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.

(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? (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. (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).
```

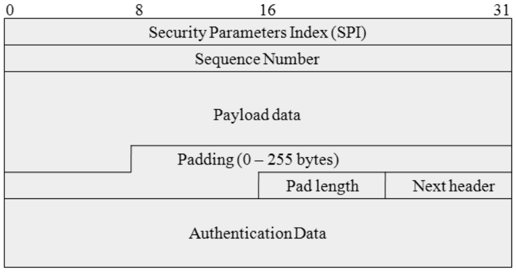
The encryption key is then extracted directly from the keyblock. For this problem, we can model the PRF as just a hash function. One reason to have the ClientRandom and ServerRandom is to protect against time memory tradeoff attacks that attempts to reconstruct the premaster secret (though the most important 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. (3 points)

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



(1+2 points)

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

(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.

(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

(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

(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: