

Privacy-Preserving Sharing and Analysis



Patrick Lincoln
SRI International

Joint Work

- SRI (Phil Porras, ...)
 - UT Austin (Vitaly Shmatikov, Vishwas,...)
 - Yale (Joan Fiegenbaum)
 - UPenn, Stanford, Cornell
-
- Implementation
 - Deployment
 - Analysis
 - Experimentation

Main Point

- Enable interesting interfaces to data
 - Protected by mathematics (cryptography)
 - Not just human trust (though that's very useful too)
 - Trusted third parties
 - Physical access control

General Goal

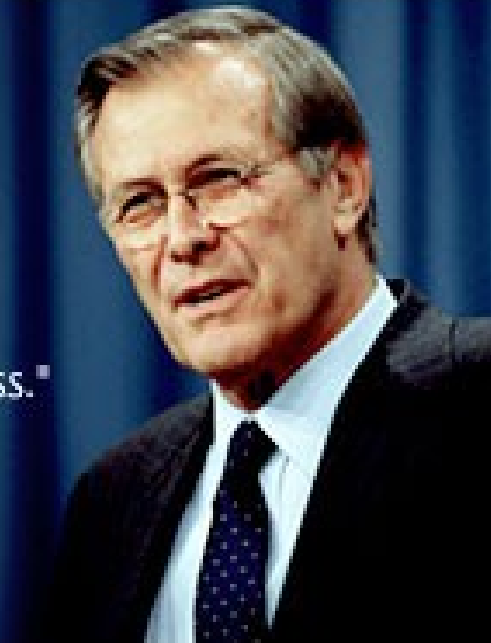
Enable enterprises to share information for sharing, regulatory and business purposes while maintaining a high level of security and organizational privacy.

Context: Networked Information Assets

- Huge and growing value of information networks
 - JV2020 predicates national security on information superiority
 - GIG (in particular, GIG-ES)

"Possibly the single most transforming thing in our forces will not be a weapons system, but a set of interconnections and a substantially enhanced capability because of that awareness."

SECRETARY OF DEFENSE
DONALD RUMSFELD
AUGUST 9, 2001



Context: Information Security

- There exist major threats to this future (present) DoD dependence on IT assets
- Defense against
 - Bots
 - Worms
 - Viruses
- The scale of the problem is large and growing rapidly
 - Robot armies
 - More and more successful attacks
 - Potential for malignant payloads

View Communications as a Threat?

- There are many serious information security threats to value, identity, and infrastructure in the present and future of our networks

Cyber Threats: Real or Imagined?

- Could someone use our cyber infrastructure against us?
- Amass an army of 1,000,000 robot machines under their control?
- Spy on all our keystrokes. Collect passwords, account numbers, our most important secrets?
- Unleash new virus/worm with devastating payload?

Brutal Reality

- Our infrastructure is being used against us
- An army of 1,500,000 robot machines was discovered by Dutch police October 2005
- Spyware toolkits used widely, SpearPhishing and other attacks compromise private information regularly
- Worms and viruses have big impact: CodeRed, I Love You, Klez, Nimda, and >75 new worms released in last 30 days

Threats to Computer Networks

- Old Problems That Won't Go Away
 - Denial of Service Attacks
 - Spam and Unwanted Email
 - DNS Hijackings
- New Problems In This Decade
 - Spyware, Adware, Phishing
 - Point-n-Click Tools
 - Large Bot Networks
 - Organized Crime and Fraud
 - Uncontrolled Wireless Access

Examples of Past Threats

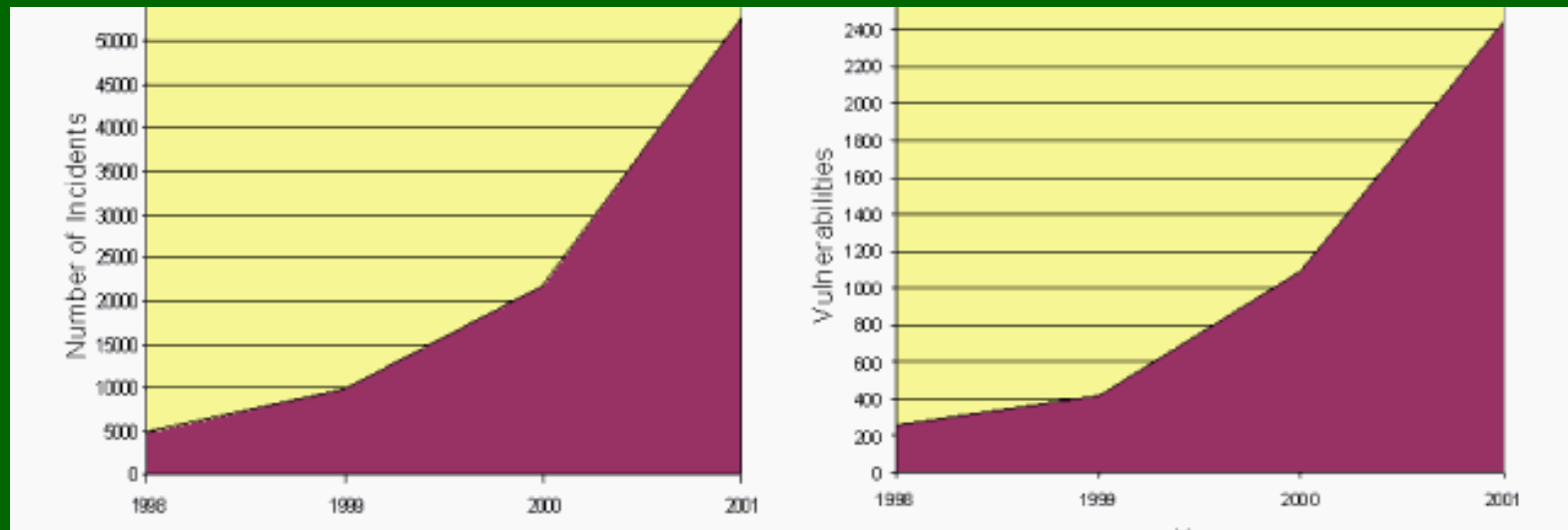
- Code Red, Code Red II, Nimda, SQL Slammer, MBlaster, MyDoom, Sasser
- Attacks of growing sophistication
 - Control, speed, infection success %
- Already serious consequences
 - Though fortunately, generally benign payloads

Name	Date	OS	Service	Infected Machines	Time
Lion	March 2001	Linux	BIND	10,000?	Days
Code Red	July 2001	Windows	IIS	200-400k	Days
Nimda	Oct 2001	Windows	IIS	100-200k	Hours
SQL Slammer	January 2003	Windows	IIS	100-200k	Minutes
MSBlaster	August 2003	Windows	IIS	300k?	Hours

Problems with Powerful Communication Technology: attacks on value, identity, and infrastructure

- Identity theft
- Phishing
- Spyware, snooping
- Password capture
- Ease of sharing
- Location, location, location
 - GPS and triangulation
- Identity of my trusted friends and partners
- Viruses
- Worms
- Games and marketplaces
 - Massive multiplayer
 - High (virtual) value
- Peer-to-peer filesharing
- Streaming, podcasting
- Calendar
- Document sharing

Vulnerabilities and Attacks Growing Exponentially

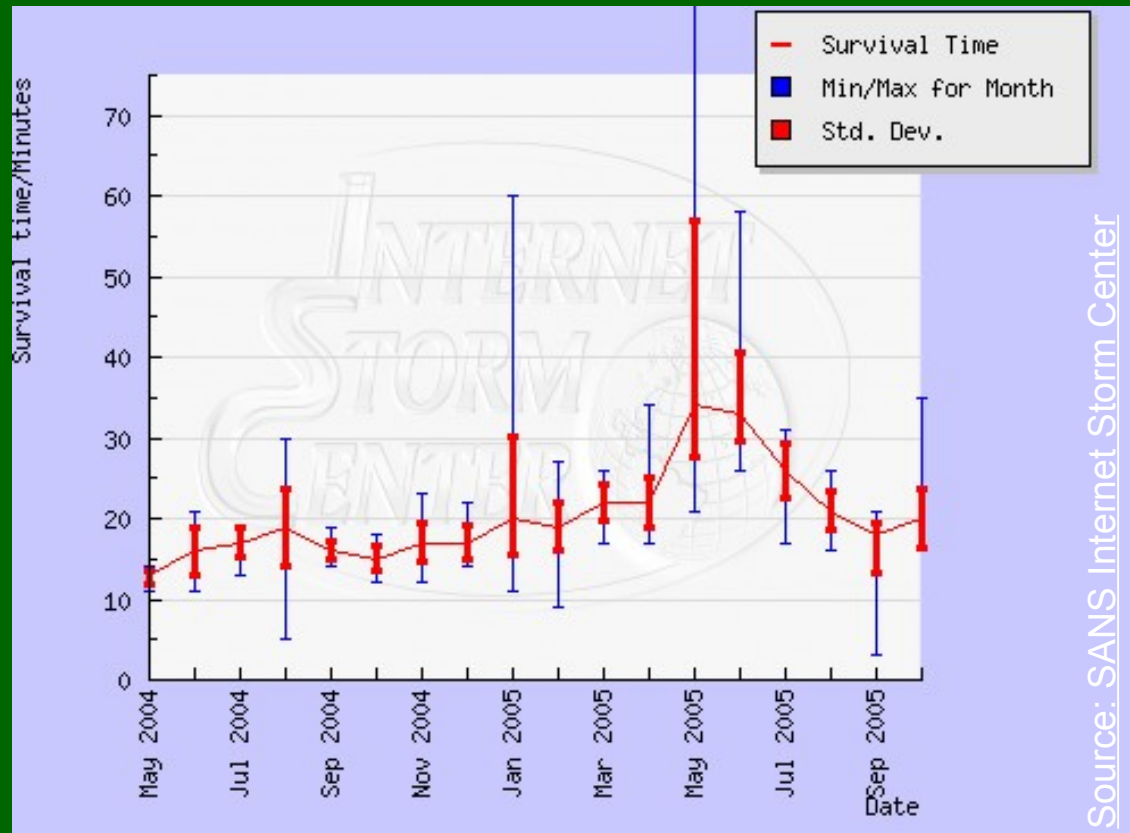


Incidents

Vulnerabilities

The Internet is a Hostile Environment

Connect a fresh, unpatched machine: How long before it is attacked?



Time-to-first-attack can be **SHORTER** than time to download and install the latest patches!

ISC Database of Infected Hosts

Persistence (days)	Infected Hosts	Last Reported	AS Number	AS Name
169	191	2005-04-25	12874	FASTWEB
167	738	2005-04-25	8070	MSFT Microsoft Corp
167	219	2005-04-24	5731	AT&T WorldNet Services
166	149	2005-04-25	11643	EBAY eBay, Inc
166	188	2005-04-25	1664	AOL America Online
164	125	2005-04-26	721	DoD NIC
164	150	2005-04-27	26101	YAOO Yahoo!
160	264	2005-04-25	12076	HOTMAI Hotmail
159	343	2005-04-25	15468	KLGELECS
158	1546	2005-03-31	6400	Codetel

Point-n-Click Tools

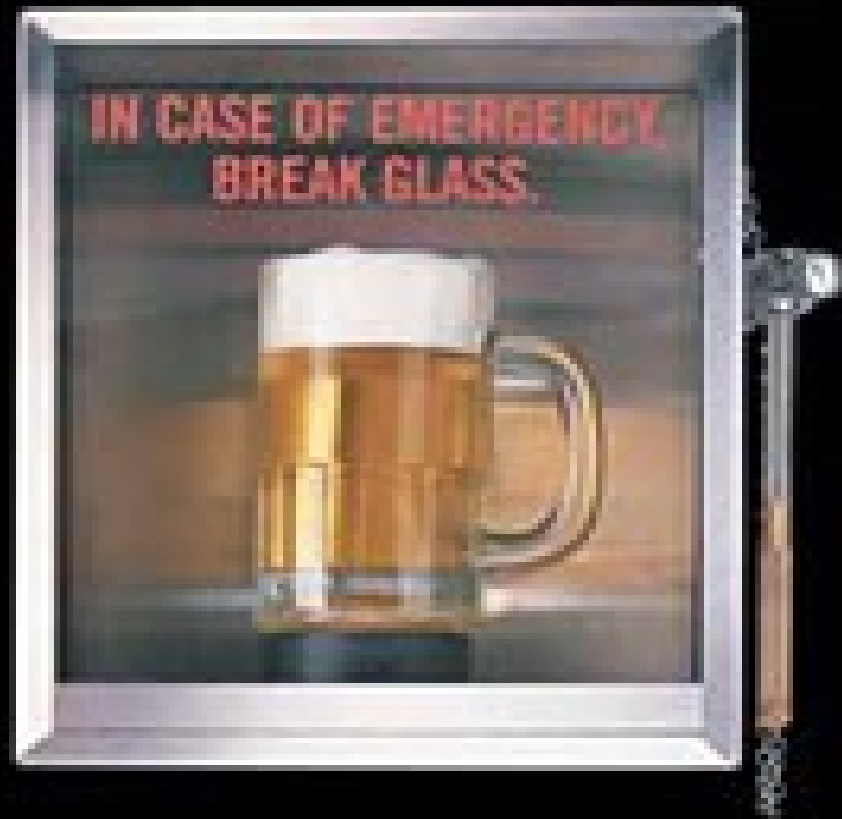
- Hacking tools are updated as new exploits are found
- Lethal when combined with a scanner
- Interface is a GUI
 - Windows/Linux application or web application
- Metasploit is most popular
 - Contains dozens of canned exploits
 - Makes hacking as easy as a mouse click
 - No understanding of computer science needed
- Defenders must move faster, share information, be aware of cracker community moves

Culture of Cyber Research?

Cyber Security Leadership

- We (The Known Universe) lack strategic vision and leadership for cyberspace security. The National Strategy to Secure Cyberspace was a good start, but few government and private sector organizations are acting on the recommendations.

In Case of Cyber-Attack



Why Are Attackers More Successful?

- More vulnerabilities

- More systems being created
- More features being added
- More automated software updates
- More instances
- More networks

Attacker's practice of sharing and building on others work

Out-Share or Lose

- Attackers and their machines share vulnerability information (rapidly, efficiently)
 - Virus writers, worm writers, crackers, script kiddies, etc.
 - Email, chat rooms, IRC, web sites, p2p, IM, etc.
 - Network effect works to their advantage
 - Build on others work
- Currently many defenders (network administrators) do not share detailed information automatically with others outside their organization
 - Precious little. Ponderously slow publication cycle

Problem:

- "Good guys" (people and organizations) are resistant to sharing
- Legal, organizational, and historical reasons NOT to share
- Perception of little individual benefit of sharing
 - Relates to main theme

Privacy Interests

- Personal privacy

- Medical, financial, other detailed information
- Implied by U.S. Constitution

- Organizational privacy

- Financial information
- Trade secrets
- Legal but secret business practices
- Competitive advantage

Preservation of competitive advantage

Information Sharing With Privacy Implications

- Communication records
 - ISP, Cellphone (calls, location)
- Financial transaction records
 - Fraud detection, corporate audit and oversight
- Medical informatics
 - Public health monitoring, research on interactions
- Airline passenger databases
 - Anti-terrorism, intelligence, law enforcement
- Computer network monitoring
 - Worm, virus, intrusion detection

Need to protect individual and organizational privacy while enabling sharing and monitoring

What is Needed

- Ability to strongly protect information from some kinds of abuse
- Delivering enough collective benefit of analysis to overcome perception of risk of sharing
- Getting the good guys to share more than the bad guys

On to Vitaly...

Joint Work

- SRI (Phil Porras, ...)
 - UT Austin (Vitaly Shmatikov, Vishwas,...)
 - Yale (Joan Fiegenbaum)
 - UPenn, Stanford, Cornell
-
- Implementation
 - Deployment
 - Analysis
 - Experimentation