Lecture 3: Standards and Lab Assignment 1

Summary

More on Non-malicious Program Errors

Incomplete mediation demo (already did this with 5:30 section)

TOC-TOU demo

Major Standards Organizations

Note: the material on standards was originally scheduled for Lecture 2.

Why standards? Interoperability, assurance of market share.

More important for security *because it is hard!*

The Internet Organization

Internet Architecture Board

Internet Engineering Steering Group

Internet Engineering Task Force (IETF)

Internet Drafts are proposed standards; Requests for Comment (RFCs) are published standards.

RFCs — not just security, but many Internet standards

http://www.ietf.org/rfc.html

Examples:

1883 — IPv6 Specification
2065 — DNS Security Extensions
3711 — Secure Real-time Transport Protocol (SRTP)
4250 - 4254 — Secure Shell (SSH)

National Institutes of Standards and Technology (NIST)

Publish Federal Information Processing Standards (FIPS) and Special Publications (SP)

Examples:

FIPS 186-4 — Digital Signature Standard
FIPS 197 — Advanced Encryption Standard
SP 800-90 — Random Number Generation
SP 800-82 — Industrial Control System Security

International Telecommunications Union (ITU)

"is responsible for studying technical, operating, and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis."

Examples:

X.509 Public Key Certificates
X.800 Security Architecture for Open Systems

Lab Assignment 1

VM download and installation

Access to Collabtive web interface and source code

Brief Introduction to SQL (you really only need to understand SELECT and UPDATE)

Exercises

None