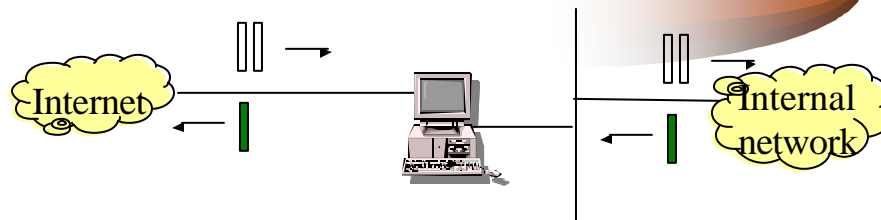


Firewall Testing



Seny Kamara, Mike Frantzen, Brian Poole, Florian Kerschbaum, Sofie Nystrom, Daniel Kim

Supervised by: Eugene Schultz (eeschultz@lbl.gov),
Sonia Fahmy (fahmy@cs.purdue.edu), Steve Hare
(hare@cerias.purdue.edu)

For more information, please see:
<http://www.cerias.purdue.edu/firewall/>

Motivation

- Current firewall testing based only on known vulnerabilities
- Firewall models lack detailed descriptions
- No prediction of potential vulnerabilities
- Difficult to implement and test firewalls

Model



- Based on a data flow model
- Details firewall functionality
- Flexible enough to model different implementations
- Provides basis for analysis and prediction

Vulnerability Categories



- Validation error
- Authentication error
- Serialization/aliasing error
- Boundary checking error
- Domain error
- Weak/incorrect design
- Other errors

Vulnerability Impacts



- Execution of code
- Change of target resource
- Access of target resource
- Denial of service

Vulnerability Fixes



- Spurious entity
- Missing entity
- Misplaced entity
- Incorrect entity

Future Work

- Statistically analyze vulnerabilities, their impacts and costs
- Develop an automated and complete firewall test environment and set of tools
- Implement/Analyze distributed firewalls

