Programming Languages and Security

University of Wisconsin
Computer Science Department
Somesh Jha
General Areas of Interest

- Security
  - verifying security and ecommerce protocols
  - program analysis to find common vulnerabilities
  - constructing statistical predictors of program behavior

- Software Engineering
  - automating test case generation
  - survivability analysis of software specifications

- Security
  - verifying security and ecommerce protocols

Somesh Jha, University of Wisconsin
Security

Verification

• protocols used in security and commerce applications are becoming increasingly complex

• my goal is to develop techniques and tools for reasoning about these protocols

  – adversary can do anything

  – requirements are sometimes fuzzy

• these protocols are increasingly hard to reason about

  – these protocols are increasingly complex
• Security

Brutus

Inputs

• specification of a protocol
• property to be verified
• adversary can never find out the credit card number
• everything is fine
• a sample attack

Outputs
Limitations of Brutus

- was unable to handle very large protocols
- formalism was not very clean
- no help in constructing correct protocols

I want remedy all these limitations
Security [Vulnerabilities]

- Poorly designed access control mechanisms
- Allowing internal data-structures to grow unbounded
- Buffer overruns

A very large class of vulnerabilities are responsible for a

• See the web-site www.cert.org
• Initially focus on finding vulnerabilities related to buffer overruns

Vulnerabilities

• Target program analysis for finding these commonly found vulnerabilities

Security [Vulnerabilities]
Intrusion Detection use audit trail data

Security [Predictors]

training

predictor

good bad
Security Predictors

Current Intrusion Detection Systems
• are signature-based, based on commonly found attack patterns

Advantages
• predictors are dynamic, can find attack patterns automatically

Ties to machine learning
• most scanners are good at finding local vulnerabilities
• example www.iss.net
• managers want global attacks

Software Engineering [Survivability]
setup web proxy
break into the DNS Server
access DNS configuration
acquire password
ignore errors
access control
exploit poor passwords
WWW.gs.com
setup web proxy
Software Engineering [Survivability]
Software Engineering [Security Testing]

- Known security holes
  - Use mechanisms
    - Subvert an operating system's memory protection
    - Subvert a data-management system's data-security
    - Devise test cases to subvert program's security checks
Test suite

Generator

Test case

System description

Security holes

Software Engineering [Security Testing]