Final exam in

Computer Security EITA25

Department of Electrical and Information Technology
Lund University

March 12, 2018, 8-13

- You may answer in either Swedish or English.
- If any data is lacking, make (and state) reasonable assumptions.
- Use legible hand writing. If your answers cannot be read, you will receive zero points on that problem.
- Only pencil and eraser is allowed.
- Grading is done as follows.
  Grade 3 = 20–29 points,
  Grade 4 = 30–39 points,
  Grade 5 = 40–50 points.

Problem 1. Consider the following permissions on a file in Windows. Determine for each case if Alice, who is member of group Students, can *read* the file or not.

a) User Alice has file permission "write", group Students has file permission "read + write".

b) User Alice has file permission "read", group Students is denied permission "read".

c) Parent folder has share permission "read" for everyone and file has file permission "write" for Alice. Alice accesses the file over the network.

Answer
a) Yes b) No c) No (1+1+1 points)

Problem 2. Stream ciphers require IVs for practical use. What is an IV and how does it improve the security of stream ciphers?

Answer
It is a *public* initialization vector that is unique for each keystream generated under a given key. It is used to make sure that two different plaintexts, p_1 and p_2, are always encrypted using different keystreams. Adding two ciphertext bits, c_1 and c_2, encrypted with the same keystream bit, will leak information about the corresponding plaintext bits.

$$c_1^i \oplus c_2^i = k_1^i \oplus k_2^i \oplus p_1^i \oplus p_2^i = p_1^i \oplus p_2^i$$

(3 points)

Problem 3. Explain how powersets and subset relations can be used as a means for access control. Give a specific example where information flow integrity can be provided using these partial orderings.

Answer
The powerset is the set of all subsets of a set. Using powersets we can define a partial ordering such that $a \leq b$ if $a \subseteq b$. By labelling subjects and objects using an element in the powerset, we can control access through the partial ordering. To achieve information flow integrity, we only allow information to flow downwards in a hierarchy. Thus, subjects can only write information to objects lower in the hierarchy (or at the same level), and subjects can only read information from objects higher in the hierarchy (or at the same level). This can be useful in any setting where we wish that information should not be confidentiality protected but the accuracy of the information is important. It is e.g., used by letting users lower the integrity level of internet explorer such that it (or malware running with its privileges) can not make modifications to the rest of the computer. It can only write to a specific folder which has also a lower integrity level. However, the process can still read regular folders on the computer. (3 points)

Problem 4. In TLS, the premaster secret (PMS) is used to compute the encryption keys by first computing the master secret (MS) as

`MS = PRF(PMS, ‘‘master secret’’, ClientRandom` $\|$ `ServerRandom)`

and the computing the keyblock as

`keyblock = PRF(MS, ‘‘key expansion’’, ClientRandom` $\|$ `ServerRandom).`

The encryption key is then extracted directly from the keyblock. For this problem, we can model the PRF as just a hash function. One reason to have the ClientRandom and ServerRandom is to protect against time memory tradeoff attacks that attempts to reconstruct the premaster secret (though the most important reason is to protect against replay attacks). Describe how to build the precomputed tables needed in a time memory tradeoff attack, both with and without the random numbers present in the protocol. Assume that a block cipher in ECB mode is used to encrypt data. HINT: You will need to do a chosen-plaintext attack on the block cipher.

Answer
Assume that there is no randomness in the functions above. Then we can model the mapping from PMS to key k as a hash function with fixed input, $k = h(PMS)$. In a chosen-plaintext on the block cipher, we can model the mapping from key to ciphertext as $c = h'(k)$. Thus, the one way function we wish to invert is $c = h'(h(PMS)) = h''(PMS)$. When building the tables, we start with a PMS in our search space of size N and generate the corresponding ciphertext. Then we use a reduction function R_i to map the ciphertext to a new PMS in the search space and so on in order to build the chains. After t steps a new chain is built. This is repeated m times and when $mt^2 = N$, a new reduction function is chosen and a new table is built with this function.

If there is randomness, the approach is very similar, but instead of letting the tables cover only the PMS, it must cover both the PMS and the randomness since the randomness used

in a particular handshake will not be known when the tables are built. Thus, the randomness significantly increases the complexity of the attack. (3 points)

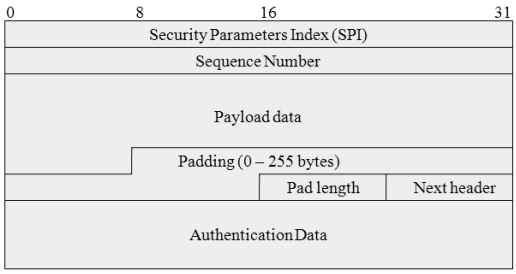
Problem 5. Explain the difference between real UID and effective UID in Linux. What are they used for?

Answer
The real UID is the UID of the logged in user. It is used to identify the logged in user in case the effective UID is temporarily changed. The effective UID can always be changed to that of the real UID. The effective UID is used for access control. Access rights for files are compared with the effective UID for the user. (3 points)

Problem 6. An ESP packet used in IPsec is given below.

a) Which part of the packet is encrypted?

b) Determine the location of the original IP header in *tunnel mode* and *transport mode* respectively.



Answer
a) The payload data, padding, pad length and the next header field.
b) In transport mode, the original IP header is placed before the ESP header, i.e., before the data represented by the packet in the figure. In tunnel mode, the original IP header is part of the payload data in the figure.

(1+2 points)

Problem 7. Explain the difference between the terms empirically secure, provably secure and unconditionally secure.

Answer
Empirically secure is a cryptographic algorithm that has not been broken despite repeated attempts to break it. It can be said to have withstood the test of time. A provably secure cryptographic algorithm can be shown to be secure if also another, well-known and difficult, problem can not be solved, e.g., factoring the product of two large primes or solving the discrete log problem. An unconditionally secure cryptographic algorithm can be shown not to be breakable under any circumstances. (3 points)

Problem 8. In order to have integrity protection of the messages in WEP, CRC-32 is used. The linear function CRC-32 is used to compute an integrity check value (ICV) of the message. The ICV is appended to the message and the resulting bitstring is encrypted using a stream cipher. To verify that the message has not been changed during transmission, the recipient decrypts the bitstring, computes the ICV of the message using CRC-32 and compares it to the value in the decrypted bitstring.

Assume that you can intercept these encrypted bitstrings, change them, and forward them to the intended recipient. Explain how you could flip the first and the last bit of the message without the recipient being able to detect this when checking the integrity of the message.

Answer

Since the function is linear we have that CRC-32$(M \oplus \Delta)$ = CRC-32(M) $\oplus$ CRC-32(Δ). The transmitted bitstring can be written as $M \| \text{CRC-32}(M) \oplus RC4(K)$. Our goal is to change M to $M \oplus \Delta$ where $\Delta = 100\ldots001$. Since we do not know the key K we do not know M or CRC-32(M). Instead we can compute CRC-32(Δ) and add these bitstrings to the received bitstring. Then the receiver will get

$$\begin{aligned} & M \| \text{CRC-32}(M) \oplus RC4(K) \oplus \Delta \| \text{CRC-32}(\Delta) \\ = \; & (M \oplus \Delta) \| \text{CRC-32}(M) \oplus \text{CRC-32}(\Delta) \oplus RC4(K) \\ = \; & (M \oplus \Delta) \| \text{CRC-32}(M \oplus \Delta) \oplus RC4(K) \end{aligned}$$

which will be accepted at the receiver side since the ICV is correct. (3 points)

Problem 9. The Linux program /bin/passwd can be used to change a user's password. Explain how this program is an example of controlled invocation and how this controlled invocation is realized in Linux.

Answer
The user is not allowed write access to the file that stores the list of hashed passwords. Still the user must be allowed to make changes to this file when updating his password. At the same time we can not allow the user to just make any changes, we (the system) have to carefully control how the changes are made. The solution is to write a program that makes the appropriate changes and then let the user run this program. This is the concept of controlled invocation. In order to give the program write access to the file we use the setuid functionality which allows the program to run with the access rights of the program owner. If the program is owned by root the program will have root privileges and can thus write to the file. (3 points)

Problem 10. Explain the concept of a *threshold* in biometric authentication. Also, what are the consequences, inte terms of FAR and FRR, of choosing a certain threshold?

Answer
The threshold is used to determine how accurately a biometric sample must match a template in order to accept a user. A high threshold will increase the probability that valid users are denied access (increase FRR) but it will lower the probability of falsely accepting the wrong user (decrease FAR). A low threshold will have the opposite effect. (3 points)

Problem 11. Windows provides a so-called *trusted path* during logon.

a) What is a trusted path and what attack does it defend against?

b) The trusted path in a) is actually called "*Secure Attention Sequence* (SAS)" in Windows. The term trusted path was defined in the Orange book. What is the Orange book and what is/was its *motivation*?

c) Common Criteria has pretty much the same purpose as the Orange book. Give two important differences between them.

Answer
a) A trusted path is a way of ensuring that users are communicating with the intended recipient. It defends e.g., against spoofing attacks, where someone creates a faked login program in order to capture passwords.

b) The Orange Book was the first initiative to evaluate operating systems. The purpose was to help developers making secure systems and also to help users to acquire secure systems.
c) While the Orange Book combined functionality and assurance, Common Criteria attempts to partly separate this using protection profiles. Moreover, Common Criteria is valid internationally and comes with a (quite significant) fee, while Orange Book evaluations where only valid nationally and were conducted for free. (1+2+2 points)

Problem 12. In the Appendix you will find a recent news article from Bleeping Computer, including a timeline of events. Read the article.

a) Explain why a CA can issue certificates to a website without being in possession of the private key.

b) Explain how Trustico could have proved possession of the private keys without sending them in an email to DigiCert.

c) Explain to which extent Trustico can mount passive attacks on the TLS sessions that their customers have with end users. How does the attack differ between RSA and Ephemeral Diffie-Hellman handshakes.

Answer
a) The CA only needs to know that the public key actually belongs to the website. For this, the private key is not needed, the party requesting the certificate only needs to show that it controls the domain, which can be achieved in several ways, e.g., showing that it can add things to the web server, send emails or add records to the DNS.
b) One simple variant would have been to sign a string using the private keys and submit the certificate used to verify the signature. If DigiCert can validate the signatures, then they can also be certain that Trustico have the private keys.
c) Since Trustico have the private keys they can, in the case of RSA, decrypt the pre-master secret and learn the encryption keys. In the case of Ephemeral Diffie-Hellman a passive attack would not be possible since learning the encryption keys would require them to solve the discrete log problem. (1+2+2 points)

Problem 13. Describe the following five terms, in the context of *Buffer Overflow attacks*. For b)-e), also describe its purpose related to the attack.

a) Return address

b) NOP instructions

c) Canary

d) ASLR

e) W $\oplus$ X

Answer
a) The return address points to the place in memory where execution will continue upon finishing a subroutine. The goal in the attack is to overwrite this address.
e) NOP instructions are instructions that do not change the state of the processor. Their purpose in a buffer overflow attacks is to allow some errors when guessing the address to overwrite the return address with. As long as execution jumps somewhere in a sequence of NOPs, the attack will still succeed.

c) A canary is a piece of known data, placed before the return address on the stack. Its purpose is to detect if the return address has been overwritten.
d) ASLR is a mechanism to randomize the memory layout for a process. Its purpose is to make it difficult for an attacker to guess what memory address to use when overwriting the return address.
e) W $\oplus$ X is a mechanism for tagging memory such that it is either writeable or executable. Its purpose is to make it impossible for an attacker to have injected code on the stack executed.

(1+1+1+1+1 points)

Problem 14. Explain shortly the following five terms:

a) Mandatory Access Control

b) Message Authentication Code

c) Nonrepudiation

d) Challenge-Response

e) LM hash

Answer
a) An access control mechanism, where access is based on the security level of subjects and objects.
b) A symmetric cryptographic function that ensures the integrity and authentication of data.
c) The property of not being able to deny having sent (or received) some information.
d) An authentication scheme that avoids sending any secrets in plaintext on a channel.
e) An old hash function that was used to store passwords in Windows systems, having limitation such as not supporting lower case characters and dividing passwords into independent chunks which could be broken separately. (1+1+1+1+1 points)

23,000 Users Lose SSL Certificates in Trustico-DigiCert Spat

By

Catalin Cimpanu

- February 28, 2018
- 06:30 PM
- 11

Over 23,000 users will have their SSL certificates revoked by tomorrow morning, March 1, in an incident between two companies —Trustico and DigiCert— that is likely to have a huge impact on the CA (Certificate Authority) industry as a whole in the coming months.

The entire saga started earlier today when DigiCert, one of the biggest certificate issuers on the Internet, sent emails to over 23,000 customers who obtained their SSL certificates through a UK reseller named Trustico.

DigiCert said that because of a security incident, they had to revoke all certificates issued to Trustico, which Trustico later sold to its own customers. Trustico General Manager Zane Lucas, on the other hand, denied that his company suffered any security incident.

At this point, it all become too complicated, so we'll just lay out a timeline of events, based on statements made by both companies, at the time of writing.

Timeline of events

⇨ **1)** On February 2, Trustico sent an email to DigiCert, asking DigiCert to revoke all certificates —around 50,000— managed by DigiCert.

⇨ **2)** Trustico drops its contract to resell Symantec certificates (now part of DigiCert) and starts a partnership with Comodo.

⇨ **3)** DigiCert denies the request to mass-revoke 50,000 certificates. DigiCert said that industry rules are not clear if a "certificate reseller" can revoke its customers' SSL certs, or only the end customer can do so alone.

⇨ **4)** Trustico says DigiCert decided to terminate its contract with Trustico on February 25, after Trustico said it would intend "to seek a legal opinion" on the matter.

Speaking to Bleeping Computer today on Twitter, a DigiCert employee confirmed the contractual obligation between the two companies was ending in 30 days.

⇨ **5)** In regards to the actual certificates, DigiCert says it told Trustico that they could mass-revoke certificates if there was evidence of a security incident during which the customers' private key were compromised.

⇨ **6)** DigiCert claims that on February 27 it received an email from Trustico containing over 23,000 private keys for Trustico customers SSL certificates.

⇨ **7)** In accordance with the CA industry rules that mandate that compromised certificates be revoked in 24 hours after a security incident, DigiCert started the certificate revocation process for the 23,000 compromised certs it received via email.

⇨ **8)** Earlier today, DigiCert sent emails to over 23,000 Trustico customers stating that their certificates would be revoked. It is unclear if DigiCert was allowed to mass-email Trustico's customers.

⇨ **9)** Several security experts have publicly accused Trustico of allegedly logging copies of SSL certificate private keys. Certificate authorities —the companies that issue SSL certificates— aren't supposed to have copies of these private keys.

Even DigiCert's COO —Flavio Martins— showed his surprise that Trustico sent an email containing the private keys of over 23,000 of its customers.

The general theory among professionals —unconfirmed at this point— is that Trustico had automated the CSR (Certificate Signing Request) process, a step in the certificate issuance process, and was generating SSL certificates, but also keeping a copy of the private key.

⇨ **10)** DigiCert notifies Mozilla of the compromise of 23,000 private keys, promising to publish the private keys at a later date, so they can be untrusted by browser makers.

⇨ **11)** Trustico answers DigiCert's report. Trustico says there was no security incident.

"At no time had any private keys been compromised, nor had we ever informed to you that any private keys had been compromised," Lucas said.

Trustico did not explain the origin of the 23,000 private keys. The company also did not reply to a request for comment sent by this reporter.

⇨ **12)** Trustico says the reason it wanted to revoke the 50,000 DigiCert certificates is because of Symantec. DigiCert bought Symantec's SSL-issuance business. The 50,000 certificates had been issued on Symatec's older network, and not by DigiCert directly. Google announced last year it would distrust all Symantec SSL certificates because of repeated security incidents. Now, Trustico says it lost faith in both Symantec (and indirectly in DigiCert) to manage their infrastructure correctly.

"During our many discussions over the past week we put it to you that we believe Symantec to have operated our account in a manner whereby it had been compromised," Lucas said. "We believe the orders placed via our Symantec account were at risk and were poorly managed. We have been questioning Symantec without response as to concerning items for about a year. Symantec simply ignored our concerns and appeared to bury them under the next issue that arose. "

"In good conscience we decided it wasn't ideal to have any active SSL Certificates on the Symantec systems, nor any that didn't meet our stringent security requirements," Lucas added. "The same management team responsible for that situation is duly employed at DigiCert and are fully managing our account, causing grave concern on our part as it appears to be business as usual with a new name. We were also a victim whereby Symantec mis-issued SSL Certificates owned by us, subsequently we were asked to keep the matter quiet, under a confidentially notice."

⇨ **13)** Lucas says that the system Trustico implemented so website owners could get a replacement certificate instead of the soon-to-be-revoked Symantec/DigiCert certs has failed today. This means over 23,000 users/companies will have to deal tomorrow with sites and apps that encounter HTTPS security errors.

In the meantime, despite Trustico's request, DigiCert has not revoked the certificates of the other 27,000 users for which Trustico wanted certificates revoked, but for which it did not present evidence of a compromise. A Mozilla representative agreed with DigiCert's decision to leave these certificates as "valid."

The entire incident is likely to end with sanctions for one company or the other. Either way, new rules will be voted to deal with the status of certificate resellers and the rights they have over end-customers certificates.

Furthermore, based on the comments by various security researchers, an investigation may be needed into whether or not a SSL reseller logged the SSL private keys of its customers.

Either way, the words "defamatory" and "legal opinion" were thrown around, meaning this issue isn't likely to die out after a few days, and the two companies may meet again, but with lawyers present.

Let's end this article with funny-guy GlobalSign trying to take advantage of this whole debacle for marketing purposes: