Prolog to Lecture 15
CS 236
On-Line MS Program
Networks and Systems Security
Peter Reiher

Another Cautionary Tale About Crypto Programming

- As discussed, proper use of crypto in programs is vital
- With improper use, the benefits of cryptography can disappear
- An interesting case (in 2014) of screwing up your crypto:
  - CryptoDefense

What Is CryptoDefense?

- Not what the name sounds like
- It's ransomware
- It encrypts data on an infected computer using public key crypto
- Makes you send money (in BitCoin) to the writer to get the decryption key
- But . . .

CryptoDefense's Little Problem

- Written for Windows machines
  - As much malware is
- Using standard Microsoft crypto infrastructure to generate keys
- Sends both keys back to its author
- But neglects to remove the private key from the local machine

What's the Effect?

- The ransomware author demands your money to give you the private key
  - So you can decrypt your data
- You can scoff at him and ridicule him
- Because he foolishly left you a copy of it on your own machine
  - In the standard place where Microsoft crypto puts keys

Some Lessons

- Criminals make mistakes, too
- Crypto is hard to get right
- You need to understand what you're doing
- Even if the crypto algorithm is strong, weak key management can kill it