Last Name:

First Name:

Student ID:

Security of Wireless Networks AS2018

(252-1411-00L)

Srdjan Capkun

Examination Rules:

1. Written exam, 90 minutes total.
2. No books, no calculators, no computers or communication devices.
3. Write all your answers on this document, space is reserved for your answers after each question. Blank pages are available at request.
4. Put your Student ID card visible on the desk during the exam.
5. If you feel disturbed, immediately call an assistant.
6. Answers will only be evaluated if they are readable.
7. Write with a black or blue pen (no pencil, no green or red color).

Question	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	Total
Points	3	3	8	9	8	4	10	8	3	6	6	4	4	4	80
Score															

This page intentionally left blank

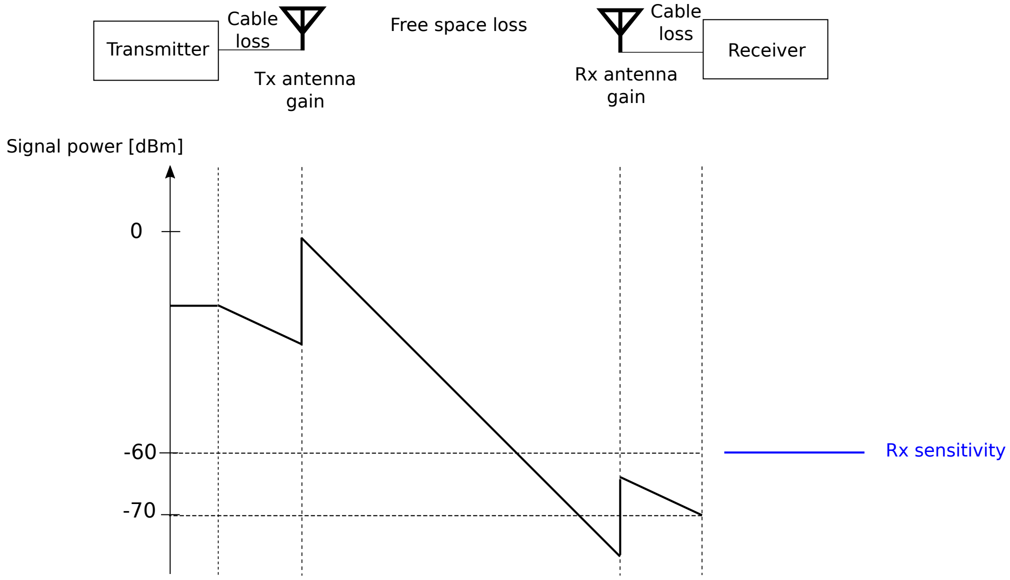


Figure 1: Example link budget

1. Wireless Basics

(a) (1 point) Figure 1 shows a link budget consisting of cable and free space losses as well as antenna gains. Is the receiver within communication range?

(b) (2 points) Instead of the omnidirectional antenna shown in the Figure you decide to make use of your home-built antenna for reception. Assume your (c)antenna provides you with an *additional* directionality gain of 20dB. Adapt the link budget accordingly by directly drawing on the Figure. Will you be able to receive? What is the resulting link margin? I.e., how much additional losses could be tolerated?

2. Jamming

(a) (1 point) What is the burn-through range?

(b) (2 points) What is the effect of jammer transmit power, signal frequency, jammer-to-receiver distance, the transmitter-to-receiver distance on the jamming scenario?

3. Broadcast Anti-jamming

(a) (2 points) Why is DSSS not sufficient for the key-establishment in the presence of a jammer?

(b) (4 points) How does UHF prevent message insertion?

(c) (2 points) What is the difference between DSSS and UDSSS?

4. **Distance Bounding**

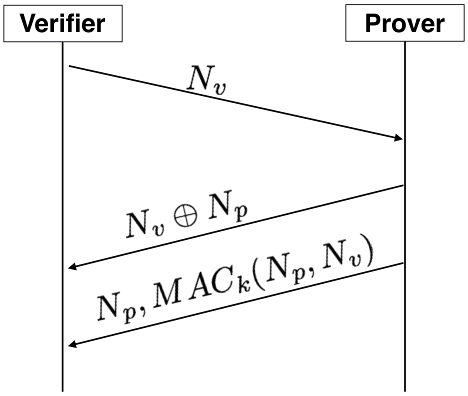
   (a) (1 point) How much distance the atttacker will advance using ED/LC attack when late commit time (E_{LC}) is 90ns, early detect time (E_{ED}) is 20 ns and hardwaere delay (E_{HW}) is 5 ns?

   (b) (1 point) How can ED/LC be prevented?

   (c) (1 point) In the distance bounding protocol, what are the restrictions on processing time (t_p)? Why?

   (d) (3 points) What is the main idea behind using Challenge Reflection with Channel Selection (CRCS) protocol?

(e) (3 points) What are the security vulnerabilities in the following distance bounding protocol?



5. **Cellular Networks**

   (a) (4 points) How will an attacker perform call interception attack on the Signalling System 7 (SS7)? List all steps.

   (b) (4 points) In the UMTS system, a mobile device is visiting a network, how will the device and network prove that they are authentic? Specify the parameters shared between the mobile device, home network and visitor network?

6. WiFi

(a) (2 points) What will the effect on the throughput of the nodes when all nodes in the network reduce backoff window size to zero?

(b) (2 points) In WPA2 protocol, what information in the handshake protocol make it vulnerable to dictionary attack? Why is this information essential to perform the dictionary attack?

7. **GNSS Security**

(a) (2 points) Assume a GPS spoofer using an omnidirectional antenna and the victim being in range. Does the fake location produced at the victim's receiver depend on the distance between spoofer and victim? Explain.

(b) (2 points) How can multiple receivers help in the prevention of GPS spoofing attacks? Assume there are two receivers. Under what conditions is an attack detected?

(c) (3 points) Why does Kuhn's scheme require loose time synchronization at the receiver? Indicate in Figure 2 the maximum time error a receiver should not exceed. Explain by referring to the elements shown in the figure.

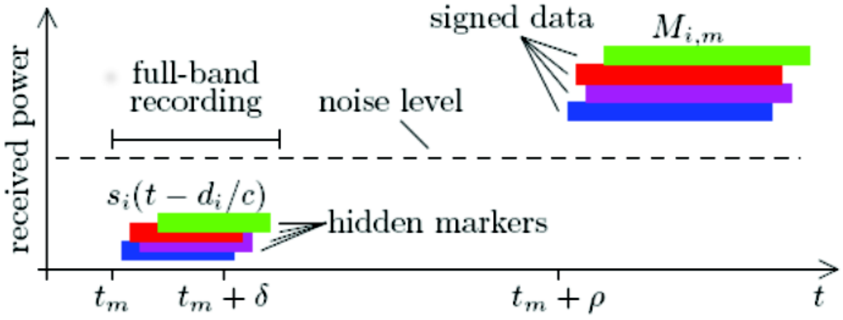


Figure 2: Kuhn's scheme.

(d) (1 point) Assume Kuhn's scheme is implemented both in GPS satellites and receivers. Is the resulting positioning system secure under any attacker?

(e) (2 points) If yes, why? If not, what attacker is not accounted for? How realistic is this threat?

8. **Broadcast authentication: TESLA**

(a) (3 points) Why does the TESLA protocol require loose time synchronization at the receiver?

(b) (2 points) Describe the operations performed at the receiver for authenticating a message in TESLA.

(c) (2 points) Which mechanism ensures that a receiver cannot predict the key used by the sender, despite the receiver being able to authenticate previous messages?

(d) (1 point) What is the advantage of TESLA over a signature-based broadcast authentication?

9. Physical-layer key establishment

(a) (1 point) Different channel properties can be used for key establishment. Assume you use off-the-shelf hardware: Which property is the easiest to use? Where does the entropy come from in that property?

(b) (2 points) Assume you want to establish keys based on channel properties in a multipath-rich environment. Which property would you use? Where does the entropy originate from?

10. Physical-layer confidentiality

(a) (2 points) In Zero Forcing, what information does the transmitter have about the legitimate and attacker receiver. How does he use this information to generate the transmission signal?

(b) (2 points) What prevents the attacker in orthogonal blinding from receiving confidential data? Is there any limitation on the position of the legitimate and attacker receiver?

(c) (2 points) Under what security assumptions, friendly jamming can achieve confidentiality? Why?

11. Integrity Codes

(a) (4 points) In Integrity Codes, how will a receiver verify the integrity of received signal?

(b) (1 point) What are the assumptions on the position of transmitter and receiver?

(c) (1 point) What are the assumptions on the capabilities of attacker?

12. Key distribution in sensor networks

(a) (2 points) Consider the key distribution scheme by Eschenauer and Gligor. Is a node guaranteed to be able to securely communicate directly with any other node? Explain.

(b) (2 points) If the answer to Question a is yes: If n the number of nodes, how many symmetric keys are required? If the answer to Question a is no: How does secure communication between two nodes work?

13. **Secure Routing Protocols**

(a) (2 points) What are the attacker's potential objectives in a route diversion attack?

(b) (2 points) What is a wormhole attack? Does the Ariadne protocol provide protection against this? Explain.

14. Multiple Choice

In this part, for each question, circle the correct answers. Each correct answer gives 1 point, a wrong answer gives −1 points and not providing an answer gives 0 points. The whole section gives at least 0 points.

(a) (1 point) Mark the correct statements.

A. Friendly jamming does not require a pre-shared secret.

B. Orthogonal blinding relies on channel knowledge for authentication.

C. Friendly jamming relies on jammer and legitimate transmitter being close such that both entities have a similar channel relative to an attacker.

D. Beamforming requires channel knowledge.

(b) (1 point) Mark the correct statements.

A. Kuhn's scheme allows to secure broadcast-based positioning systems against any known attacker.

B. Verifiable multilateration is based on the notion that an attacker cannot reduce the measured distance.

(c) (1 point) Integrity Codes are used for

A. Broadcast authentication with a pre-shared secret key.

B. Broadcast authentication with no any pre-shared secret key.

C. Confidentiality with a pre-shared secret key.

D. Confidentiality with no any pre-shared secret key.

(d) (1 point) In a spread-spectrum system – if a 1 kHz signal is spread to 100 kHz, the processing gain is

A. 10 dB

B. 20 dB

C. 30 dB

D. 50 dB