EP2500 Networked Systems Security
Homework 2 Problems Set

Total: 200 points. Required to pass: 110 points.

December 10, 2015

Deadline: 23:59 (UTC +1), January 4, 2016

Please send your solutions by e-mail to papadim@kth.se in PDF format from ONE of the team members. Please include in the PDF your names and a brief (5 lines max.) explanation of the contributions of each team member, as you see fit. Subject line of the email: `[NSS 2015 HW2] <your name 1, your name 2>`

Contents

1 Unauthorized Access

Exercise 1 Firewalls (20 pts.)

InSecure AB just hired you as their networked systems administrator. The network address of your new company is 17.0.0.0/8 and an internal web server is running on 17.0.0.1. The first thing you are asked to do is to secure the corporate network from intruders. Remembering your Networked Systems Security courses at KTH, you decide to setup a firewall; each firewall rule has the following form:

DIRECTION	SOURCE	DESTINATION	PROTOCOL	SOURCE PORT	DESTINATION PORT	STATE	ACTION
IN/OUT	Host or Network Address/*(ANY)	IP/HOSTNAME/*(ANY)	ICMP/UDP/TCP/*(ANY)	[1 to 65535] / * (ANY)	[1 to 65535] / * (ANY)	NEW/ESTABLISHED	ACCEPT/REJECT/DROP

If one (or more) field(s) is (are) not applicable for a specific rule, they can be left blank. For example, if you want to block ICMP traffic, there is no need to specify any source/destination ports.

The policy of the company includes the following rules:

1. *All incoming and outgoing ICMP packets should be dropped.*
2. *We do not accept any incoming traffic from our competitors. Their network address is 207.46.130.0/24 (Microsoft)*
3. *Our internal server can be accessed only through HTTPS.*
4. *The administrators can externally manage the web server via SSH.*
5. *The users of the internal network are allowed only to browse the Internet via HTTP and HTTPS.*
6. *We do not want our employees in the internal network to access Facebook (assume that the IP of Facebook is 69.171.239.12).*
7. *No other traffic is allowed.*

Assume that the default policy is **ALLOW-ALL**; in other words, unless you explicitly specify rules to reject packets, the packets will be accepted by the firewall.

1. What are stateless and stateful firewalls? Which type of firewall is better?

   Now that you understand the difference between stateless and stateful packet filters, it is time to implement some more complex policy rules. (hint: use the STATE field of the rules)

2. Please specify the rules needed to enforce this policy and briefly justify your design.
3. What is the difference between REJECT and DROP? Which one is preferred?
4. Describe briefly an attack that can circumvent the firewall (hint: consider DNS and WEB based vulnerabilities).

Answer of exercise 1

Q1

For first question check Unauthorized Access slides.

Q2

DIRECTION	SOURCE	DESTINATION	PROTOCOL	SOURCE PORT	DESTINATION PORT	STATE	ACTION
IN	*	17.0.0.1	TCP	*	443	NEW/ESTABLISHED	ACCEPT

DIRECTION	SOURCE	DESTINATION	PROTOCOL	SOURCE PORT	DESTINATION PORT	STATE	ACTION
IN	*	17.0.0.1	TCP	*	22	NEW/ESTABLISHED	ACCEPT

DIRECTION	SOURCE	DESTINATION	PROTOCOL	SOURCE PORT	DESTINATION PORT	STATE	ACTION
OUT	17.0.0.0/8	69.171.239.12	TCP	*	80/443	*	REJECT (/DROP)

DIRECTION	SOURCE	DESTINATION	PROTOCOL	SOURCE PORT	DESTINATION PORT	STATE	ACTION
OUT	17.0.0.0/8	*	TCP	*	80/443	NEW/ESTABLISHED	ALLOW

We must also allow DNS so that clients can resolve domain names.

DIRECTION	SOURCE	DESTINATION	PROTOCOL	SOURCE PORT	DESTINATION PORT	STATE	ACTION
OUT	17.0.0.0/8	*	UDP	*	53	*	ALLOW

All other traffic should be dropped.

DIRECTION	SOURCE	DESTINATION	PROTOCOL	SOURCE PORT	DESTINATION PORT	STATE	ACTION
*	*	*	*	*	*	*	REJECT (/DROP)

Q3
When we use REJECT we give information that there is a firewall that actually blocked this connection. This information can be used by the attacker. When we drop, an attacker cannot understand if the packet was dropped by a firewall or if the host does not exist. One could argue that security through obscurity is not a good strategy. Actually, this was an open-ended question.

Q4 As we saw during the recitations, packets can be encapsulated inside other packets. For example even if a firewall is blocking ICMP messages, then still these messages can go through by encapsulating them inside packets that are allowed by the firewall.

Exercise 2 Public Key Infrastructure (20 pts.)

Figure 1 shows a hierarchical PKI for a vehicular communications system scenario. Certification Authorities (CAs) are responsible for issuing certificates for different countries and parts of those countries. The European CA issues certificates for UK and Germany. Switzerland implemented its own CA and has a cross-certification relation with the European CA.

1. Would cars from Zurich be able to travel in UK? Explain the chain of trust (certificates) that a British car would check, if it received a Swiss certificate in London.
2. What actions should be taken and by which authority(ies), if the German CA gets compromised (i.e., its private key gets compromised).
3. In the above scenario, after the security breach, would cars from Zurich be able to communicate with cars in Munich? Why?
4. Suppose that a Swiss car V_{CH1} sends messages at a frequency of 4HZ. Each message includes the actual content m, a signature on m using a private key and a certificate signed by the Swiss CA, that includes the public key for the corresponding private key known only by the vehicle. The message has the following format: $m, sig(m), Cert_{CH1}$, where sig is the digital signature and $Cert_{CH1}$ is the certificate issued by the Swiss CA.

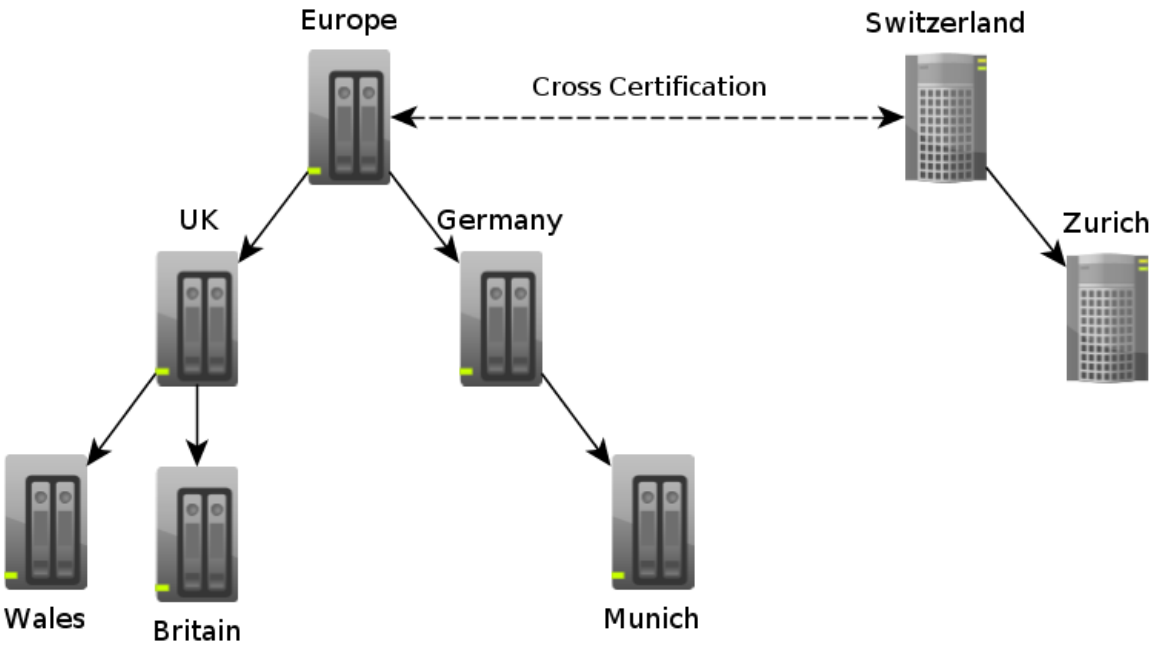

Figure 1: Vehicular PKI example

Suppose that V_{CH1} is identified as faulty and its certificate is revoked just after a CRL is published by the Swiss CA.

Explain how the CRL is used by the vehicles. Compute the period for the CRL publishing, so that the car is able to send no more than 1000 messages without its peers (other cars or road side units) knowing it is revoked. Assume ideal conditions, i.e., that the downloading of a CRL is instantaneous right after its publication by the CA and that all CRL-related processing is negligible.

Answer of exercise 2

1. Yes they would. The reason is that they both trust the European CA. In more detail a simple scheme would be the following: A Zurich car appeares in London and wants to communicate with the British cars. It broadcasts its message and its certificate appended to it. (Remember that a certificate in Vehicular Adhoc Networks: VANETS is usually a digital signature or a simple enryption of a public key from a CA.) In other words, the CA certifies that the public key sent is the correct one to decrypt/verify the message transmitted from the car. If the receiving car trusts the CA, then it will also trust the certificate (because it is signed/encrypted with the secret key of the CA) and consequently, it will trust the message itself.

   Back to question, the British car would be interested in learning if the CAs it trusts, indeed trust the certificate shown by the Zurich car. The chain of the checks would be: Britain (answer: check UK) -> UK (answer: check Europe) -> Europe (I trust Switcherland and thus Zurich so YES).

2. If a CA Z gets compromised, then the CA X which trusted Z must now declare that it NO longer

trusts that certificate (using revocation lists). Therefore in this example Europe should revoke the German certificate and consequently all the certificates of the CAs below germany.

3. If no further actions where taken after the breach then no. see 2.1
4. First, the signature on Certificate Revocation List (CRL) should be verified using the public key of the Certificate Authority (CA). Then, the certificate validity is checked, i.e., if the ceritfiate serial number exists in the CRL. If it is valid, check the signature of certificate. The answer is 1000/4=250 seconds.

2 Secure Routing

Exercise 3 Secure Link-State Routing (30 pt.)

Consider the autonomous system shown in Fig. 2, where nodes A,...F, are routers running a link state protocol. OSPF (Open Shortest Path First) is such a protocol. However, for this problem it is not necessary to consider or recall the details of OSPF. It suffices to consider a generic link state operation: (i) each router discovers its neighbors, (ii) it determines the cost of its incident links, and (iii) it broadcasts across the network, periodically or when there is a change in link cost, a link state update (LSU), a message that "advertises" the state of these links. (iv) Each router retransmits once each new LSU messages it receives. Then, (v) each router, having the state of the latest link state of the entire network, calculates the shortest path to all other routers.

Assume the shown network is stable, i.e., no links are fluctuating, and that all routers have the same link state. Moreover, assume that both routers incident on a link determine the same cost. E.g., for the link connecting D and F, that is (D, F), the two costs are $cost(D, F) = cost(F, D) = 5$.

a) Compute the shortest paths from D to every other router. You are free to use any algorithm you wish. Please redraw the topology and show the paths.

b) Assume that B is a faulty router, e.g., it malfunctions and it transmits once a link state update that erroneously advertises $cost(B, A) = 1$ and $cost(B, C) = 1$. Assume that A and C ignore this LSU but E retransmits it. Eventually, the erroneous LSU arrives at D that recalculates its shortest paths. Explain what happens to data originating D and destined to A.

c) Again in the presence of the faulty router, consider now C and A transmitting again their LSU messages, including the correct costs for the (C, B) and (A, B). Explain what will later happen to data originating D and destined to A. Is this positive or negative?

d) Assume now that all routers in the network can digitally sign their LSU messages, and that all other routers can validate these signatures. Assume they all can verify that the signer's public key is indeed the signer's. What is necessary for this to be possible?

e) With signed LSUs, what is necessary so that every router receiving a digitally signed LSU can validate its freshness? What else can the receiving router verify thanks to the digital signature?

f) Can signed LSUs prevent the effect of the malfunction in (b) above? If so, please explain how. If not, is there a benefit digital signatures offer against malfunctioning routers?

g) Consider now that B is under the control of an adversary. Assume that it announces deliberately that link (B, F) is up and its $cost(B, F) = 1$. What would be the effect for data traffic originating D and destined to A?

h) In the presence of the adversarial, malicious B, F advertises soon afterwards that (B, F) is down. Does this solve the problem? What if B persists with the fake link and LSU?

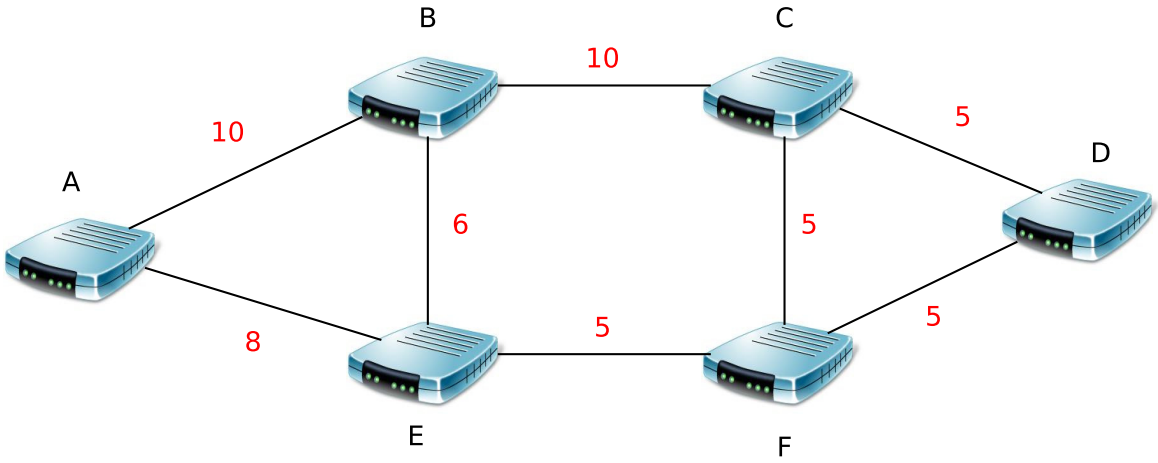

Figure 2: Wired network topology. Labels over links indicate routing costs.

Answer of exercise 3

a) D, C, B (cost 15) and D, F, E, A (cost 18)

b) The shortest path now becomes D, C, B, A, cost 7, and D-to-A data go over the malicious router. (do all paths go through B?)

c) This is positive, as D will get again the correct values and recalculate the shortest path to A, which is D, F, E, A and avoids the misbehaving routers.

d) PKI/CA and knowledge of certificates of the senders (signing routers).

e) A sequence number and/or timestamp is needed. the receivers can verify the integrity/auth of the LS. Pinpoint the senders (non-repudiation) and later possibly have then evicted.

f) partly, it can help the identification of possibly offending nodes. but the false advertisement is possible.

g) it will now take the D, F, B, A path of cost = 16 < 18 (actual shortest path). But there is no existent path, so traffic is dropped. Or the F router knows it does not have the link to B and uses F-E link. Both answers correct ...

h) yes, if B does not persist, not really, as long as B persists, it would if the protocol used the two inconsistent links to disqualify links.

3 Data Plane Attacks

Exercise 4 CASTOR (30 pts.)

Alice (A) and Bob (B) are relaying packets in an untrusted network using the Continuously Adapting Secure Topology-Oblivious Routing (CASTOR) protocol[1].

In CASTOR each packet contains the following fields:

$$(A, B, H, b_k, f_k = (x_1, \ldots, x_l), e_k, M) \tag{1}$$

where H is the *flow identifier*, b_k is the *packet identifier*, f_k is the *flow authenticator* used for verifying that the packet belongs to the flow H, e_k is an *encrypted ACK authenticator*, while M is the payload.

Alice and Bob will forward the packets if and only if they belong to the flow H. To verify a packet, the intermediate node checks whether

$$h(\ldots h(h(h(b_k)||x_1)||x_2)||\ldots x_l) = H \tag{2}$$

i.e., if $h(b_k)$ is a leaf of the Merkle tree with root H. The operator $||$ is the string concatenation.

NOTE: Alice and Bob are using an 8-char truncated Message Digest v5 (MD5) hash function[2]. That is:

$$\begin{aligned} \text{MD5}('\text{NSS}') &= \textbf{248cdc66}\text{c441a6612309f6e2ce80a63c} \\ h('\text{NSS}') &= 248\text{cdc66} \end{aligned}$$

1. Bob received the first packet of the flow containing
   - $H = \text{efe50337}$
   - $b_k = 50\text{d}02858$
   - $f_k = (\text{c7e2b366}, 23\text{f}140\text{ad}, 95294\text{aec}, \text{a4745acb})$

   Will Bob forward the packet b_k? Justify the answer.
2. Alice instead received the first packet of a new flow containing
   - $H = 12328\text{e}72$
   - $b_k = 07\text{fd}01\text{d}5$
   - $f_k = (5\text{a}9\text{d}0480, 93\text{aded}1\text{d}, \text{d}97\text{d}3412, 414833\text{e}5)$

   Will Alice forward the packet b_k? Justify the answer.

[1] Castor: Scalable Secure Routing for Ad-hoc Network

[2] You can find an online hash calculator here or use the `md5sum` command line utility (in the text format)

Answer of exercise 4

1 Yes.

$$
\begin{aligned}
H &= H' \\
H &= h(h(h(h(h(b_k)||x_1)||x_2)||x_3)||x_4) \\
efe50337 &= h(h(h(h(h(50d02858)||x_1)||x_2)||x_3)||x_4) \\
efe50337 &= h(h(h(h(045afeae||c7e2b366)||x_2)||x_3)||x_4) \\
efe50337 &= h(h(h(a7626801||23f140ad)||x_3)||x_4) \\
efe50337 &= h(h(1461c8e3||95294aec)||x_4) \\
efe50337 &= h(9cb546a7||a4745acb) \\
efe50337 &= efe50337
\end{aligned}
$$

2 No.

$$
\begin{aligned}
H &\neq H' \\
H &\neq h(h(h(h(h(b_k)||x_1)||x_2)||x_3)||x_4) \\
12328e72 &\neq h(h(h(h(h(07fd01d5)||x_1)||x_2)||x_3)||x_4) \\
12328e72 &\neq h(h(h(h(0561a9ca||5a9d0480)||x_2)||x_3)||x_4) \\
12328e72 &\neq h(h(h(833f7176||93aded1d)||x_3)||x_4) \\
12328e72 &\neq h(h(c30c554b||d97d3412)||x_4) \\
12328e72 &\neq h(70779187||414833e5) \\
12328e72 &\neq ede9aa5f
\end{aligned}
$$

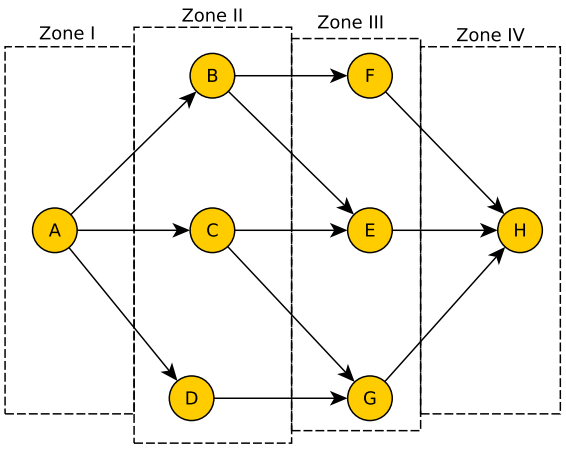

Figure 3: Network Setup

Exercise 5 Data Plane Attacks (20 pt.)

Consider the network of Figure 3. Assume all nodes make a purely random routing choice and an adversary who captures nodes, in order to intercept network traffic. **When a node is captured, all packets going through the node are dropped.**

1. Suppose the adversary captures node C. What is the probability that a packet sent from A to H will be dropped?
2. Now, suppose that the adversary captures node E. What is the probability that a packet sent from A to H will be dropped?
3. When a packet is received H sends back an acknowledgement (ACK) to A, following again the random routing policy. What is the probability that an ACK will be dropped, if E is captured? Show an example route for the original packet and the ACK (hint: Be aware of our adversarial model).

Moreover, the network is divided in areas according to the required effort to capture one node. To quantify the adversarial effort, consider the following values per field: Zone I$\mapsto$3, Zone II$\mapsto$2, Zone III$\mapsto$0.5, Zone IV$\mapsto$3.

4. If the adversary has resources with value 0.5 to capture nodes, which tactic would maximize the adversarial benefit?
5. If the adversary has resources with value 2 to capture nodes, which nodes should be captured to have at least 90% probability to drop a packet sent from A to H.
6. Given your choice in 4, what is the expected amount of dropped traffic (in bytes) by the adversary after 10 minutes, if A sends 1 byte per minute.

notes: For calculations set your precision to two decimals when necessary. The arrows of the figure show the possible routes for packets. For ACKs you can reverse the arrows. Do not consider jamming. For all your answers you must show your work and calculations.

Answer of exercise 5

1. One out of three possible routes, 0.33.
2. Routes ABE and ACE, so: $0.33 \times 0.5 + 0.33 \times 0.5 = 0.33$
3. The possible routes are: ABFHE, ADGHE and ACGHE, so probabilities calculated as above. The packet has to reach H in order to generate the ACK.
4. F: 0.165, E: 0.33 and G: 0.495. So, G should be captured.
5. All nodes of zone III.
6. 5 bytes

4 Domain Name System (DNS) Security

Exercise 6 Birthdays (20 pt.)

Read *DNS Cache Poisoning - The Next Generation*, http://www.secureworks.com/research/articles/other_articles/dns-cache-poisoning/ (up to and including the first attack).

1. What is the Birthday paradox?
2. Why is the BIND birthday attack so much more effective than regular conventional spoofing?
3. Using the article's formula for the probability of collision, what is the required number of spoofed replies ("n number of spoofed replies for n queries") needed to achieve at least 25% chance of collision?

Answer of exercise 6

1) The birthday paradox is the name given to the probability to find collisons when you pick k elements out of n possible. It is called a paradox because the probability is much higher than the intuitive answer.

It is called the *birthday* paradox because the illustration that is often used is to answer questions like "How big a class of students do you need for an at least 50% probability that two students share the same birthday?" Some would answer 183 students (since there are 366 possible dates), but the answer is just 23.

2) Since multiple queries are sent, the spoofed replies only need to match one of them. The chance of such a collision is much greater.

3) 195.

$$P_{\text{collision}} = 1 - \left(1 - \frac{1}{t}\right)^{\frac{n(n-1)}{2}} \tag{3}$$

with $t = 65535$. To simplyfy calculations, approximate to

$$P_{\text{collision}} \approx 1 - \left(1 - \frac{1}{t}\right)^{\frac{n^2}{2}} \tag{4}$$

and solve for n,

$$\frac{1}{4} = 1 - \left(1 - \frac{1}{t}\right)^{\frac{n^2}{2}} \tag{5}$$

$$\frac{3}{4} = \left(1 - \frac{1}{t}\right)^{\frac{n^2}{2}} \tag{6}$$

$$\ln\left(\frac{3}{4}\right) = \frac{n^2}{2}\ln\left(1 - \frac{1}{t}\right) \tag{7}$$

$$n = \sqrt{2\frac{\ln\left(\frac{3}{4}\right)}{\ln\left(1 - \frac{1}{t}\right)}} \tag{8}$$

$$n \approx 194.18 \tag{9}$$

And verifying our answer in (3) yields

$$P_{\text{collision}}(n = 194) \approx 0.24849 \tag{10}$$

$$P_{\text{collision}}(n = 195) \approx 0.25071 \tag{11}$$

which verifies that $n = 195$ is our solution.

Exercise 7 DNSSEC (15 pt.)

1. What is the difference between DNSSEC and DNS?
2. What problems does DNSSEC solve?
3. If legitimate sites use SSL with valid certificates, why will we still need DNSSEC?
4. Why do we want authenticated denial of existence replies? Why do they need to contain information about the query it is a reply to?

Answer of exercise 7

1) The key diffreence is that DNSSEC signs (authenticates) replies. Note that it does not provide confidentiality.

2) It solves problems related to attacks where an untrusted adversary injects or changes DNS replies. The user can now, to the extend she trusts the CAs, trust the reply, not just "it usually works".

3) If the uncareful user is presented a simple http connection instead, few will notice. With no certificate to invalidate, SSL becomes more or less useless.

Also, as said on unixwiz.net[1], *"But the bad guy can subvert even SSL: since many Certificate Authorities validate a user's control over a domain by sending email, hijacking a mailserver by attacking the cert vendor's resolving DNS, this may well mean that an attacker can obtain a fully-valid certificate for the target domain."*

4) By answering a DNS query by a does-not-exist, the attacker can trick the user into believeing that that host does not exist. DNSSEC prevents these attack elsewhere, so it is sensible to prevent them here too.

[1] http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html

5 Web Security

Exercise 8 Securing Web Services (40 points)

The KTH library wishes to launch a web service for students to check-out (purchase or borrow) e-books on-line. You were hired to design and implement the security for this project. The KTH library administrator informed you that students were already issued with an electronic ID: a smartcard containing the student's private key and her/his certificate. All such student certificates are produced by the *KTH certification authority*, CA_{KTH}, which, of course, produces and distributes the certificate of the KTH library web-server.

Please answer the following questions (under the aforementioned assumptions, refraining from stating that the students could simply use their usernames and passwords, as you currently do). Please refrain from simply stating that "standardized protocol such and such" could be used; rather, spell out your protocol(s). Please state briefly but explicitly your assumptions and justify them:

1. Alice, a student, wishes to check-out an e-book. Please describe the authentication protocol between Alice (actually, her smartcard, which you can assume attached to her laptop) and the KTH e-library web server. Your protocol must ensure integrity and freshness and reassure Alice that it actually interacts with the KTH library server.
2. Augment your protocol in the previous step to ensure that, in addition, the communication remains confidential; Alice does not want an eavesdropper to know her choices of books and she does not want to make any assumption on the security of the underlying network protocols.
3. After partying hard, Bob, unfortunately, forgot his wallet in the bus on his way home. For the smartcard-based system, this implies his credential must be revoked. Describe why, what is the vulnerability? Then, describe how the revocation can be done. How would this functionality be integrated in the protocol you proposed at the first step of this exercise?
4. The previous incident (fortunately, still, a beta under evaluation with a limited number of users and resources) gets the administrator worried - asking you now to strengthen the system: loss of a card should prevent anyone (while she/he possibly can) from using it to impersonate the legitimate user and check-out any e-book. How can you strengthen the system to achieve that while, for example, the unfortunate user has not yet realized the loss of his/her card?
5. Once the new KTH system gains traction, the Stockholm University (SU) adopts the same system! But, needless to say, it administers its students/users of its new system separately (i.e., CA_{SU} issues and manages credentials). What needs to be done if KTH and SU want to enable their students to check-out e-books from each others e-libraries?
6. Describe the authentication between Alice (KTH student) and the SU e-library web server.
7. Based on this success, KTH now wants ERASMUS students to be able to use the new web-service. Unfortunately, the library administrator informs you that ERASMUS students cannot be provided KTH digital IDs and smart cards. Instead, they will have to use usernames and passwords. The

database containing the ERASMUS students' usernames and passwords is shown below. What problem(s) do you see? How can you address it(them)?

username	password (MD5 output; input: user provided password)
Greta	d739111b266f6ec2f72c0b5740a6f374
Maria	60dc9346ca65100c31326993df44dd9e
Sylvie	60dc9346ca65100c31326993df44dd9e

8. Finally, the administrator provides you with the piece of (JAVA) code shown below; this performs the authentication of ERASMUS students. Is there any problem? If yes, how can you address it?

```
conn = pool.getConnection();
String sql = "select * from user where
      username='" + username +"'
      and password='" + password + "'";
stmt = conn.createStatement();
rs = stmt.executeQuery(sql);
if (rs.next()) {
loggedIn = true;
        out.println("Successfully logged in");
} else {
        out.println("Invalid credentials");
}
```

9. *Extra credit, up to 15 points; beyond the 80 points for this exercise and the HW set 2 total* Please provide your comments regarding standardized technologies, possibly widely used, that could solve parts (or all?) of the above problems. Please be brief and technically precise.

Answer of exercise 8

a) Here you had to design a challenge/response protocol leveraging asymmetric cryptography. The idea is that Alice with her private key should generate a signature of a challenge provided by the server.

b) Besides the authentication protocol of the previous question here you have to establish a session key. The session key can be generated by Alice and should be sent to the server encrypted with the server's public key.

c) The certification authority of KTH (CA_{KTH}) should include Bob's certificate to its Certificate Revocation List (CRL). The CRL must be, of course, accessible by the server.

d) Two factor authentication is an acceptable answer here. One option would be to protect the smartcards with a PIN. Additionally, combining TLS authentication with passwords would also work.

e) To implement such a system you would have two options:

- Assume a higher-level CA that would issue certificates both for CA_{KTH} and CA_{SU}.
- Establish a cross-certification scheme where each CA issues certificates for the other.

f) Here you have describe the process of verifying the certificate of a user by checking the whole certificate chain.

g) Passwords must be both hashed and salted

h) Of course, this piece of code is vulnerable to SQL injection. Prepared statements and stored procedures could be used to avoid this.

i) Here we wanted to see keywords like TLS, stored and salted passwords, CRLs, cross-certification, stored procedures and prepared statements.

6 Web Security and Privacy

Exercise 9 k-Anonymity (5 pts)

A football team in Stockholm provided you with the following table that contains some of its players and the number of goals they have scored.

First Name	Family Name	Age	Goals
Jimmy	Durmaz	28	12
Sebastian	Larsson	32	18
Jimmy	Wernbloom	28	12
Renne	Larsson	29	7

You were asked to **2-anonymize** the table. This means that you will have to suppress data (i.e., substitute them with *) so that the resulting paper will have 2 pairs of identical rows.

Answer of exercise 9

First Name	Family Name	Age	Goal
Jimmy	*	28	12
*	Larsson	*	*
Jimmy	*	28	12
*	Larsson	*	*