Final Assignments

Below you find a list of possible assignments related to the topics discussed in the lecture. Please hand in (signed and encrypted by mail to a.t.huelsing@tue.nl with the subject starting with "[AppliedCrypto]"; see, e.g., http://www.win.tue.nl/applied_crypto/2017/ for the public key) your first, second, and third preferred choice before **December 21st (Thursday) 23:59**. Whenever possible you will get one of your choices. The topic will be assigned to you till Wednesday, December 27th.

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

If not explicitly stated otherwise, your paper 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. Focusing only on, e.g., cryptographic primitives is not sufficient in this assignment. If the lecture already dealt with your assigned topic, your work should clearly go beyond what was explained in the lecture.

You should have a problem-oriented approach, i.e., clearly describe the security problem your literature deals with, 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: **January 28th (Sunday), 2017 at 23:59**.

Allowed languages: English.

Deliver your paper in electronic form by e-mail, signed and encrypted, to Andreas as a pdf document named "[FIRST_NAME][LAST_NAME].pdf", again the subject line starting with "[AppliedCrypto]". 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 your final mark.

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 me an email.

Individual Literature Assignments

The following list contains proposals from my side. If you have a topic that you are interested in but for which the list contains no assignment, you can contact me **before** the deadline. Please name a paper and a question related to that work that you want to answer. I will decide if this topic meets my requirements. The topic has to be closely related to one of the topics of the lecture.

Topics

1. Replacing PKI. Study "Certificate-based Encryption" by Gentry (http://eprint.iacr.org/2003/183.pdf). Describe the cryptographic tools used and compare it to traditional PKI. Would you replace PKI with this? Why?
2. Replacing PKI. 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. Would you replace PKI with this? Why?
3. Password-hashing. There recently was a password hashing competition running (https://password-hashing.net/) that tried to find a new password hashing scheme to replace old schemes like bcrypt or PBKDF2. Describe the security requirements a password-hashing scheme should fulfill. Sketch the winner Argon2, describe how / why this algorithm met the requirements, and what issues where found recently.
4. eCash: Double-spending in bitcoin. 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 and describe at least two.
5. ecash: Proof-Of-Stake. Read https://eprint.iacr.org/2016/889.pdf. Explain the concept of Proof-Of-Stake protocols. What is the difference to traditional bitcoin? How is security reasoned?
6. Quantum algorithms. Read Grover's original paper on his algorithm (http://arxiv.org/abs/quant-ph/9605043). Explain the algorithm such that it is accessible by a master student in computer science. Also, discuss the implications for cryptography and the lower bound results.
7. Privacy-preserving bitcoin. Study zero-cash (http://zerocash-project.org/), read their scientific paper and compare it to bitcoin. What is improved, what is getting worse? Describe the protocol, discuss the claimed security properties and if they are achieved.
8. Key transport. Take a look at A. Dent: "A designer's guide to KEMs" (https://eprint.iacr.org/2002/174/20051031:161821). Explain the concept of the KEM/DEM terminology, summarize the generic transformations presented, and explain one of the security reductions in detail. For the latter, focus on intuition and main ideas rather than technical details.
9. Mass surveillance. Explain the concept of Big-key cryptography. Which problem is tackled and how? Possible starting points are P. Rogaway: "The moral character of cryptographic work" (http://web.cs.ucdavis.edu/~rogaway/papers/moral.pdf) and Bellare, Kane, Rogaway: "Big-Key Symmetric Encryption: Resisting Key Exfiltration" (https://eprint.iacr.org/2016/541.pdf).
10. Tor. 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)?

11. Tor: Elligator. Read https://elligator.cr.yp.to/elligator-20130828.pdf. How does the scheme work. What does it achieve? How is this related to Tor (give context). What are possible limitations / attacks.
12. OTR. 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.
13. Private messaging. Read "A Formal Security Analysis of the Signal Messaging Protocol" (https://eprint.iacr.org/2016/1013). Explain the security model used and give an intuition for the main proofs.
14. TLS. 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".
15. TLS attacks. 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.
16. TLS attacks. Study the "Logjam" attack on TLS as described 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.
17. TLS security. Summarize the paper "Indiscreet Logs: Persistent Diffie-Hellman Backdoors in TLS" (https://eprint.iacr.org/2016/999.pdf). Specifically explain how the the trapdoor with composite moduli works and how the backdoor was found in practice.
18. TLS security: Reaction attacks. Read the original paper on reaction attacks (https://www.schneier.com/academic/archives/1999/06/reaction_attacks_aga.html). Explain the attack. Explain how and under which conditions the attack works.
19. Attacks on RSA. Study the recent ROBOT attack (https://robotattack.org/). Read the scientific paper by the authors, explain the attack and its impact. Discuss countermeasures.
20. Passwords: Honeywords. Describe the Honeywords method used to improve the security of hashed password files from (https://people.csail.mit.edu/rivest/pubs/JR13.pdf). Discuss its strengths and weaknesses and how this system makes hashed password files more secure against attackers.
21. Lattice-based Crypto: LWE. Describe the LWE encryption scheme and the underlying security assumption (See the original paper http://www.cims.nyu.edu/~regev/papers/qcrypto.pdf and the survey http://www.cims.nyu.edu/~regev/papers/lwesurvey.pdf). What does this have to do with lattices? In addition describe how Dual LWE Encryption works.
22. Lattice-based Crypto: GGH. Describe how the GGH signature scheme works and how to attack the scheme by using "Learning a Parallelepiped: Cyptanalysis of GGH and NTRU Signatures" (http://www.cims.nyu.edu/~regev/papers/gghattack.pdf). For more information on the GGH signature scheme, see http://groups.csail.mit.edu/cis/pubs/shafi/1997-lncs-ggh.pdf.
23. Lattice-based Crypto: NTRU. Describe how the NTRU cryptosystem works (See for instance the PKCS Tutorial on https://www.securityinnovation.com/products/encryption-libraries/

ntru-crypto/ntru-resources.html and the original paper on https://www.securityinnovation.com/uploads/Crypto/ANTS97.pdf). Describe how a Meet-in-the-Middle attack on the NTRU secret key pair works (https://www.securityinnovation.com/uploads/Crypto/NTRUTech004v2.pdf).

24. Hash-based signatures: PRUNE-HORST. Read the NIST-submission document for PRUNE-HORST (https://github.com/gravity-postquantum/prune-horst/blob/master/Supporting_Documentation/submission.pdf). Describe the scheme, the security reasoning and explain how it differs from the original HORST scheme.