

University of Southern California
Center for Software Engineering

A Value Driven Approach to Balance Security, Maintainability, and Usability in Configuring Firewall Policies

Automated Firewall Rules Generation Based on Value-Centric Threat Modeling

Yue Chen, Dr. Barry Boehm
USC-CSSE

March 2006

© All rights reserved by authors

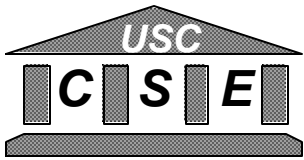
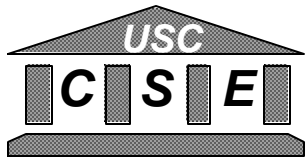


Table of Contents

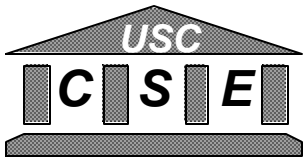
Background

- **Nature of the Problem**
- **Threat-minimized solution**
- **Results**
 - **Mini-Demo**
 - **Numbers for better decisions**
- **Conclusions, constraints, and future work**

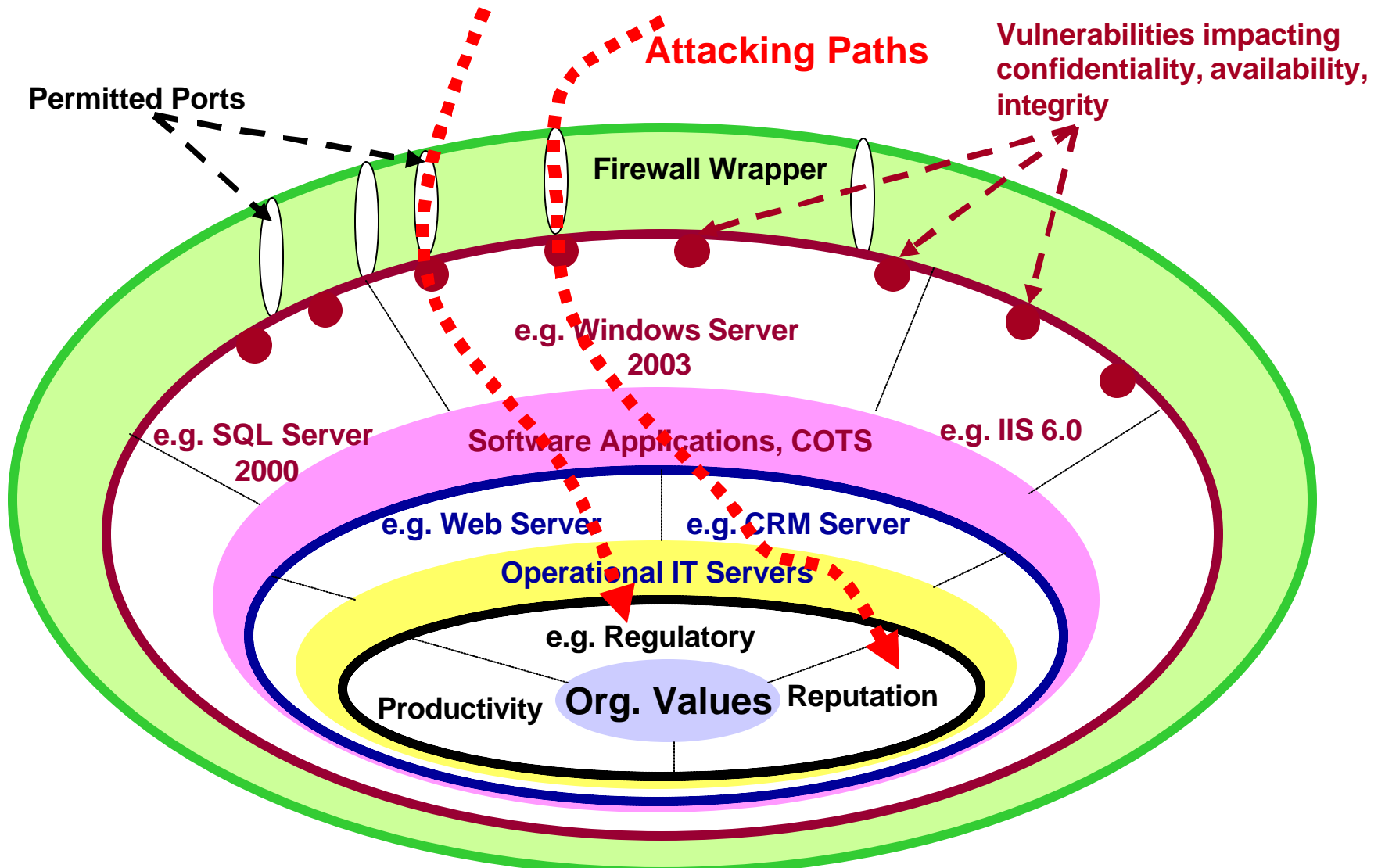


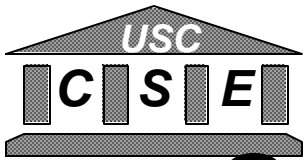
Background

- **Strategic relationship with USC-Information Service Division**
 - **Mr. Michael Pearce, Deputy CIO**
 - **Mr. Luke Sheppard, Head of IT Security**
 - **Difficult to configure firewall policies tight and right to exact needs**
 - **Effort consuming to maintain a large number of firewall rules**
 - **Need cost-effective firewall solutions to balance security, maintainability, usability**



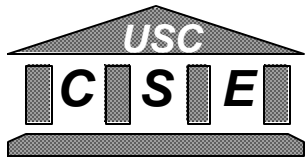
Nature of The Problem





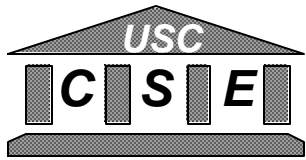
Quantify Threat with Weighted Attacking Paths

- **Minimize the number of Weighted Attacking Paths associated with opened ports on Firewalls**
- **Weight Each Attacking Path by How Easy It Is to Implement Such An Attack (0 weight 1), considered attributes are:**
 - if vulnerability patch available
 - if can be launched remotely
 - if attacker need an account on target computer
 - if user needs to open an email attachment
 - Importance of the target asset and possible value impact



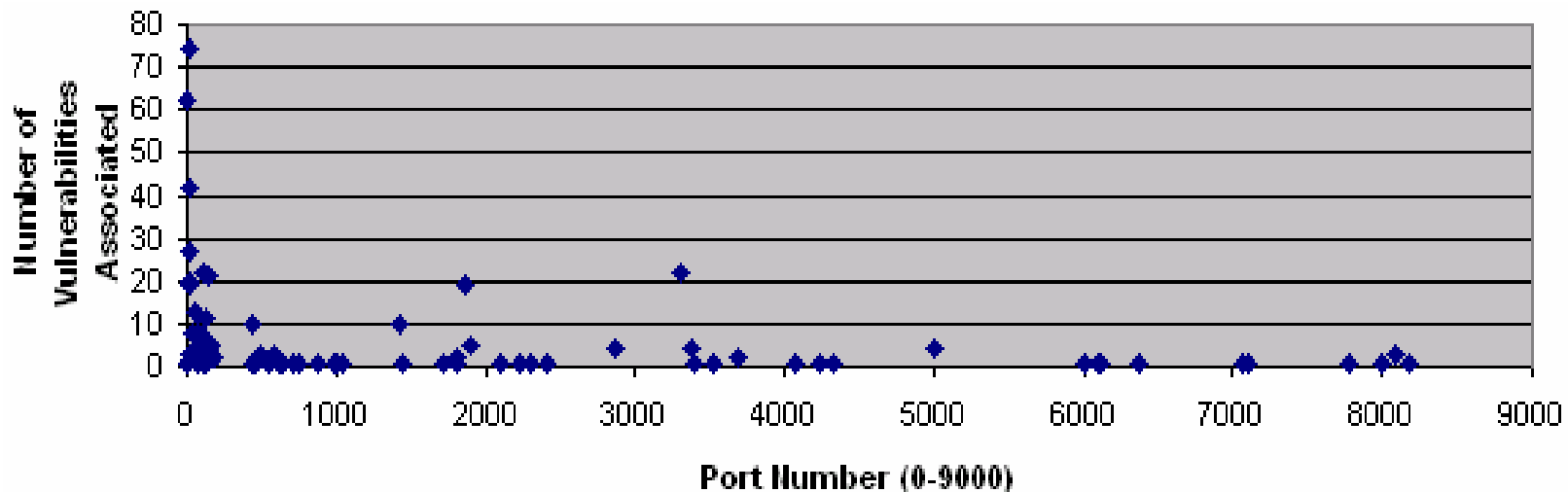
Step 1: Profile useful ports

- **Clients' requirements**
- **Application specifications**
- **Network packets monitoring tool**
 - **TCP Dump, Netflow**



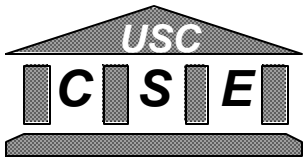
Step 2: Understand Threats Distribution

- Chart below is plotted from 717 vulnerabilities in our database*



- Vulnerabilities affect confidentiality, availability and/or integrity of IT infrastructure

*Includes vulnerability information from Cert, First, Frsirt, Microsoft, Nist, Sans, Symantec



Step 3: Associate Server Status to Organization Values

Example: A Department Web-Server

		Values		
		Productivity	Reputation	Regulatory
Server Status	Integrity	Medium	High	Complete
	Availability	Medium	High	Complete
	Confidentiality	None	Medium	Complete

Above metrics and ratings are **user-definable**

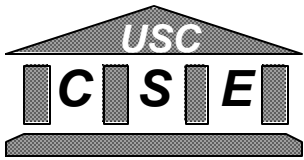
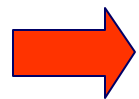


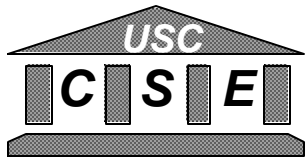
Table of Contents

- Background
- Nature of the Problem
- Threat-minimized solution



Results

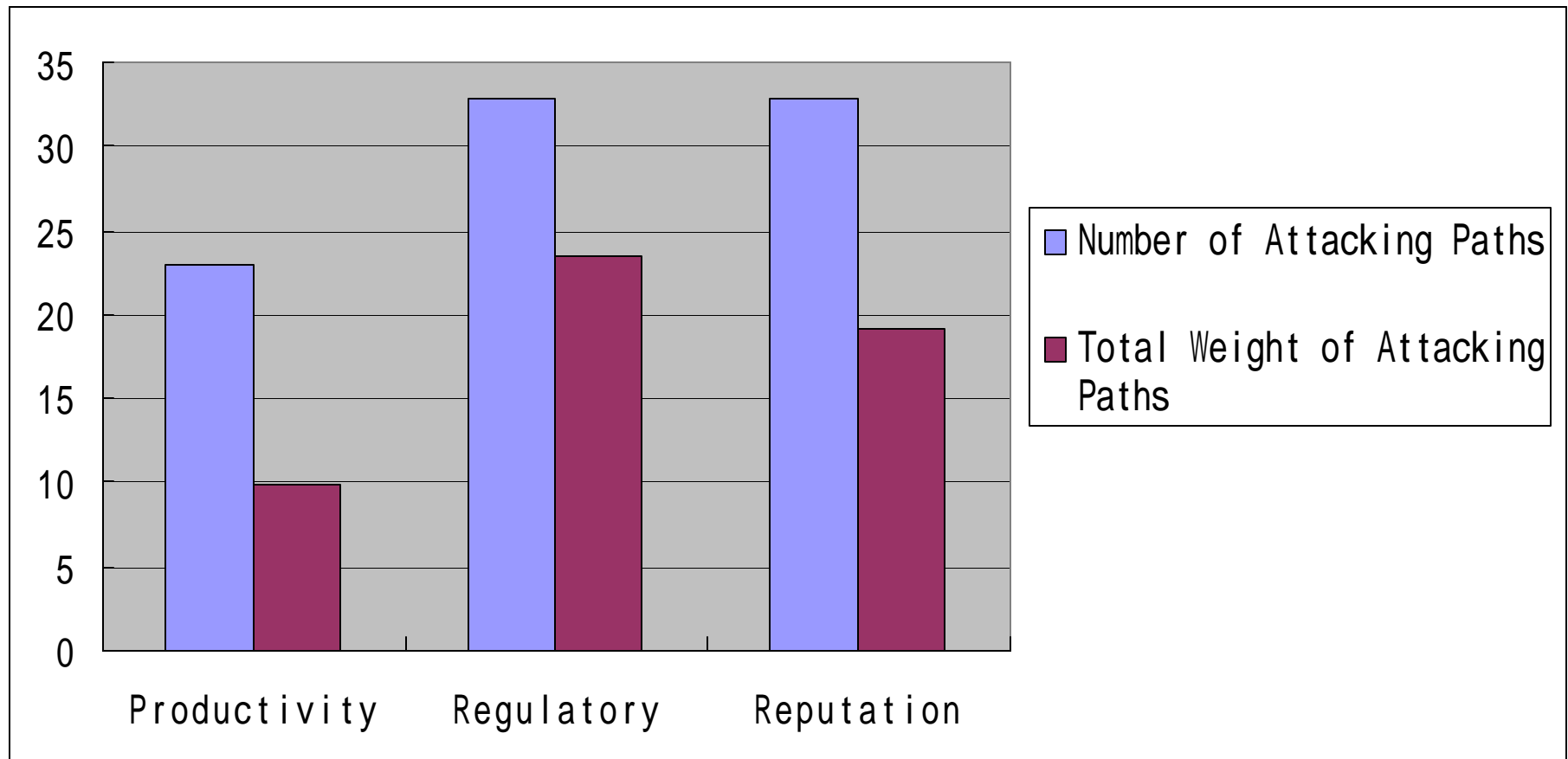
- Mini-Demo
- Numbers for better decisions
- Conclusions, constraints, and future work



University of Southern California
Center for Software Engineering

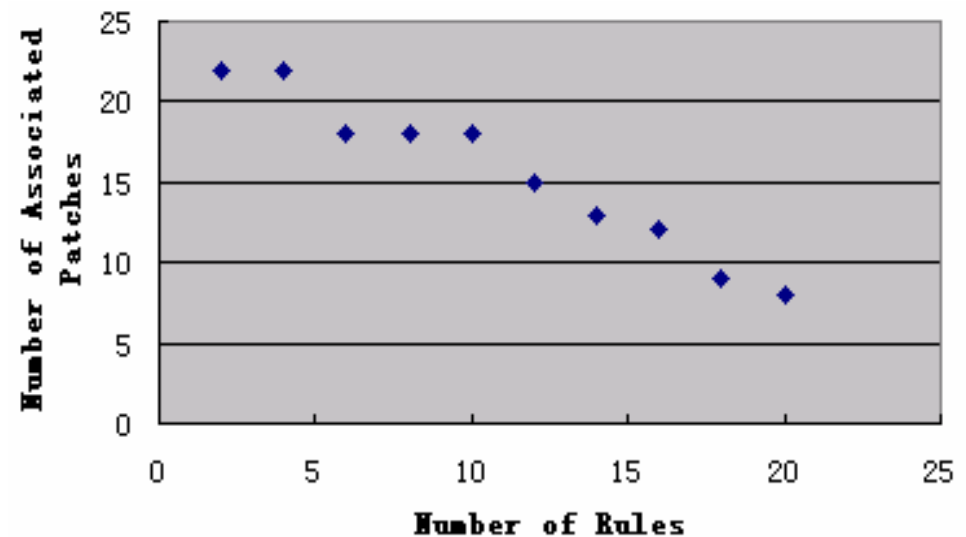
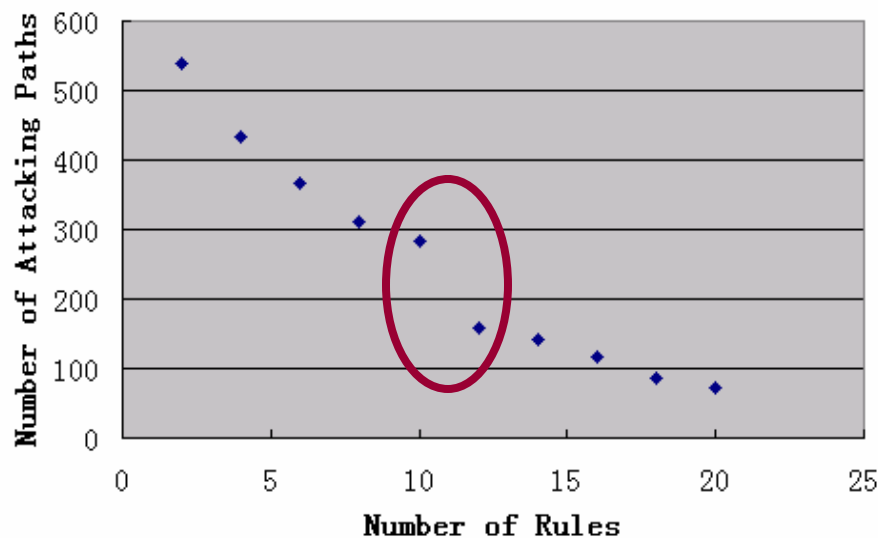
Tool Mini-Demo (If Time Allows)

Threat to Organization Values



Security vs. Maintainability

- **Maintainability Indicators:** Number of firewall rules; Number of patches that have to apply
- **Determine how many rules would be ideal in terms of balancing maintainability and security**

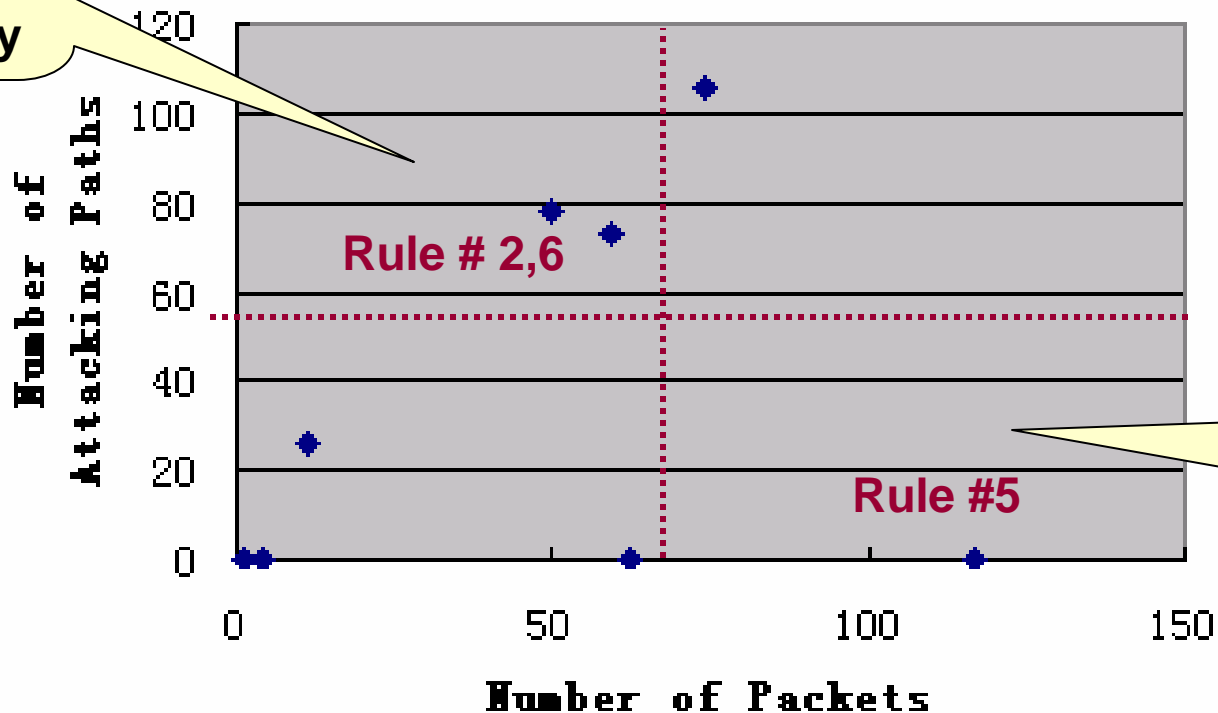


Security vs. Usability

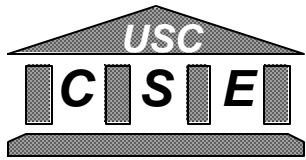
Usability Indicator: the recorded number of packets enabled by each firewall rule

Security Indicator: the total Weight of All Attacking Paths

Few packet flow, but very risky



Many packet flow, but not very risky



Conclusions and Future Work

- **Clients feedbacks to date**
 - Organization Value Sensitive
 - Organization IT Environment Sensitive
 - But not sensitive to unknown vulnerabilities
- **Future work**
 - COTS security evaluation
 - Extending vulnerability database
 - Better tool UI