Security: Myths, Reality, Effectiveness

Abe Singer & Sean Peisert
San Diego Supercomputer Center
Quick Overview

Intro
Myths, realities, and unknowns
What security is
Security strategies
Evolution of security at SDSC
DTF/Teragrid
Incident management
Parting thoughts
SDSC Story

3 years, no intrusions
No Firewalls
Myths
Myths

It takes a genius
I’m not a target
“Hackers” are the biggest threat
Imperfect Security == No Security
Myths

Obscurity is good enough
The end-user is responsible
They don’t really do any damage
<technology> is the answer
Realities
Myth 1

It takes a genius
It only takes one genius
Myth 2

You’re not a target
Many attacks are “random”
Myth 3

“Hackers” are the biggest threat
“Insiders” are an even larger threat
Myth 4

Imperfect security == no security
Decent security raises the bar
Myth 5

Security through obscurity is good enough
Only the first time
Myth 6

The user is responsible...

Users can’t fix broken software
Myth 7

Intruders don’t really cause damage

Intrusions cost somebody money
Myth 8

<technology> will solve everything

- Firewalls,
- PKI
- Anti-virus
- Intrusion Detection

Technology is only a piece of the puzzle
Where firewalls fail

Can’t handle high speed and multi-route networks
Don’t protect from internal attacks
Don’t work well with many protocols
Are difficult to configure and maintain
Don’t pay attention to content
Where PKI fails

PKI is only an authentication mechanism
- no authorization included

User certificates must be kept safe
- and the Certificate Authority

Revocation doesn’t scale well
Where AVI and IDS fail

Reactive -- only address known threats
  • always behind the curve
IDS is detection only
NIDS doesn’t scale well
Unknowns
Unknown

We don’t really have any good metrics

How long until a system is compromised?

What’s the acceptable window of time for installing patches?

Is product A more secure than product B?
Practicality
What is Security

It’s a process to provide…

- Reliability
- Integrity
- Confidentiality
- Accountability
What is Security

Three points of security:

- Prevention
- Detection
- Recovery
Why Security?
Why Security

Reduce support costs
Reduce downtime
Reduce loss
Measure (and charge) for usage
Improve efficiency
Prevent being used to attack someone else
General Security Strategy
Strategy

Protect what you can
Detect what you can’t
Strategy

Software
Network
Systems
Plan for failure
Group Therapy
Don’t roll your own
Test for failure
Keep a list
  • naughty *and* nice
Network

No plaintext passwords
Strong authentication
Systems

Patch early, patch often
Strong configuration management
Good audit trails
Incident management
Policy enforcement
User awareness
The SDSC Story
Rapidly changing environment
  • sometimes bleeding edge
Very high speed networks
Most users not local
Heterogeneous environment
SDSC Story

In the beginning
Rampant intrusions
Fix one system, they’d compromise another
  • “whack-a-mole”
SDSC Story

The cleanup

- Took everything off-line
- Systems not brought on-line until they were in a known, secure configuration.
- Director said he never wanted to do that again
SDSC Story

Since then

- “Reference Systems” -- scalable configuration management
- Aggressive patch installation
- “Trusted” vs. “un-trusted” networks
- Slowly eliminated plaintext passwords
Reference system

Known good configurations

- no unnecessary services
  - workstations aren’t servers
- only setuid where necessary
- tcp-wrappers on all allows services
- proper permissions on files, directories
- replace config files
Reference system

Cfengine for scalable configuration management

- central database containing configuration information
- detects and fixes things out which have been changed
  - self-healing
- OS independent
Reference System

• Database kept on central, read-only NFS partition
  - can’t be changed from a compromised desktop

• Run on boot and nightly

Cost of adding or replacing a host is nominal
Patching

One person per OS
  • tests
  • distributes

Different distribution schemes per OS
Networks

Trusted networks

- only reference systems allowed
- NFS server has routes only to these networks
- SMB only on windows network
- Appletalk only on Mac network

Untrusted networks

- for non-reference systems
Eliminating Plaintext Passwords

Started with

- Kerberos
- SSH
- SNK when Kerberos and SSH not available
- Still had to support telnet, as clients were unavailable and/or costly
- No solutions for FTP, POP, IMAP, etc.
Eliminating Plaintext Passwords

Over time

- Open source/free SSH clients became available
- Open source SSL software
- September 1998, we turned off telnet
Eliminating Plaintext Passwords

The last steps

• IMAP/S, KPOP, APOP, and secure webmail for e-mail access.
• Secure-FTP software developed
• SFTP protocol as part of SSH v.2
• Recently eliminated SNK
Audit trails

Central syslog server
• All host forward log entries
• Windows logging coming soon
• Moving to secure syslog and reliable transport

System process accounting
User session accounting (wtmp)
DTF/Teragrid
DTF -- What it is

5 sites, each with their own

- “Similar” clusters
- Security policy
- Certificate Authority
- User Account Management
- GSI authentication “standard”
DTF -- What’s not there

No global security policy
No incident response plan
DTF -- Current issues

How to honor a certificate from another CA with a different policy
Dependence on particular software packages (e.g. Globus)
What is acceptable patching strategy?
DTF -- Future

More Sites
Different OS’s -- more complexity
More trust relationships between sites
Centralized account management
Automated jobs across clusters
Incident Management
Incident Management

General principles

- Don’t Panic!
- Don’t change anything!
- Get some help
- Take copious notes
- Be clear what your goal(s) are...
Incident Management

What are your goals?

- Stop the activity
- Restore the system/repair damage
- Close the hole
- Hunt down/destroy the intruder
- How about reporting to law enforcement?
Incident Management

Verify there’s a compromise
  • often there isn’t

Determine the nature of the compromise
  • who, what, when, where, how

Maybe watch for a while

Collect and preserve evidence
Incident Management

Take down system(s)
- don’t use shutdown
- pull the plug instead

Image drive(s)
- preserve original drive if possible

Reformat and re-install system
- don’t try and repair existing system
Incident Management

Be sure to plug the hole that the intruder used

- On all systems that are vulnerable
Some Questions you should be able to answer
Some questions

How fast can you locate a machine?
- Given its IP address?
- Given some traffic indicators?
- If it’s wireless?

What activity is logged?

How long are logs kept?

What has user X done?

How fast can you rebuild a system?
The End