ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Institut für
Technische Informatik und
Kommunikationsnetze

Department ITET — Lecturer: Prof. B. Plattner, Dr. T. Dübendorfer, Dr. S. Frei, Prof. A. Perrig
Lecture HS 2014 — Coordinator: Mahdi Asadpour

Exam

Network Security

Sat. 24. Jan. 2015, 09:00 – 10:30, HG E 5&7

General Remarks:

- ▷ Put your **student/identity 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 - 16**).
- ▷ **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	/6		8	/6	
2	/5		9	/8	
3	/6		10	/7	
4	/6		11	/6	
5	/7		12	/5	
6	/8		13	/6	
7	/6		14	/8	
Σ	/44		Σ	/46	
Σ_{ALL}	/90				

Task 1: Introduction/Insecurity, Risk, and Vulnerability Lifecycle 6 Points

a) Security Goals (2 Points)

The following four statements are about the security goals we covered in class. Tick true or false for each. (Each correct answer gives 0.5 points. For each incorrect answer 0.5 points are subtracted. No answer gives zero points. This subtask gives at least zero points.)

true □ false □ Encrypting a message provides authenticity.

true □ false □ Signing a message provides confidentiality.

true □ false □ A site that continually provides its services has integrity.

true □ false □ A site ensuring that customers cannot deny their online actions provides reputation.

b) Vulnerability Lifecycle (2 Points)

Fill in each blank with one of the following terms: creation, disclosure, discovery, exploit, patch available, patch installed.

(i) Pre-disclosure risk is the time between ________________________ and ________________________. (1 Point)

(ii) Post-disclosure risk is the time between ________________________ and ________________________. (1 Point)

c) Risk Management (2 Points)

Suppose you run a flower shop. Like any other business owner, you face security risks from thieves, vandals, etc.

(i) Give an example of an action you could take to **avoid** your risk. (1 Point)

____

(ii) Give an example of an action you could take to **transfer** your risk. (1 Point)

____

Task 2: Availability and DoS 5 Points

a) Availability (2 Points)

You are planning a high availability cloud service data center. Your server supplier offers you a 99.99% availability for the overall server infrastructure. The network supplier offers you a networking infrastructure with 99.999% availability. Can you offer your clients a SLA with 99.99% availability for your cloud service? (Explain your answer)

b) Denial of Service (3 Points)

(i) A compression bomb is a tool that can be utilized in what kind of DoS attack? (1 Point)

(ii) Give one advantage and one disadvantage of **network** level DoS attacks from the point of view of the attacker. (1 Point)

(iii) Give one advantage and one disadvantage of **service** level DoS attacks from the point of view of the attacker. (1 Point)

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

a) Secure Channels (2 Points)

Alice sits down in a coffee shop, gets a WPA password for the WiFi connection from the barista, and connects her laptop to her corporate VPN (using tunnel-mode IPsec) to check her email. While she is downloading her messages, Bob notices she is online, and calls her via Skype.

(i) How many times is the content of the Skype call encrypted (as seen from the viewpoint of Eve, who is sitting in the coffee shop with Alice), and at which layers? (1 Point)

(ii) Name one advantage and one disadvantage of this arrangement. (1 Point)

b) Attacks Against SSH (2 Points)

List two strategies to increase SSH's resistance to password cracking attacks.

c) VPNs (2 Points)

Tick true for each guarantee provided by the use of HMAC in a VPN, and false for those not provided by HMAC. (Each correct answer gives 0.5 points. For each incorrect answer 0.5 points are subtracted. No answer gives zero points. This subtask gives at least zero points.)

true	false	
□	□	Confidentiality
□	□	Authenticity
□	□	Integrity
□	□	Geolocation

Task 4: Firewalls, IDS and NAT Traversal 6 Points

a) NAT (1 Point)

Does segregating machines used mainly for Web browsing onto an RFC 1918 network address (private-use, e.g. 10.0.0.0/8) using NAPT effectively prevent attacks against the browser? Briefly explain your answer.

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? (0.5 Points)

(ii) How many false alarms will be generated per day, on average? (0.5 Points)

(iii) How many alarms will be generated in total per day, on average? (0.5 Points)

(iv) What is therefore the probability of an alarm being false? (0.5 Points)

c) Firewalls (3 Points)

A Linux server with a single interface `eth0` has the following iptables rules:

```
1:  -A INPUT -i lo -j ACCEPT
2:  -A INPUT -i eth0 -p tcp -s 129.132.0.0/16 --dport 22 --state NEW -j ACCEPT
3:  -A INPUT -i eth0 -p tcp --dport 80 -j ACCEPT
4:  -A INPUT -i eth0 -p tcp --dport 443 -j ACCEPT
5:  -A INPUT -i eth0 -p udp --sport 53 -j ACCEPT
6:  -A INPUT -i eth0 -p udp --dport 123 -j ACCEPT
7:  -A INPUT -i eth0 -p icmp -j ACCEPT
8:  -A INPUT -i eth0 -j DROP
9:  -A OUTPUT -i eth0 -j ACCEPT
```

The server provides HTTP and HTTPS services, synchronizes its clock to a public NTP pool, and is remotely administered via SSH. After establishing these firewall rules, the administrator can no longer log in via SSH from 129.132.254.12. Why not?

Task 5: Session State, SQL Injection 7 Points

a) Session State (3 Points)

Alice logs in to https://www.bob.example.com, presenting her username (`alice.muster@gmail.com`) and password (`TuXbA#4dnA6339mp`) to log in. The web app (written in Python 3) creates a session ID as follows:

```
def create_session_id(username, password):
# seconds since 1970, in decimal
randomness = str(int(time.time()))

# hash it together with the userid
hash = hashlib.sha1((randomness + username).encode("utf8"))

# return first 16 digits of hash digest
return hash.hexdigest()[:16]
```

On logging in, the session ID (`d6826fb6b31de8f6`) is stored in Alice's browser as a cookie with the name `sid`.

Briefly explain how Eve, who does not have access to Alice's computer, could impersonate Alice to https://www.bob.example.com.

b) SQL Injection (4 Points)

(i) Does SQL injection exploit a vulnerability in the web application code (custom code) or in the web server/database (eg. Apache/MySQL)? Explain your answer. (1 Point)

(ii) Why are input strings such as `' OR '1' = '1` a security risk for SQL if not properly checked? (1 Point)

(iii) Suppose that the web service checks for the occurrence of the substring ‘ `OR` ’ (`OR` with a space on either side) in the input, so that an input string such as `' OR '1' = '1` would be caught and rejected. How can the server's defence be defeated? (1 Point)

(iv) Now suppose the web service checks for the equals sign in the input, so `' OR '1' = '1` and `' OR 'a' = 'a` are both detected. How can this check be defeated? (1 Point)

Task 6: TLS 8 Points

a) Key Exchange Mechanism Analysis (2 Points)

(i) Briefly explain the principle to achieve perfect forward secrecy (PFS) for TLS connections. (1 Point)

____

____

(ii) Briefly explain the main difference in key exchange mechanism metrics between RSA and DH based key exchange. (1 Point)

____

____

b) TLS System Improvements (3 Points)

(i) Briefly explain the idea behind certificate pinning. (1 Point)

____

____

(ii) For each of the following questions about certificate transparency (CT) add a tick for either true or false. (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.) (2 Points)

true	false	
□	□	CT is the solution to root CA abuse.
□	□	CT documents all issued certificates.
□	□	A malicious CA can prevent another CA from publishing an issued certificate to a CT log.
□	□	CT makes the CA accountable for mis-issued certificates.

c) TLS Web Services **(3 Points)**

Bank x.com has a secure website to log in to bank accounts. They want to make sure that the username/password dialog is only entered on a TLS-protected page. When you access http://www.x.com they immediately redirect your access to a TLS-protected page: https://www.x.com.

(i) Describe one possible attack when you type https://www.x.com versus typing http://www.x.com? Is there any difference? Explain. (2 Points)

(ii) You want to obtain a certificate from a CA named CAsimple. You submit your meta data and key material. Explain which type(s) of key(s) are part of your certificate signing request. (1 Point)

Task 7: Malware 6 Points

For each of the following six examples of malware, tick the box corresponding to the type that it is closest to out of the following: trojan, worm, rootkit, keylogger, or ransomware. Some types may be answered more than once, and some not at all. Explain your answers. (1 point for each correct answer, and you must include an explanation to get credit.)

(i) The program exploits vulnerabilities in Unix utilities to get a shell, then finds other computers connected to the infected machine and attempts to get a remote shell on the other machines to infect them as well.

□ Trojan □ Worm □ Rootkit □ Keylogger □ Ransomware

Explanation ______________________________

(ii) The program encrypts the user's documents and photos, and only releases the decryption key when the user pays a fee. If the user does not pay within 24 hours, it permanently deletes the decryption key.

□ Trojan □ Worm □ Rootkit □ Keylogger □ Ransomware

Explanation ______________________________

(iii) A gaming company allows users to play online games against each other by downloading a free gaming client to their machines. However, when the user is not playing a game, the client software mines for Bitcoin and sends the results to the company.

□ Trojan □ Worm □ Rootkit □ Keylogger □ Ransomware

Explanation ______________________________

(iv) A file-sharing program's installer requires the installation of several components. Among the required components is a program that redirects any mistyped URL to its own search page with results.

□ Trojan □ Worm □ Rootkit □ Keylogger □ Ransomware

Explanation ______________________________

(v) A copy-protection program for an audio CD intercepts all accesses to the CD drive of the machine, only allowing access through the software's own music player. The program also exploits administrative privileges to stop system tools from displaying processes or files whose names begin with `$sys$`.

□ Trojan □ Worm □ Rootkit □ Keylogger □ Ransomware

Explanation ______________________________

(vi) A smartphone with a malware app lies on a table next to a laptop. The app uses the smartphone's accelerometer to determine what the user typed on the laptop.

□ Trojan □ Worm □ Rootkit □ Keylogger □ Ransomware

Explanation ______________________________

Task 8: DNS Security 6 Points

a) Properties of DNSSEC (2 Points)

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 □ In DNSSEC, confidentiality was a primary design goal.

true □ false □ DNSSEC makes the execution of some DoS attacks easier.

true □ false □ Today, DNS resolvers don't need to perform bailiwick checks any more because of DNSSEC.

true □ false □ When the chain of trust can be verified to a well-known anchor, the corresponding DNS record should be trusted.

b) Attacks on DNS (4 Points)

(i) For the convenience of their laptop users, an enterprise allows recursive queries towards their resolver not only from inside the company, but also from the Internet. Give two reasons why this is a security problem for this enterprise and explain. (2 Points)

(ii) How can clients belonging to the same subnetwork as the attacking host be tricked into using a malicious DNS server? Give one attack vector and explain. (2 Points)

Task 9: Malware Development and Demo, Botnets 8 Points

a) Botnets (2 Points)

Check whether the following statements are true or not. 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 □ Full understanding of the technology is sufficient for understanding cyber security.

true □ false □ "CnC" is often used to describe capture and control of bots.

true □ false □ Crypters are part of malware detection evasion tactics.

true □ false □ Fast flux techniques speed up communication within the botnet.

b) Polymorphism Techniques (4 Points)

Briefly describe four techniques to mutate malware code while keeping its functionality intact. Also provide a short (code) example for each technique.

1. __________________________________

2. __________________________________

3. __________________________________

4. __________________________________

c) Code Signing (2 Points)

One proposed defense against malware is code signing, where the developer ships his programs with a digital signature. The program will only run if the signature can be successfully verified beforehand.

(i) Why is this not a complete defense against malware? (Hint: what cryptographic problem is solved by signatures?) (1 Point)

(ii) Imagine an implementation of the signature-checking code that stores the keys it uses to check the code signatures in publicly readable files. Is this a security risk? Justify your answer. (1 Point)

Task 10: Cross Site Scripting (XSS) 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 and curious user, discovered that she can include HTML content in the *about me* section of her profile page that is displayed to users who view her profile.

a) Privacy Violation (2 Points)

How can Eve discover the usernames of the users visiting her profile?

b) Monetizing the Vulnerability (2 Points)

How can Eve make money from including HTML content in her profile?

c) Blocking HTML (3 Points)

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.

(i) How can Eve still include HTML content in her profile? (2 Points)

(ii) How can the administrators of lessfriendly.com prevent that? (1 Point)

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

a) Vulnerability (2 Points)

Is it more cost-effective for a cyber criminal to buy the latest vulnerability information or rather use some well-known vulnerabilities to build a botnet? Explain your answer.

b) Zero-day Vulnerabilities (2 Points)

Newspapers recently reported that the German BND intends to buy vulnerabilities which are unknown to the public.

Please state two ways (one offensive and one defensive) in which the BND could use these vulnerabilities.

1. ______

2. ______

c) Customized Software (2 Points)

Assume you are the Information Security Officer of a Swiss bank. During routine penetration testing you discover a new critical vulnerability in a business-critical customized application provided by an external contractor. Now, you have to decide how to solve the problem.

(i) If the vendor of this software is hesitant in fixing the vulnerability, will a *full disclosure* help you? Explain. (1 Point)

(ii) Do you have options other than a full disclosure to mitigate the risk? Explain. (1 Point)

Task 12: Email Spam **5 Points**

Answer the following questions regarding **greylisting**.

(i) Briefly explain how greylisting works. **(1 Point)**

(ii) How could a spammer circumvent greylisting? Explain. **(1 Point)**

(iii) In your opinion, why is greylisting still so effective? Give two possible reasons. **(3 Points)**

Task 13: Identity, Authentication, and Anonymity 6 Points

a) Authentication (2 Points)

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

Weak: ____

____

Strong: ____

____

b) Authorization Protocols (2 Points)

802.1x and OAuth (RFC 6749) both provide a mechanism for separating authorization from resource access, for IEEE 802 (Ethernet) network connections and HTTP connections, respectively. Tick true for each statement below about 802.1x and/or OAuth which is true, and false for those which are false. (Each correct answer gives 0.5 points. For each incorrect answer 0.5 points are subtracted. No answer gives zero points. This subtask gives at least zero points.)

true □ false □ The OAuth Client entity is equivalent to an 802.1x Supplicant: both want access to a resource and present credentials in order to get that access.

true □ false □ A generalized form of OAuth would not be applicable to the use case supported by 802.1x, because OAuth has no entity equivalent to the 802.1x Authenticator.

true □ false □ An OAuth authorization grant represents the resource owner's intention to make a resource available to a client, provided that client can be authenticated by the authorization server.

true □ false □ 802.1x's EAP-TLS authentication method provides PKI authenticated transport, requiring both the client and the server to present X.509 certificates.

c) Onion Routing and Pseudonymity (2 Points)

Alice uses the TOR onion routing anonymity service to browse www.bob.example.com. She authenticates to the website using a pseudonym ("Anne") that she only uses when connecting to www.bob.example.com, and always uses TLS when connecting to the website. Eve compromises www.bob.example.com, and would like to know the real identity of "Anne". Name one strategy she could follow to link Alice's pseudonym back to her identity.

____

____

____

Task 14: Lab **8 Points**

a) **iptables** **(2 Points)**

Create an `iptables` rule for the firewall to prevent packets to port 23 from reaching the web server with IP: `A.B.C.D`.

____

b) **nmap** **(2 Points)**

What is the tool `nmap` used for? And what is the meaning of its three states `open`, `filtered` and `unfiltered`?

____

____

____

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

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

____

____

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

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

____

____

e) **Application Security** **(2 Points)**

The following functions `real_escape_string()` and `htmlentities()` are used in the lab to prevent the mentioned SQL injection and XSS attacks. Explain what does each function do?

real_escape_string():____

____

htmlentities():____

____