Wireless exam

June 30, 2024

1 Quiz or closed questions

1.1 General

What is a stream cipher?

Which of the following defines a cipher text attack?

what is known plaintext attack

Classification of wireless network, adhoc/infrastructure, fixed/mobile, wwan/wlan

Wireless Communication

In digital Communication system which type of waveforms are propagated in the channel?

Order the elements in the transmission chain (encoder, modulator, channel etc.)

Why the definition of the bandwidth 3db

PSK modulation - about the energy level of symbols and saturation level of a power amplifier

1.2 GNSS

How can a spoofing attack be detected?

Why monitoring GNSS spectrum is insufficient for spoofing detection?

GNSS - Why is line of sight to satellites important to have correct pseudorange calculations?

Are the clocks of Satellite and receiver synchronized?

What is broadcasted by the satellite

Do Out-Of-Band interferences affect GNSS?

Which of the following is a common indicator of a GNSS spoofing attack?

1. A gradual decrease in signal strength over time
2. Enhanced accuracy and reliability of GNSS signals
3. Sudden and significant deviations in position, velocity or time calculations
4. None of the others
5. Discrepancies between GNSS-based positions and those from alternative navigation systems (eg., inertial navigation systems)

1.3 WLAN / wifi

Two devices connected in Wi-Fi without RTS/CTS assumed to collide, order what happened (and there where a series of steps like A sends, B, sends, DATA(A) collide with DATA(B) etc,)

Sort the exchanged messages to connect to an AP

Algorithm used in OWE

How WEP key management ic compared to WPA/WPA2

why not csma/ cd in wifi

authentication service - in the context of wireless networks

CDMA networks - why is power control important?

Purpose of DIFS in wifi networks

802.11 network - using ISM BW range, how many independent channels can be used?

Which wifi protocols are considered secure? (wpa with tkip, wpa2, wep, wpa3)

ranking throughput higher to lower 802.11g 802.11n using tcp or udp and using or not rts/cts

Definition of authenticator supplicant port server authentication

Maximum goodput that can be reached with this technology from 1 to 9

- 802.11n, RTS/CTS enabled, UDP+IP
- 802.11n, RTS/CTS disabled, UDP+IP
- 802.11g, RTS/CTS enabled, UDP+IP
- 802.11g, RTS/CTS disabled, UDP+IP
- 802.11n, RTS/CTS enabled, TCP+IP
- 802.11g, RTS/CTS disabled, TCP+IP
- 802.11g, RTS/CTS enabled, TCP+IP
- 802.11n, RTS/CTS disabled, TCP+IP
- Fast ethernet 100 Mbps

1.4 WPAN / Bluetooth

How does Bluetooth Classic handle privacy concerns compared to Bluetooth LE?

1. Bluetooth Classic uses encryption keys for all data transmissions.
2. Bluetooth Classic limits the number of devices that can connect simultaneously
3. Bluetooth Classic randomizes MAC addresses for improved privacy.
4. Bluetooth Classic does not have any privacy features
5. None of the other options.

What is bluesnarfing?

BT secure services

How prevent MITM on Bluetooth Secure Simple Pairing?

Which multiple access mechanism BT uses?

1.5 WWAN / mobile

What is Stingray vulnerability?

Which of the following are 2G vulnerabilities?

Ss7 vulnerability

Purpose of paging and location are in mobile network

Differences between VLR and HLR

Describe device authentication in GSM (completare l'immagine con le parti date.)

4G networks - techniques used to enhance security

2 Open questions

2.1 General

2.2 Wireless Communication

2.3 GNSS

Explain the informations sent by the GNSS satellite to the received and how they are used to compute the PVT

Difference between Jamming and spoofing in GNSS, how they influence the PVT , what is more harmful and why?

Describe meaconing compare work other type of GNSS ATTACKS.

Describe two interferences mitigation techniques in GNSS

Explain in general detection and mitigation techniques for interference signals in both domain. Explain in detail mitigation technique in frequency domain and in time domain

Describe the mitigation techniques (at least 3) of GNSS spoofing and the relative leves in which they act.

List and describe some possible spoofing countermeasures for satellite navigation systems. (3 points) Identify at least three spoofing countermeasures. Briefly describe how each countermeasure works. Explain the effectiveness of each countermeasure in mitigating spoofing attacks. Specify the levels of a satellite navigation system at which these countermeasures can be implemented. (3 points) Identify the different levels within a satellite navigation system. For each of the countermeasures mentioned above, indicate the level(s) at which they can be applied.

What are the effects of a spoofing attack on a GNSS receiver? (2 pts) How can a receiver fail or fail to respond to a spoofing attack? (2 pts) Possible disruptions of the attack? (2 pts)

2.4 WLAN - wifi

Power saving mode in 802.11 + attack

Consider a setup in which 2 STA (STA-1 and STA-2) are connected to the same WLAN managed by an AP, A third device (ETH 1) is connected with Ethernet technology. For each setup, describe and justify the expected good put in the following cases: Scenario 1(3 points): Both STA-1 and STA-2 use 802.11g on the ISM band, ETH-1 uses Fast Ethernet technology with a physical link capacity of 100Mb/s

1. STA-1 sends data to ETH-1 using UDP
2. STA-1 sends data to ETH-1 using TCP
3. STA-1 sends data to STA-2 using UDP
4. STA-1 sends data to STA 2 using TCP

Scenario 2 (2 points): What changes if STA-1 now connects to the same WLAN but using the 5GHz band? Again, consider the cases

1. STA-1 sends data to ETH-1 using UDP
2. STA-1 sends data to ETH 1 using TCP
3. STA-1 sends data to STA-2 using UDP
4. STA-1 sends data to STA-2 using TCP

Scenario 3 (1point), what changes if now both STA-1 (on 5GHz band) and STA-2 (on 2.4GHz band) upgrade their technology to using 802.11ax (WiFi 6)?

1. STA-1 sends data to ETH-1 using UDP
2. STA-1 sends data to ETH-1 using TCP
3. STA-1 sends data to STA-2 using UDP
4. STA 1 sends data to STA-2 using TCP

Consider UDP header of 8B, TCP header of 20B, IP header of 20B, Ethernet header c' of 38B.

Describe the frames exchanged by an STA and an AP to inform the STA about the SSID of the AP; what kind of attack exploits this mechanism?
Descrive step For OPEN AUTH sydtem when the Ap communicate EESID and when not

Describe the sequence of messages that an STA and an AP exchange during association and authentication processes in an open system(?) in the following cases:
case 1 - AP broadcasts beacon messages (2 points)
case 2 - ESSID is hidden, AP does not broadcast WLAN EISS in beacons (2 points)
(enumerate the steps) which types of attacks do these mechanisms allow? (2 points)

2.5 WPAN - Bluetooth

Secure simple pairing + MITM attack

Differences between BT BR/EDR and BLE (frequencies, FEC/ARQ, . . .)

Which are the privacy offered by Bluetooth? Describe how the IRK is used to provide resolvable private addresses.

What are the 4 association modes in Bluetooth and what capabilities a device must have to support them(in general); Why they are used? For every association mode, tell which capabilities a device must have to support them (for Numerical comparison the devices must have these capabilities and so on and so forth)

Bluetooth modes OOB, Just works, passkey entry, numeric comparison and hardware required to use them

Describe the 4 states of a Bluetooth device (standby, advertiser, scanner, initiator and master/slave) (3 porints) and prove an example with all the steps, A sends frame to B, B sends broadcast to A, A extract YYYY, ZZZZ from XXX to get GGGG etc (3 points)

Explain the main design goals for the BT technology and the technical constraints that guided the design (2 pts). Describe BT network topologies and the role of nodes in each scenario (2 pts). Describe the physical layer com mechanisms implemented in BT BR/EDR and the differences since BLE was introduced: which frequency range does it use, which multiple access scheme does it use, which FEC/ARQ mechanism it provides etc. (2 pts)

2.6 WWAN - mobile