ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

TIK Institut für Technische Informatik und Kommunikationsnetze

Department ITET
Lecture HS 2011

Lecturer: Prof. B. Plattner, Dr. T. Dübendorfer, Dr. S. Frei
Coordinator: Dilip Many

Exam
Network Security

Mi 25. Jan. 2012, 09:00 – 10:30, HG F1

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 - 28**).
- ▷ **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 paper sheet 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	/7	
2	/6		10	/6	
3	/7		11	/9	
4	/7		12	/5	
5	/6		13	/3	
6	/6		14	/2	
7	/6		15	/7	
8	/8				
Σ	/51		Σ	/39	
Σ_{ALL}	/90				

Task 1: Insecurity, Risk, Vulnerability Lifecycle 5 Points

a) Security goals (3 Points)

Consider an online e-banking site. Which security goal is preserved in each of the following scenarios:

i) The e-banking site continues to provide its services to its customers.

Solution: Availability

ii) The e-banking site is able to ensure that its customers cannot deny their online actions.

Solution: Non repudiation

iii) The e-banking site is able to ensure that customer data have not been tampered with.

Solution: Integrity

Which security properties would be compromised in the case of an intelligent attacker that succeeds in doing the following:

iv) Compromise the client's RSA private key and use it for decryption.

Solution: Confidentiality

v) Exploit a buffer overflow in the client's web browser.

Solution: Integrity

vi) Compromise the web-server and acquire root access using it to manipulate user data.

Solution: Confidentiality, Integrity.

To corrector 0.5 point for subquestions i-vi.

b) Dynamics of insecurity **(1 Point)**

State two reasons due to which the patching policies that are applied to fix discovered vulnerabilities are in most cases not as effective as the respective malware that attempts to exploit them.

Solution:

1. High dynamics around disclosure day (50% of patches 80% of exploits available at 0-day)
2. Security is slow (many vulnerabilities unpatched even 100 days after disclosure)
3. Insiders (many vulnerabilities known to closed group before disclosure)

c) Software Vulnerability **(1 Point)**

The two main parties involved in remediating vulnerabilities are the vendor from the one side and the security officers and network administrators from the other side. State which party is responsible for dealing with the following risks.

Solution: Pre-disclosure risk: Noone - there is nothing we can do about this risk.

Post-disclosure risk: The vendor - needs to provide a patch.

Post-patch risk: The admins - need to roll-out the patch to their systems. To corrector 0.5 point if two out of three are correct.

Task 2: Secure Shell, Secure Channels 6 Points

a) SSH (2 Points)

List the names and briefly describe the three individual protocols that are used to build the SSH protocol architecture.

Solution:

1. SSH-CONN for connection multiplexing.
2. SSH-AUTH for client authentication.
3. SSH-TRANS for server authentication, confidentiality, integrity.

To corrector 1 point for two correct, 2 points if all correct

b) Attacks against SSH (2 Points)

Assume that a client and a web server communicate using the SSH protocol. Against which attacks can SSH successfully defend? 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 □ SYN Flood attack against the web server.

true □ false □ Traffic analysis attacks to determine the amount of traffic exchanged between the communicating hosts.

true □ false □ Connection hijacking at the TCP level.

true □ false □ Man-in-the-middle attack to eavesdrop communication.

Solution: false,false,false,true.
To corrector 0.5 points for each subquestion

c) Secure Channels (2 Points)

Consider an Internet Protocol v4 packet consisting of six consecutive parts, which transports data in IPSec transport mode.

Section	Order	Encryption
Data		
TCP		
ESP Header		
ESP Trailer		
ESP Auth		
Original IP Header		

i) In the table shown above under **Order** use numbers **1 to 6** to denote the ordering of the different packet parts.

Solution: 4,3,2,5,6,1

To corrector: 0.5 if sequence Original IP header, TCP, Data is correct. One point if all parts are correct.

ii) Tick each section which is encrypted in the **Encryption** column of the table.
Solution: Parts TCP, DATA and ESP trailer are encrypted.

0.5 P if all correct; 0 otherwise

iii) If our security concern is to protect the identity of the communicating end-hosts, which IPsec mode should we use?

Solution: Tunnel mode with ESP.
To corrector:0.5 P if correct

Task 3: Firewalls, IDS and NAT Traversal 7 Points

a) Firewalls and NAT (3 Points)

i) What is the difference between a stateless vs. stateful firewall?

Solution: A stateless firewall does not keep state (information) about existing connections e.g. TCP sequence numbers. It analyzes packets independently without taking into account packet sequences. Stateful firewalls keep track of the state of current connections and make decisions based on the session state

ii) Can a stateless firewall prevent probing against a specific port without completely blocking all communication utilizing this port? Briefly explain your answer.

Solution: No. If traffic is allowed in this port, then the probe can use an existing connection to send its packets since the firewall is not aware of the state of the connection (stateless).

iii) Someone suggests that firewalls are not needed if all communication is properly encrypted. Do you agree? Explain briefly your answer.

Solution: No. Encryption provides a solution for confidentiality and integrity (e.g. eavesdropping and data modification). However, it does not safeguard network devices from vulnerabilities.

b) IDS systems (1 Point)

Are the following statements true or false? Tick the correct box. (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	
□	□	Anomaly based detection, in contrast to signature-based detection, can potentially detect novel attacks.
□	□	To defend against evasion, network-based detectors must analyze each packet in a stateless fashion.

Solution: true,false.

c) Firewall rules (3 Points)

Suppose that we use a stateless network firewall to filter TCP traffic exchanged between the local network 129.132.5.64/26 and the Internet, as shown in Figure 1.

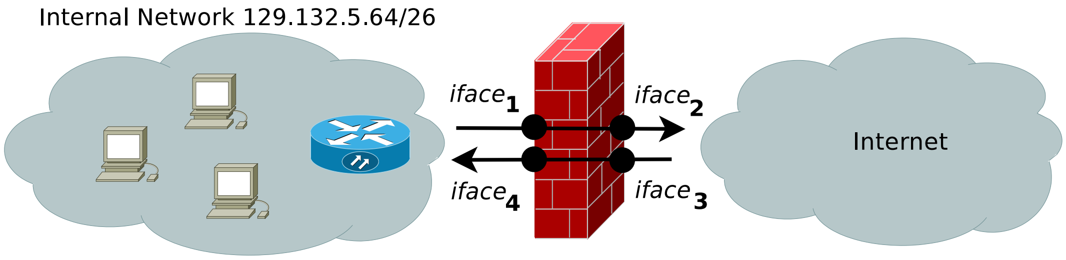


Figure 1: Network topology.

Consider that the filtering table for interface $iface_1$ is:

Rule ID	Action	Source IP	Source Port	Destination IP	Destination Port
1	ALLOW	129.132.5.*	*	*	*
2	BLOCK	*	*	*	*

whereas the filtering table for interface $iface_3$ is:

Rule ID	Action	Source IP	Source Port	Destination IP	Destination Port
3	BLOCK	195.170.50.*	80	129.132.5.*	*
4	ALLOW	*	80	129.132.5.*	*
5	ALLOW	*	*	129.132.5.4	25
6	BLOCK	*	*	*	*

i) For each of the following packets arriving at interface $iface_3$, determine which rule is used to determine whether the packet will be forwarded or blocked. You only need to denote the corresponding Rule ID on the table shown below.

Source IP	Source Port	Destination IP	Destination Port	Rule ID
195.170.50.10	2500	129.132.5.4	23	
132.210.102.8	80	129.132.5.4	6000	
132.210.102.8	25	129.132.5.4	25	
195.170.50.10	80	129.132.5.4	23	

Solution: 6, 4, 5, 3

ii) What is the purpose of introducing the filtering rules for interface $iface_1$?

Solution: Prevent spoofing from nodes located in the LAN - in this way prevent potential outbound DoS

iii) Does the firewall permit a host from the local network to establish an HTTP connection with a web server with IP address 195.170.50.10? Explain briefly your answer.

Solution: No. Rule 3 rejects the SYN/ACK of the TCP connection.

Task 4: Malware 7 Points

a) **Worms** **(1 Point)**
Which are the two defining features of a worm?

Solution: A worm is a self-contained software that can replicate itself from computer to computer across network connections. Upon arrival, the worm may be activated to perform some unwanted operation and continue propagating.

b) **E-Mail Worms** **(1 Point)**
Do e-mail worms necessarily rely on social engineering (the user being naive enough and executing a file that came as attachment)? Explain in detail your point of view.

Solution: No, not necessarily. There have been situations (see http://www.ubuntu.com/usn/usn-200-1/) where a vulnerability of the mail client itself could be exploited. In that particular instance, the Unicode string parser was vulnerable to buffer overflows and the Javascript engine was vulnerable to integer overflow.

1 point

c) **Social Engineering** **(1 Point)**
Describe a way through which a person receiving an e-mail containing an attached file could be tricked into believing that it has a different extension.

Solution: The file could be named 'file.pngbbbbbbbbbbbbbbbbbbb.exe', where b denotes a blank/space. Since the name is long, many mail clients would simply display it as 'file.png ...' and the user would have the impression it is going to open a PNG image, when in fact he would be executing a possibly malicious file.

alternative potential answer: use double extension: kurnikova.pdf.exe; some windows systems will hide the real extension making it look like a pdf

see: http://www.f-secure.com/weblog/archives/00001678.html

1 point

d) LoJack for Laptops (4 Points)

LoJack is a software for laptops. The company that maintains it (Absolute Software) advertises that if a user buys the LoJack license and a special subscription, then in case of a theft, the company can remotely extract location information from the stolen laptop, thereby helping the owner and the authorities to recover the stolen item.

The following elements are not disclosed to the customers:

1. LoJack comes preinstalled in the BIOS of most portable computers (Apple, Dell, Toshiba etc.). This BIOS function is usually disabled and can only be activated if the owner purchases a yearly subscription from the software vendor. However, in many cases the laptop comes with LoJack activated and operational (without the user being aware of this) even though the user has not bought a license.
2. LoJack operates by triggering a hidden Windows program that periodically sends location data to a pre-determined server operated by Absolute Software.
3. Even after erasing/changing the hard disk and reinstalling the operating system, the BIOS function (if activated previously by the user or computer vendor) will silently access the Windows partition, reinstall and activate the tracking program.
4. If activated, LoJack will send to Absolute Software GPS location (for devices with GPS chips), the IDs of the WLANs in the surroundings and other location data to the server, even if the laptop has not been declared stolen.

i) A security analyst has discovered that an active LoJack instance can be exploited through a vulnerability. Argue why an exploited LoJack instance can now be considered both a rootkit and a trojan.

ii) Explain why is it possible to create BIOS malware/viruses that persist even after the BIOS has been reflashed by the host on which it runs.

Solution:

i) The software becomes primarily a rootkit, because it hides from the operating system, it activates during boot, but it is also self-healing. It can also be considered a Trojan, in the sense that the owner thought the program can be used for a specific purpose, but in addition LoJack also leaks location details irrespective of whether the laptop has been reported as stolen or not. 2 points for any of the answers.

ii) The BIOS has to be reflashed after turning on the computer, which means that it has already been loaded into RAM and can either interfere with the reflashing process or can reinstall itself after reflash. 2 points

Task 5: Malware Development and Demo, Botnets 6 Points

a) Protection techniques (1 Point)

Give three concrete examples of techniques that malware can employ to avoid displaying malicious behavior while being analyzed by an anti-virus heuristic.

Solution:

1. read flags/API that would indicate the process is being debugged
2. self debugging: failure indicates that the program is already being debugged
3. measuring deltas between timestamps around exception handlers

1 point if all are correct

b) Polymorphism techniques (2 Points)

Enumerate four polymorphism techniques which can be used to better hide malware. Briefly explain what each of them consists of.

Solution:

1. using different code constructs with the same effect (use while instead of do - while)
2. changing the order of code (reorder instructions, define functions in a different order etc.)
3. insert noise (adding statements such as sleep(0), if (1==1) or NOPs)
4. compiler setting modulation (using different compiler options).

0.5 points for each correct answer

c) Bot Lifecycle (2 Points)

There are different ways to control botnets. These are called bot command models. Explain the defining features of three such bot command models (**not** topologies).

Solution: 1. No Control: default malicious behaviours, self propagation defaults, less flexible, most likely detected by signatures, most resistant to global shutdown

2. Private Channels: custom and covert channels, abuse and alteration of common protocols, short-term stealth, signature detection easy once CnC observed

3.Public Infrastructure: use common applications API, generally reliable and anonymous, mostly IRC, some P2P and microblogging

4. Resilient hybrids (all models): default malicious behaviors, fall-back plans if CnC unavailable, pre-programmed contact points (drop boxes)

Two points if three of them are correct.

d) Botnets **(1 Point)**

Explain the functionality of each of the following botnet entities:

Bot Agent: ________________________________

Botnet: ________________________________

Bot Master: ________________________________

Command and Control: ________________________________

Solution:

A botnet consists of:

1. Bot Agent – crime-ware tool installed on victims
2. Botnet – collection of all bot agents
3. Bot Master – the criminal(s) operating the botnet
4. Command and Control (CnC) – botnet management system

Task 6: Email Spam **6 Points**

a) Nigerian Money Scam **(1 Point)**

Describe two features of the Nigerian money scam scheme to explain how the spammer makes money.

Solution:

1. the scammers will find important details about the person (date of birth, account number, address, account number etc.) which could be used to access his funds
2. the victim is required to send money in advance for fictitious tasks (lawyer fees etc.)
3. scammers can capture people and extort money from people that travel to Nigeria to get their money back

(To corrector: 1 point if two bullets are correct.)

b) Spam Distribution Channels **(2 Points)**

Describe three spam sending tactics (ways in which the spammer can convey the spam messages) that are often employed by spammers.

Solution:

1. spam sent from accounts that have been compromised
2. sending spam from short-term officially registered domains
3. using botnets

(To corrector: 1 point if three bullets are correct.)

c) Blacklist Lookup **(1 Point)**

Explain which type of DNS record is returned by a query for an IP address directed to the realtime blacklist sbl-xbl.spamhouse.org.

Solution: The returned DNS A record indicates if the IP address is on the list or not. How to interpret the answer from the DNS system depends on the implementation chosen by the blacklist provider.

More details (to corrector: these details are not required for a full score): Some blacklists don't contain an A record in the response if the address isn't in the list (as discussed in the lecture). Provider spamhouse.org uses different predefined IP addresses to indicate several possible states of an IP address (not discussed in the lecture).

d) Spammers and Web Bots **(2 Points)**

Try to think of a method a webmaster could use to fill spammers's databases with non-existing addresses. Mention one possibility for the spammer to circumvent it.

Solution:

1. One frequently employed method to gather addresses for later use in spamming is to crawl web sites and to gather these addresses. An approach would be to create a CGI script that dynamically creates web pages containing several randomaddress@randomdomain addresses and which contains several links to the same CGI script, thereby causing another such page to be generated and crawled by the spammer. The CGI script would be accessible via links hidden in the web pages of the targeted site.

2. The spider can become aware of this technique (for instance, if the entropy of the gathered addresses is too high).

1 points for devising a method that works reasonably well; 1 points for mentioning the weakness.

Task 7: DNS Security 6 Points

a) DNS and DHCP (1 Point)

How can clients belonging to the same subnetwork be tricked into using a malicious DNS server?

Solution: An attacker can install a malicious DHCP server that replies very fast to DHCP requests broadcasted by computers seeking to acquire an address. DHCP replies contain also the address of a local recursor, which can be the same machine as the malicious DHCP and which will produce false replies.

b) Resolvers (1 Point)

Consider an ISP has its own DNSSEC-enabled recursor. On which of the following entities:

1. client computers
2. recursor (recursive resolver)

can the verification of signatures be performed?

Solution: The authenticity of the response is verified at the recursor, but can be also implemented on the client. Not required: It is possible to do a manual verification on the client machine. 1 point if both are correct.

c) Zones vs. Domains (2 Points)

Explain the difference between the concept of (sub)domain and zone. Give an example.

Solution: A (sub)domain is basically just a name, a part of the naming hierarchy of the DNS. A zone comprises portion of the DNS name hierarchy for which the management responsibilities are performed by the same entity. (1 point)

Example: bc.ca and on.ca are subdomains of .ca. However, if .ca and .bc.ca are managed as an entity by the same organization, then they belong to the same zone. If .on.ca is managed by another authority (different from the one that manages .ca), then it belongs to another zone. (1 point)

d) DNSSEC (2 Points)

i) What does the DS record contain?

ii) Explain the role of the DS record in constructing the chain of trust by detailing the steps that the resolver has to make.

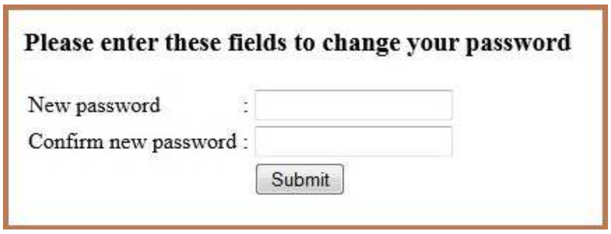
Solution: i) The DS record contains a hash of the KSK key signing key belonging to the child zone). (1 point).

ii) Once the DNS resolver knows the contents of DS, it can retrieve the KSK and ZSK (zone signing key) belonging to the child zone. KSK is checked against DS. ZSK is validated using the KSK. Not required: Finally, if the child zone is the actual target of the query, the answer can be checked by using the ZSK. (1 point).

Task 8: Cross Site Scripting **8 Points**

a) Changing Password (4 Points)

A webservice provides logged in users the form shown (Figure 2) to change their password.



Please enter these fields to change your password

New password :

Confirm new password :

Figure 2: Change password page.

i) Name (i.e. **specific** type of XSS attack) and describe the attack, which such a password change dialog is most likely susceptible to. How would such an attack harm the user? (2 Points)

Solution: The attacker can persuade the user to open a page that causes his password to be set to another password (a blind write-only attack). This attack belongs to Cross-site request forgery (XSRF), and the attacker can log in with the victim's account as long as the user is not notified and does not reset his password in another way (via security questions etc).
(To corrector 1 point for a correct explanation, 0.5 for the category name - XSRF, and 0.5 for the harms)

ii) How could the HTTP_REFERER be used to mitigate the attack? What is the problem faced when relying on HTTP_REFERER for attack mitigation? (1 Point)

Solution: The HTTP referrer indicates the page that brings the user to the change password page. The server can check HTTP_REFERER headers and deny changing password if referrer is empty or from a different domain. Due to proxies, the HTTP referrer is not always set.

iii) Name two other prevention techniques (rather than checking the HTTP_REFERER) for your proposed attack. (1 Point)

Solution:

1. Ask for old password
2. Security token
3. Challenging with a CAPTCHA

b) XSS Attack **(2 Points)**

What are the two root causes for XSS attacks? For each of them, describe a general solution.

Solution:

1. Partial or missing user input sanitization: Fix XSS problems by attempting to filter out meta-characters ($'$, $<$, $>$, etc).
2. Partial or missing HTML output encoding: Ensure that every user supplied parameter is HTML output encoded before it is sent to a web browser. (Example: < is replaced with &lt;).

c) HttpOnly Cookies **(2 Points)**

i) Describe HttpOnly cookies as a means of preventing XSS attacks. (1 Point)

Solution: The server creates a cookie with HttpOnly flag (optional) and sends this to the client. If the HttpOnly flag is included, the browser prevents a client side script to access the cookie, of course if the browser supports it.

(To corrector 0.5 points for correct explanation, 0.5 for mentioning the browser prevents the client from accessing it)

ii) Give one advantage and one disadvantage of using them. (1 Point)

Solution:

- Advantage: Can not be read by a client script (only sent from/to server); therefore mitigates the attack well.
- Disadvantage: Browsers ignore it or downgrade to normal cookie; Only IE6 SP1 and up support it.

Task 9: Session state, SQL injection 7 Points

a) Session Management (3 Points)

A user logs into `http://www.TIKbook.tld` by entering his username and password. After a successful login, the user closes the browser tab without pressing on the `Log Out` button. If he browses `http://www.TIKbook.tld` again, his browser will be redirected to the welcome page on the TIKbook (without any need to enter the password again).

i) How does the TIKbook re-authenticate this user? Explain what happens on the client and what happens on the server. (1 Point)

Solution: Using a session id stored as a cookie. The server generates and returns back a unique and random session id after a successful login, and this cookie is stored on the client's browser and the server (usually in a database). Whenever the client requests for another page, this request is automatically accompanied by the corresponding cookie (done by the browser) and therefore the server is able to re-authenticate the user.

ii) Give 2 possible attacks on this system. (1 Point)

Solution: Possible attacks:

1. cookie stealing and therefore session hijacking by eavesdropping
2. stealing the password, again by eavesdropping
3. phishing is also possible, no SSL certificate (just HTTP)

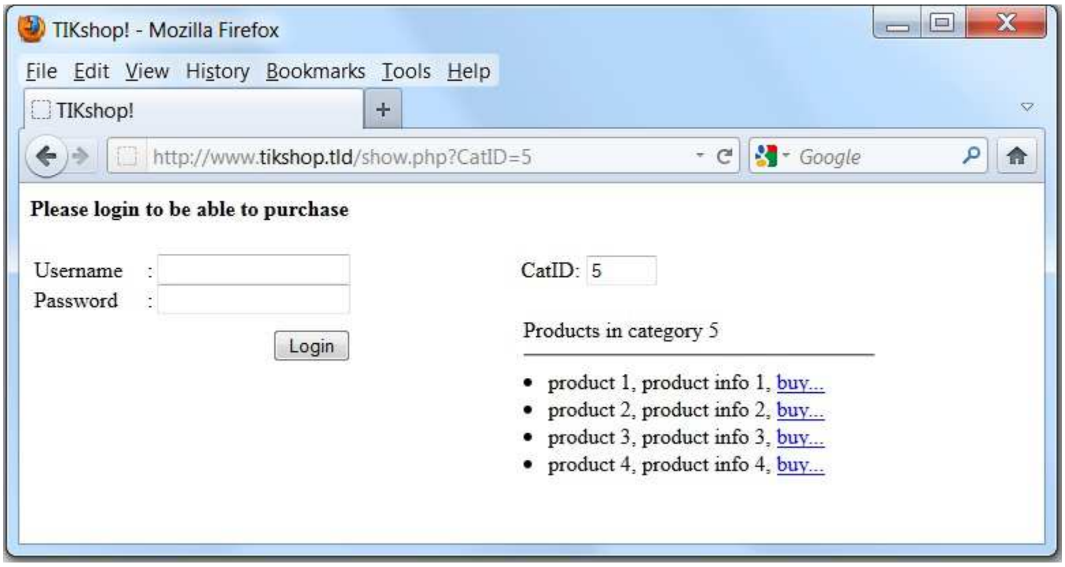
iii) Explain 2 solutions that can improve the security of the session management of the TIKbook. (1 Point)

Solution:

1. using HTTPs with valid SSL certificate, at least for the authentication part
2. time out after sometime inactivity

b) SQL Injection (4 Points)

An online shop allows visitors to look up different product categories by specifying a category number *CatID*, e.g. 5 (See Figure 3).



TIKshop! - Mozilla Firefox
File Edit View History Bookmarks Tools Help
TIKshop!
http://www.tikshop.tld/show.php?CatID=5
Google

Please login to be able to purchase

Username :
Password :
Login

CatID: 5

Products in category 5

- product 1, product info 1, buy...
- product 2, product info 2, buy...
- product 3, product info 3, buy...
- product 4, product info 4, buy...

Figure 3: An online shop.

This category number is entered via a **textfield** on the page as $CatID variable. On the server this query is executed to retrieve and display the requested data:

```
SELECT product_name, product_info
    FROM products WHERE CatID=$CatID
```

Users of this system can log in with a username and password, and then can purchase whatever product they want (the same figure).

In addition assume an attacker knows, based on some error messages returned by the system, that there is another database table named `users` consisting of `username` and `password` of all the users in the system.

Given this knowledge, answer the following questions.

i) Propose an attack to acquire all usernames and passwords in the system. Please explain in detail (including the resulting SQL query). (2 Points)

Solution: Adding this tainted category id:

1 UNION SELECT username, password FROM users WHERE 1=1

That runs this query:

SELECT product_name, product_info FROM products WHERE CatID=1
UNION SELECT username, password FROM users WHERE 1=1

In the result-set, it shows username and password in the same place as the columns product_name and product_info respectively.

(To corrector In the tainted query, 0.5 points for “1”, 0.5 for “UNION SELECT”, 0.5 for “username, password FROM users” and 0.5 points for mentioning correctly the result-set)

ii) Propose 2 solutions for this specific scenario to mitigate possible attacks. (2 Points)

Solution:

1. using stored procedure on the database (i.e. input sanitization on the database)
2. using parameterized statement in the application (i.e. input sanitization on the **server-side** application)
3. error messages not to show plainly to the client

"To verify CatID is numeric on the server" is also a solution, substituting one of the first two (i.e. input sanitization).

(To corrector client-side sanitization is NOT a solution!)

Task 10: Security Ecosystem, Network Security Research 6 Points

a) Security Ecosystem (2 Points)

You discover a high risk vulnerability in one of the Microsoft windows operating systems and report it to the Microsoft security team. But the team denies the existence of such a vulnerability. What other steps can you take? Mention 2 steps and describe each.

Solution:

1. stay silent: tell nobody. Are you really the first and only one who discovered the vulnerability?
2. go full disclosure: publish the vulnerability. Public pressure gives vendor a strong incentive to fix the problem quickly, which on the other hand arms criminals with relevant information
3. sell vulnerability: make profit by selling it to the vendor or in a black market.
4. As another possible step, you can build the vulnerability and exploit the system yourself.

b) Vulnerability (2 Points)

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

Solution: To use well-known vulnerability, due to the fact that patching is slow. Even if just 1% of the systems un-patched, still a blackhat can launch some attacks with very low-cost.

c) Security Information Provider (2 Points)

What is a Security Information Provider (SIP), and its role in the security ecosystem?

Solution:

- Several private and government organizations specialize in collecting and publishing vulnerability intelligence
- These organizations efficiently monitor the primary sources of security information, validate the content found, and publish their findings as security advisories in a consistent format

(To corrector mentioning each of these keywords: collect, validate, monitor, publish has 0.5 points)

Task 11: Identity and Authentication 9 Points

a) Identity Theft (1 Point)

Name four different variants of Identity Theft:

Note that you get only one point if all four variants are named correctly

Solution:

1. Financial Identity Theft

2. Criminal Identity Theft

3. Identity Cloning

4. Business/Commercial Identity Theft

b) Authentication (1 Point)

Complete the following sentences:

Solution: Authentication is the process of verifying(checking,testing) (0.5) an identity claim of an entity.

It binds the principal(actor,entity) (0.5) to an identity.

c) Level of Anonymity (2 Points)

Name for each scenario below the level of anonymity that is provided. Why?

i) A blogger that signs each blog entry using his personal SuisseID.

Solution: Level: Public Pseudonyms: Identification

Why: Link between the pseudonym and a human being is publicly known or easy to discover and checked.

ii) A student providing feedback for this lecture using the evaluation form of ETH.

Solution: Level: Unlinkable Pseudonyms: Anonymity

Why: Link is not known to system operators and cannot be determined.

d) IEEE 802.1X **(5 Points)**

A small company relies on the IEEE 802.1X protocol to grant access to their network. To simplify the task, we assume that the network consists only of two workstations and one server providing a DHCP and an authentication service (RADIUS). The nodes are interconnected with the help of one hub and one switch as illustrated in Figure 4. Please note that the switch acts as IEEE 802.1X authenticator. Assume, that in the beginning no workstation is authenticated.

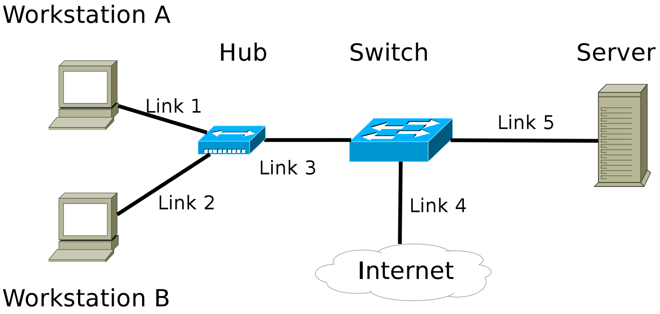


Figure 4: IEEE 802.1X Network

Answer the following questions:

i) (1 Point) Workstation A sends a DHCP request toward the DHCP server. What's the reply of the server? Why?
Solution:

No reply. Request is blocked at the switch.

ii) (1 Point) Workstation A sends an EAP-Response packet. List all links that can observe this packet.
Solution:

Link 1,2,3,5.

Now assume the Workstation A is authenticated using IEEE 802.1X.

iii) (1 Point) Workstation B tries to access http://www.example.ch on the Internet. Does it receive an answer, why?
Solution:

Yes, workstation A has opened the port on the switch for both machines.

iv) (1 Point) In this network, IEEE 802.1X prevents malicious users/hosts to steal http session cookies. Is this statement true or false? Why?
Solution: False, Workstation B can collect all HTTP sessions cookies of workstation A. IEEE 802.1X does not provide any encryption.

v) (1 Point) The IEEE 802.1X protocol requires fully functional DHCP and DNS services. Is this statement true or false? Why?
Solution: Nonsens, IEEE 802.1X works on MAC Layer ... nothing above MAC is required.

Task 12: Availability, DoS 5 Points

a) Service Level Agreement (1 Point)

If a system has a service level agreement (SLA) of 99.999% availability. How many seconds can the service be down during January 2012 at most to still satisfy the SLA?

Solution: (100% - 99.999%) * 31 * 24 * 3600 = 26.784 seconds of downtime in January 2012.

b) DDoS (4 Points)

Assume, a simple web-shop application is accessible over HTTP using the standard TCP protocol. For each client surfing on the web-shop the application logic stores a shopping cart data structure in the main memory. Recently, it was noticed by the server administrators that the web-shop application crashed several times due to lack of free main memory. They assumed that the application is challenged by a DoS attack.

i) (0.5 Point) Name the specific type of this DoS Attack:

Solution: Memory Starvation Attack (Storage Resource Starvation Attack) ________

ii) (1 Points) As a network security officer, name three generic countermeasure against this type of DoS attacks that should be part of the design of this web application.
Solution:

1: Encode state in data and send it to client________________________

2: State loss affects only specific client/server________________________

3: Client cannot tamper with encoded data_(Correction: 1 point if three, 0.5 points if two)

iii) (2 Points) A network administrator proposes enabling SYN cookies to solve the problem. Explain why this countermeasure would be successful or wouldn't be successful depending on the attack vector.

Solution: Success if: Attack targets OSI Layer 4 (Networking/TCP/IP Stack) using a SYN Flood attack________________________________

____

Failure if: Attack targets OSI Layer 7 (Application Logic) using e.g. large number of items stored inside the shopping cart.________________________

_[Alternative: Botnet makes full three way handshake]________________________

iv) (0.5 Point) Assuming you have root access to the server. How could you quickly check if enabling SYN cookies will be a success to defend against the ongoing attack?

Solution: Count the number of half opened connection (e.g. netstat). (0.5)

If number ¿ large than use SYN cookies.

Task 13: Phishing, Social Networks as attack platforms/Cyberwar 3 Points

a) Money Mule (1 Point)

What is a money mule?

Solution:

A money mule is a person who transfers stolen money from one country to another, either in person, through a courier service, or electronically. The term is commonly used to describe on-line scams that prey on victims who are unaware that the money or merchandise they are transferring is stolen.

b) Low Orbit Ion Cannon (1 Point)

In December 2010, PostFinance closed the accounts of WikiLeaks founder Julian Assange. As a reaction the WikiLeaks community used the software 'Low Orbit Ion Cannon' to perform a DDoS attack against the webservers of PostFinance.

i) Name the type of the botnet used in this attack:

Solution: Opt-in Botnet (0.5)

ii) What is the major difference between this and 'traditional' botnets?

Solution: Participant volunarly to run a bot and render control to the social network group. (0.5)

c) Cyber Warfare (1 Point)

Recently the Pentagon declared that Cyber-Attacks can constitute an act of war, deserving an armed response. Name two major problems that the Pentagon has to overcome to carry out this armed response.

Solution:

1:Plausible Deniability: Identification of the true attacker

2:Limited attack surface: Attacker are probably not governments but civil persons. What should the CIA attack? Their swimming pool?

Task 14: Case Study: 'Secure Online Ticket Shop' 2 Points

a) **Session IDs** **(2 Points)**

A ticket shop generates session IDs using MySQL's auto_increment feature. This guarantees unique session IDs. Is this a good practice from a security standpoint? If not, explain!

Solution: Sequence numbers are predictable.

Attacker can guess the session numbers and access the data of other users.

Always use random numbers for sequence numbers.

Task 15: Lab and Guest Talks 7 Points

a) Hunt (1 Point)

The tool 'hunt' was used in the NetSec lab to hijack a telnet session.

i) Which attack technique is used by hunt to impersonate the sender and hijack the connection?

Solution: ARP spoofing (0.5 point); NOT: TCP hijacking; IP spoofing (without ARP spoofing, otw. packets won't reach hijacker)

ii) What are the benefits of a telnet connection running over IPSec?

Solution: authentication and encryption (ALT: sniffing protection, confidentiality) (0.5 P: both keywords)
NOT: MitM attack, cannot be hijacked (authentication means also modifications (also by 'accident') are detected); integrity (not same as authentication)

b) Spam Filtering at ETH (1 Point)

ETH has deployed spam filtering using SMTP envelope information and allows its users to decide whether spam is discarded or just flagged.
Name two advantages of using SMTP envelope information to decide if an email is spam or not.

Solution: To minimize network and CPU usage (ALT: fast). (0.5 P: per keyword)
ALT: avoids collateral spam / no use of non-delivery reports; Sender gets nfo that mail not accepted (is on slide 5; NDR of post-SMTP-time filtering might go to 'wrong sender')
NOT: less false negatives (we have less nfo: rather fp. will increase if we decide conservatively); less false positives (depends on algorithm)

c) Certification Authority (2 Points)

The display of a class 3 smart card reader is too small to present an entire document.

i) Could displaying of a short hash solve this problem? (Assuming the user understands hashes.) Explain your answer.

Solution: No. Then we have the problem of determing over what the hash was computed. (1 Point); ALT: user can't compute/check hash; ALT, 0.5P: hash intercepted on bus
NOT: hash doesn't provide info about original document (it does; but none usefull for user to know of which it was computed)

ii) A class 3 smart card reader is attached to a PC like a normal keyboard. How is it possible that despite that, the PIN entered on a class 3 reader is safe from a keylogger?

Solution: Contrary to a normal keyboard that sends the input to a potentially infected PC the **PIN** entered in a class 3 reader **never leaves the device**. (1 Point)
ALT: data sent by card reader (to server, not PC) is encrypted
NOT: hashed in reader

d) NetSec Reality Check - Network security in a large organization (3 Points)

i) List 3 network segmentation technologies:

Solution: - Virtual LANs - Routing domains - Virtual Private Networks (IPsec, SSL) (1P for all, 0.5 for two correct)
ALT: physical(ly disconnected networks); subnets
NOT: private network (doesn't mean same like VPN), NAT, Router, Firewall

ii) When a company evaluates a new security measure, there's a trade-off between two requirements. Which are those?

Solution: Security benefit (NOT: just benefit; ALT: security improvement) and operational feasibility (ALT: cost, operational effort, operational efficiency). (0.5 P per keyword)
NOT: availability, usability (/= operational effort; can also mean how easy to use by handicaped persons, etc.)

iii) Describe the most serious potential data leakage that even the best technical data leakage prevention system can't protect from.

Solution: There are always users that need to use the system. They will be displayed information that they can memorize and leak later on. (1 Point)
(It needs to be clear that the user has to be shown data to work with it and that he can memorize the data and carry it outside (and leak it there; not within the comapny) for the full amount of points.)
NOT: Camera photo (can scan at entrance for electronic devices); password stealing, weak passwords (we can use biometrics);
analog channel (radio is analog, can be blocked); human error: sending nfo to wrong person (preventable, we have the 'best' sys.: check with list of ok persons, analyze content, ...)
ALT, 0.5P: Whistleblower / human may leak data (without clearly describing how) / human error (student must not describe something tech. preventable) / social engineering (0.5 P: missing that human has to be displayed nfo to work)