Resit

Below you find a list of assignment topics. If you want to participate in this resit, you must tell Andreas (signed and encrypted by mail to a.t.huelsing@tue.nl, 152BFF2E with the subject starting with "[AppCrypto]") your first, second, and third preferred choice before **April 24th (Monday), 2017 at 23:59**. Missing the deadline means no resit!

You are not allowed to choose a topic that already was assigned to you previously.

Whenever possible you will get one of your choices. The topic will be assigned to you until **April 28th (Friday)**.

Each assignment asks you to study some literature on a cryptographic system, and to write a report of **10 pages**; use the Springer style file from `http://www.springer.com/computer/lncs?SGWID=0-164-6-793341-0`. These assignments are individual.

Every assignment provides specific tasks related to the given literature. Follow these tasks (it is not enough to write a summary of the paper!), write your own text (following the original works too closely will result in subtraction of points), and add your own opinion / criticism. Make sure when you are asked to explain some scheme or algorithm that you do not simply copy the formal definition of the scheme but try to give some intuition behind the construction and explain the important steps.

Note that this time we do a single assignment with 10 pages. This means that you also have to cover more background literature. It is not enough to just stick to the single paper that we mention in the assignment. We want you to search related literature yourself and compare.

The policy on *copying* and *citing* text not written by yourself as described in the regular assignments also holds for this assignment. Any misbehavior in this regard will be reported to the exam committee.

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

Deadline: **June 5th (Monday), 2017 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 "[AppCrypto]". 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 grade for the resit constitutes the final mark you will get for Applied Cryptography and supersedes all previous marks for the class.

Most cited papers are available online (sometimes only from within the TU/e network). Books should be in the TU/e library.

Individual Literature Assignments

Supervisor: Andreas Hülsing

(a.t.huelsing@tue.nl, 152BFF2E)

1. Replacing PKI. Study "Certificate-based Encryption" by Gentry (`http://eprint.iacr.org/2003/183.pdf`) and "Certicateless Public Key Cryptography" by Al-Riyami and Paterson (`http://eprint.iacr.org/2003/126.pdf`). Describe the cryptographic tools used, compare the approaches to each other and to traditional PKI. Would you replace PKI with one of these? Why?
2. 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.
3. 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.
4. 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.
5. 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.
6. 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.
7. 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`).
8. 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)?
9. 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.

Supervisor: Christine van Vredendaal
(c.v.vredendaal@tue.nl, 4BAFF310)

10. 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".

11. 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.

12. 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.

13. 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.

14. 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.

15. 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`.

16. 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`).

17. 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. Summarize the paper "Naturally Rehearsing Passwords" (`https://eprint.iacr.org/2015/166.pdf`). Focus on the security models used and how these are satified for the Shared Cues scheme.