Prolog to Lecture 11
CS 236
On-Line MS Program
Networks and Systems Security
Peter Reiher

The Heartbleed Bug

- A bug in the OpenSSL implementation of SSL/TLS
- Effect was to reveal potentially secret information from a remote process
  - Cryptographic keys, passwords, Social Security Numbers, etc.
- A *buffer overread* problem

SSL Heartbeat Messages

- SSL requires heartbeat messages
- One side sends the other a buffer containing some content
- The other side must send the same content back
- The heartbeat message contains the buffer and its length

The Security Flaw

- The OpenSSL implementation did not verify the length field
  - Didn't check that it matched the actual buffer supplied
- Instead, it returned whatever was in the buffer plus any extra specified length
- Which was something else in the process' memory

For Example,

- The attacker sends a buffer containing "hello" and a buffer length of 512
- The other side of the SSL connection returns "hello"
  - Plus the next 507 characters in its memory
  - Which might contain "interesting" data

Exploiting Heartbleed

- Establish an SSL connection to a vulnerable server
- Repeatedly send these buffer overread requests
- Examine what you get back looking for "good stuff"

Fixing Heartbleed

- Simple in principle
- Update the software to check the buffer length in heartbeat messages
- In practice, required updating software in literally millions of sites
  - Some still not patched

Impacts of Heartbleed

- Could be used to steal private keys associated with certificates
  - Many web sites had to get new certs
  - Many that should haven't
  - Old certs are still out there
- One Heartbleed attack compromised 4.5 million hospital patient records

Lessons From Heartbleed

1. Open source doesn't mean safe
   - Even for popular stuff
2. Difference between protocol bugs and implementation bugs
3. Dangers of serious bugs in popular software
   - Especially utility software
   - Often secondary bad effects