

Threat Modeling Networks

Jesper M. Johansson
 Senior Security Strategist
 Microsoft Corporation

jesperjo@microsoft.com
http://blogs.technet.com/jesper_johansson

Fundamental Tradeoff

Secure

Usable

Cheap

You get to pick any two!

© 2004, Microsoft Corporation, All Rights Reserved

Perimeters Are Weak

© 2004, Microsoft Corporation, All Rights Reserved

Defense in Depth

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

© 2004, Microsoft Corporation, All Rights Reserved

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

© 2004, Microsoft Corporation, All Rights Reserved

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

© 2004, Microsoft Corporation, All Rights Reserved

Document

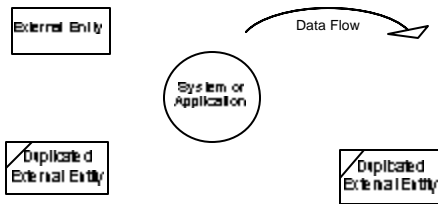
© 2004, Microsoft Corporation, All Rights Reserved

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

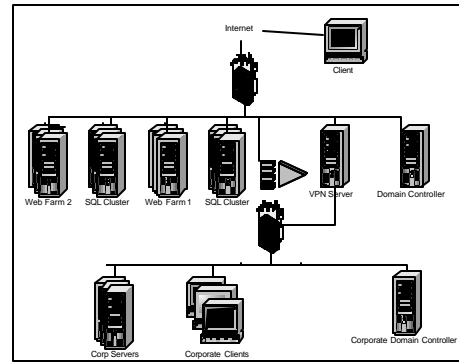
© 2004, Microsoft Corporation, All Rights Reserved

Modified Data Flow Diagram Conventions

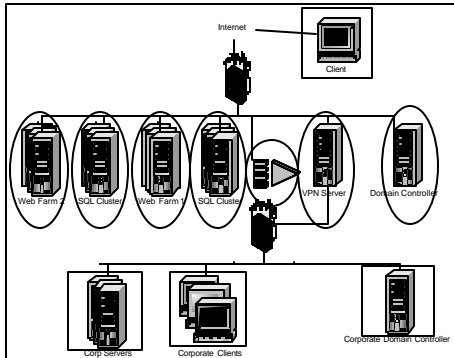


© 2004, Microsoft Corporation, All Rights Reserved

Model The Network



Superimpose a DFD



© 2004, Microsoft Corporation, All Rights Reserved

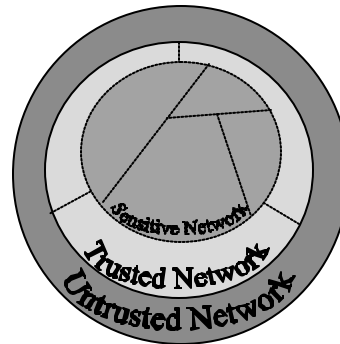
Component Segmentation

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

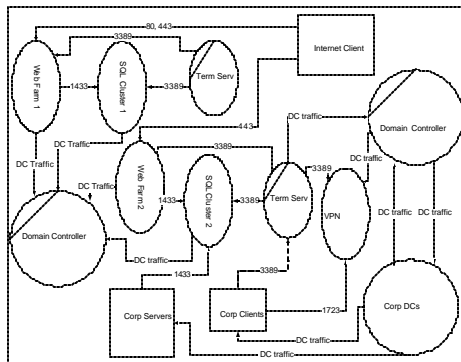
© 2004, Microsoft Corporation, All Rights Reserved

End Goal



© 2004, Microsoft Corporation, All Rights Reserved

Documenting Segments

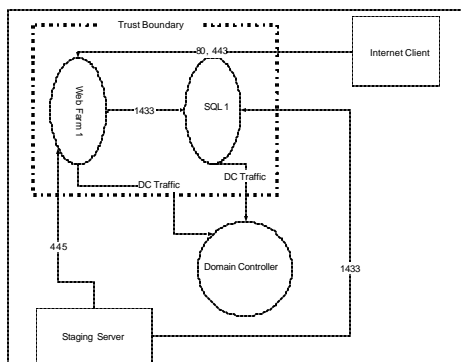


Trust Boundaries

- 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 ...

© 2004, Microsoft Corporation, All Rights Reserved

Trust Boundaries



Threat Analysis

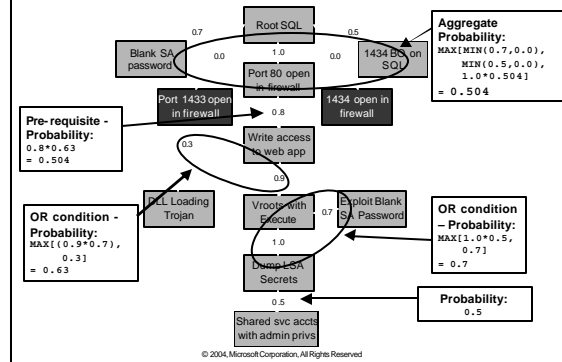
© 2004, Microsoft Corporation, All Rights Reserved

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

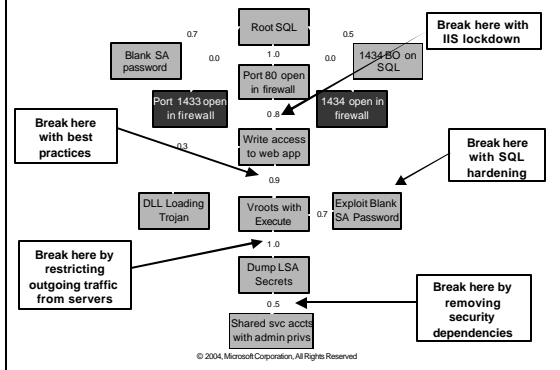
© 2004, Microsoft Corporation, All Rights Reserved

Goal: Root the SQL Server



© 2004, Microsoft Corporation, All Rights Reserved

Preventative Measures



© 2004, Microsoft Corporation, All Rights Reserved

Restrict

© 2004, Microsoft Corporation, All Rights Reserved

Restrict

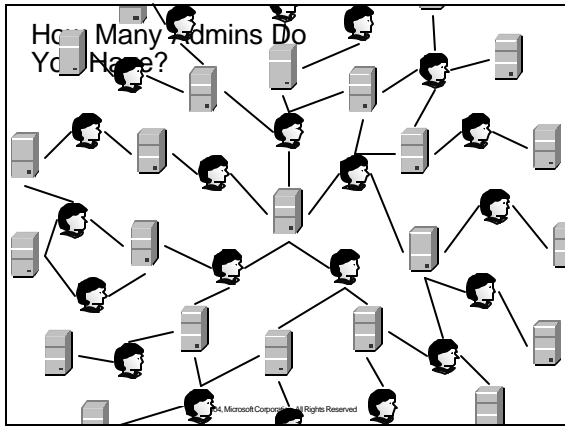
- Policies allow nothing but...
 - Disable unnecessary services
 - Remove users
 - Restrict privileges
 - Turn on security tweaks
 - Remove permissions
 - Set very strong passwords
- Restrict communications
 - IPSec
 - RRAS filters

© 2004, Microsoft Corporation, All Rights Reserved

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

© 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

© 2004, Microsoft Corporation. All Rights Reserved

Dependency Chain Example

- Hacks Test-H... gets account "Cedric"
- Uses Cedric... to compromise SQL Server
- SQL Server... account "Bob"
- Bob is an Admin on the Web Server
- Web server has service account _Svc
- _Svc is a domain admin!

Attacker

© 2004, Microsoft Corporation. All Rights Reserved

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
 - Document
 - Segment
 - Restrict

© 2004, Microsoft Corporation. All Rights Reserved

For more information

See Chapters 8 and 9

Order online:
<http://www.awprofessional.com/title/0321336437>

Use promo code
JJSR6437

jesperjo@microsoft.com

© 2004, Microsoft Corporation. All Rights Reserved

Resources

Tools Registry Monitor, File Monitor, Process Explorer, etc. http://www.systemmax.com My Email: jesperjo@microsoft.com	Security news Security Bulletin Notifications http://go.microsoft.com/fwlink?LinkID=21163 Security Bulletins http://www.microsoft.com/technet/security/current.aspx
Technical information Security Guidance Center http://www.microsoft.com/security/guidance MBSA http://www.microsoft.com/technet/security/tools/mbsa.ms QoSack IV Hardening http://msdn.microsoft.com/library/whidsp/zh-hk/sec/html/qsack.asp Jesper's Security Columns http://go.microsoft.com/fwlink?LinkID=29702 Threats and Countermeasures http://go.microsoft.com/fwlink?LinkID=15153	Security guidance and training Windows 2000 Security Hardening Guide http://go.microsoft.com/fwlink?LinkID=28591 Windows Server 2003 Security Guide http://go.microsoft.com/fwlink?LinkID=14846 Windows XP Security Guide http://go.microsoft.com/fwlink?LinkID=14839 Exchange Server 2003 Security Hardening Guide http://go.microsoft.com/fwlink?LinkID=26210 Microsoft Guide to Security Patch Management http://go.microsoft.com/fwlink?LinkID=16264

Jesper M. Johansson
jesperjo@microsoft.com

Microsoft
Your potential. Our passion.

© 2004-2005 Microsoft Corporation. All rights reserved.
This presentation is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.