Security Checklists for Commercial IT Products

June 11, 2003

Timothy Grance
grance@nist.gov

Overview

- Drivers & Challenges
- Operational Concept
- Granularity or levels of checklists
- Implementation and submission details
- Issues
- Future Steps

Drivers & Challenges

- PL 107-305 says develop checklists/settings that minimize security risks with each hardware & software system widely used in Federal Govt.
- Apply efficient and effective coalesced security expertise
- Demonstrable, clear reduction in vulnerability exposure
- No additional funding
- Solicit help from vendors/organizations/consortia

About Checklists

Under the Cyber Security Research and Development Act, NIST is charged with developing security checklists. These checklists describe security settings for commercial IT products.

Security Levels

Each security checklist describes its the risk/ environment for which it is intended to be used. These generally specify levels consistent with the government wide security categorizations for information and information systems as contained in FIPS 199.

Partners

The checklists provided on this website are provided by a wide variety of vendors, government agencies, consortia, non-profit organizations, and user organizations. For a complete list, click here. NIST gratefully acknowledges their contributions and assistance in providing this security service.

Disclaimer

The content of each checklist is the responsibility of the submitting organization. We encourage users to send comments on specific checklists to the appropriate author.

Search the Security Checklist Database

Search

By specific product

By security level

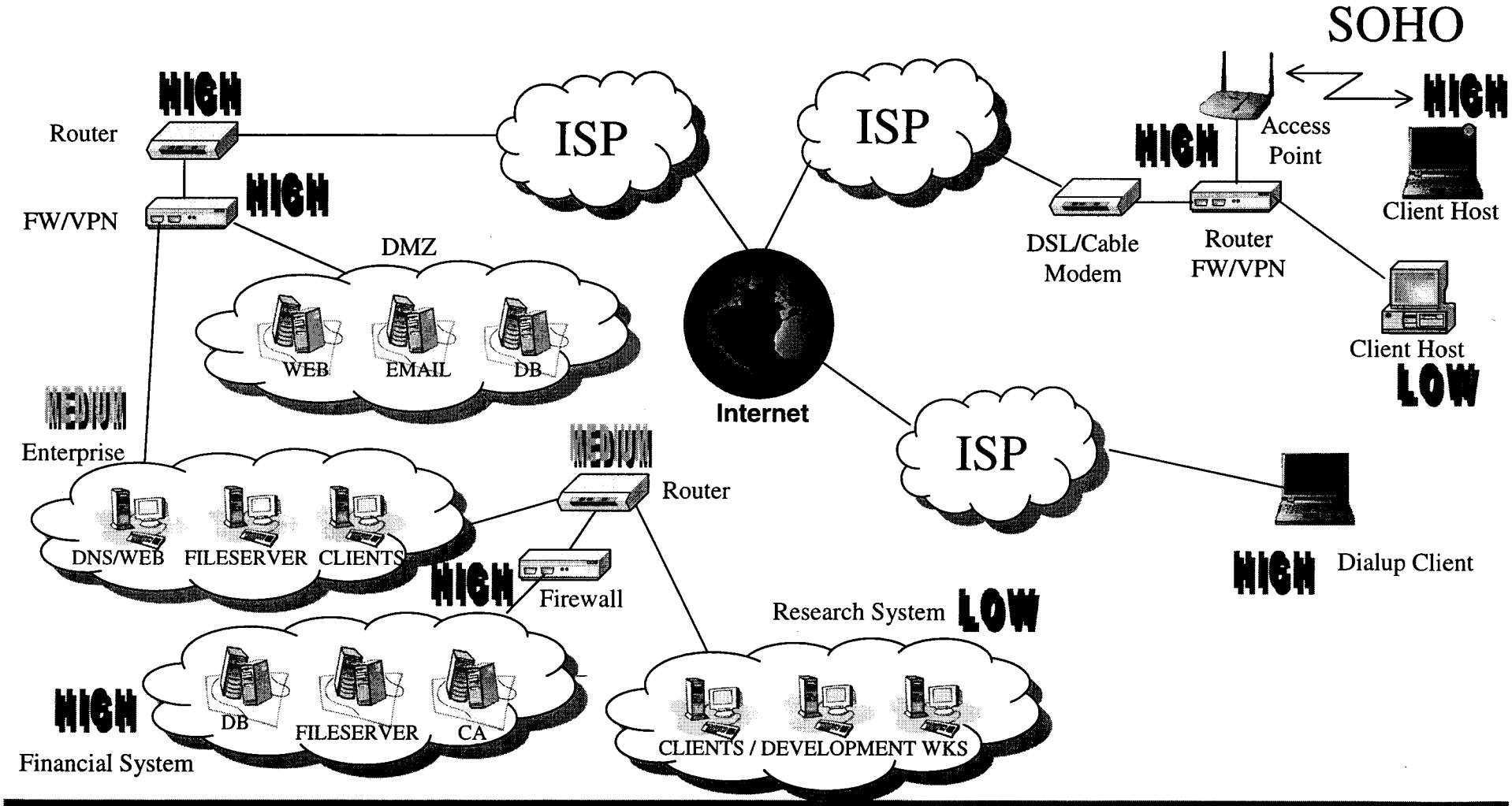
By product type Operating Systems

Results

(list of checklists)	(list of vulnerabilities from ICAT)
Linux (DISA)	Vulnerabilities
Linux (CIS)	Vulnerabilities
IOS (CIS)	Vulnerabilities
IOS (NSA)	Vulnerabilities
Windows 2000 (DISA)	Vulnerabilities
Windows 2000 (Gold)	Vulnerabilities
Windows 2000 (Microsoft)	Vulnerabilities
Windows 2000 Professional (NIST)	Vulnerabilities
Windows 2000 (NSA)	Vulnerabilities

Levels in a Deployed Environment

(Levels shown are for example only)



Levels

- Based on the technical functions, deployment environment, degree of lockdown
- NIST mandated to create standard system risk levels
- Need for consistency / mapping
- Proposed defined levels (strongly encouraged)
  - Legacy - Low
  - Enterprise - Medium
  - High Security - High
- Custom level (permitted)
  - Custom characterization
  - In addition to the proposed levels

Legacy Level

- Maximum functionality
- Interoperability with legacy system
- Mix and open environment
- Easy to use and implement by novice user in a SOHO environment
- Basic security
- Protect from the "out-of-the-box" vulnerabilities
- FIPS 199 risk level: LOW

Enterprise Level

- Reduce functionalities
- Minimum interoperability with legacy system
- Managed environment
- Complete and extended settings
- Advanced users and system administrators
- Acceptable security level
- FIPS 199 risk level: MODERATE

High Security Level

- Single purpose function
- Limited interoperability with legacy system
- Managed environment
- Complex configuration
- Experienced security specialists and seasoned system administrators
- High security level
- FIPS 199 risk level: HIGH

Custom-defined Level

- Specialized profile
- Target as defined by checklist author
- Custom environment
- Custom security level
- Examples (specialized application/environment such as manufacturing, medical, etc.)

Level Designation

- Submitters specify target level(s) in checklist
- May target more than one level with a single checklist, as appropriate
- Submitters encouraged to submit checklists for all 3 defined levels
  - First priority: enterprise level?
- Submitters encouraged to use custom levels sparingly
- NIST will further develop characterization of the three standard defined risk/environment levels

Security Checklists for Commercial IT Products - Template Framework -

Information Technology Laboratory
Computer Security Division
NIST
National Institute of Standards and Technology

Template Information

- Need for 'standard template' for construction of checklists
  - Usability
  - Searchability
- Consistent database entries
  - Standard defined fields (following slides)
- Classify, order, and sort the security checklists
- Search the database based on the fields

Security Template Fields - 1

1. Vendor name, *i.e. Microsoft.*
2. Product category, *i.e. Client Operating System*
3. Product name, *i.e. Windows 2000 Professional*
4. Product version, *i.e. Service Pack 3*
5. Name of the checklist, *i.e NIST System Administration Guidance for Windows 2000 Professional Document*
6. Submitting organization/authors, *i.e. NIST Computer Security Division*
7. Checklist creation Date / latest rev Date, *i.e. November 2002*

Security Template Fields - 2

8. Target FIPS 199 risk level, *i.e. High*
9. Target environment, *i.e. Managed environment, corporate network protected by border routers and firewalls*
10. Target audience, *i.e. Security Specialists*
11. System role, *i.e. Client desktop host*
12. Firmware/software patch levels, *i.e. MS03-008*

Security Template Fields - 3

13. Prerequisite, *i.e. familiar with active directory, group policy, etc.*
14. Tools, *i.e. HFNetChk 3.86, Security Configuration Analysis, Secedit, etc.*
15. Configuration guidance, *i.e. installation, application of patches, lock-down process, etc.*
16. Configuration files or templates, *i.e. win2kpro_consensus.inf*
17. Summary checklist, *i.e. table summarizing the recommended parameters*

Security Template Fields - 4

18. Assessment, *i.e. CIS Scoring tool, MBSA, Nessus, etc.*
19. Known issues, *i.e. Null session, LanMan, IIS, etc.*
20. Change history, *i.e. Version 1.1*
21. Point of contact, *i.e. itsec@nist.gov*
22. References, *i.e. Microsoft Windows 2000 Security Guide, NSA Windows 2000 Guidance, DISA Windows 2000 Guidance, CIS Windows 2000 level benchmark, etc.*
23. References to published vulnerabilities, *i.e. ICAT, CERT, FedCIR, NIPC, SecurityFocus, etc.*

Lessons Learned

Issues in Producing Checklists

- *Mixed environments*
- *Lengthy and detailed process requires intense testing*
- *Must work with product vendors, security professionals/checklist producers, and operational players*
- *Multiple security levels (mapping guides to levels is hard)*
- *Life cycle (built, test, update, and maintain)*
- *Labor/skill/collaboration intensive*
- *Customer and audience*

Issues for NIST

- Logos/Stickers
- Rogue submitters (Osama's Guide to VOIP)
- Review process
- Maintenance of guides by submitters
- Customer feedback to vendors
- Funding
- Agency skill levels

Future Steps

- Issue a Federal Register Notice (June 03)
- Conduct workshop (Sept 03) to solicit ideas and feedback on NIST approach for producing and disseminating checklists
- Special Publication on producing checklists

Questions