Experiences in Computer Security

CSC 4992 Cyber Security Practice

Frank Adelstein

Wayne State University

February 28, 2017

Overview

- R & D and Applications (Programming)
- Learning About Security
- Customers

Research and Development and Applications

- Research
  - University research, grants, private company: goals, pressures, constraints
- Development
  - 1st cut: Prototype and Proof of Concept
  - Multi-phase approaches: design it all, but don't try to build it all at once
- Applications
  - Secure Coding
    - Minimize root, distrust user input
    - Always ask: "What could possibly go wrong?"
    - Complexity is the enemy, composability allows flexibility
  - Testing: Think about how to break it, not how to show it works
  - Security demos are hard/boring: Hard to show something NOT happening

CAYUGA NETWORKS

Learning About Security

- Hands on
  - Write programs, do different things, understand how it works
  - Understand the tools, but don't let them become crutches
- Low level
  - Be comfortable with C and Assembly, know what the CPU can do and why (e.g. ++)
  - OS libraries and system calls (Linux, Windows, Mac, FreeBSD)
  - Network protocols (802.3, IP, TCP, HTTP, HTML, SMTP, 802.11, …)
  - Command line
  - What happens, what's changed
- Read Documentation
  - Man pages (know the difference between sections?)
  - Source code (reading other people's code is useful, even if just as counter-examples)
  - IETF RFCs (this is where major Internet protocols are specified)
  - Do NOT use StackOverflow/ServerFault/SuperUser/StackExchange as primary source
  - Plus appropriate web sites to keep up with trends

CAYUGA NETWORKS

Customers

- Users
  - Government agencies (sometimes: useful, clueless, or apathetic)
  - Law Enforcement (some technical, some not)
- Sys Admins/Incident Responders
- Administrative/Executive
  - Might care about different things (security vs. publicity/embarassment)

CAYUGA NETWORKS