Threat Modeling Networks

Jesper M. Johansson
Senior Security Strategist
Microsoft Corporation
jesperjo@microsoft.com
http://blogs.technet.com/jesper_johansson

Fundamental Tradeoff
You get to pick any two!
Secure
Usable
Cheap

Perimeters Are Weak

Defense in Depth
Threat Modeling is one part of a Defense in Depth strategy
Supplement it with other measures

People, Policies, & Process
OS hardening, patch management, authentication, HIDS
Firewalls, VPN quarantine
Guards, locks, tracking devices
Application hardening, antivirus
ACL, encryption
Network segments, IPSec, NIDS
User education

Lessons Learned From Experience
Most security tweaks do not improve security
Security changes without a threat model do not improve security
Focus is often on the wrong thing
Analysis of target environment is essential
Threat model must correlate with security policy
Group policy is a bonus
Careful smoke-testing needed

Applying the lessons - DSR
Document
Model applications and services
Environment dependent
Segment
Applications
Security requirements
Restrict
Disable services
Close ports
Use IPSec or RRAS filters
Use different passwords
Modeling Systems with DFDs

- Graphic representation showing communication between objects
- Describes activities that process data
- Shows how data flows through a system
- Shows logical sequence of associations and activities
- Sometimes known as a process model
- We are appropriating and modifying this method

Modified Data Flow Diagram Conventions

- Data Flow
- External Entity
- System or Application
- Replicated External Entity

Model The Network

Component Segmentation

Superimpose a DFD
**Network Segmentation**

- Segment systems by application and security requirements
- Should you trust systems that are not part of your application?
  - Which systems do they trust?
  - What are their security requirements?
- Less sensitive systems may depend on more sensitive systems
- More sensitive systems MUST NEVER depend on less sensitive systems

**End Goal**

**Documenting Segments**

**Trust Boundaries**

- Systems and entities you trust are included within your trust boundary
- Never share administration and accounts across boundaries
- Should your trust boundary include databases?
  - It depends…

**Threat Analysis**
Fault Trees

- Demonstrate logical paths through a system
- Used to highlight faults in a system
- Points out relationships between faults
- Allow us to estimate the interactions between faults

Goal: Root the SQL Server

Preventative Measures

- Break here by restricting outgoing traffic from servers
- Break here with best practices
- Break here with SQL hardening
- Break here with IIS lockdown

Restrict

- Policies allow nothing but...
  - Disable unnecessary services
  - Remove users
  - Restrict privileges
  - Turn on security tweaks
  - Remove permissions
  - Set very strong passwords
  - Restrict communications
  - IPSec
  - RRAS filters

Manage Administrative Dependencies

- An administrator on any given machine can run code as any user logging on to that machine
- What other machines do your admins log on to?
- Who administers those machines
- Administrative dependencies balloon – fast!
- Enumerating actual administrators is hard
Dependency Chain Example

1. Hacks Test Host, gets account “Cedric”
2. Uses Cedric’s account to compromise SQL Server
3. SQL Server gives up account “Bob”
4. Bob is an Admin on the Web Server
5. Web server has service account _Svc
6. Uses Cedric’s account to compromise SQL Server
7. SQL Server gives up account “Bob”
8. Bob is an Admin on the Web Server
9. Web server has service account _Svc
10. _Svc is a domain admin!

Conclusion

- Hardening networks requires understanding the environment.
- Optimal hardening requires deep understanding.
- There is a fundamental tradeoff between security and usability.
- Three-phase approach to network hardening.

Resources

- Microsoft Guide to Security
- Windows XP Security Guide
- Security Bulletins
- Security News
- Patch Management
- Security and Training
- Security Guidance Center
- Technical Information
- My Email: jesperjo@microsoft.com
- Use promo code JJSR6437

For more information

See Chapters 8 and 9

Order online:
http://www.awprofessional.com/title/032133643
7
Use promo code JJSR6437

© 2004, Microsoft Corporation, All Rights Reserved

Limit Service Account Trust Environment

- Any admin can retrieve service account credentials.
- Service accounts frequently have administrative privileges...
- ...on several machines.
- Implements the “least common security denominator”.
- Consider security needs.
- NetworkService and LocalService are useful, to a point.

Secure Your Environment

- Limit Service Account Trust
- Three-phase approach to network hardening
- Consider security needs
- Use promo code JJSR6437

Conclusion

- Hardening networks requires understanding the environment.
- Optimal hardening requires deep understanding.
- There is a fundamental tradeoff between security and usability.
- Three-phase approach to network hardening.
- Consider security needs
- Use promo code JJSR6437

For more information

See Chapters 8 and 9

Order online:
http://www.awprofessional.com/title/032133643
7
Use promo code JJSR6437

My Email: jesperjo@microsoft.com

© 2004, Microsoft Corporation, All Rights Reserved

Resources

- Microsoft Guide to Security
- Windows XP Security Guide
- Security Bulletins
- Security News
- Patch Management
- Security and Training
- Security Guidance Center
- Technical Information
- My Email: jesperjo@microsoft.com
- Use promo code JJSR6437

© 2004, Microsoft Corporation, All Rights Reserved