Final Assignments

Below are eleven topics about cryptographic systems. You must tell Ruben (signed and encrypted by mail to r.niederhagen@tue.nl, 7BB8F395, with the subject starting with "[crypto2]") your first, second, and third preferred choice before **June 18th (Thursday) 23:59**. Whenever possible you will get one of your choices. The topic will be assigned to you on **June 19th (Friday)**.

Each assignment asks you to study some literature on a cryptographic system, and to write a report of **6 pages**; use the Springer style file from http://www.springer.com/computer/lncs?SGWID=0-164-6-793341-0. These assignments are individual.

In your paper you should focus on cryptographic-systems aspects. This means that your paper should cover all relevant cryptographic aspects of the entire system, such as key management, which type of primitives to use where, which protocols to use where, etc., and you should provide argumentation and motivation why the system is secure or not, and what exactly 'security' means in this context. Focussing only on, e.g., cryptographic primitives is not sufficient in this assignment.

You should have a problem-oriented approach, i.e., clearly describe the security problem your literature is concerned about, the security requirements on the system level, and the way cryptography is used to solve this problem and meet the requirements. At least address the following points (when relevant to your situation):

- What is the exact security problem your literature addresses?
- What relevant (cryptographic) attacks do you see?
- What are the security requirements that any solution to the problem should meet?
- Give an overview of the solution that the assigned literature proposes. How is cryptography used in meeting the security requirements, solving the security problems, defending against the attacks?
- Address any additional topic mentioned in the assignment description below.
- Add your own comments and criticism.

The policy on *copying* and *citing* text not written by yourself as described in the first assignment also holds for this assignment.

The paper will be judged on relevance, sensible argumentation, and also on readability.

Deadline: **July 12th (Sunday), 2015 at 23:59**.

Allowed languages: English.

Deliver your paper in electronic form by e-mail, signed and encrypted, to the specified supervisor as a pdf document, again the subject line starting with "[crypto2]". Make sure that your public key is available, either in a public directory or attached to your email.

You will receive feedback and your mark by e-mail. The marks for the two assignments together (i.e., 1/3 times the mark for the first assignment, 2/3 times the mark for the second assignment) constitute half of the final mark you will get for Cryptography 2, the other half coming from Berry Schoenmakers' part of the course.

Most cited papers are available online (sometimes only from within the TU/e network). Books should be in the TU/e library. If you can't find papers and/or books, write us an email. You can find some links on the resource page http://www.win.tue.nl/~bdeweger/Cryptography2/resources.html.

Individual Literature Assignments

Supervisor: Ruben Niederhagen (r.niederhagen@tue.nl, 7BB8F395)

1. Study SSLv3, TLSv1.0, TLSv1.1, TLSv1.2, and the draft for TLSv1.3. Give a clear description of the differences of these versions of the protocols, and provide reasons for these differences. What attacks are prevented, what improvements are made? SSLv3 is described in RFC 6101, TLS versions are in RFC 2246, 4346 and 5246; the draft of TLSv1.3 is available online as well. Also have a look at Eric Rescorla: "SSL and TLS, Designing and Building Secure Systems".
2. Study the weaknesses of TLS as pointed out in the paper "Lucky Thirteen: Breaking the TLS and DTLS Record Protocols" by AlFardan and Paterson, 2013. Include a description of their attack and suggested countermeasures.
3. Study the "Logjam" attack on TLS as described out in the paper "Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice" by Adrian et. al., 2015. Focus on the protocol-related aspect of the attack and include a description of suggested countermeasures.
4. The Tor Network does not use, e.g., steganography in order to hide Tor traffic; however, there are mechanisms to prevent governments from blocking Tor. Study the security of Tor in respect to censorship avoidance (e.g., blocking of Tor in China). What countermeasures are discussed in literature (e.g., "How China Is Blocking Tor" by Winter and Lindskog)?
5. Study the TextSecure OTR protocol; describe the changes from version 1 to version 2 and the relation to the Axololt protocol. Use `https://github.com/WhisperSystems/TextSecure/wiki` as starting point when searching for literature.

Supervisor: Andreas Hülsing (a.t.huelsing@tue.nl, 152BFF2E)

6. Study "Certificate-based Encryption" by Gentry (`http://eprint.iacr.org/2003/183.pdf`). Describe the cryptographic tools used and compare it traditional PKI.
7. Study "Certicateless Public Key Cryptography" by Al-Riyami and Paterson (`http://eprint.iacr.org/2003/126.pdf`). Describe the cryptographic tools used and compare it traditional PKI.
8. Password-hashing. There is currently a password hashing competition running (`https://password-hashing.net/`) that tries to find a new password hashing scheme to replace old schemes like bcrypt or PBKDF2. Get an overview of the current state of the competition. Describe the security requirements a password-hashing scheme should fulfill. Sketch the concept for two candidate schemes of your choice.
9. Analyze Chaum's eCash system. Start "Blind signatures for untraceable payments" by Chaum, 1983. Describe the basic concept and the underlying cryptographic tools. Compare the approach to the Bitcoin system.
10. Get yourself an overview of the bitcoin protocol. Then look into Double-Spending-Attacks ("Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin" by Karame, Androulaki, and Capkun). Describe the problem, the attack, and the proposed counter-measure. Then search for other counter-measures in literature.
11. Bitcoin: Get yourself an overview of the bitcoin protocol. Then look into alternative Schemes that use proof of storage schemes to replace the proof of work. Describe how these schemes work. What is the motivation behind these schemes? What are the advantages and disadvantages compared to proof of work based schemes? What are the cryptographic tools used?