Project Overview

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 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.

Dates

- Before Wed March 1 (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.

- Wed March 8: optionally send me a first draft to receive feedback.

- Fri March 17: send me the final version.
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.