6.857 Homework | **Problem Set 1** | # 1-3 - Subverting Cryptography
Erica Du
Skanda Koppula
Jessica Wang
February 22, 2015

1. Insecure implementation: the implementation of a theoretically secure algorithms might have vulnerabilities

   - The OpenSSL library this year was revealed to have a buffer over-read bug, Heartbleed.
   - The NSA has inserted faulty code/backdoors in commonly used random number generators.

   DEFENSE: Verify 3rd party code. Otherwise implement and test everything, like random number generators, on your own.

2. Improper use: users may misuse otherwise secure software and/or algorithms

   - Users may create short or weak keys
   - Users may re-use passwords

   DEFENSE: Create strong restrictions for user inputs to ensure strong key creation.

3. Hardware injection: tampering with physical devices

   - Hardware keyloggers to track keystrokes and potentially passwords
   - Inserting backdoors into internet routers

   DEFENSE: Only use devices from a trusted resource, only use devices you create yourself (i.e. create all your own routers and keyboards).

4. Government: Legal Retrieval

   - Court orders to obtain private keys (compulsion)
   - Abusing trust commercial trust has in a body like the NSA, and just asking for the data

   DEFENSE: Host data in a different country, start your own country without these rules. Don't put your trust in governmental bodies, or other bodies of "authority." Get a good lawyer.

5. Social engineering: extracting personal information to gain useful information

   - Email or phone phishing

   DEFENSE: Adblock. Spam filters. Common Sense.

6. Indirect Computational Data

   - Timing attacks (i.e. side channel timing attacks) that determine message based on how long it
   - Using metadata of a message to learn information about the messagetakes per step of computation

DEFENSE: Introduce more randomness (i.e. in length) into actual message, to make timing more uniform. Introduce randomness into metadata.

7. Coercion: bribery and corruption

   - Pay NSA employees more than the government to spill secrets
   - Give money in exchange for information

   DEFENSE: Pay your employees a sufficient wage. Only hire people you trust.

8. Go after key aggregators instead of the actual message.

   - Instead of trying to break the crypto, just try to steal the keys.

   DEFENSE: Don't use key aggregators. Use one-time keys.