Esecurity: secure internet & e-cash, summer 2012

MICHAEL NÜSKEN, RAOUL BLANKERTZ

9. Exercise sheet
Hand in solutions until Sunday, 17 June 2012, 23:59

Exercise 9.1 (Vulnerability of Certificates). (12 points)

(i) Read Soghoian & Stamm (2010) and summarize. Why should website operators and user consider the country of the CA? [4]

(ii) Read up on DigiNotar and their fraudulent certificates. What had happened and what was the consequences? [2]

(iii) Read Stevens *et al.* (2009) and summaries. What are the implication on X.509? [4]

(iv) Read up on the malware "Flame" and describe how it could authenticate against the Microsoft Windows operating system. [2]

Exercise 9.2 (Secret sharing). (5 points)

Suppose there is some secret s that we want to give to a group of n people. Yet, the secret is very valuable and we do not trust a single person far enough to give him the secret. Think of the access code of the central safe of a bank or the start code of nuclear weapons. The solution is to distribute the secret: each person only gets part of the secret.

To achieve this we randomly choose $n-1$ stings $a_1, \ldots, a_{n-1}$ of the same length as s and compute $a_n = s \oplus a_1 \oplus \ldots \oplus a_{n-1}$. Then the ith person gets a_i.

Prove that

(i) all n persons together can recover the secret s, [1]

(ii) for any other secret s' and any $1 \leq i \leq n$ there is another choice of the a_i' such that $s' = a_1 \oplus \ldots \oplus a_i' \oplus \ldots \oplus a_n$, [2]

(iii) less than n persons can not recover the secret. [2]

Exercise 9.3 (Capturing SSH and SSL). (8 points)

For the this exercise we recommend to use the tool "Wireshark". For privacy reasons, do not include the whole captured pcap files in your assignment (unless you have anonymized them)!

(i) Capture an SSH connection from your computer to `login.bit.uni-bonn.de`.

(ii) Capture an SSL connection from your computer to `https://en.wikipedia.org/wiki/Main_Page`.

(iii) Answer the following questions for both captured connections.

2 (a) Which version of the respective protocol was used? Is it the up to date version?

2 (b) Which cryptographic schemes were proposed and which were chosen?

2 (c) If there are any identifiers, which identifies the client and which the server?

2 (d) Describe the key exchange. How many messages where exchanged before the key exchange started? Which key exchange scheme was used? How is it authenticated?

References

CHRISTOPHER SOGHOIAN & SID STAMM (2010). Certified Lies: Detecting and Defeating Government Interception Attacks Against SSL. URL `http://ssrn.com/abstract=1591033`.

MARC STEVENS, ALEXANDER SOTIROV, JACOB APPELBAUM, ARJEN LENSTRA, DAVID MOLNAR, DAG ARNE OSVIK & BENNE WEGER (2009). Short Chosen-Prefix Collisions for MD5 and the Creation of a Rogue CA Certificate. In *Proceedings of the 29th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '09, 55–69. Springer-Verlag, Berlin, Heidelberg. ISBN 978-3-642-03355-1. URL `http://dx.doi.org/10.1007/978-3-642-03356-8_4`.