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.

Grading Criteria

Write a 2- to 5-page report on the problem:

► Clearly and concisely describe the real-world system and its mechanics related to the cryptographic problem.

► What was the intent of the designer in using cryptography?

► What cryptography was actually used, and how was it implemented / integrated into the system?

► 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 a fix for the problem and why it is an improvement. What security guarantees can a more appropriate choice of cryptography provide? In discussing this, appeal to the relevant cryptographic primitives & security definitions from class.

Dates

► Before Wed March 2 (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 9: optionally send me a first draft to receive feedback.

► Thu March 17: send me a final draft.

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, etc.