
ESTD1845
QUEEN'S
UNIVERSITY
BELFAST

Wireless/Mobile Security

Dr. Sandra Scott-Hayward

CSC3064 Lecture 20

School of Electronics, Electrical Engineering and Computer Science

Session Overview

- Security aspects of mobile communication
- Security aspects of wireless communication
- IEEE 802.11 security claims/issues
- IEEE 802.11i (Robust Security Network)

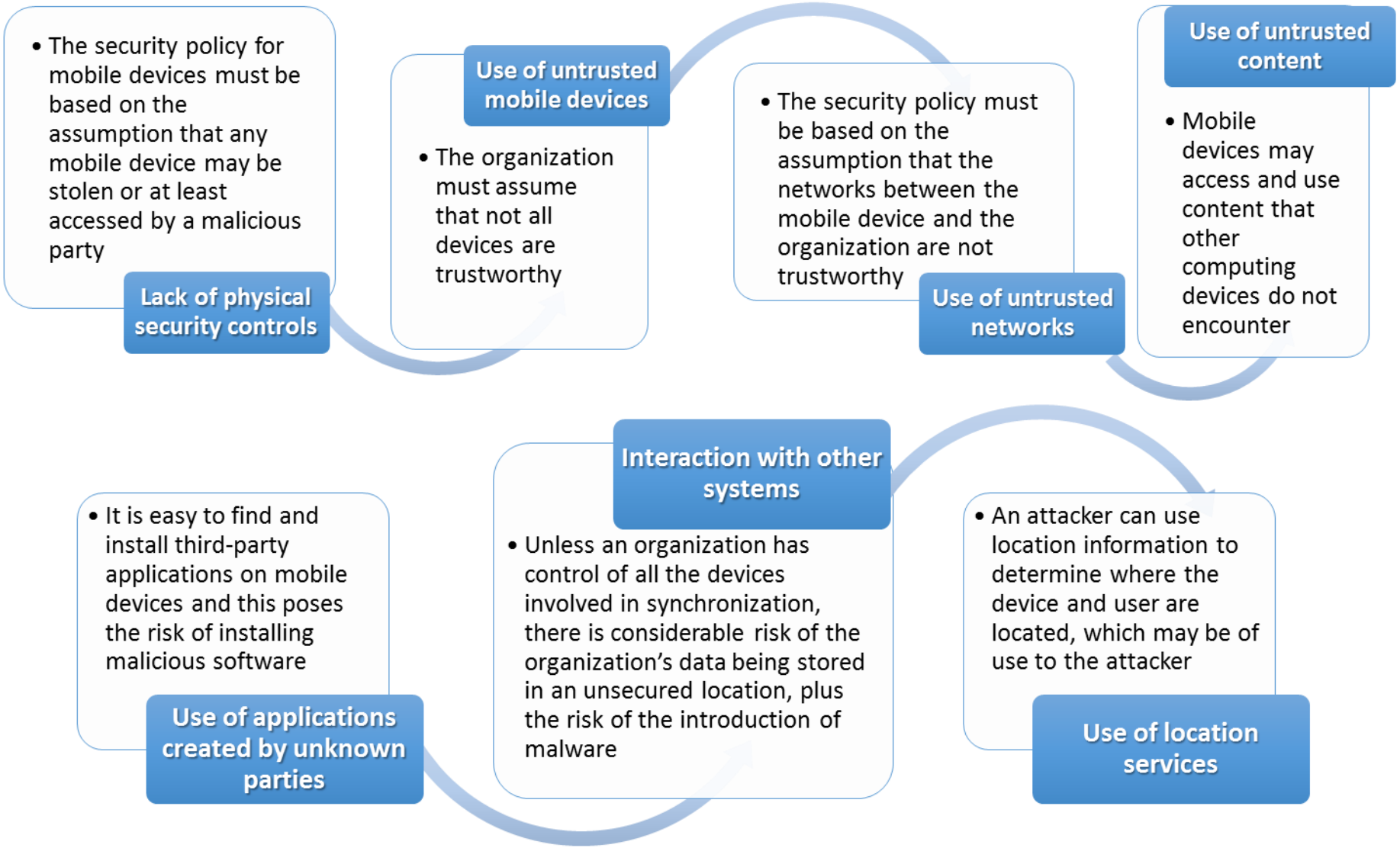
References:
Schäfer, Günter, and Michael Rossberg. *Security in Fixed and Wireless Networks*. John Wiley & Sons, 2016.
Stallings, William. *Network security essentials: applications and standards*. Pearson Education India, 2014.

QUEEN'S UNIVERSITY BELFAST

Security aspects of mobile communication

- Mobile communication faces all fixed network threats …
- Plus some specific issues arising out of mobility of users and / or devices:
  - Some existing threats become more dangerous:
    - Wireless communication is more accessible for eavesdropping
    - The lack of a physical connection makes it easier to access services
  - Some new difficulties for realizing security services:
    - Authentication has to be re-established when the mobile device moves
    - Key management gets harder as peer identities can not be pre-determined
  - One completely new threat:
    - The location of a device / user becomes a more important piece of information that is worthwhile to eavesdrop on and thus to protect

Security issues of mobile devices



QUEEN'S UNIVERSITY BELFAST

Location privacy in mobile networks

- There is no appropriate location privacy in today's mobile networks:
  - GSM / UMTS / LTE:
    - Active attackers can collect IMSIs (international mobile subscriber identity) on the air interface
    - Visited network's operators can partially track the location of users
    - Home network operators can fully track the location of users
    - However, at least communicating end systems can not learn about the location of a mobile device
  - Wireless LAN:
    - No location privacy, as the (world-wide unique) MAC address is always included in the clear in every MAC frame

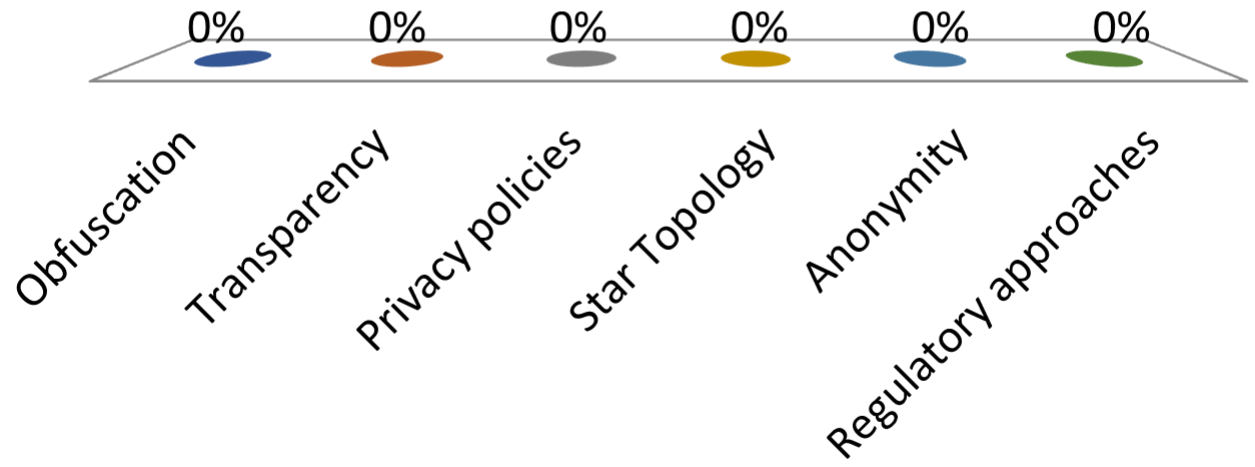
Location privacy in mobile networks

- The basic location privacy design problem:
  - A mobile device should be reachable
  - No (single) entity in the network should be able to track the location of a mobile device
- Four classes of protection strategies:
  - *Regulatory approaches*
    - *Legal rules for collecting and handling location information*
  - *Privacy Policies*
    - *Automatic ways for users to prevent certain uses of their personal data*
  - *Anonymity*
    - *Attempt to hide individuals' identities, either by using pseudonyms or by withholding identity information altogether*
  - *Obfuscation*
    - *Implementing the need-to-know principle i.e. reducing information to what is absolutely necessary for a requested service*

QUEEN'S UNIVERSITY BELFAST

From the list below, identify all the classes of protection strategies to preserve location privacy in wireless networks.

- ✓ A. Obfuscation
- B. Transparency
- ✓ C. Privacy policies
- D. Star Topology
- ✓ E. Anonymity
- ✓ F. Regulatory approaches



Security Issues of wireless networks

Some of the key factors contributing to the higher security risk of wireless networks compared to wired networks include:

Channel

- Wireless networking typically involves broadcast communications, which is far more susceptible to eavesdropping and jamming than wired networks
- Wireless networks are also more vulnerable to active attacks that exploit vulnerabilities in communications protocols

Mobility

- Wireless devices are far more portable and mobile than wired devices
- This mobility results in a number of risks

Resources

- Some wireless devices, such as smartphones and tablets, have sophisticated operating systems but limited memory and processing resources with which to counter threats, including denial of service and malware

Accessibility

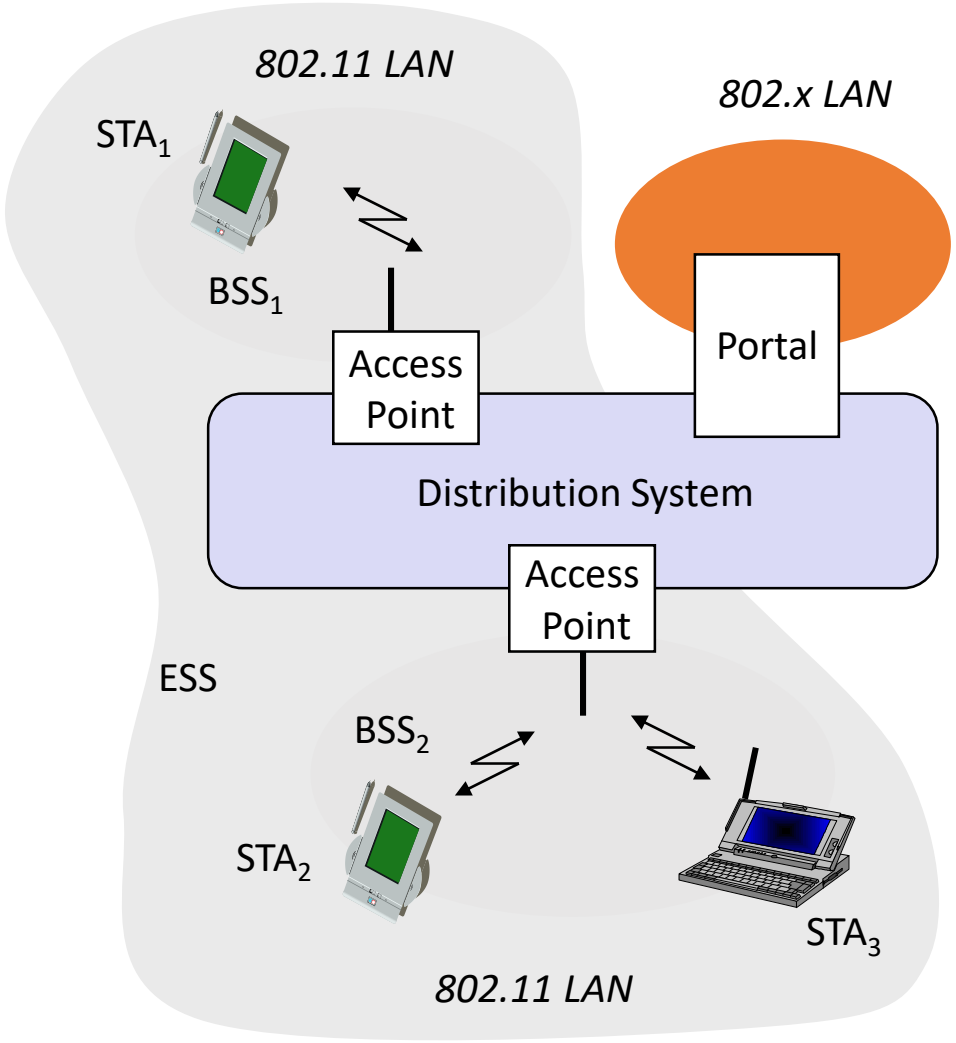
- Some wireless devices, such as sensors and robots, may be left unattended in remote and/or hostile locations
- This greatly increases their vulnerability to physical attacks

QUEEN'S UNIVERSITY BELFAST

IEEE 802.11

- 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 standardizes medium access control (MAC) and physical characteristics of a wireless *local area network (LAN)*

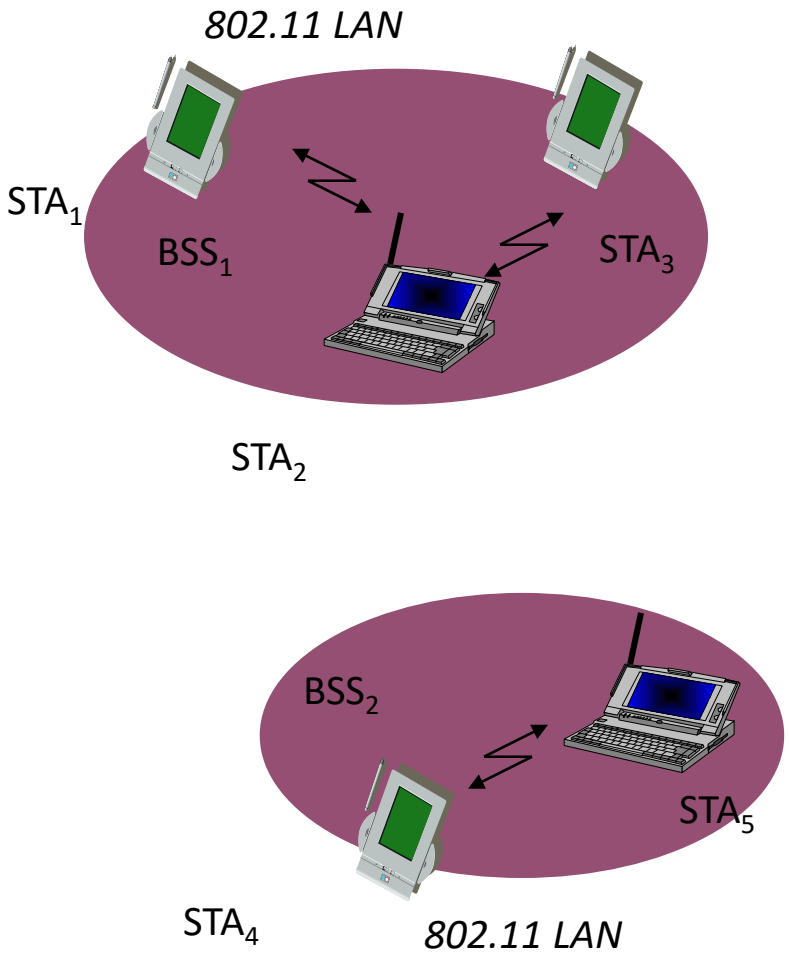
IEEE 802.11 – Architecture of an infrastructure network



- *Station (STA):*
  - Terminal with access mechanisms to the wireless medium and radio contact to the access point
- *Basic Service Set (BSS):*
  - Group of stations using the same radio frequency
- *Access Point:*
  - Station integrated into the wireless LAN and the distribution system
- *Portal:*
  - Bridge to other (wired) networks
- *Distribution System:*
  - Interconnection network to form one logical network *(extended service set, ESS)* based on several BSS

QUEEN'S UNIVERSITY BELFAST

IEEE 802.11 – Architecture of an ad-hoc network



- *Station (STA):*
  - Terminal with access mechanisms to the wireless medium
- *Basic Service Set (BSS):*
  - Group of stations using the same radio frequency

- Ad-Hoc networks allow direct communication between end systems within a limited range
- As there is no infrastructure, no communication is possible between different BSSs

QUEEN'S UNIVERSITY BELFAST

Wireless Network Threats

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

- In this situation, 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)

- This occurs when 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

- This attack involves 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)

- This attack occurs when 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

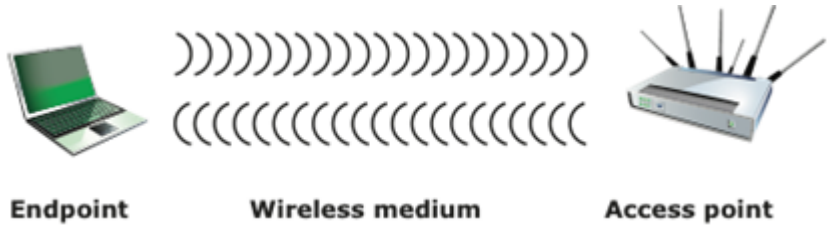
- This attack targets wireless access points that are exposed to nonfiltered network traffic, such as routing protocol messages or network management messages

Securing wireless transmissions

- The principal threats to wireless transmission are eavesdropping, altering or inserting messages, and 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

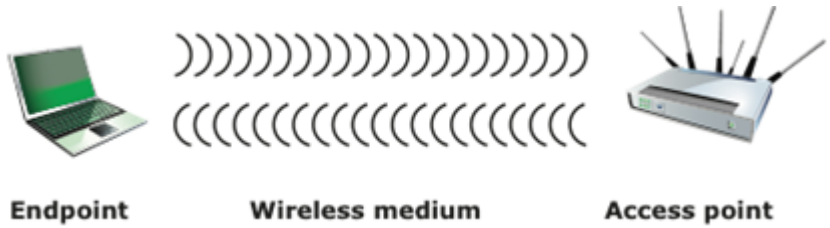
  Encryption
  - Is effective against eavesdropping to the extent that the encryption keys are secured



QUEEN'S UNIVERSITY BELFAST

Securing wireless access points

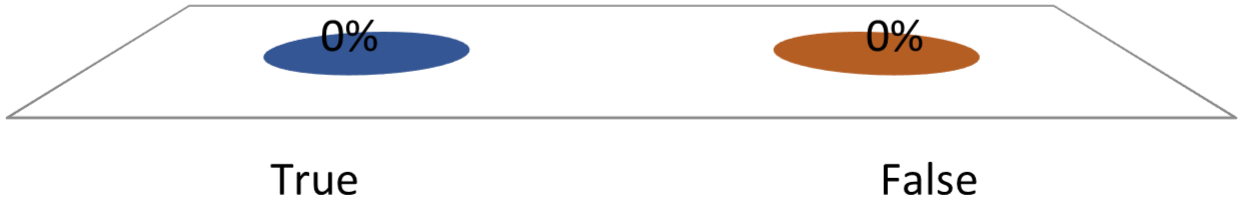
- The main threat involving wireless access points is unauthorized access to the network
- The principal approach for preventing such access is the IEEE 802.1x standard for port-based network access control
  - The standard provides an authentication mechanism for devices wishing to attach to a LAN or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



QUEEN'S UNIVERSITY BELFAST

Accidental association is when a client offers an irresistibly strong signal intentionally for malicious purposes.

A. True
✓B. False



Security services of IEEE 802.11

- Security services of IEEE 802.11 were originally realized by:
  - Entity authentication service
  - *Wired Equivalent Privacy (WEP)* mechanism
- WEP is supposed to provide the following security services:
  - Confidentiality
  - Data origin authentication / data integrity
  - Access control
- WEP makes use of the following algorithms:
  - The RC4 stream cipher
  - The Cyclic Redundancy Code (CRC) checksum for detecting errors

IEEE 802.11's security claims

- The WEP has been designed to ensure the following security properties:
  - Confidentiality:
    - Only stations which possess K_{BSS} can read messages protected with WEP
  - Data origin authentication / data integrity:
    - Malicious modifications of WEP protected messages can be detected
  - Access control in conjunction with layer management:
    - If set up, only WEP protected messages will be accepted by receivers
    - So stations that do not know K_{BSS} can not send to such receivers

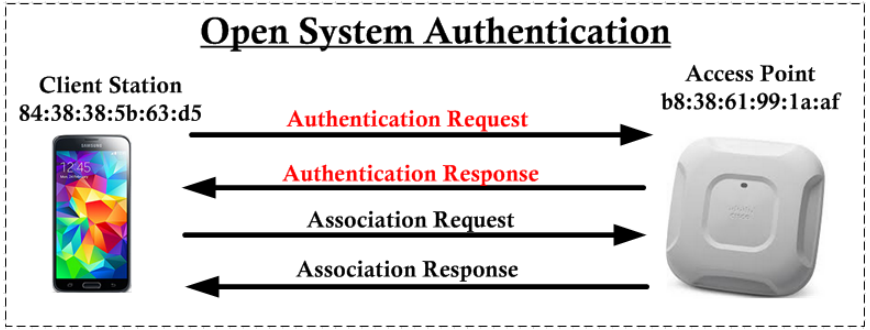
- Unfortunately, none of the above claims holds...

IEEE 802.11 entity authentication

Originally, IEEE 802.11 authentication came in two “flavours”:

Open System Authentication:

- “Essentially it is a null authentication algorithm.” (IEEE 802.11, section 8.1.1)



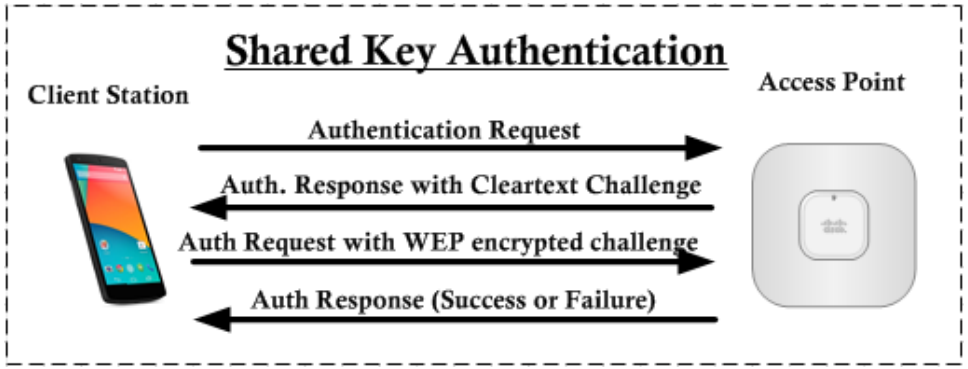
Shared Key Authentication:

- “Shared key authentication supports authentication of STAs as either a member of those who know a shared secret key or a member of those who do not.” (IEEE 802.11, section 8.1.2)
- “The required secret, shared key is presumed to have been delivered to participating STAs via a secure channel that is independent of IEEE 802.11”

QUEEN'S UNIVERSITY BELFAST

IEEE 802.11 entity authentication

- IEEE 802.11's *Shared Key Authentication* dialogue:
  - Authentication should be performed between stations and access points and could also be performed between arbitrary stations
  - When performing authentication, one station is acting as the *requestor (A)* and the other one as the *responder (B)*
  - The authentication dialogue:
    1.) $A \rightarrow B$: (Authentication, 1, ID_A)
    2.) $B \rightarrow A$: (Authentication, 2, r_B)
    3.) $A \rightarrow B$: {Authentication, 3, r_B}$_{K_{A,B}}$
    4.) $B \rightarrow A$: (Authentication, 4, Successful)



  - Mutual authentication requires two independent protocol runs, one in each direction

QUEEN'S UNIVERSITY BELFAST

Summary of IEEE 802.11 deficiencies

- Original IEEE 802.11 does not provide sufficient security:
  - Missing key management makes the use of the security mechanisms tedious and leads to rarely changed keys or security being switched off
  - Entity authentication and encryption rely on a key shared by all stations of a BSS
  - Insecure entity authentication protocol
  - Reuse of key stream makes known-plaintext attacks possible
  - Linear integrity function allows to forge Integrity Check Values (ICVs)
  - Unkeyed integrity function allows to circumvent access control by creating valid messages from a known plaintext-ciphertext pair
  - Weakness in RC4 key scheduling allows to cryptanalyze keys
- Even with IEEE 802.1X and individual keys the protocol remains weak
- Some proposed countermeasures:
  - Place your IEEE 802.11 network outside your Internet firewall
  - Do not trust any host connected via IEEE 802.11
  - Additionally, use other security protocols, e.g. PPTP, L2TP, IPSec, SSH, ...

So, what security can you expect in a WLAN hotspot?

- For most hotspots: Unfortunately almost none!
- If you do not have to configure any security parameters besides typing in a username and password in a web page, expect the following:
  - The hotspot operator checks your authenticity at logon time (often protected with SSL to protect against eavesdropping on your password)
  - Only authenticated clients will receive service as packet filtering is deployed to only allow access to the logon page until successful authentication
  - Once logon authentication has been checked: no further security measures
  - No protection for your user data:
    - Everything can be intercepted and manipulated
    - However, you can deploy your own measures, e.g. VPN or SSL, but configuration is often tedious or not even supported by communication partner and performance is affected because of additional (per-packet-) overhead
  - Plus: your session can be stolen (session hijacking)
- Consequence: better WLAN security is urgently required

Fixing WLAN security: IEEE 802.11i, WPA and WPA2

- Scope: Defining the interaction between 802.1X and 802.11 standards
- Two classes of security algorithms for 802.11:
  - Pre-RSN security Network ($\rightarrow$ WEP)
  - Robust Security Network (RSN)
- RSN security consists of two basic subsystems:
  - Data privacy mechanisms:
    - TKIP - rapid re-keying to patch WEP for minimum privacy (marketing name WPA)
    - AES encryption - robust data privacy for long term (marketing name WPA2)
  - Security association management:
    - Enterprise mode – based on 802.1X
    - Personal mode – based on pre-shared keys

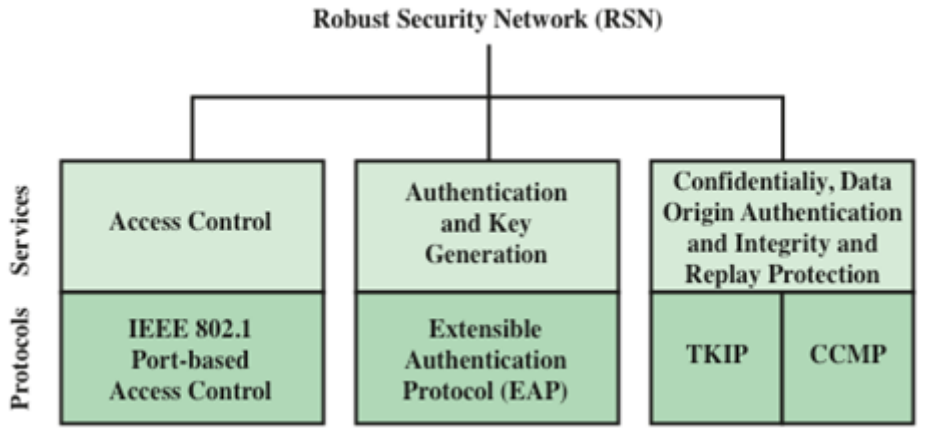
Comparison of WEP, TKIP and CCMP

	WEP	TKIP	CCMP
Cipher	RC4	RC4	AES
Key Size	40 or 104 bits	104 bits	128 bits encrypt, 64 bit auth.
Key Life	24-bit IV, wrap	48-bit IV	48-bit IV
Packet Key	Concat.	Mixing Fnc.	Not Needed
Integrity			
Data	CRC-32	Michael	CCM
Header	None	Michael	CCM
Replay	None	Use IV	Use IV
Key Mgmt.	None	EAP-based	EAP-based

→ Currently TKIP is deprecated, AES is recommended

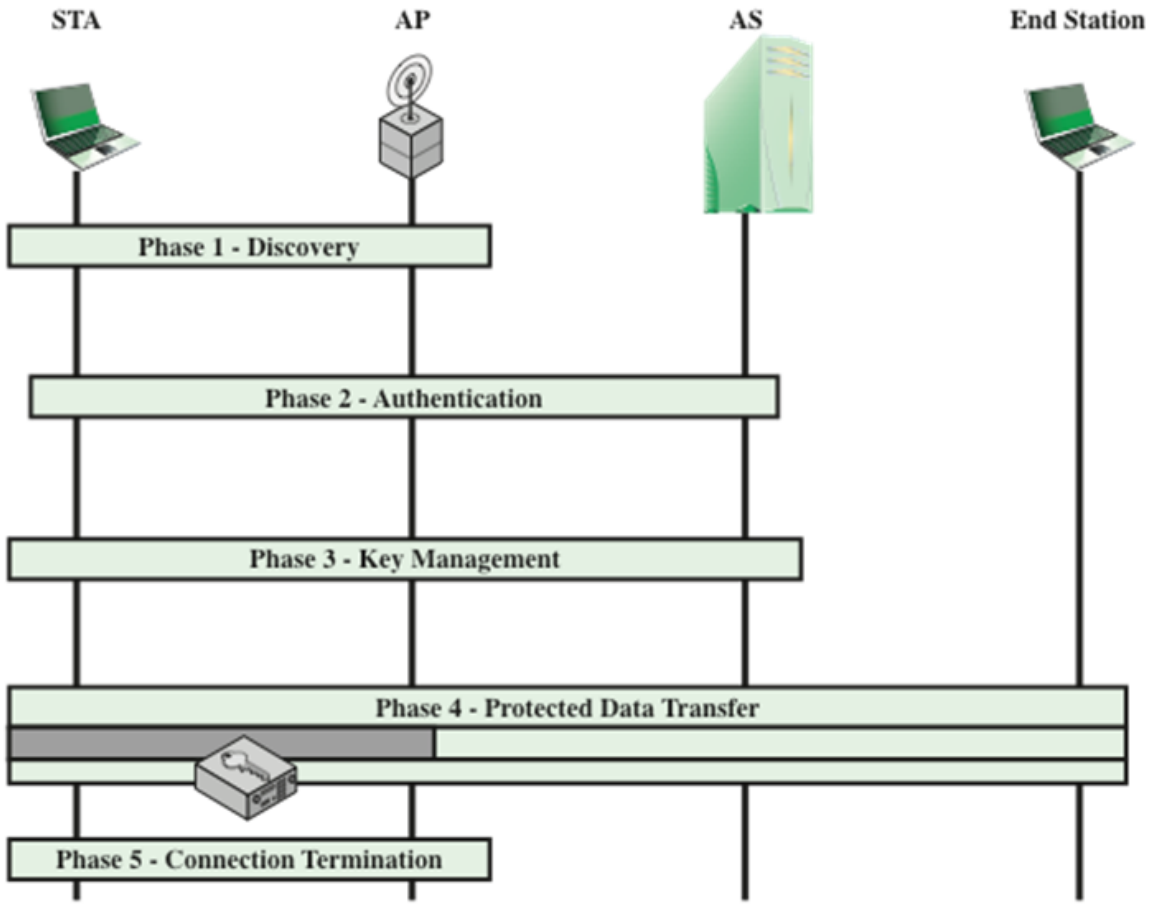
RSN Services and Protocols

Wired Equivalent Privacy (WEP)	Wi-Fi Protected Access (WPA)	Robust Security Network (RSN)
The privacy portion of the 802.11 standard	A set of security mechanisms that eliminates most 802.11 security issues	Final form of the 802.11i standard
Contained major weaknesses	Based on the current state of the 802.11i standard	Complex



QUEEN'S UNIVERSITY BELFAST

802.11i Phases of Operation



QUEEN'S UNIVERSITY BELFAST

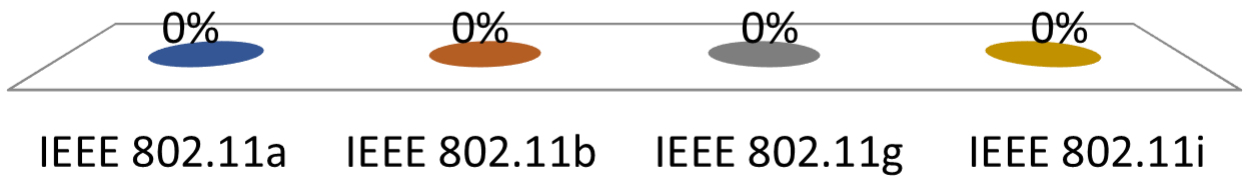
Securing wireless networks

- 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

QUEEN'S UNIVERSITY BELFAST

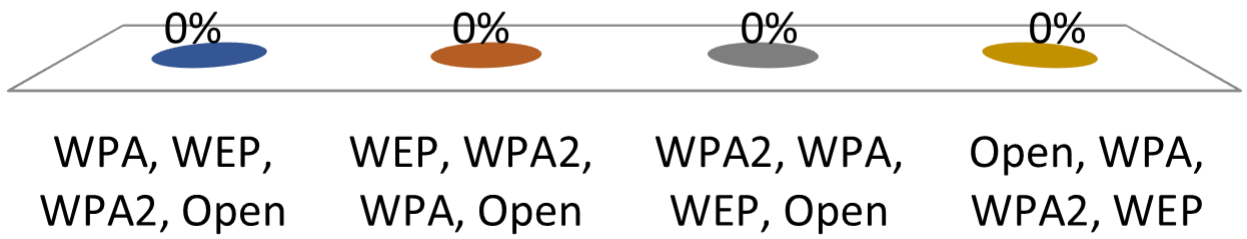
Which of the following specifies security standards for wireless?

A. IEEE 802.11a
B. IEEE 802.11b
C. IEEE 802.11g
✓ D. IEEE 802.11i



Which of the following options shows the protocols in order from strongest to weakest?

A. WPA, WEP, WPA2, Open
B. WEP, WPA2, WPA, Open
✓C. WPA2, WPA, WEP, Open
D. Open, WPA, WPA2, WEP



Summary

- Security aspects of mobile communication
- Security aspects of wireless communication
- IEEE 802.11 security claims/issues
- IEEE 802.11i (Robust Security Network)

Questions?

End of CSC3064 Content

QUEEN'S UNIVERSITY BELFAST