NPACI/SDSC Security Activities

Tom Perrine
San Diego Supercomputer Center
tep@sdsc.edu

1

My Goal is...

- to convince you that
  - you need to care about security
  - security is the core service that enables all other services
- to explain what we are doing to protect our users
- to help you learn to protect yourself

2

NPACI Incident Response

- users report to local security activity (if any)
- users may report directly to UTexas or SDSC (7x24 coverage)
- NPACI security contacts at security.sdsc.edu

3

SDSC Security Activities

- Research - PICS
- Operational - Security Technologies
- Awareness, education, partnerships

4

Pacific Institute for Computer Security (PICS)

- funded directed research
- complementary to SecTech, CERT, COAST, vendors
- multi-year program
- looking at (designing!) next years threats

5

Security Technologies (SecTech)

- operational day-to-day security
- network and host monitoring
- policies, standards, guidelines, procedures
- consult to system administrators
- testbed for PICS tools

6

Partnerships

- San Diego Regional Information Watch (SDRIW)
- High Tech Criminal Investigation Association (HTCIA)
- NPACI
- UCSD Network Operations
- DoD HPC Modernization Office

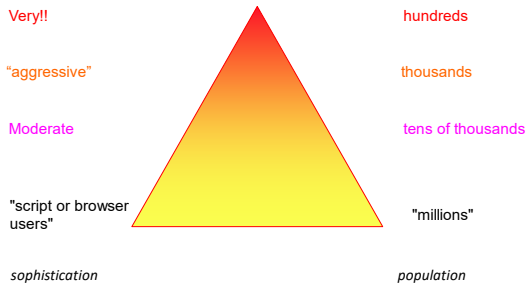
Our Security Goals

- safe, but otherwise as open as possible
- low cost to recover from incidents
- "It's not our (only) job."
- protect our computing infrastructure and our customers
- be a security asset to the Internet community

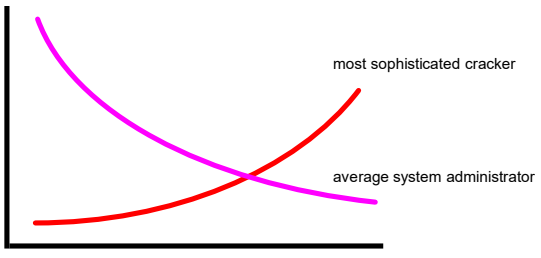
The Threat

- threats at differing levels of sophistication
- lots of "ankle-biters", mostly harmless to us
- fewer, but more sophisticated
- very few, but extremely dangerous
- they exploit the tool "food chain"

Threat Pyramid



Sophistication Trends



Sample of Incidents

- East Coast University
- Web Servers
- Denial of Service
- DoD "joy riders"
- Theft of intellectual property
- university web site defaced with porn

East Coast University

- hundreds of hosts
- tens of groups of intruders
- "wars" over parts of the campus nets
- took months to clean up

Denial of Service

- "smurf", "flood", "teardrop", etc.
- can cause DoS to large networks with a PC and a modem
- common as dirt
- very hard to trace

DoD "joy riders"

- two California teens
- dozens of DoD sites (and .COMs and .EDUs)
- could have unintentionally masked more serious efforts
- we were lucky

Theft of PhD work

- northern California
- PhD thesis notes stolen and accepted for publication in journal by someone else
- never proven - suspected stolen from public file server
- a different University has ID'ed theft of work as **primary** security concern

Funded work stolen and patented

- industry-funded research at a .EDU stolen/copied
- patents filed by funding company's competitor
- grant not renewed

Phantom Menace and The Matrix

- illegal copies found on university computers
- advertised on web for sale
- university served with court orders

University Web Site defaced with porn

- research group's web and FTP site taken over and used to distribute pornography
- massive embarrassment
- also held stolen software, could have cost $$$ from SPA

Current events (since 1 June)

- 2 intrusions at SDSC
  - password sniffed at remote site
- 60+ probes/sweeps at SDSC
- 5+ intrusions at UCSD
- 297 web site defacements
  - 6 .MIL
  - 33 .EDU
  - 6 NASA
  - 25 .GOV

Security Policy

- protect users - data, proprietary information, privacy
- protect infrastructure
- enable new ways to use resources (safely)
- avoid service interruptions
- prevent unauthorized use and abuse of resources

User Authentication

- "be liberal in what you accept"
- support as many authentication schemes as we can afford
- end goal - no plain-text passwords for any service

Supported Authentication Mechanisms

- Kerberos Version 5
- Secure Shell (SSH)
- SSL+LDAP for HTTP - integrate w/K5 when practical
- SecureNetKey (SNK) tokens
- S/Key
- plain text passwords - GONE!

Host/network monitoring

- TCP wrappers installed on ALL UNIX hosts
- PICS research network monitors on DMZ network
- centralized logging of all UNIX hosts, NT in progress
- PICS/SecTech log analysis - 1.1 million records/day (6/29/1999)

Why you should protect yourself

- you have things of value
  - intellectual property
  - reputation
  - personal privacy
- "privacy act data"/"medical records data"
- possible loss of $$$ sponsorship

How you can protect yourself

- insist on secure services
- encryption is Good (https, imaps, SSH, Kerberos)
- install SSH and use it
- turn off TELNET and FTP

References

- http://security.sdsc.edu
- http://www.sdriw.org
- http://sd-htcia.com
- http://www-no.ucsd.edu