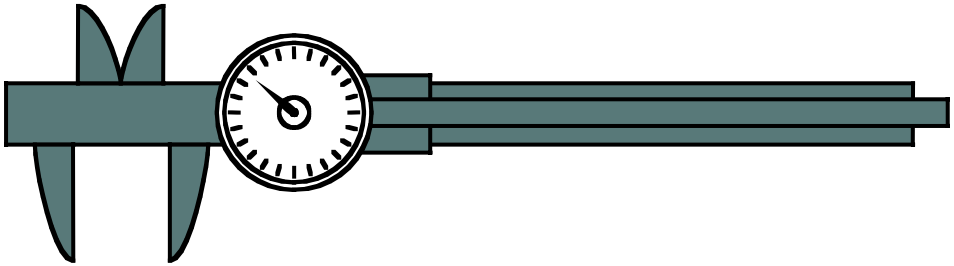
Measuring Assurance in Cyber Space



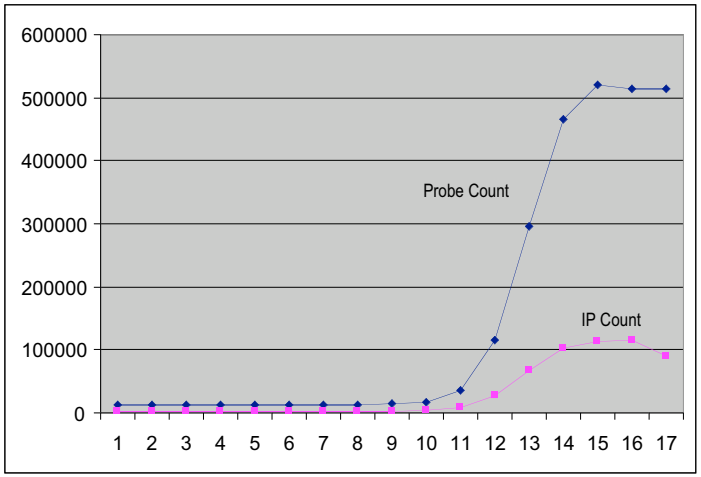
Jaynarayan H. Lala
DARPA
&
William H. Sanders
UIUC

44th Meeting of IFIP WG10.4
Monterey, CA
26 June 2003

Example Cyber Attack

Reality

- **Code Red Worm***
  - –Code Red I - July 17, 2001; Code Red II - August 4, 2001
  - –Exploits vulnerability in Microsoft's IIS Web Server software
  - –Performed a DOS attack against www.whitehouse.gov.
  - –Relatively benign payload. Defaces web sites.
  - –Infected 250,000 systems in 9 hours; 975,000 total



*GAO Report GAO-01-1073T of 29 August 2001

Imaginable

- **Andy Warhol Worm**
  - –Spreads throughout internet in 15 minutes
  - –Malicious payload, such as the Nimda virus
    - –Provides remote attackers "Administrator" privileges and access to entire file system

Sapphire/Slammer Worm

- Sapphire/Slammer worm recently affected Microsoft SQL servers.
- Required roughly 10 minutes to spread worldwide
- At its peak, Sapphire scanned the Internet at over 55 million IP addresses/second, causing major disruptions on the net*

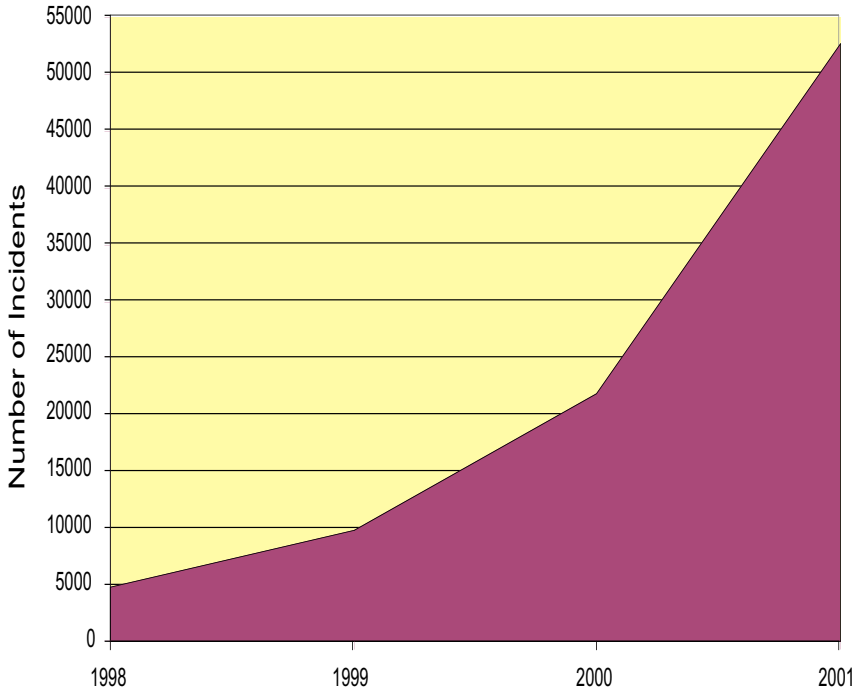
* http://www.silicondefense.com/sapphire/

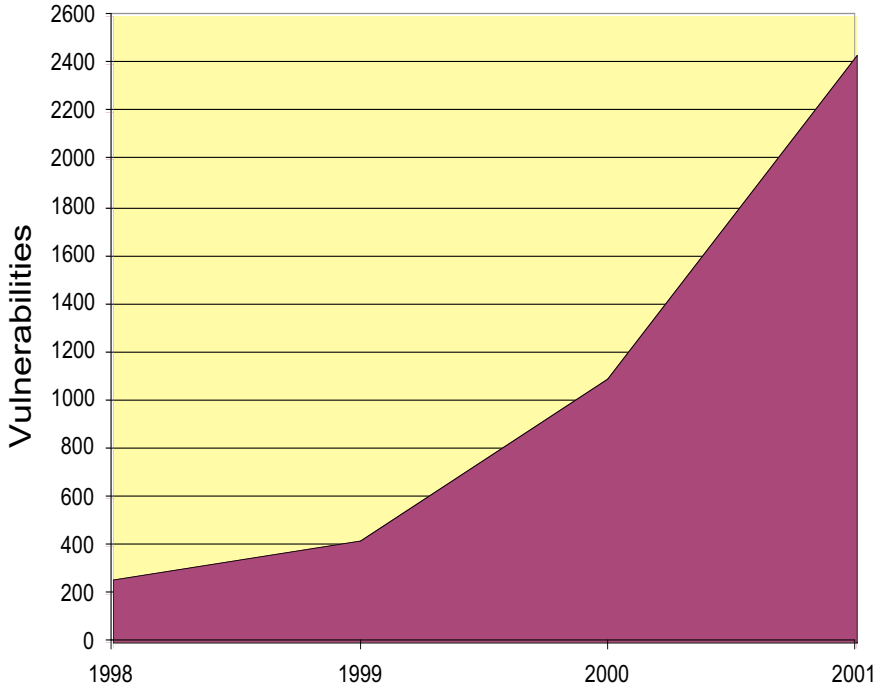
What was only imaginable a year ago, is now a reality!

Defending Against the Most Serious Attacks

Perfection is Impossible

Exponentially Growing Incidents and Vulnerabilities





****

SANS Critical Vulnerability Analysis

April 28, 2003 Vol. 2. No. 16

****

Widely Distributed S/W (1) HIGH: Cisco Secure ACS Username Buffer Overflow
(2) MODERATE: Microsoft IE Multiple Vulnerabilities
(3) LOW: Microsoft Outlook Express MHTML Vulnerability

Other Software (4) HIGH: BadBlue Server ext.dll Command Execution Vulnerability
(5) MODERATE: Apache mod_ntlm Heap Overflow and Format String Vuln
(6) MODERATE: Monkey HTTPd POST Body Buffer Overflow
(7) MODERATE: rinetd Connection List Resizing Vulnerability

Exploit Code Releases (8) Snort stream4 Exploit

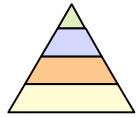
Intrusion Tolerance: A New Paradigm for Security

Prevent Intrusions
(Access Controls, Cryptography, Trusted Computing Base)

Trusted Computing Base

Access Control & Physical Security

Cryptography



Multiple Security Levels

But intrusions will occur

1st Generation: Protection

Detect Intrusions, Limit Damage
(Firewalls, Intrusion Detection Systems, Virtual Private Networks, PKI)

Firewalls

Boundary Controllers

Intrusion Detection Systems

VPNs

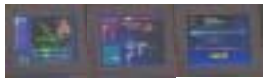
PKI

But some attacks will succeed

2nd Generation: Detection

Tolerate Attacks
(Redundancy, Diversity, Deception, Wrappers, Proof-Carrying Code, Proactive Secret Sharing)

Intrusion Tolerance



Big Board View of Attacks Real-Time Situation Awareness & Response

Graceful Degradation

Hardened Operating System

3rd Generation: Tolerance

Information Assurance Attributes*

- **Integrity**
  - Maintain data and program integrity in the face of intrusions and malicious faults.
- **Availability**
  - Counter Denial-of-Service attacks and maintain high system availability.
- **Confidentiality**
  - Prevent unauthorized disclosure of information.
- **Authentication**
  - Prevent unauthorized access.
- **Non-repudiation**
  - Method by which the sender of data is provided with proof of delivery and the recipient is assured of the sender's identity, so that neither can later deny having processed the data.

* Joint Pub 3-13 "Joint Doctrine for Information Operations"

Measuring Assurance: Research Goal

CONTEXT: Create robust software and hardware that are fault-tolerant, attack resilient, and easily adaptable to changes in functionality and performance over time.

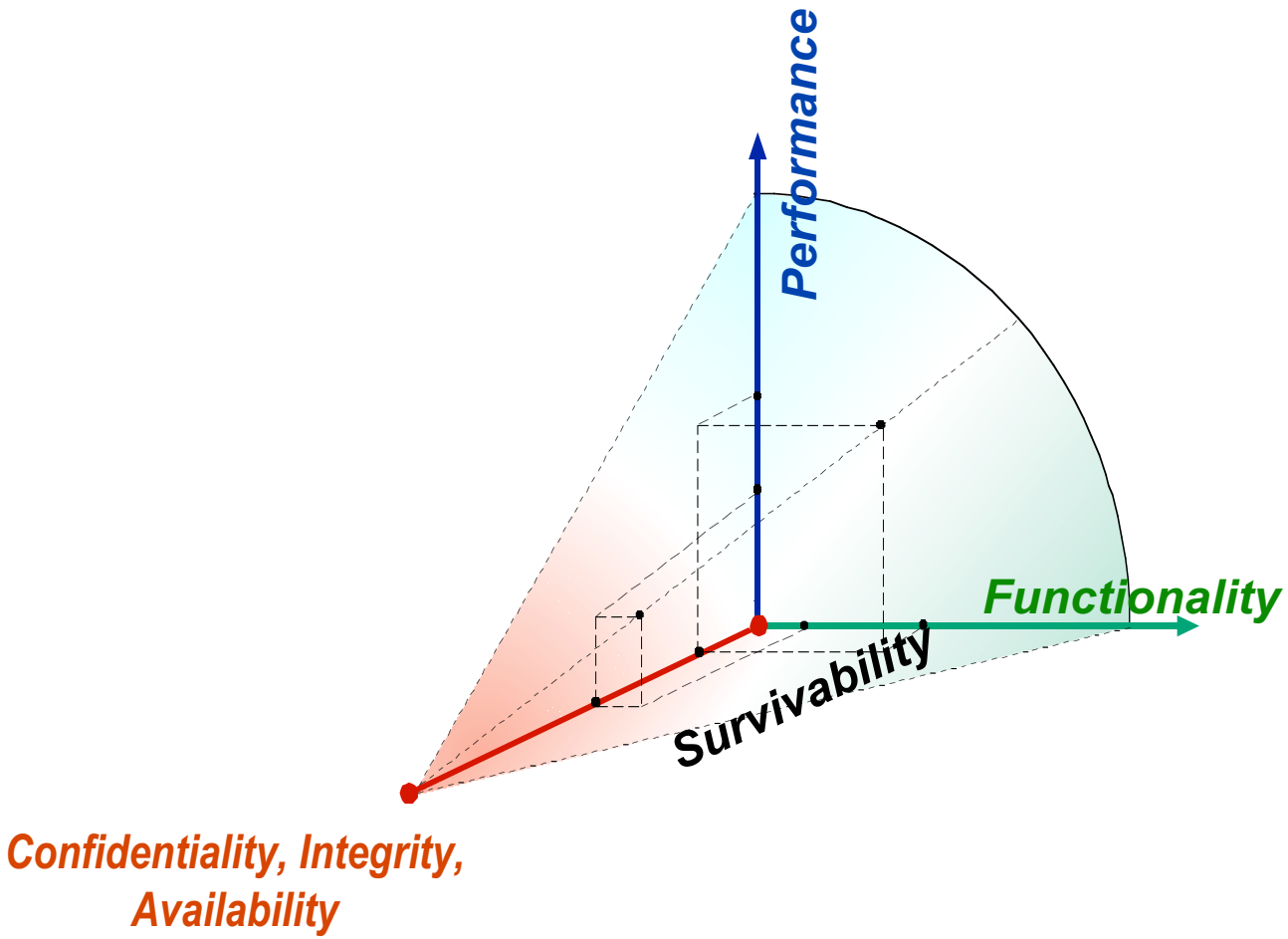
GOAL: Create an underlying scientific foundation that will:

- enable clear and concise specifications,
- quantify the effectiveness of novel solutions,
- test and evaluate systems in an objective manner, and
- predict system assurance with confidence.

Measuring Assurance: Challenges

- Unable to quantify how assured systems and networks are.
- Unable to quantify the ability of protective measures to keep out intruders.
- Difficult to characterize capabilities of intrusion detection systems to detect novel attacks.
- Benefits of novel response mechanisms cannot be measured comparatively or absolutely.

Placing a System in the Cone



Measuring Assurance: Major Focus Areas

- Basic concepts and terminologies to succinctly express IA domain issues
- Security and survivability requirement specifications
- Threat, attack and vulnerability taxonomies
- Models of attacker intent, objectives, and strategies
- Measures: Work factor metrics, survivability metrics, operational security metrics, cryptographic protocol metrics
- Methods for validating (via multiple methods) protection and tolerance mechanisms

Quantification Method Possibilities

- **Red Teaming**
- **Intrusion-Tolerance Cases**
  - Inspired by safety cases, where one reasons about the process used to create a system
  - Could involve Peer review
- **Intrusion Injection / Testing**
  - Inspired by fault injection from the fault-tolerant computing community, but requires new models of “attacks”
- **Probabilistic Modeling / Discrete Event Simulation**
  - Requires a probabilistic model of how an attacker behaves
- **Formal Methods**
  - May be untimed, timed but not probabilistic, or probabilistic

Claim: Some combination of these methods will be needed to gain confidence that system is intrusion tolerant.

Research Questions

1) **What are appropriate assurance measures?**
   - Binary - "Does the realization meet the specification?"
   - Multivalued - Reward/Penalty (or Cost) analysis
2) **In what system environment will the assessment/validation be performed?**
   - System context is as important as the scheme itself in the assessment/validation process!
3) **How will the attacker be modeled (just as important as system context)?**
4) **At what level of detail does a particular scheme, environment, and attacker need to be expressed?**
5) **Can we quantify the likelihood of the assumptions that are made (and use ideas from assumption coverage work and risk analysis to provide overall assessment)?**
6) **What existing techniques can be used, and what new techniques need to be invented?**

Who Benefits

- System integrators who are faced with hard tradeoffs between functionality, cost, and security
- System engineers who assemble systems from components and must say something about the security of the results
- Customers of the system integrators desiring assurance that the systems will behave as advertised
- Critical infrastructure operators and national security personnel using software with a known level of assurance

Workshop Goals

- Assess the state-of-the-art for quantifying system assurance
- Discuss recent research results
- Formulate the challenges to moving forward and potential new technical approaches to address the goals outlined earlier
- Have a good time!