Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Institut für
Technische Informatik und
Kommunikationsnetze

Department ITET
Lecture HS 2013
Lecturer: Prof. B. Plattner, Dr. T. Dübendorfer, Dr. S. Frei, Dr. S. Neuhaus, Prof. A. Perrig
Coordinator: Mahdi Asadpour

# Exam

# Network Security

Tue. 21. Jan. 2014, 09:00 – 10:30, HIL G61

General Remarks:

- ▷ Put your **legitimation card** on your desk.
- ▷ Write your **name** and your **ETH student number** on this front page.
- ▷ Check if you have received **all task sheets** (Pages **1 - 18**).
- ▷ **Read** each task completely before you start solving it.
- ▷ Please answer either in **English or German**.
- ▷ **Cancel** invalid parts of your solutions **clearly**.
- ▷ If extra space is needed, ...
  - Use a **new sheet of paper** for **each task**.
  - Write your **name** and the exam **task number** in the **upper right corner** on **each** extra sheet of paper that contains your solutions.
- ▷ At the end of the exam, hand your **solutions in together with all tasks**.
- ▷ Do **not separate** the **task sheets**.
- ▷ **For the best mark, it is not required to score all points.**

Special aids:

- ▷ A summary of the course content of six A4 pages (3 sheets) maximum is allowed.
- ▷ The use of a scientific calculator is allowed.
- ▷ Use of electronic communication tools (mobile phone, computer etc.) is strictly forbidden.

Family name: ..... Student legi nr.: .....

First name: ..... Signature: .....

Do not write in the table below (use by correctors only):

| Task | Points | Sig. | Task | Points | Sig. |
|---|---|---|---|---|---|
| 1 | /5 | | 9 | /6 | |
| 2 | /5 | | 10 | /7 | |
| 3 | /6 | | 11 | /6 | |
| 4 | /6 | | 12 | /5 | |
| 5 | /6 | | 13 | /6 | |
| 6 | /8 | | 14 | /4 | |
| 7 | /6 | | 15 | /8 | |
| 8 | /6 | | | | |
| $\Sigma$ | /48 | | $\Sigma$ | /42 | |
| $\Sigma_{ALL}$ | /90 | | | | |

**Task 1: Insecurity, Risk, Vulnerability Lifecycle** **5 Points**

**a) Security Goals** **(1 Point)**

*ETHMail* provides webmail services to its customers. State which security goal is preserved in each of the following scenarios (1 point if all answers are correct).

**(i)** *ETHMail* site is able to ensure that sent email has not been tampered with.

---

**(ii)** *ETHMail* is able to ensure that its customers cannot deny their online actions.

---

**(iii)** *ETHMail* site continues to provide its services to its customers.

---

**(iv)** *ETHMail* is able to validate the identity of the senders.

---

**b) Security Properties** **(4 Points)**

**(i)** *SecureMail* wants emails sent between two parties to be **authenticated** and **protected** from modifications while in transit. Consider that Stephan sends an email message M to Roger. Taking into account *SecureMail*'s security guarantees, which of the following options is a secure way to protect the email message M? Add a tick to the correct answer(s) (2 points per question if only the correct answer(s) are selected).

☐ Stephan's email client should encrypt M using Roger's public key. Therefore, Stephan sends $[E_{K_R}(M)]$ to Roger, where $E_{K_R}(M)$ denotes the encryption of message M with public key $E_{K_R}$.

☐ Stephan's email client sends M and a digital signature on M using Stephan's private key. Therefore, Stephan sends $[M, Sign_{S_{K_S^{-1}}}(M)]$, where $Sign_{S_{K_S^{-1}}}(M)$ denotes the encryption of message M with private key $K_S^{-1}$.

☐ Stephan's email client generates a new symmetric key s, sends an encryption of s using Roger's public key, and an encryption of M under s using the $RC_4$ stream cipher. Therefore, Stephan sends $[E_{K_R}(s), M \oplus RC_4(s)]$

**(ii)** Consider that Stephan wants to send a confidential message to Roger. $K_R$ is Roger's public key and $K_S^{-1}$ is Stephan's private key used for signing. Which of the following option would you consider best for protecting confidential emails?

☐ Send $[E_{K_R}(M), Sign_{S_{K_S^{-1}}}(K_R)]$

☐ Send $[E_{K_R}(M), Sign_{S_{K_S^{-1}}}(M)]$

☐ Send $[E_{K_R}(M), Sign_{S_{K_S^{-1}}}(\text{SHA-2}(M))]$, where SHA-2 is a hash function.

**Task 2: Availability and DoS** **5 Points**

**a) Redundant Array of Inexpensive Disks (RAID)** **(2 Points)**

For increased availability, you are equipping a storage system with two drives that both contain the same data (mirrored storage). If one disk fails, the data is still available from the other disk. Each of your disks has an individual failure rate of 0.05 per month.

**(i)** Assuming that you followed all best practices while buying the disks, what is the probability that both disks fail within one month?

**(ii)** Now assume that both disks come from the same manufacturer and batch and were produced one after the other on the same assembly line. This will obviously not affect the disks' individual failure rate, but does this affect the combined failure rate? Explain your answer.

**b) SYN Cookies** **(2 Points)**

**(i)** What is the goal of SYN cookies?

**(ii)** Against what type of attack they are being used?

**c) Amplification Attack** **(1 Point)**

A system operates an insecure authentication system as follows. The client $C$ takes a user name and password and asks the server $S$ in plaintext to authenticate that user. The server replies with a simple fixed length yes-or-no message:

$$C \to S : (\text{username}, \text{password})$$
$$S \to C : (\text{username}, \text{result})$$

Usernames and passwords are 16 byte fields, the result is 1 byte. An attacker now sends messages as $C$, spoofing $C$'s IP address. Can this protocol successfully be used in an amplification attack? Explain your answer.

**Task 3: Secure Channels: Principles, VPN, SSH** **6 Points**

**a) Secure Channels** **(2.5 Points)**

Add checkmarks (✓) on the following table, to denote at which OSI layer(s) each one of the respective secure channels operates.

| | TLS | Skype | OpenVPN | IPSec | PGP |
|---|---|---|---|---|---|
| Data Link | | | | | |
| Network | | | | | |
| Transport | | | | | |
| Application | | | | | |

**b) SSH Protocol Architecture** **(1 Points)**

List the names of the 3 protocols which are the main building blocks of SSH.

---

**c) Attacks against SSH** **(2.5 Points)**

Assume that a client and a web server communicate using the SSH protocol. Against which attacks can SSH successfully defend if properly used? Tick true if SSH is successfully being used to defend the communication against potential attackers. (Each correct answer gives 0.5 points. For each false answer 0.5 points are subtracted. No answer gives zero points. This subtask gives at least zero points.)

true ☐ false ☐ TCP RST attack against the web server.

true ☐ false ☐ Traffic analysis attacks to determine the communicating hosts.

true ☐ false ☐ Brute-force password cracking.

true ☐ false ☐ Eavesdropping the communication by performing a man-in-the-middle attack.

true ☐ false ☐ IP spoofing, where a remote host sends out packets which pretend to come from a trusted host.

**Task 4: Firewalls, IDS and NAT Traversal** **6 Points**

**a) NAT Traversal** **(4 Points)**

Two computers $A$ and $B$ are each separately connected to the Internet behind a NAT. They do not share the same local network.

**(i)** Sketch the two-step process by which $A$ and $B$ can punch holes in their respective NAT devices so that afterwards, $A$ and $B$ can exchange UDP packets. Assume that $A$ knows $B$'s public session endpoint and vice versa. (3.5 Points)

**(ii)** Explain in one sentence why your sketch works. (0.5 Points)

**b) IDS** **(2 Points)**

An IDS sees $10^7$ flows (sets of related packets) a day. Let the probability of any flow being malicious be $10^{-6}$; let the probability that a malicious flow raises an alarm be 1 (in other words, all malicious flows raise an alarm); and let the probability for a legitimate flow to raise an alarm be $10^{-5}$. (IDS vendors dream of accuracies like this.)

**(i)** How many malicious flows are there per day, on average?

**(ii)** How many false alarms will be generated per day, on average?

**(iii)** How many alarms will be generated in total per day, on average?

**(iv)** What is therefore the probability of an alarm being false?

**Task 5: Session State, SQL Injection** **6 Points**

**a) Session State** **(3 Points)**

Batman is looking for a new black cape online. He logs into three different websites at the same time: forum.superhero-fashion.com, www.he-buy.com and www.batbank.com. Penguin hacks Batman's computer and gains access to the URLs of the websites currently open in his browser.

**(i)** Assume Penguin can hijack Batman's session in forum.superhero-fashion.com. Can you explain how?

**(ii)** Assume Joker has a better luck and in addition to the URLs he can also read the content of the cookies stored by browser. Joker hijacked Batman's session in www.he-buy.com but Penguin couldn't. Can you explain how Joker did it and why Penguin couldn't?

**(iii)** Joker couldn't hijack Batman's session in www.batbank.com (although it was not expired yet). Mention at least one possible reason for that.

**b) SQL Injection** **(3 Points)**

**(i)** Can a secure connection such as SSL or VPN prevent SQL injection attacks? Explain.

**(ii)** Why should a website avoid disclosing detailed database error information to the client?

**(iii)** Why is using a whitelist of allowed characters is a better practice than using a blacklist of forbidden characters to sanitize input?

**Task 6: TLS** **8 Points**

**a) Dumbing Down Attack** **(1 Point)**

Explain the idea of a dumbing down attack on TLS.

**b) MD5 Collision Vulnerability** **(1 Point)**

Assume that an attacker can create 2 certificates C1 and C2 which both have the same MD5 hash: MD5(C1) = MD5(C2)
How could an attacker benefit from such a fact in attacking TLS connections?

**c) Intelligence Agency - Targeted Attack** **(2 Points)**

Assume an intelligence agency can legally force a certificate authority to cooperate. How would the agency mount an undetectable man in the middle attack on the targets communication with a specific TLS server using the CA's help?

**d) A New TLS Variant** **(4 Points)**

Assume a TLS variant with the following properties:

- User enters credentials (username/password) in browser
- User authentication is done with preshared password during protocol handshake
- Client Hello message contains username
- Server uses username to look up password
- Subsequent handshake messages are protected using the password

There are two proposed authentication methods below, in which $J$ =H( password ), where H is a secure cryptographic hash function. The two protocol steps for each proposed method below indicate phases 2 and 3 of the TLS key handshake protocol. Please justify if the method is safe from an eavesdropping attacker and explain your answer.

Hint: think whether a passive attacker can brute force the password after observing a connection setup.

**(i)** Anonymous Diffie-Hellman key exchange method is used. $MAC_J(x)$ indicates computation of a secure message authentication code on input x using key J.

$S \rightarrow C: \quad g^s \ mod \ p, MAC_J(\ g^s \ mod \ p)$
$C \rightarrow S: \quad g^c \ mod \ p, MAC_J(\ g^c \ mod \ p)$

(2 Points)

**(ii)** Anonymous Diffie-Hellman key exchange method is used. The Diffie-Hellman public key is encrypted by 128-bit AES and $J$ is used as the encryption key, thus:

$S \rightarrow C: \quad \{g^s \ mod \ p\}_J$
$C \rightarrow S: \quad \{g^c \ mod \ p\}_J$

(2 Points)

**Task 7: Malware** **6 Points**

**a) SIS Model** **(1 Point)**

What are the stages of the worm spreading in the SIS model?

1. _____

2. _____

3. _____

**b) Worm Propagation** **(1 Point)**

List three factors affecting the worm propagation speed.

1. _____

2. _____

3. _____

**c) Worm Detection** **(1 Point)**

Give two examples of network measurements which could indicate worm outbreak. For each of them, explain why the worm operation would result in abnormal measurements.

1. _____

2. _____

**d) Social Engineering** **(1 Point)**

An attacker wants to infect a target network that has no internet connectivity. Give an example of an attack that involves social engineering and gives the attacker at least a good chance to infect a machine in the target network. In this attack, the attacker must not physically enter the site.

_____

_____

_____

**e) Trojan** **(1 Point)**

Define the malware type "Trojan" and give one example.

_____

_____

_____

**f) Anti Virus Software** **(1 Point)**

Where can anti virus software be deployed? For each deployment location indicate what information the anti virus software uses for its analysis.

**Task 8: DNS Security** **6 Points**

**a) Stub Resolver** **(1 Point)**

Explain the role of a stub resolver.

**b) DNS Account Takeover** **(2 Points)**

Most domain accounts are managed through Web interfaces provided by Registrars or Resellers.
How can an attacker take over such an account (give 1 answer)?

What can an attacker do once she has control over an account (give 2 answers)?

How could such an attack be mitigated (give 1 answer)?

**c) DNS Server Takeover** **(2 Points)**

The computers in your home network get their network configuration from a small router. An exploit that gives complete control over the DNS software (but nothing else) in the router becomes available. How could an attacker use such an exploit against your computers?

What could you do to mitigate the effects of the attack on your computers until a patch becomes available (while maintaining internet connectivity for your computers)?

**d) DNSSEC Glue Records** **(1 Point)**

DNS needs "glue records" between authoritative name servers from upper to lower levels to make sure that queries can successfully be resolved. The higher level name server must know the name and IP address for every lower level domain that is made available by another name server, so that a resolver can work its way down the DNS tree over multiple servers. What is required in this regard if DNSSEC is deployed?

**Task 9: Malware Development and Demo, Botnets** **6 Points**

**a) Malware Development** **(2 Points)**

Briefly explain the following objectives in malware development to best utilize infected machines: (1) persistence, (2) modularity, (3) scalability, (4) anonymity.

Persistence: _____

Modularity: _____

Scalability: _____

Anonymity: _____

**b) Botnets** **(3 Points)**

Check whether the following statements are true or not. Each correct answer gives half a point. For each false answer half a point is subtracted. No answer gives zero points. This subtask gives at least zero points.

| true | false | |
|---|---|---|
| ☐ | ☐ | Being a single point of failure is one of the main disadvantages of a single centralized CnC (Command and Control) resource to communicate to all bot agents. |
| ☐ | ☐ | Low speed of control is one of the main disadvantages of a single centralized CnC. |
| ☐ | ☐ | Geographical optimization is an advantage of a multi-server CnC topology. |
| ☐ | ☐ | High degree of command latency is a disadvantage of a hierarchical CnC topology. |
| ☐ | ☐ | Botnet enumeration is a disadvantage of a random CnC topology. |
| ☐ | ☐ | Random CnC topology is not very resilient to shutdown. |

**c) IP Flux** **(1 Point)**

How does IP Flux help botnets?

_____

_____

**Task 10: Cross Site Scripting (XSS)** **7 Points**

**a) XSS through Embedded HTML Content** **(7 Points)**

friendly.com is a social network website with the following properties:

- A user cannot know who visited his profile.
- When a user logs in, his username is displayed for him at the corner of the page.
- The logout button leads to friendly.com/logout which logs the user out.

Eve, a malicious curious user, discovered that in the *about me* section she can include HTML content to be viewed by the users visiting her profile.

**(i)** How can Eve discover the usernames of the users visiting her profile? **(1.5 Points)**

**(ii)** Eve's mom likes to send Eve annoying messages every day. She browses to Eve's profile page, and there she clicks on *send message* at the top of the page (not part of the *about me* section). Lately, every time the browser tries to load the *send message* to Eve, Mom discovers that she was logged out of the system. Can you explain how Eve managed to do that? **(2 Points)**

**(iii)** lessfriendly.com is a social network website, HTML content is not allowed. When a user edits his *about me* page and presses the *update* button, a client-side script checks the text before sending it to the server. If the script detects HTML content, it will show an error message instead of sending the content to the server.

1. How can Eve still include HTML content in her profile? **(2 Points)**

2. How can the adminstrators of lessfriendly.com prevent that? **(1.5 Points)**

**Task 11: Security Ecosystem, Evasion Modeling, Detections Failures and Endpoint Security** **6 Points**

**a) Zero-day Vulnerabilities** **(2 Points)**

A recent report (Sept. 13) claims that the NSA (the American National Security Agency) purchased data on zero-day vulnerabilities from a security company called VUPEN.

Please state two ways (one offensive and one defensive) in which the NSA can use zero-day vulnerabilities. (Assume that *disclosure to the vendors* is not one of them).

1. _____

2. _____

**b) Full Disclosure Debate** **(2 Points)**

What are the main arguments of the proponents of the *Full Disclosure* and *Bug Secrecy* stance in handling vulnerability information?

Full Disclosure: _____

_____

Bug Secrecy: _____

_____

**c) Security Information Provider** **(2 Points)**

**(i)** What are the three main tasks that Security Information Providers execute in order to provide the public and customers with information about vulnerabilities?

**(1.5 Points)**

1. _____

2. _____

3. _____

**(ii)** Within the security ecosystem, what is the role of security information providers?

**(0.5 Points)**

_____

_____

**Task 12: Email Spam** **5 Points**

**a) Greylisting and Token-Based Whitelisting** **(2 Points)**

Why do some email administrators prefer not to use greylisting? List two reasons.

1. _____

2. _____

How does token-based whitelisting differ from greylisting?

_____

_____

List an unwanted side-effect introduced by token-based whitelisting.

_____

_____

**b) DNS Blacklists** **(1 Point)**

The blacklist operator Spamhaus offers the DNS blacklist *ipblacklist.spamhaus.org*. You would like to know whether the IP address 82.130.120.1 that you are using is blacklisted. How would you perform the respective lookup?

_____

_____

**c) Email Authentication** **(2 Points)**

Check whether the following statements are true or not. Each correct answer gives half a point. For each false answer half a point is subtracted. No answer gives zero points. This subtask gives at least zero points.

| true | false | |
|---|---|---|
| ☐ | ☐ | PGP and S/MIME both have the ability to: encrypt the email message and authenticate the sender. |
| ☐ | ☐ | In PGP each participant is allowed to have only one key. |
| ☐ | ☐ | DKIM uses the same certificate format (X.509) as S/MIME. |
| ☐ | ☐ | In the DKIM architecture only a single original mail server is allowed to sign outgoing messages. |

**Task 13: Identity and Authentication** **6 Points**

**a) Privacy and Anonymity** **(3 Points)**

Briefly describe the Onion Routing and Mixnets anonymity methods and also state which is the major advantage when using Mixnets instead of Onion Routing.

Onion Routing: _____

_____

Mixnets: _____

_____

Mixnets advantage: _____

_____

Check whether the following statements are true or not. Each correct answer gives half a point. For each false answer half a point is subtracted. No answer gives zero points. This subtask gives at least zero points.

| true | false | |
|---|---|---|
| ☐ | ☐ | Onion-routing schemes like the Tor anonymity network use a distinct cryptographic key for each hop that a given message takes through the network. |
| ☐ | ☐ | Tor can prevent end-to-end timing attacks |
| ☐ | ☐ | When using a system like Tor, to ensure privacy the DNS traffic must be routed through the system even if the client always uses DNSSEC for its DNS lookups. |

**b) Authentication** **(2 Points)**

Explain the difference between weak and strong authentication. Give an example for each.

Weak: _____

_____

Strong: _____

_____

**c) Anonymization** **(1 Point)**

What type of pseudonymity does each of the following services offer to its typical users? Explain your choice. If you are not familiar with the nature of the service, please state the assumptions that you make in your answer.

Facebook: _____

_____

Online auction websites (ebay.com, ricardo.ch etc.): _____

_____

**Task 14: Case Study: "Secure Online Ticket Shop", Guest Talks** **4 Points**

**a) Advanced Persistent Threat (APT)** **(1 Point)**

In what timeframe (from infection to detection) do APTs evolve?

You detect APT traffic in your network. Should you immediately block it with your firewall?

**b) Attacks and Defenses in Wireless Networks** **(1 Point)**

Give two basic properties that would be expected of a wireless firewall (e.g. WiFire).

**c) Malware today - Investigation Techniques** **(1 Point)**

Briefly explain the investigation technique blackboxing.

What is the dilemma for an attacker if an online file reputation mechanism is in place?

**d) Case Study - Secure Online Ticket Shop** **(1 Point)**

The security of the server should be increased. As the private key of the SSL server is a critical security element, it is removed from the server and now stored on a CDROM in a safe.

**(i)** Does this increase the security of the system (explain briefly)?

**(ii)** Does it have any side effects on the operation of the secure online ticket shop (explain briefly)?

**Task 15: Lab** **8 Points**

**a) Iptables** **(2 Points)**

What does this `iptables` rule/command do? Explain briefly, in particular, which packets are examined by the "FORWARD" part of this command.

```
iptables -A FORWARD -d 192.168.0.1 -p tcp --dport 23 -j DROP
```

**b) Nmap Tool** **(2 Points)**

Describe briefly two methods `nmap` tool uses to determine whether a scan target is online.

1.

2.

**c) Scapy Tool** **(1 Point)**

What is the `scapy` tool used for? Briefly explain its mechanism.

**d) IPSec Tools** **(1 Point)**

What are the usage cases of the tools `racoon` and `setkey` in IPSec?

**e) SSH Applications** **(2 Points)**

Explain briefly "Proxy Forwarding" and "X Forwarding" applications of SSH.