	Used to provide integrity protection for key material distributed during the 4-Way Handshake.	128	Message integrity key
EAPOL-KEK	EAPOL-Key Encryption Key	Used to ensure the confidentiality of the GTK and other key material in the 4-Way Handshake.	128	Traffic key / key encryption key
WEP Key	Wired Equivalent Privacy Key	Used with WEP.	40, 104	Traffic key

Stockholm University

Pairwise Keys

- Used for communication between a pair of devices, typically between a STA and an AP
  - **Pre-shared key (PSK)**
    - A secret key shared by the AP and a STA and installed in some fashion outside the scope of IEEE 802.11i
  - **Master session key (MSK)**
    - Also known as the AAAK, and is generated using the IEEE 802.1X protocol during the authentication phase
  - **Pairwise master key (PMK)**
    - Derived from the master key
    - If a PSK is used, then the PSK is used as the PMK; if a MSK is used, then the PMK is derived from the MSK by truncation
  - **Pairwise transient key (PTK)**
    - Consists of three keys used for communication between a STA and AP after they have been mutually authenticated
    - Using the STA and AP addresses in the generation of the PTK provides protection against session hijacking and impersonation; using nonces provides additional random keying material
- These keys form a hierarchy beginning with a master key from which other keys are derived dynamically and used for a limited period of time



(a) Pairwise key hierarchy

PTK (Pairwise Transient Key) Parts

Stockholm University

- The three parts of the PTK are:

EAP Over LAN (EAPOL) Key Confirmation Key (EAPOL-KCK)	• Supports the integrity and data origin authenticity of STA-to-AP control frames during operational setup of an RSN (e.g., to generate MIC) • It also performs an access control function: proof-of-possession of the PMK • An entity that possesses the PMK is authorized to use the link
EAPOL Key Encryption Key (EAPOL-KEK)	• Protects the confidentiality of keys and other data during some RSN association procedures
Temporal Key (TK)	• Provides the actual protection for user traffic

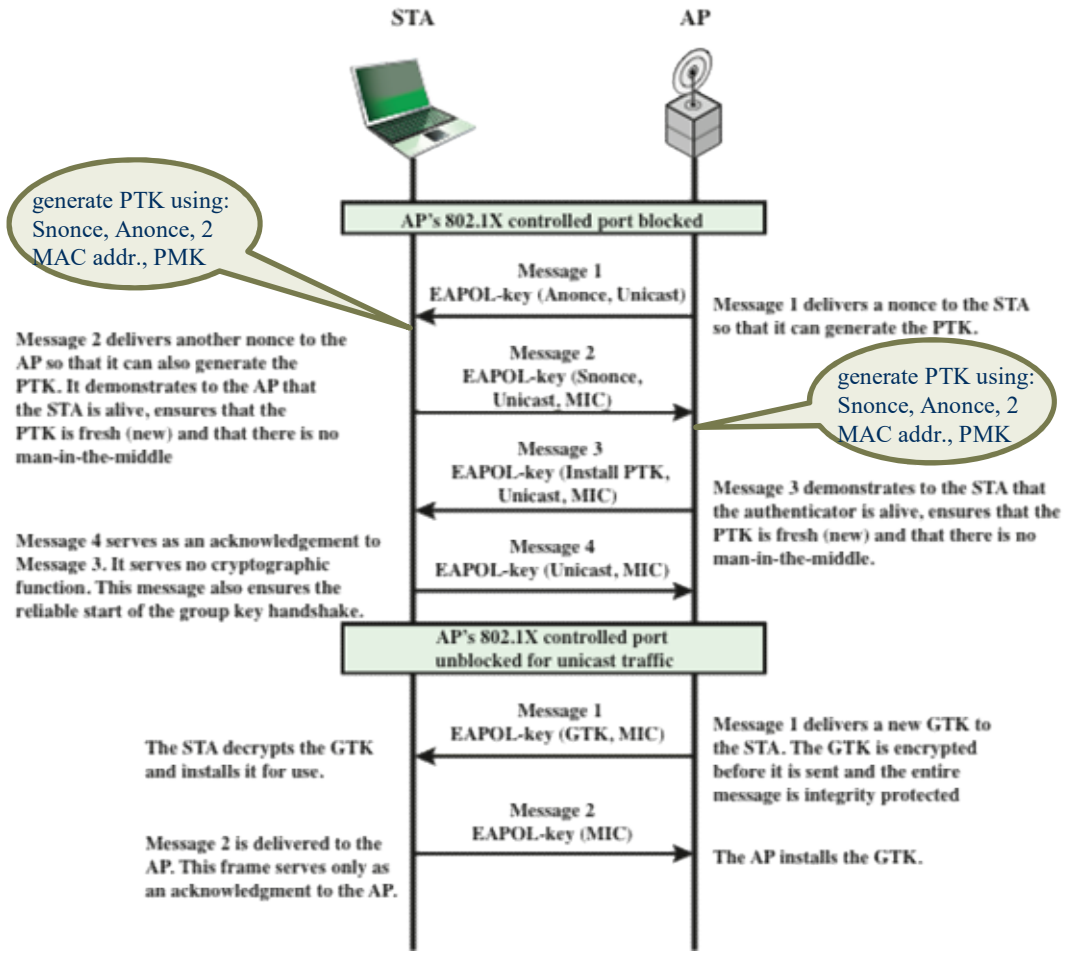
Group Keys

Stockholm University

- Group keys are used for multicast communication in which one STA sends MPDUs to multiple STAs
  - Group master key (GMK)
    - Key-generating key used with other inputs to derive the GTK
  - Group temporal key (GTK)
    - Generated by the AP and transmitted to its associated STAs
    - IEEE 802.11i requires that its value is computationally indistinguishable from random
    - Distributed securely using the pairwise keys that are already established
    - Is changed every time a device leaves the network

Phase 3： Key Management

Pairwise Key and Group Key Distribution:
Four-way handshake and group key handshake

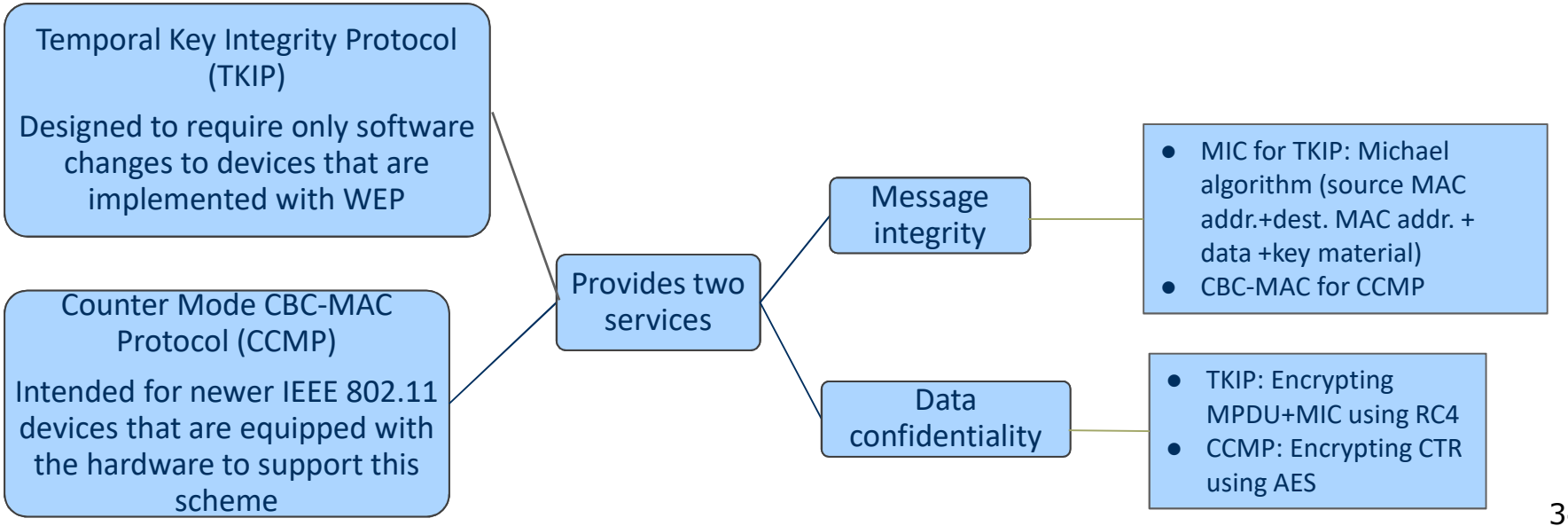


MIC: Message Integrity Code
MAC: Message Authentication Code
MAC: Media Access Control (e.g., MAC address)

Phase 4: Protected Data Transfer Phase

Stockholm University

IEEE 802.11i defines two schemes for protecting data transmitted in 802.11 MPDUs:



IEEE 802.11i Pseudorandom Function (PRF) -1

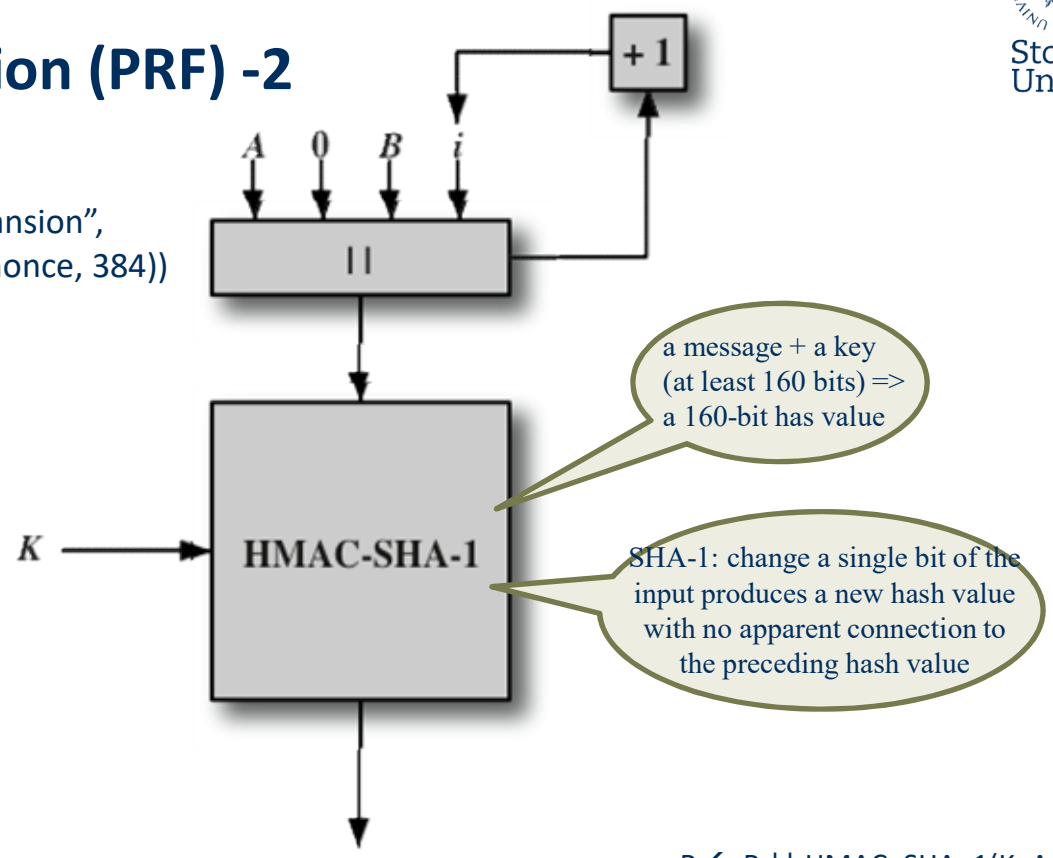
Stockholm University

- Used at a number of places in the IEEE 802.11i scheme (to generate nonces, to expand pairwise keys, to generate the GTK)
  - Best security practice dictates that different pseudorandom number streams be used for the different purposes
  - For implementation efficiency, make use of a relative small shared secret value to generate longer blocks of keys
- Built on the use of HMAC-SHA-1 to generate a pseudorandom bit stream

IEEE 802.11i
Pseudorandom Function (PRF) -2

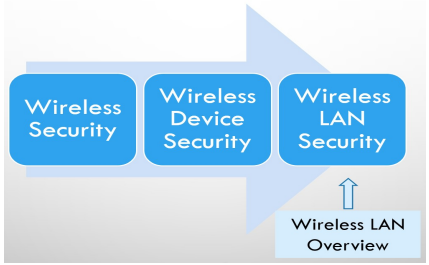
PTK= PRF(PMK, “Pairwise key expansion”,
STA-Addr||AP-Addr||Snonce||Anonce, 384))

➡ 384bits PTK



R ← R || HMAC–SHA–1(K, A ||0 ||B ||i)
Return Truncate–to–Len(R, Len)

Summary



- Wireless transmission security
  - Network threats
  - Security measures
- Mobile device security
  - Security threats
  - Security strategy
- IEEE 802.11 wireless LAN overview
  - IEEE 802 protocol architecture
  - IEEE 802.11 network components and architectural model
  - IEEE 802.11 services
- IEEE 802.11i wireless LAN security
  - IEEE 802.11i services
  - IEEE 802.11i phases of operation
    - Discovery phase
    - Authentication phase
    - Key management phase
    - Protected data transfer phase
  - The IEEE 802.11i pseudorandom function

Expected Learning Outcomes

Stockholm University

- Understand the protocol stack of IEEE 802.11.
- Understand and apply the terminologies of IEEE 802.11.
- Understand and explain the security threads specialized for wireless network systems.
- Understand and apply the security services provided by IEEE 802.11i.
- Understand and explain each phase of IEEE 802.11i, and the security mechanisms used in each phase of IEEE 802.11i.

Stockholm University

Thank you!