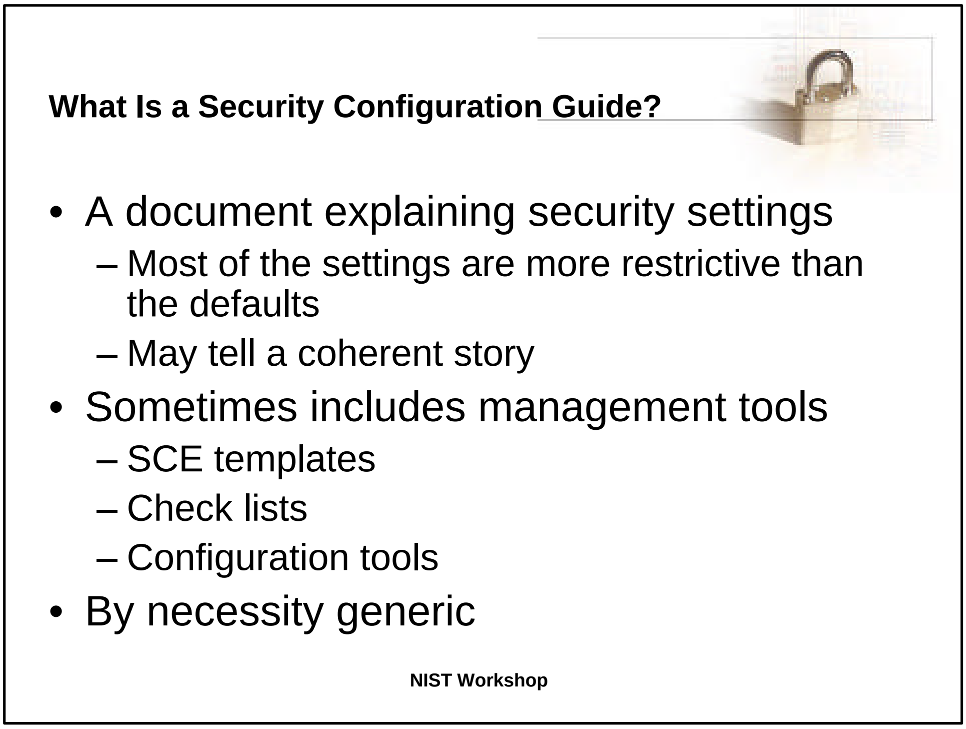
Producing Quality Security Checklists

Jesper M. Johansson, Ph.D., MCSE
Security Program Manager
Security Business Unit
Microsoft Corporation

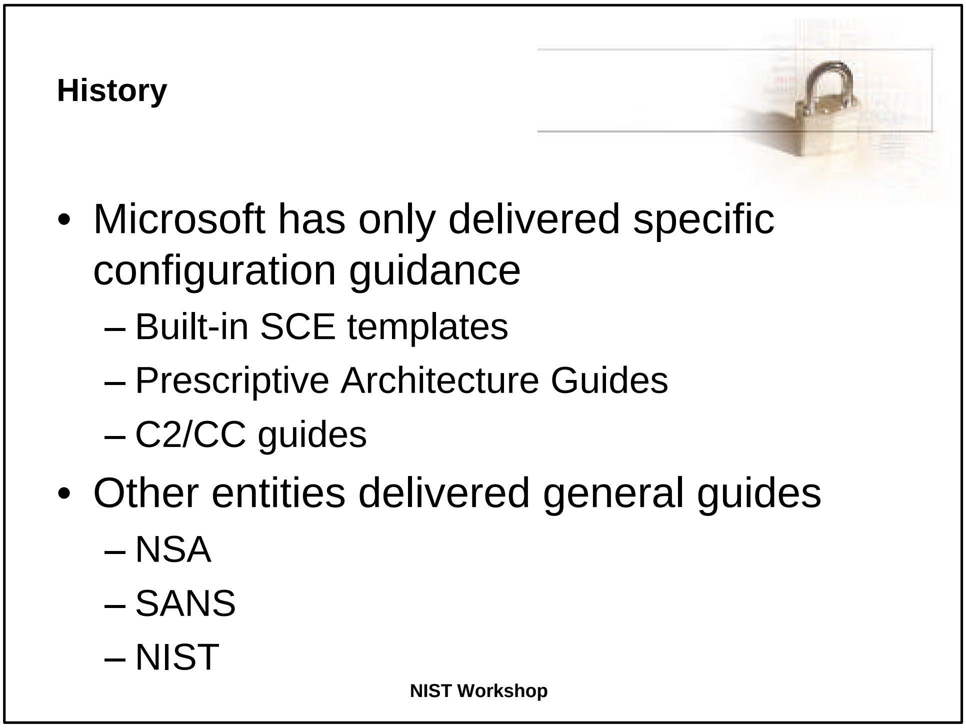
Overview

- History behind security configuration guidance
- Why it is difficult to produce security configuration guidance
- Security configuration guidance is by necessity simplistic
- Microsoft roadmap
- Conclusion



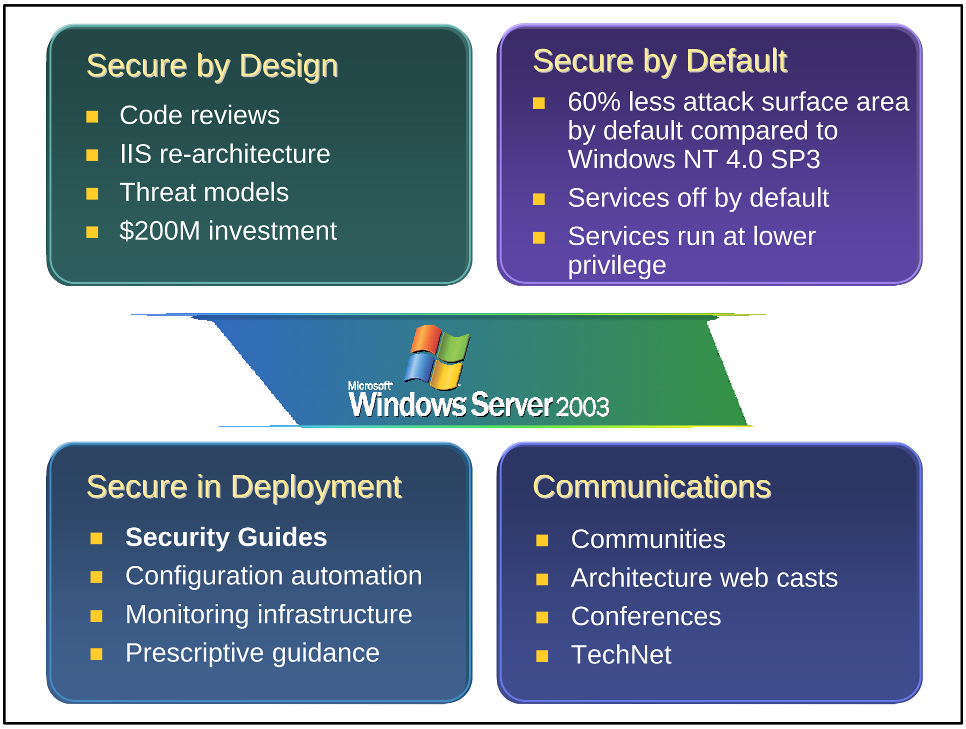
What Is a Security Configuration Guide?

- A document explaining security settings
  - Most of the settings are more restrictive than the defaults
  - May tell a coherent story
- Sometimes includes management tools
  - SCE templates
  - Check lists
  - Configuration tools
- By necessity generic



History

- Microsoft has only delivered specific configuration guidance
  - Built-in SCE templates
  - Prescriptive Architecture Guides
  - C2/CC guides
- Other entities delivered general guides
  - NSA
  - SANS
  - NIST



Secure by Design

- Code reviews
- IIS re-architecture
- Threat models
- $200M investment

Secure by Default

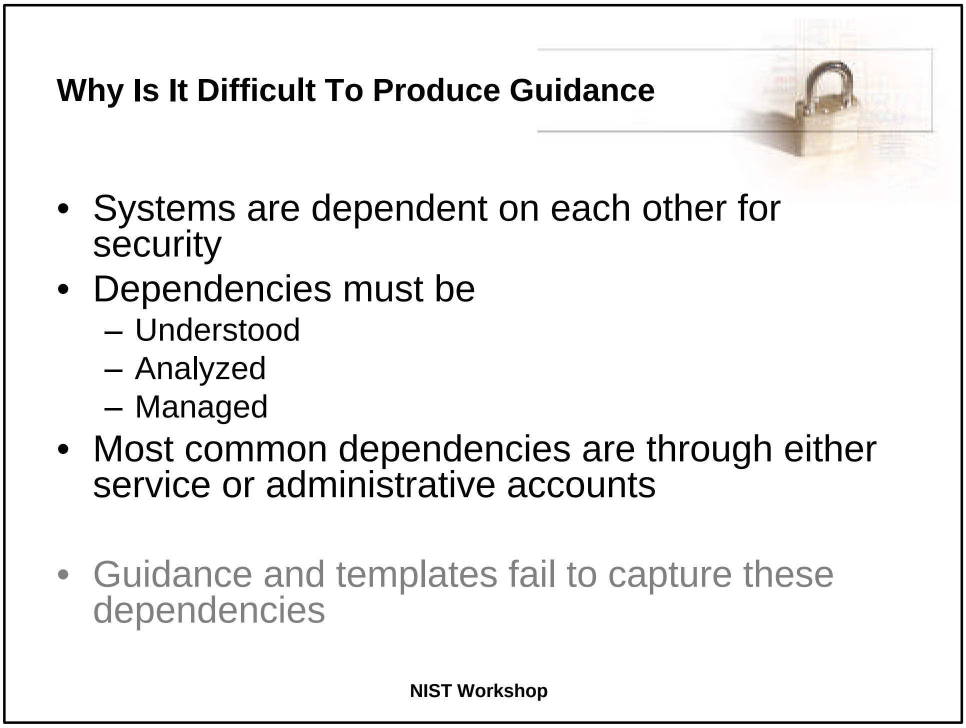
- 60% less attack surface area by default compared to Windows NT 4.0 SP3
- Services off by default
- Services run at lower privilege

Secure in Deployment

- **Security Guides**
- Configuration automation
- Monitoring infrastructure
- Prescriptive guidance

Communications

- Communities
- Architecture web casts
- Conferences
- TechNet



Why Is It Difficult To Produce Guidance

- Systems are dependent on each other for security
- Dependencies must be
  - Understood
  - Analyzed
  - Managed
- Most common dependencies are through either service or administrative accounts

- Guidance and templates fail to capture these dependencies

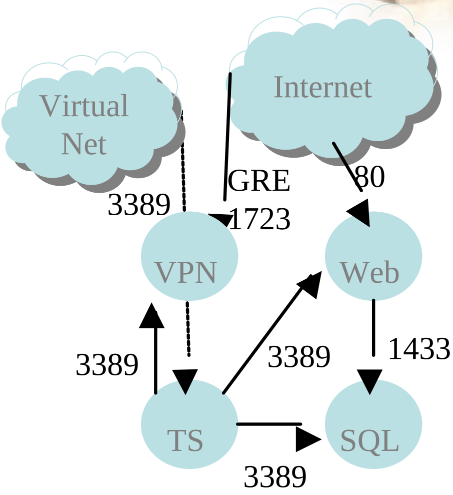
Customer Challenges

- Too many guides
- Conflicting advice
- Analysis of network is hard
  - Many guides fail to point this out
- Guides ignore application compatibility
- Application difficult
- Testing is spotty or none-existent

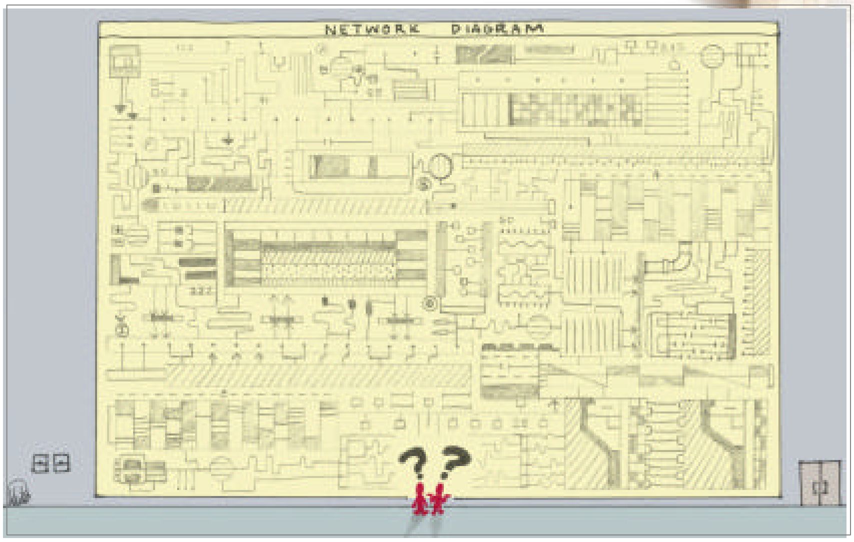
- Guidance is often too simplistic

Abstract Example: Open Hack IV

- Four systems
  - Web Server
  - SQL Server
  - Terminal Server
  - VPN Server
- Well-understood environment
- Limited Scope



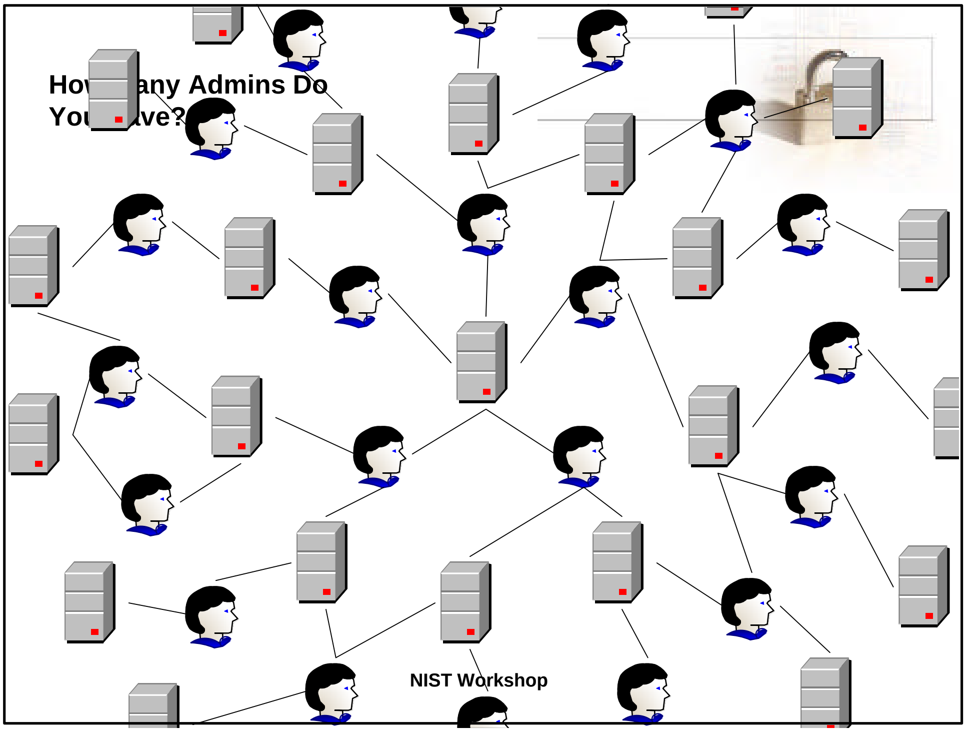
Realistic example: Your Network



Example: Administrative Dependencies

- An administrator on any given machine can run code as any user logging on to that machine
- Administrative dependencies balloon – fast!
- Enumerating actual administrators is hard

How Many Admins Do You Have?



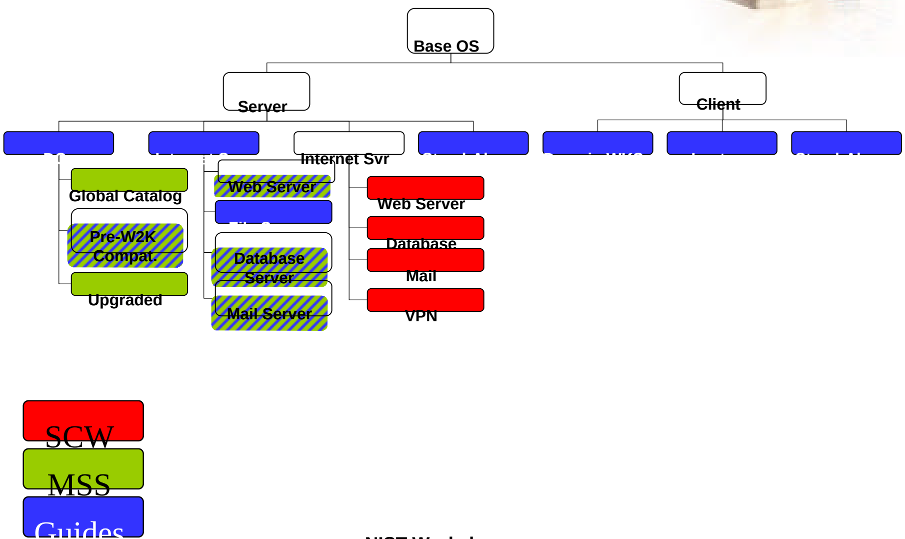
Lessons Learned

- Analysis of target environment is absolutely essential
  – Must include analysis of protocols
  – Understanding what is unnecessary is hard
- Baseline and deltas works well
- Group policy is a bonus
  – Easy configuration of baseline/deltas
  – Includes IPSec policies
- Careful smoke-testing needed

Applying the lessons

- Three thrusts
  - Microsoft Security Solutions Offerings
  - Security Hardening Guides
  - Security Configuration Wizard
- Why are servers not hardened by default?
  - The hardening has to be in response to the environment
  - One-size does not fit all
  - Breaks all existing applications
- Need to work with the community

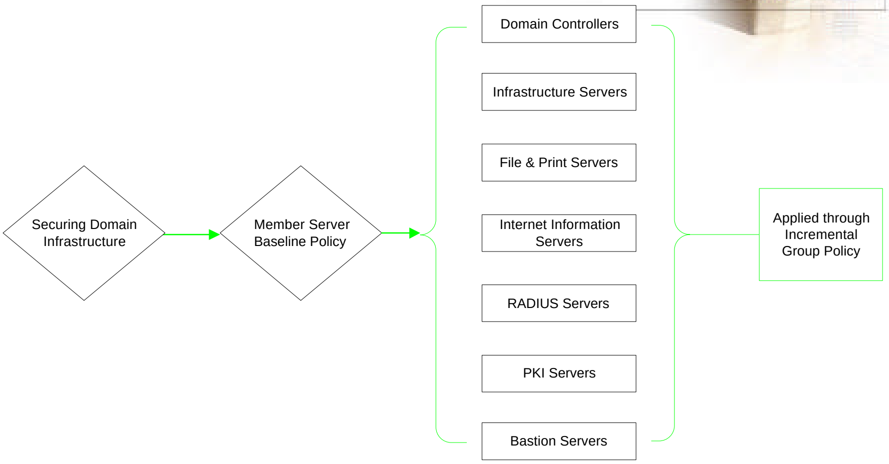
Targeting configuration guidance



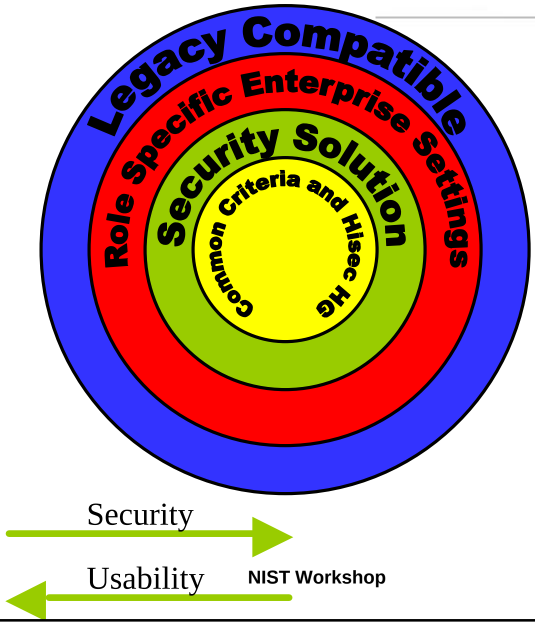
Windows Server 2003 Security Guide : Design Goals

- Provide actionable, authoritative, guidelines for
  - End users
  - System Administrators
  - Security Administrators
- Guidelines are
  - Proven in real world testing
  - Relevant and address real security concerns
  - Accurate

Windows Server 2003 Security Guide Structure


Securing Domain Infrastructure
Member Server Baseline Policy
Domain Controllers
Infrastructure Servers
File & Print Servers
Internet Information Servers
RADIUS Servers
PKI Servers
Bastion Servers
Applied through Incremental Group Policy

The Layered Approach



Legacy Compatible

Role Specific Enterprise Settings

Security Solution

Common Criteria and Hisec HG

Security

Usability

Future Efforts

- Guidance at launch
  - Guide for Windows Server 2003 at launch
  - Windows XP a month later
- Other products
  - SQL Server
  - Exchange Server
  - Others?
- Short checklists
  - Most of the value are in very few settings
- Better application compatibility documentation

Microsoft®