Best Practices in Configuration Management for Security
or
“It’s 11 O’Clock – Do You Know Where Your Routers Are?”

If instituted properly, configuration management offers a straightforward and relatively inexpensive way to protect against many security threats. This report outlines a number of configuration management best practices that many organizations can readily put into place. It defines configuration management and outlines its benefits, and offers best practices pertaining to networks, mainframes and servers, IT staff desktops, user desktops, and wireless devices.

What Do We Mean By Configuration Management?

Depending on whether your background is in telecommunications, or in traditional software development, you may have specific, varying definitions of configuration management. Configuration management has traditionally been part of the world of software development and change control, especially in mainframe environments. The term is still most commonly used to refer to software configuration management (SCM), a discipline for controlling the evolution of software systems throughout their life cycles. The Software Engineering Institute (SEI) at Carnegie Mellon University created a large body of work defining the field in the late 1980s and early 1990s.

In the telecommunications world, the term has long been used for installation, activation, and provisioning of telecom resources. Configuration management is one of the five systems management functional areas specified by ITU Recommendation X.700, the Management Framework for Open Systems Interconnection (OSI) for CCITT Applications (ISO/IEC 7498-4 OSI Basic Reference Model).

With the growth and increasing complexity of networks, the role of configuration management has expanded to include all manner of devices, servers, desktops, operating systems, system values, and configuration files – in other words, asset management. Configuration management is an important component of asset protection and management, enabling effective and efficient provisioning of all IT services. Our goal in this paper is to look at the importance of configuration management for network security, and in particular, to an enterprise vulnerability management program, as well as to provide readers with a roadmap for establishing or improving their own configuration management practices.

According to IEEE standards, the four classic operational aspects of configuration management are Identification, Control, Status Accounting, and Audit and Review. These categories can be reinterpreted to meet the needs of network configuration management, as follows:

1. Identification: We need to have an identification scheme for all devices and components we intend to track. This involves locating and identifying each item, assigning it a name or unique label, and cataloging specific characteristics, such as hardware and software version, revision, or patch level.

2. Control: We want to be able to control the deployment of, subsequent access to, and maintenance of devices on the network.

3. Status Accounting: This includes recording and reporting the status of, changes to, and operational statistics about devices and their components.

4. Audit and Review: Finally, we want to have a capability for revisiting and validating the configurations of devices, and for tracking who made what changes and when.

Breaking these four general categories out into network management activities, we come up with a list that looks like this:

- Physical inventory control of hardware devices and associated components or peripherals, including logging of location, vendor, and serial or other identifying numbers

- Operating system software tracking, including version, patch levels, and updates

- Tracking configuration files (such as access control lists, filters, and services) for all devices, including routers, firewalls, remote access servers, database servers, etc.

- Real-time status monitoring and activity logging

- Establishment and maintenance of standard, common computing environments, including secure software update and configuration administration

- Regular auditing and spot-checking of desktop, mobile, and server systems

- Prevention and tracking of unauthorized changes that may deliberately or inadvertently reduce the effectiveness of security controls.

Benefits

These activities, when performed and documented consistently, provide general and security-specific benefits. The organization will have better control over its IT infrastructure, and the associated core software, which will result in more efficient network management, and subsequent cost savings. Configuration tracking can also be tied to license management for the installed software base. The database of hardware and software is a core tool for trends analysis, capacity and contingency planning, and disaster response. Reducing disruption in network services and improved help desk support should provide increased productivity for desktop users as well.

From a security perspective, configuration management boils down to fundamental good housekeeping. If you don't track what is on your network, you may find yourself in the position to the very, very messy householder whose home is burgled and ransacked, but who doesn't figure this out for a week or more – it was a mess before, and it's still a mess! Not only is hard to figure out that someone other than yourself has been rummaging through your drawers, and when, but it is hard to figure what, if anything, was taken. Worst of all, it will be nearly impossible to document losses for the insurance company, or to take steps to prevent future losses.

Configuration management combines standards and policies, procedures and best practices, and tools. It plays a key role in several security functions, including intrusion detection, incident response and recovery, and vulnerability prevention and vulnerability management – the process of identifying or being informed about new vulnerabilities, identifying what systems are affected, and patching and testing systems.

In particular, vulnerabilities can be greatly reduced through the deployment of standard, hardened configurations, starting with a "golden master" configuration for each operating system or functional role (server, desktop, etc.). Once systems are deployed, handling new vulnerabilities should be an ongoing, intentionally managed process. After all, it's to your competitive advantage to be able to mediate security threats as quickly and efficiently as possible. By far the single most common reason that companies are subject to break-ins and Web site defacements is that they fail to patch well-known vulnerabilities. In that light, configuration management becomes critical – if you don't know what's on your network, how are you going to know what to fix?

Vulnerability management is almost impossible without current configuration information. There is so much vulnerability data disseminated daily that the only way to get a handle on the situation is to have an established management process. This process should be integrated with, but also go above and beyond, normal day-to-day system administration activities. It should encompass the following components:

- Developing and distributing policies and associated procedures
- Designating specific roles and functions, with associated responsibilities and accountability
- Screening and evaluating information for its applicability to the given network
- A means for quickly running checks to determine which and how many systems may be affected
- Setting priorities for patching systems

- Following through to see that affected systems have been appropriately upgraded

Best Practices for Configuration Management

This section discusses best practices for configuration management in four broad technology areas.

- Networks
- Mainframes and servers
- Desktop environment (IT and Users)
- Wireless

Most organizations will already have at least some of these practices in place; others may be trying to establish formalized programs but need more support from senior management. For these people, the following can provide a roadmap for building a program and for justifying requirements.

Some of the recommendations can be accomplished with technology alone, but many require policy statements or establishing new standards. Some will be procedures drawn up to fulfill a policy requirement. Some are strictly practices, and some will require the use of freeware or commercial tools or specialized software packages.

In most large organizations, different groups handle network components, servers, and desktops. For most functions, that division of labor works well, but for enterprise-wide configuration management and vulnerability management there need to be channels for sharing common tools and disseminating appropriate information. For example, the same scanning tool that can be used to inventory all network devices can also identify servers and desktops, and the tool and its information should be stored in a central database and made available to every group that needs it.

NETWORKS

Many large organizations already employ network management tools, such as HP OpenView, but few use them to the fullest extent. There is a range of less expensive commercial tools that provide network discovery and mapping functionality, but it is also possible to do this with open source tools like *nmap*. If your network is fairly dynamic, it may not be a bad idea to scan it on a regular basis (monthly, for example) and burn the results on a CD-ROM for future reference and even forensics, if needed.

Best practices include:

- Each device attached to the network should be uniquely identified, with information retained on where it is located, what operating system (or equivalent) software it runs (including the version and revision levels), current settings (such as access control lists for routers), the last time it was revised or altered, and by whom. Write access to such information should be strictly limited and monitored.

- You should archive master copies of the baseline-installed configurations (the “golden master”), for each type of device or system, in a secure location, preferably in a media safe or other media-rated storage container. Copies should also be kept off-site in secure storage. If the systems from which the masters are made are kept available, they should be segregated from the rest of the company intranet, preferably by an air gap, to prevent tampering.

- Router access control lists, firewall rule sets, and similar configuration files for critical network devices should be securely maintained using source code control. This enables changes to be tracked, integrity checking, and the ability to back out changes when necessary.

- Remote administration of devices should only be done through secure channels (SSL (Secure Sockets Layer), SSH (Secure Shell), other forms of VPN, etc.), and only using strong authentication (smart cards, OTP (One-Time Password) authentication, biometrics). Only authorized administrators should be allowed to make changes, and only to resources within their jurisdiction. If possible, you should limit the network addresses from which changes can be originated.

- Departments or individual users should not be allowed to connect devices to the company network without going through a documented business process and getting the appropriate approvals.

- Wherever possible, network managers should incorporate the use of integrated status monitoring and anomaly detection tools with configuration management databases and processes to provide more efficient and complete coverage. The extent to which this can be done depends a great deal on the particular devices and tools in question, as some interoperate better than others, and none offers a comprehensive solution.

MAINFRAMES AND SERVERS

As with network devices, designated individuals or groups should be responsible for creating and maintaining baseline configurations and installation images for mainframes, mid-range systems, and Windows NT or Windows 2000 servers. At the server level, applications can be a complicating factor. Some applications can only run on a specific version of the operating system, and patches have been known to cause production applications to break. It then becomes even more important to track what versions are running on which platforms, the relative priorities of the platforms, and any mitigating factors affecting configuration decisions. Without some means of tracking, such kind of information may become departmental folklore or “oral tradition”, which is lost in the event of staff turnover.

Best practices include:

- Each server should be uniquely identified, and all information regarding hardware configuration, peripherals, firmware revision levels, operating system version, revisions, and patch levels should be tracked.

- Strong authentication should be used for administrator access to all critical servers, and secure channels should be used for remote administrator access.

- Servers should be regularly scanned and checked against baseline configurations to ensure that no new, unauthorized services have been added. This can be automated using freeware tools or commercial scanners. Some software vendors combine scanning tools with “policy management” software to further automate the whole process.

- Someone, most likely system and data center managers, should be responsible for providing physical and environmental protection and accountability for magnetic tapes, diskettes, compact discs, and other storage media. There should be controls established and followed for all backup media, and for all installation media for operating system and critical application software.

DESKTOP ENVIRONMENT

The desktop environment is usually the most difficult one to control, because it is the largest in extent, and involves the greatest number of unpredictable variables (otherwise known as “users”!) This is where it is most important to devote resources to training and awareness, backed up by well-publicized and enforced policies. Policy requirements differ from company to company, so not all of the recommended user practices may apply to a given organization, or even to all groups within a single organization.

Maintaining network configuration information for desktops is often made more difficult through the use of DHCP (Dynamic Host Configuration Protocol), which allows any open network port to be used to access the corporate network. This is very convenient for network users and administrators, but also very convenient for anyone who walks in off the street and plugs a laptop into the network. In a Windows environment, it is possible to restrict DHCP access through the use of assigned IP “reservations” which are usually (but not necessarily) tied to the client’s MAC address as an identifier.

Best practices for IT staff include:

- Desktop platform administrators should be responsible for establishing, distributing, and maintaining a common desktop hardware and software package, including standard operating systems, virus checking software, and common desktop tools. “Exception” packages may be created to serve the needs of specific subgroups, such as software developers, Web content developers, etc., but keep these to a minimum.

- If feasible, work with your organization’s Purchasing Department to develop lists of approved hardware and COTS applications that may be ordered directly through Purchasing. Ideally, any purchase of hardware or software not on the approved list should require written justification, review by the appropriate IT managers, and approval from a senior manager.

- Wherever possible, use electronic distribution of software packages, recommended configurations, and updates and patches, with appropriate follow-up to determine the rate of success and compliance.

- Wherever possible, use operating system-level permissions to prevent users from administering their own desktops. Even when this is not feasible, use desktop boot and login passwords to reduce the possibility of unauthorized user access.

- You will need to develop additional procedures and controls for dealing with mobile laptops and desktop systems that are located in the homes of teleworkers. Such systems require additional security, and at the same time are harder to maintain and update.

- Consider working with the corporate Internal Audit department to institute an audit program. The goal would be to audit a selection of desktop and mobile systems on a regular basis, and remove and/or track noncompliant components. Users should be made aware that there is an audit policy, and any such policy needs to be enforced to have any effect.

Best policies and practices for users include:

- Establish policies covering expectations for all users, and follow up with training and awareness exercises. Be consistent, be persistent, and make sure that there are consequences for non-compliance.

- Users should not install non-approved software on their desktop or mobile systems. This should include software downloaded from the Internet, browser plug-ins, and executable attachments in electronic mail.

- Users should not disable virus-checking software on their desktop or mobile systems. Users may be responsible for regularly updating virus checking or other software, or for making their platforms available for automated updates.

- Even though it should go without saying, it is still important for users to pick strong desktop passwords, and never disclose them.

- Users should not alter, upgrade, or swap hardware with other users without written approval. All hardware configuration changes should be logged and tracked.

- Users should report lost, stolen, or damaged hardware immediately.

WIRELESS

All of us increasingly carry out business and personal matters on wireless devices such as personal digital assistants, palmtop or other handheld computers, two-way text pagers, and cellular telephones. We use them to store contact information about colleagues and customers, notes from confidential meetings, or business-critical scheduling information. Unfortunately, we are also prone to losing them, sitting on them, having them stolen, or dropping them, any of which will result in data and property loss. At a minimum, these devices must be tracked, maintained, and protected from physical and electronic threats. Beyond such measures, however, configuration management and security options still tend to be sparse, as protocols are still argued over, and few widespread standards have emerged.

Best practices include:

- If possible, staff should provide an “approved” selection of additional or upgraded software, and management policy can prohibit download of anything else. Most wireless devices, including cell phones and PDAs, have some means for automated software updates, including virus detection software. There are many, many freeware programs available for download over the Internet, which can have embedded viruses or backdoors.

- Consider investing in third-party encryption solutions to protect data on handheld devices.

- In most instances, users should be responsible for backing up data stored on company-provided wireless devices. The appropriate IT group should provide the necessary software or facilities. Monitor logs for synching operations to make sure that no unauthorized operations have taken place.

- Many times, employees will use their own personal devices for company business, and will store company data on them, particularly with handheld devices and PDAs. However, some models and versions may be less secure, and IT staff may have no control over personal devices. The organization may want to prohibit such use, which may engender resentment. At the very least, employees should be educated on possible risks and on what is or is not acceptable use. The same applies to cell phones, whose calls can readily be intercepted.

Summary

Configuration management is quotidian and often mundane, but it can form an excellent line of defense against a broad range of security threats. The key to success is to establish policies, procedures, and processes, and to document them. A process that isn’t documented, and that only one or two people know about or understand, is not a process at all. It’s an assumption, and it will be lost whenever there are staff changes or changes in routine. Surprises are never good news to system and network administrators, and configuration management is the best tool you have to reduce the number of surprises in your environment.