## Important Dates

- Before Wed February 28 (but as soon as possible): email me your topic and a link to a primary source about it. Start early: first come, first served. If you find several reasonable topics, also let me know so I can share unused ones with others who are having trouble finding one.
- Fri March 9: optionally send me a first draft to receive feedback.
- Fri March 16: send me the final version.

## Project Overview for Undergrads:

Find an example of cryptography being used inappropriately or implemented incorrectly, *in a real-world system.*

Systems can be vulnerable in many ways, but for this project you must focus on a vulnerability that is *primarily due to cryptography.* In other words, the fix for the vulnerability should involve a more appropriate use of crypto. Social engineering, buffer overflows, etc., are fascinating but not cryptography.

**Grading Criteria:** Write a ~5-page report on the problem:

- Clearly describe the real-world system and its mechanics related to the cryptographic problem.
- Why was cryptography being used? What was the system designer trying to achieve (e.g., authentication, privacy, secrecy)?
- What cryptography was actually used, and how was it implemented / integrated into the system? If this involves some algorithms not described in class, then give a high-level overview of what the algorithms were doing.
- *Why was the use of cryptography wrong?* How could an attacker exploit the system? What is the most severe thing an attacker accomplish by the exploit?
- How was the problem discovered? Was the problem reported responsibly?
- Describe and justify a fix for the problem. What security guarantees can a more appropriate choice of cryptography provide? In discussing this, appeal to the relevant cryptographic primitives & security definitions from class.
- Properly acknowledge your references / sources.

**Suggestions for Finding Ideas:**

- CVE is a list of categorized software vulnerabilities; try the cryptography categories.
- Interesting vulnerabilities are often posted to the netsec subreddit. Try browsing the archives.

- Search for likely terms: ECB mode, padding oracle attack, unauthenticated encryption, chosen ciphertext attack, deterministic encryption, side-channel attack, timing attack, replay attack, unsalted hash, etc.

## Project Overview for Grads:

Read, understand, and report on an academic paper on cryptography. The paper must either introduce a new formal security notion, introduce a cryptographic construction with a formal analysis/proof of security, or introduce a new attack with formal analysis of its performance/effect.

**Grading Criteria:** Write a ~5-page report on the paper. Your target audience are your peers in this class, who have a solid background in the classic fundamentals of cryptography and want to learn more about other kinds of crypto.

- Clearly articulate the objectives of the paper, with minimal jargon. What is the problem and why is it hard? In other words, why did the world need this paper?
- What was the state of the art before this work? What were the limitations?
- Clearly state the main contribution(s) of the paper.
- Present the main technical ideas of the paper, whether it's a security proof or an analysis of an attack, etc. Since you are writing a summary, don't just repeat what the paper says. Instead, **identify the new "tricks" or "insights"** of this paper, as if it were a tool you'd encourage others to use in their own research. Try to differentiate between the main ideas and the kinds of things that are "standard." As much as you can, try to translate the results into the terminology used in our course (e.g., security statements in terms of libraries).
- Explicitly discuss a motivating application of the results or a scenario in which the results of this paper would be used.
- Explicitly discuss the relationship between the results in the paper and concepts discussed in class. If the paper defines new security targets, compare/contrast with the classical ones covered in class.

**Some possible ideas:** These are not exclusive. Please feel free to suggest your own. These papers are mostly on interesting aspects of symmetric-key encryption.

You can find the papers via Google Scholar.

- A Joux. "Multicollisions in iterated hash functions. Application to cascaded constructions." Crypto 2004.
- J Black, P Rogaway, T Shrimpton. "Black-box analysis of the block-cipher-based hash-function constructions from PGV." Crypto 2002.
- M Bellare, VT Hoang, P Rogaway. "Foundations of garbled circuits." ACM CCS 2012.

- P Rogaway, T Shrimpton. “A provable-security treatment of the key-wrap problem." Eurocrypt 2006.
- D McGrew, J Viega. “The security and performance of the Galois/Counter Mode (GCM) of operation." Indocrypt 2004.
- M Liskov, R Rivest, D Wagner. “Tweakable block ciphers." Crypto 2002.
- U Maurer. “Conditionally-perfect secrecy and a provably-secure randomized cipher." Journal of Cryptology 1992.
- S Halevi, P Rogaway. “A Tweakable Enciphering Mode." Crypto 2003.
- S Halevi, P Rogaway. “A Parallelizable Enciphering Mode." CT-RSA 2004.
- M Bellare, D Hofheinz, E Kiltz. “Subtleties in the Definition of IND-CCA: When and How Should Challenge-Decryption be Disallowed?" J Cryptology 2015.
- G Bertoni et al. “On the indifferentiability of the sponge construction." Eurocrypt 2008.
- O Dunkelman, N Keller, A Shamir. “Minimalism in cryptography: The Even-Mansour scheme revisited." Eurocrypt 2012.
- M Fischlin et al. “Data Is a Stream: Security of Stream-Based Channels.” Crypto 2015.
- S Gueron, A Langley, Y Lindell. “AES-GCM-SIV: Specification and Analysis.”
- A Juels, T Ristenpart. “Honey Encryption: Security Beyond the Brute-Force Bound.” Eurocrypt 2014.
- E Dahmen et al. “Digital Signatures out of Second-Preimage Resistant Hash Functions.” PQCrypto 2008.
- M Bellare et al. “Format-preserving encryption.” Selected Areas in Cryptography 2009.