Final Exam

Network Security Autumn 2016

04 February 2017

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.
- Once the exam starts, make sure you have received **all** pages of the exam. The exam should have **15 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 **must** answer questions 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.
- The use of notes, textbooks or other written materials is **not** allowed. You are allowed to use a **scientific calculator** during the exam. Any other device that provides communication or document storage capabilities is **not** allowed (this includes smart watches).
- At the end of the exam, please **remain seated** while we collect the exams. You may hand in your exam before the end, except in the last 10 minutes of the exam. Please **hand in all exam sheets**: if any sheet is missing, the examination will be marked with grade 1.0 and counts as failed.
- You are **not** required to score all points to get the maximum 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.
- When answering questions, always **explain your reasoning**. If a question asks, for instance, whether A is more secure than B, a plain "yes" or "no" answer will not be awarded any points.

Question:	1	2	3	4	5	6	Total
Points:	16	15	14	15	19	11	90
Score:							

1. DNS Security (16 points)

Peer-to-peer DNS. Today's DNS is highly centralized and hierarchical. Alternative designs for name-to-address resolution have been proposed which aim for full decentralization instead. We consider one such design here, which we call **P2P-DNS**: in P2P-DNS, all authoritative name servers for all domains participate as equal *peers*. These N peers (assume that $N = 2^l$) are each assigned a unique l-bit identifier. Each peer stores the records (which are exactly the same as DNS records) for all domain names whose hashes start with the same l bits as the peer's identifier. If for instance $l = 4$ (in practice it would be much larger) and `hash`("`www.example.com`") = `10110110`..., then the peer with identifier `1011` would store the records for `www.example.com`.

A consequence of this design is that peers store records for which they are not authoritative: to keep them up to date, each peer regularly receives updates for all stored records from the corresponding authoritative name servers (i.e., from the domain owners). Additionally, popular records are automatically replicated across multiple peers, and if a peer becomes unavailable, other peers can detect this and take over its duties.

The P2P-DNS peers run a distributed protocol among them which allows routing to any peer in an expected number of hops $\mathcal{O}(\log N)$. A query works as follows: (1) a client sends a (plaintext) query over UDP to any peer; (2) the peers forward the query (based on the routing protocol) until the query reaches a peer that stores the corresponding record; (3) this peer replies via UDP directly to the original client providing the record the client requested.

(a) (7 points) You now have to compare P2P-DNS with traditional DNS.

i. (2 points) What advantage does P2P-DNS offer compared to DNS in terms of *resilience*?

ii. (3 points) What advantage and disadvantage does P2P-DNS have in terms of *privacy* compared to DNS?

iii. (2 points) What additional *integrity* concern does P2P-DNS cause compared to DNS?

(b) (4 points) Consider a variant of P2P-DNS based on DNSSEC rather than plain DNS, which we call **P2P-DNSSEC**. In P2P-DNSSEC, in addition to normal DNS records, the peers store DNSSEC cryptographic records (RRSIG, DS, DNSKEY, etc.) *for the entire DNSSEC hierarchy*, but other than that it works exactly like P2P-DNS. What are the main advantages and disadvantages of P2P-DNSSEC compared to P2P-DNS?

(c) (3 points) DNS can be leveraged for amplification attacks, a form of DoS attacks. Is P2P-DNS as described above (i.e., using UDP) vulnerable to amplification attacks? What about P2P-DNSSEC?

(d) (2 points) The design of P2P-DNS offers the opportunity to deviate from the query format of DNS: what would be a clean and simple way to protect P2P-DNS from cache poisoning attacks? (Excluding solutions that rely on authentication—we have P2P-DNSSEC for that!)

2. Web-Application Security (15 points)

(a) (6 points) Recall the same origin policy and its exceptions as applied by a web browser. Also recall how these exceptions enable Cross Site Request Forgery (CSRF) attacks. To counter the CSRF attack, one approach is to include a secret validation token in the webpage generated by the server.

A web developer working at Secure Bank (www.securebank.com) decides that he can use timestamps to defend against the CSRF attack. He intends to include a hidden field containing the current time stamp (the time on the server when the page was generated) in every web page served by the server:

```
<input type="hidden" name="auth_token" value="Thu Mar 4 11:00:00 EST 2010"/>
```

Now, whenever any form is submitted to the server, the server code checks that the `auth_token` is included and that its value is within 15 minutes of current time of the server (besides checking the session cookie). If the `auth_token` is missing or its value is more than 15 minutes off, the server rejects the transaction and requests the user to log-in again.

i. (2 points) Is this scheme secure? Explain why or why not?

ii. (2 points) Give a technique (different than the one above) to generate authentication tokens to defend against CSRF attacks.

iii. (2 points) Will the CSRF attack work if the server uses HTTPS? Explain why or why not?

(b) (9 points) The website of Secure Bank contains a search field for transactions. A user can input a transaction ID to get the details about that particular transaction. The transactions are stored in a single table in a SQL database. You discover that the search field is vulnerable to SQL injection and that the developers at Secure Bank left error reporting enabled, i.e., a user can see the errors returned by the SQL database. Assume there exists a second table named "cc_info", containing the credit card information for each customer of Secure Bank and that the website displays all records returned by a query. Describe in detail how you would perform an SQL injection attack to extract credit card information from other customers. Specifically, you should try to answer these questions:

- What type of SQL injection attack would you use?
- You may need to refine your query during the attack, how?
- How would you extract the data?

3. Botnets and DDoS Attacks (14 points)

(a) (5 points) On October 21, 2016, several waves of DDoS attacks against the DNS provider *Dyn* knocked dozens of popular websites offline, among them Twitter, SoundCloud, Spotify, and Reddit. More precisely, the authoritative name servers of certain domain names were attacked by a large number of *conventional* DNS queries (i.e., following the DNS protocol, no invalid messages, etc) from vulnerable devices ("bots") attempting to saturate the network resources that are close to the locations of the authoritative name servers. These bots are assumed to be hacked customer devices that reside in domestic networks behind correctly operating routers with NAT functionality.

Under this assumption, state whether preventing *source address spoofing* can help mitigate this attack. If so, explain how. If not, explain why not. Mention at least two different arguments.

(b) (3 points) Dyn reported "We observed 10s of millions of discrete IP addresses associated with the Mirai botnet that were part of the attack." This lets us conclude that the attack was not against the regular DNS infrastructure (i.e., not against the recursive resolvers), but directly against the authoritative name servers which were evidently overwhelmed and started dropping (also legitimate) queries. The reason for this conjecture is that the authoritative name servers would otherwise have seen the usual set of recursive resolvers only.

If this assumption is correct, how could the Dyn infrastructure be better protected? (Adding more power, more capacity, more servers, etc is not part of a correct answer).

(c) (6 points) The impact of the attack with respect to the public highly depends on the caching behavior of the recursive resolvers (which are typically used by the legitimate public).

i. (3 points) Explain in two sentences why caching and the time-to-live (TTL) play an important role here. (Hint: what happens if a cache entry expires? What impact does the TTL have on the effectiveness of the attack?)

ii. (3 points) Explain how a different TTL and a different caching strategy could mitigate the attack. Think of how the existing hierarchical structure of DNS could be leveraged better?

4. Public Key Infrastructure (15 points)

Recall that Certificate Transparency (CT) is a mechanism that makes issuance and existence of SSL/TLS certificates public for the examination by domain owners, Certificate Authorities (CA), and domain users. Figure 1 briefly explains how CT works.

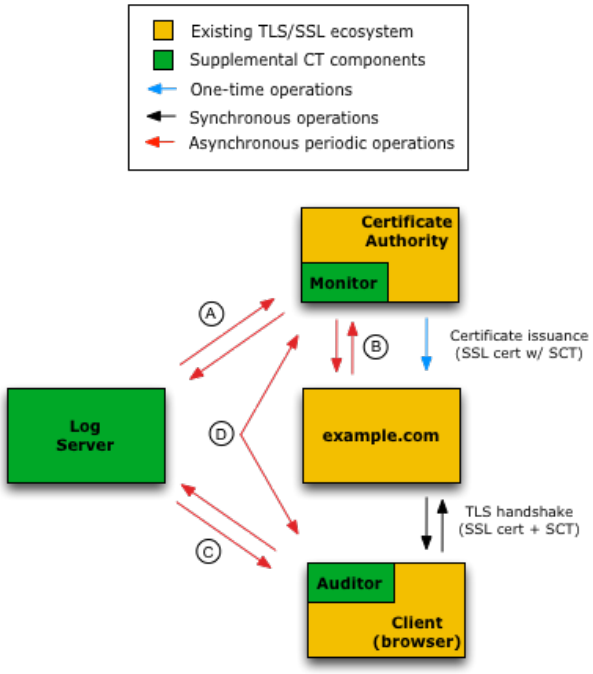

Figure 1: Certificate transparency. A: Monitors watch logs for suspicious certificates and verify that all logged certificates are visible. B: Certificate owners query monitors to verify that nobody uses illegitimate certificates for their domains. C: Auditors verify that a particular certificate has been logged. D: Monitors and auditors exchange information about logs to help detect malicious logs.

(a) (7 points) Signed Certificate Timestamps (SCT). During the certificate issuance, together with the SSL/TLS certificate, the CA also sends an SCT to the domain owner.

i. (3 points) What is the purpose of SCT? Which entity creates SCT? (Hint: The log server can only periodically update its log.)

ii. (4 points) What is the problem of issuing SCT if a malicious log server colludes with a malicious CA? How can this be detected?

(b) (6 points) A malicious log server can also launch a "branched log" attack (or "split world" attack). In this attack, a malicious log server maintains two versions of the log. For example, the log of version 1 contains a certificate *cert*, but the log of version 2 does not. The log server can then distribute logs of different versions to different requesters (monitor/auditor).

i. (3 points) Describe how a malicious log server can use the branched log attack to trick an auditor on the client side to accept an invalid certificate (e.g., a certificate from another compromised CA) without being detected by monitor on the benign CA.

ii. (2 points) Describe how step D in Figure 1 prevents the "branched log" attack.

iii. (1 point) Recall that the log server maintains the log as a Merkle hash tree. What information about the log does the monitor and auditor exchange?

(c) (2 points) What is the privacy problem of step C in Figure 1?

5. TLS (19 points)

(a) (5 points) We consider an enterprise network that connects to the Internet via a gateway G, as shown in Figure 2. The gateway G is deployed by the administrator of the enterprise network who wants to stealthily intercept TLS communications between an internal host (e.g., H_1 or H_2) and an external server S. G can decrypt TLS traffic and re-encrypt it after inspection. Essentially what G does is create a fake certificate of the server S and perform a man-in-the-middle (MitM) attack between the host and the server.

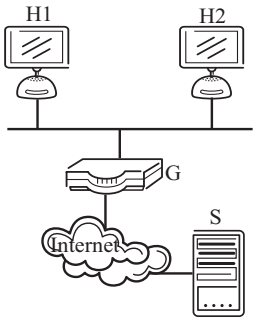

Figure 2: Enterprise network.

i. (2 points) Now consider H_1 initiates a TLS session to S. What modification has to be done on H_1 so that the user will not realize that an invalid certificate was created by G (i.e., the browser will not pop out a warning message)?

ii. (1 point) Can the server S detect such a MitM attack? Briefly justify your answer.

iii. (2 points) You are a student intern at this company, and you suspect that the company is intercepting your TLS traffic. What can you do to detect such an attack when you are using H_1?

(b) (10 points) The TAs and the instructors for the NetSec class have long term public-private key pairs. While preparing the exam, having to use the open campus wireless network, the TAs use a TLS-protected channel to discuss the questions and solutions to this exam. Shortly before the exam, the instructors and the TAs find out that their long-term private keys may have been learned by one of the students who came to their office hours. While they are sure that no communication about the exam took place since the compromise, they know that the students might have been actively listening on the communication channel in the past. For the following, comment on whether

the instructors should be worried that the exam solutions could have been leaked. Briefly describe why or why not they are secure.

i. (2 points) Anonymous Diffie-Hellman was used as a key exchange method, 128-bit AES, and 128-bit SHA-1 based MAC.

ii. (2 points) Ephemeral Diffie-Hellman was used as a key exchange method, 128-bit AES, and 128-bit SHA-1 based MAC.

iii. (2 points) Ephemeral Diffie-Hellman was used as a key exchange method, 40-bit DES, no MAC.

iv. (2 points) Fixed Diffie-Hellman was used as a key exchange method, 128-bit AES, and 128-bit SHA-1 based MAC.

v. (2 points) Fixed Diffie Hellman was used as a key exchange method, 40-bit DES, and 128-bit SHA-1 based MAC.

(c) (4 points) Bank x.com has a secure web site for its customers to log into their accounts. The bank wants to make sure that the username/password dialog is only shown on a TLS-protected page.

A customer accessing `http://www.x.com` is immediately redirected to the TLS-protected page `https://www.x.com`.

i. (2 points) Is there a difference in security between (a) typing `https://www.x.com` directly and (b) typing `http://www.x.com` and then being redirected to `https://www.x.com`? Briefly explain.

ii. (2 points) Present at least one reason why a bank would still want to redirect the login from an `http` site to a TLS protected page, instead of simply using only TLS-protected web sites?

6. Identity and Authentication (11 points)

Captive Portal. A *captive portal* is a popular solution to authenticate users to (insecure) public wireless networks in public places (e.g., airport, coffee shops). In this problem, we investigate possible security vulnerabilities of captive portal systems.

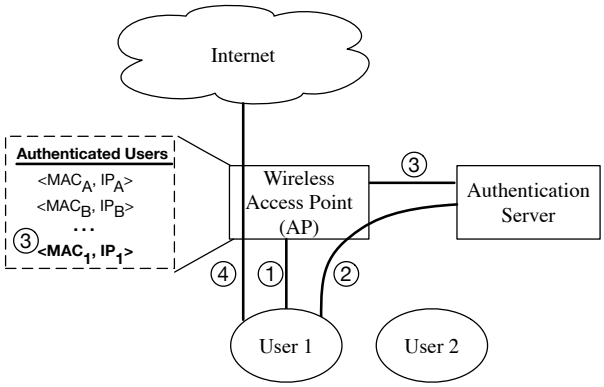

Figure 3: A simplified description of Captive Portal Systems

Figure 3 shows a simplified protocol description of a captive portal system. The following actions take place at the correspondingly enumerated steps:

1. *User 1* joins the wireless access point (AP). The AP assigns an IP address (IP_1) to *User 1*.
2. *User 1* is redirected by the wireless AP to the authentication server. The authentication server authenticates the user using information such as e-mail address, mobile phone number.
3. Once authenticated, the authentication server instructs the AP to whitelist the user. The AP adds the MAC address of the user's wireless interface (MAC_1) and the assigned IP address (IP_1) to the *Authenticated Users* table.
4. Upon receiving *User 1*'s traffic, the AP consults its list of authenticated users to verify the user and forwards his/her traffic to the Internet.

(a) (3 points) Assume that *User 1* has already authenticated to the public wireless network and is connecting to the Internet. Then *User 2* comes within the wireless coverage area of the AP. Can *User 2* see the packets between the AP and *User 1*? Why or Why not? If so, what information can *User 2* learn from the packets to/from *User 1*?

(b) (4 points) Is this system secure? That is, can *User 2* access the Internet without authenticating itself to the wireless network? If not, why is this impossible? If so, describe your mechanism step-by-step.

(c) (4 points) Which additional measure would you implement to further increase the security of this system? Discuss advantages and disadvantages of your proposal.

Extra Page

Please use this page in case you run out of space elsewhere in the exam.

Extra Page

Please use this page in case you run out of space elsewhere in the exam.