i

Exam information

UiO : Department of Informatics
University of Oslo

Digital home exam in IN3210/IN4210 *Network and Communications Security* (Autumn 2020)

Date and time: **30. November 2020, 10:00AM - 12:00PM (2 hours)**

Permitted materials: **All (e.g. lecture notes, books, online material)**

It is not allowed to collaborate or communicate with others during the exam!

In addition, the general regulations of the MN faculty for exams in autumn 2020 apply.
Note that after the home exam you can be randomly selected for a control interview.
The purpose of such a control interview is to give the teacher an opportunity to check whether it is actually you who has written the home exam. The control interview will not affect the grade you have received. However, if (after the interview) the teacher suspects that you have not written the assignment yourself, the department can issue a suspicion-of-cheating case.

Please regard the following directions on the exam:

- Answers can be given in English or Norwegian.
- Each task states the maximum possible points in the title, e.g. (10 P) means maximum 10 points.
- The exam has a total of 100 points
- For multiple choice questions you get 1 point for correct answers, -1 for incorrect answers, 0 points for no answer**.** However, the overall score for a question is always at least 0 points (even if the sum over all answers is negative).
- Be concise and precise when answering the free text questions.
- If you have questions on exam tasks, you can contact the lectures: Lecture's round
- If you have technical problems with Inspera, you can contact the Student support for home exams

1

Axioms of Information Security (8 P)

Pick one of the three "CIA" axioms of information security and pick an example from your daily (digital) life where this security goal is important. Explain why it is important, how it is secured and what might happen, if the security goal would be violated.

Fill in your answer here

- Scenario (2 P): e.g. online banking
- Security goal (2 P): e.g. integrity on transactions
- Security measure (2 P): e.g. TLS (includes integrity protection)
- Violation (2 P): e.g. attacker can modify a transaction and transfer money to his own account

Maximum marks: 8

2 Man-in-the-middle Attacks (15 P)

An important type of attacks are *man-in-the-middle attacks*. It requires that the communication between the client and the server is going through a device controlled by the attacker. How can an attacker come into this communication path?

Fill in your answer here

Name and short explanation (3 P): e.g. redirection, DNS poisoning, etc.

Select from the security protocols/mechanisms presented in the course one that is *vulnerable to* ***active*** *man-in-the-middle attacks*. Name it and explain how the attack works. Is the protocol/mechanism also vulnerable to a ***passive*** *man-in-the-middle* attack?

Fill in your answer here

(7 P): Name (e.g. DH), explanation, passive MITM?

Select from the security protocols/mechanisms presented in the course a protocol that is ***not*** *vulnerable to* ***active*** *man-in-the-middle attacks*. Name it and explain why the attack is not possible.

Fill in your answer here

(5 P): Name (e.g. TLS), explanation

Maximum marks: 15

3 Communication security (6 P)

You are to secure a networked system, deployed at two geographically separate sites. This is an old legacy system that must be kept operational for some more years. You discover that the communication between the two sites is performed in plaintext, even sensitive information is being exchanged. How would you propose to mitigate this security vulnerability? Justify your answer.

Fill in your answer here

(3 P): Name (e.g. IPSec, Wireguard)
(3 P): explanation

Maximum marks: 6

4 Encryption (11 P)

Some colleagues of you are implementing encryption using a block cipher and asks you about what mode of operation to use. What would you advise and why?

Fill in your answer here

Name (2 P): e.g. GCM; explanation (3 P): e.g. GCM not vulnerable to attacks against CBC, includes also authentication

The same colleagues wonder how to create a key management for this system. The users are all internal users within the company. What options for key management are there? Present 2 different possibilities incl. their advantages/drawbacks.

Fill in your answer here

(6 P): Kerberos + PKI; advantages / disadvantages

Maximum marks: 11

5 Digital Signature (6 P)

You are sending a digitally signed message to a friend. She is calling you later and says "I am sorry, I am unable to verify your signature." What might be the problem? Or what might have gone wrong? Give 2 possible reasons!

Fill in your answer here

e.g. message was modified, signature was modified, public key not available, wrong public key available

Maximum marks: 6

6 Attack Detection (6 P)

What method(s) is/are most suitable for detecting *unknown* attacks? Why is this difficult?

Fill in your answer here

(2 P): Anomaly-based detection
(4 P): explanation (e.g. false positives/negatives; attacks on machine learning)

Maximum marks: 6

7 Wireless network security (6 P)

What are the most important choices if you are to secure a wireless network using WPA2, and what would be the deciding factor(s)?

Fill in your answer here

WPA2-Personal/PSK vs. WPA2-Enterprise; number of users; scenario (café, cooperate network); strong network password to mitigate offline dictionary/brute-force attacks etc.

Maximum marks: 6

8 BGP (6 P)

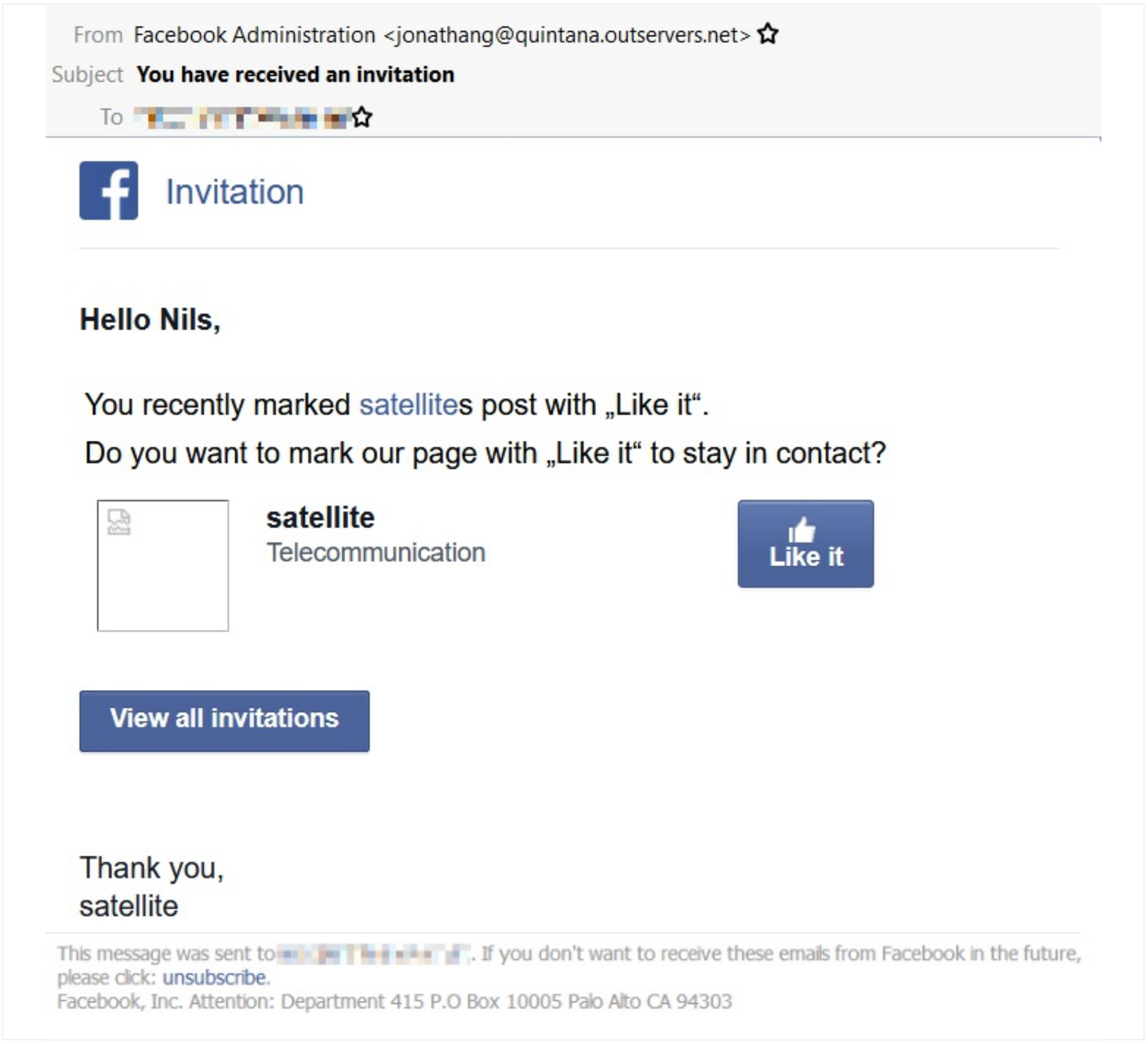
What would you say are the two most serious security vulnerabilities of BGP, and how can they be mitigated?

Fill in your answer here

Prefix hijacking - mitigated using RPKI
Manipulation of the AS path in BGP update messages - mitigated by BGPsec

Maximum marks: 6

9 Phishing (10 P)



Look at the email shown in the figure. You have the suspicion that it is a phishing email. What caught your suspicion? (Ignore the two blurred bars; assume your own email address is shown there.)

Fill in your answer here

(2 P): wrong email domain

What information (not visible in the picture) should you check next?

Fill in your answer here

(3 P): URLs the buttons are referencing to. It is the right domain? Must check careful wrong domain might we disguised (e.g. www.bank.com.evil.net)

It seems, that the image was not loaded by the email program. You click the button "show external images" to see the whole email. Is this a good idea? Why?

Fill in your answer here

(5 P): image might be a “tracking image”, i.e. every email contains a unique URL for the image (e.g. A7jwi123Jsd.png).
When loading the image, the request is logged at the server and the phisher can see which specific email was viewed and that the email address is valid

Maximum marks: 10

10 Email Security (12 P)

Pick one email you have received on your UiO email account from an address outside UiO and look at the source code of this email.

(You can for example go to https://mail.uio.no/, log in, select an email, click on "..." next to "-> FORWARD" and select "View message detail".)

Look for elements in this source that give a hint on the usage of email security measures. Select two of these, copy them into the fields below and give explanations on their function. (If the copied lines include personal information, like an email address, please replace this information with "XXX".)

First element:

From email source:

e.g. SPF, DKIM, TLS transport between email servers, SPAM detection

Explanation:

Second element:

From Email Source:

Explanation:

Maximum marks: 12

11 TOR (2 P)

Mark the statements on TOR that are true.

Select one or more alternatives:

- If the client accesses a Web server trough the TOR nework, the client's ISP knows the IP address of the server.
- If the client accesses a Web server trough the TOR nework, the client's ISP knows the IP address of the client. ✔
- TOR can not hide the identity of a service.
- The main security goal of TOR is anonymity of the client. ✔

Maximum marks: 2

12 Darknet (2 P)

Mark the statements on the Darknet that are true.
Select one or more alternatives:

- [ ] The darknet is used to mine Bitcoins.
- [ ] The darknet offers illegal as well as legal services. ✔
- [ ] Access to the darknet is done via cryptographic protocols. ✔
- [ ] The darknet is only accessible via TOR.

Maximum marks: 2

13 Ransomware (2 P)

Mark the statements on Ransomware that are true.
Select one or more alternatives:

- [ ] Modern ransomware uses a combination of symmetric and asymmetric encryption. ✔
- [ ] Infection can happen via USB keys. ✔
- [ ] Infection is prevented by keeping the OS up-to-date.
- [ ] Infection is stopped by IDS systems.

Maximum marks: 2

14 NFC/RFID (2 P)

Mark the statements on NFC/RFID that are true.
Select one or more alternatives:

- [ ] RFID tags require a battery
- [ ] RFID can be used to track items and are therefore a privacy risk. ✔
- [ ] NFC communication only works with certified payment terminals.
- [ ] NFC payments are vulnerable to relay attacks. ✔

Maximum marks: 2

15 5G (2 P)

Mark the statements on 5G that are true.
Select one or more alternatives:

- [ ] 5G uses up-to-date encryption schemes. ✔
- [ ] 5G needs a infrastructure separate from 4G
- [ ] Higher frequencies lead to higher data rates but shorter ranges ✔
- [ ] The main benefit for IoT communication will be the high data rates (up to 10 GB/s)

Maximum marks: 2

16 Side-channel attacks (2 P)

Mark the statements on side-channel attacks (SCA) that are true.
Select one or more alternatives:

- [ ] SCAs only work on IoT devices.
- [ ] A typical goal of SCAs is the extraction of a secret key. ✔
- [ ] The chosen algorithm has no influence on the SCA vulnerability.
- [ ] Different CPU instructions have different power consumption. ✔

Maximum marks: 2

17 QUIC (2 P)

Mark the statements on QUIC that are true.
Select one or more alternatives:

- [ ] By sending 2 streams the throughput is increased by the factor 2.
- [ ] QUIC ensures packet authenticity. ✔
- [ ] QUIC can be one RTTs faster than (the fastest mode of) TLS 1.3. ✔
- [ ] One feature of QUIC that TLS does not offer is perfect forward secrecy.

Maximum marks: 2

18 Web Application Security (2 P)

Mark the statements regarding Web Application Security that are true.
Select one or more alternatives:

- [x] The code for an XSS attack can be stored in a user review for a Web Shop's product.
- [x] With SQL injection reading, modifying and deleting of data base entries is possible (assuming a vulnerable Web application).
- [ ] In CSRF attacks malicious JavaScript code is injected.
- [ ] A countermeasure against SQL injection is client side (i.e. inside the browser) input validation.

Maximum marks: 2

19 VPN (2 P)

Mark the statements that are true.
Select one or more alternatives:

- [ ] A typical application for VPN is online banking.
- [x] Wireguard detects lost IP packets.
- [ ] WireGuard includes a public key exchange mechanism.
- [x] A VPN ensures less anonymity than TOR.

Maximum marks: 2

20 Denial-of-Service (2 P)

Mark the statements on Denial-of-service (DoS) or Distributed DoS (DDoS) attacks that are true.
Select one or more alternatives:

- [x] DDoS attacks can be executed using an IoT botnet.
- [ ] DoS attacks use an huge number of network packets to overwhelm the victim.
- [x] In UDP-based attacks the source IP address can be spoofed.
- [ ] TLS offers protection from SYN-flooding attacks.

Maximum marks: 2

21 MITRE ATT@CK (2 P)

Mark the statements about MITRE ATT@CK that are true.
Select one or more alternatives:

- MITRE ATT@CK is based on real-world observations ✔
- MITRE ATT@CK is a tool for attackers
- MITRE ATT@CK is a knowledge base of adversary tactics and techniques ✔
- MITRE ATT@CK is a theoretic framework

Maximum marks: 2

22 Vulnerability Scanning (2 P)

Mark the statements about vulnerability scanning that are true.
Select one or more alternatives:

- Typical vulnerability scanning tools are effective in identifying known vulnerabilities ✔
- Vulnerability scanning will typically be able to identify most unknown vulnerabilities
- Vulnerability scanning can be performed as an authenticated or unauthenticated entity ✔
- Vulnerability scanning is a fully automated process

Maximum marks: 2

23 AI Cyber Defense (2 P)

Mark the statements about autonomous (AI) cyber defense that are true.
Select one or more alternatives:

- Solutions for autonomous cyber defense will result in less available jobs in the coming years
- Machine learning may be utilized for network anomaly detection ✔
- Machine learning models trained on sensitive data may pose a risk to the confidentiality of the training data ✔
- Machine learning is synonymous with artificial intelligence

Maximum marks: 2