Method for Enforcing Access Control Policies on NCMS

Zhigang Zhao
Institute for Infocomm Research, Singapore
zzhao@i2r.a-star.edu.sg

Huaqun Guo
Institute for Infocomm Research, Singapore
guohq@i2r.a-star.edu.sg

***Abstract*—Configuration of large-scale networks is difficult and error-prone. Misconfigurations known as vulnerabilities are a major cause of network outages and security problems. This paper proposes an effective Network Configuration Management System (NCMS) with the enforced Access Control policies and centralized management method to provide a controllable security access interface for the configuration management of internal network devices and leads to better network resiliency, security, and scalability.**

***Keywords*-Controllable Security; enforced Access Control policies; Network Configuration Management System (NCMS);**

I. Introduction

Deploying and managing device configurations in large-scale networks with hundreds of devices is a challenging, time-consuming, and error-prone process. Network administrators and network auditors, both in enterprise and industrial control networks, require the ability to summarize and manage configuration changes to a network. Network administrators must update configuration files to implement new services and to maintain security and compliance. Without frequent updates, their networks may be less useful, vulnerable to attack, or non-compliant. On the other hand, with frequent updates, there is the possibility of human error, the introduction of configuration errors and consequent potential major network outages. Hackers may take advantage of configuration errors to obtain system privileges, causing extensive damage.

Network misconfigurations and vulnerabilities create huge security risks. 50-80 percent of network failures arise from human-error in network device configuration [1] [2]. A large percentage of congestion/overload scenarios are also due to poor or outdated network configurations. Some analysts have indicated that 65 percent of cyber-attacks are enabled by configuration errors [3], and likewise, 62 percent of infrastructure downtimes are due to the same reason [4].

As configurations change over time, the complexity of network configuration increases and human errors accumulate. This degrades the connectivity of networks and increases management costs. The following lists the security concerns of companies identified by the Yankee Group Network Downtime Survey [4]:

- Half of the respondents reported unauthorized changes made in the past year.
- Of these changes, forty-seven percent of the changes could not be recognized for correctly.
- Seventy percent of companies managed network devices using shared passwords.
- Sixty-eight percent of respondents had no method of tracking operator logins and configuration changes.

Given the increasing criticality and complexity of the services offered over computer networks, the cost of downtime is estimated to grow substantially, motivating the need for more effective configuration management techniques.

Most organizations do not have effective configuration management strategies and opt to manage network changes on an ad-hoc basis, or node-by-node, without recording changes on the fly. Ignoring or operating without changing control processes will eventually cause configuration errors that lead to major network outages.

The use of ad-hoc tools and absence of an enforced management system leads to the following problems, with the effect of longer downtime, longer repair time and lower service reliability:

- **Configuration inconsistency:** Misconfiguration occurs when different administrators iteratively make small changes to many network elements. The baseline state for a given device is lost when the settings of similar elements are changed.
- **Loss of critical information in documents:** Improper documentation of changes lead to out-of-date or inaccurate data, causing network operators to act inefficiently when searching for configuration information or acting on incorrect information.
- **Extended downtime:** Quickly restoring the device to a stable state is critical during troubleshooting. Without a baseline state for a given device, a troubled device will stay down longer, creating negative business impacts.
- **Extended time to repair:** Absence of information about configuration changes causes prolonged troubleshooting and incident resolution.
- **Lack of validation and auditing difficulties:** Absence of an effective configuration management system means there is no guarantee that proper changes are made as planned or authorized, or that improper changes can be detected efficiently.

This paper is precise to solve these problems, proposes an effective Network Configuration Management System (NCMS) that helps enforce policies, identify security holes

and prevent unauthorized changes to network elements.

The rest of the paper is organized as follows: In section II, we first discuss related work and our evaluation of existing products in the domain of Network Configuration Management System. Section III covers the proposed system model and architecture. Section IV discusses the security analysis and enhanced solutions and describes the detail of our solutions and technological innovations. Finally, the conclusions are covered in section VI.

II. Related Work and Evaluation of Existing Products

Network configuration management (NCM) strategies enable the more convenient organization and maintenance of the components of a network. The network administrator can access the NCM database for comprehensive information and actualization when he needs to repair, modify, expand or upgrade the network.

Different configuration management tools vary in architecture, and address different subsets of user requirements, but can be categorized as vendor-neutral or specific. Vendor-specific tools generally offer better performance for same-vendor devices, but cannot manage multi-vendor networks efficiently.

We have surveyed and evaluated on vendor-neutral products with network configuration-related capabilities, including both commercial and open source tools [5] [6]. These products belong to several categories:

- Configuration management tools, either in the form of web-based server or stand-alone application, with or without agents embedded in the network.
- Network monitors tools, which perform device discovery, reporting of network and hardware status, and to execute initiative-based or pre-scheduled tasks.
- DevOps developer-oriented tools, which focus on product agility and continuous delivery.

Regarding Network Change and Configuration Management (NCCM), we have evaluated or surveyed the following existing products:

- **Remote tools:** RANCID, Cacti, What's Up Gold, Kiwi CatTools
- **Enterprise tools:** Cisco Prime LMS, SolarWinds NCM, ManageEngine NCM, Zabbix NetMonitoring
- **Enterprise frameworks:** NMS part of HP OpenView, BMC MainView, IBM Tivoli, CA Unicenter

There are key features in most of the existing NCMS products:

- Backup network devices' specific configuration in an external, centralized common data store.
- Full historical or incremental backup and restore capability.
- Centralize and automate the configuration changes in the network and rollback when necessary.
- Alerts on configuration changes.

But there are also some drawbacks in the evaluated products, such that they cannot match the specific requirements from enterprise companies and national industrial control networks. There are some functional limitations in both commercial and open source products. In general, these products cannot really prevent unauthorized changes or configuration drift effectively. For example, one currently popular configuration tool is the Really Awesome New Cisco Configuration Differ (RANCID) [7]. This product provides some command line tools to modify scheduled checks on the device and backup changes to the revision control system, but it lacks either a unified management interface or enforced access control policies. Its users are inconvenienced by having to remember the access information of each of the network devices. In summary,existing products mainly focus on the network and configuration part, but lack the fully comprehensive capabilities that prevent unauthorized modification of network configurations in the enterprise-wide network.

The following are limitations we summarized from the evaluated existing products and related work [8]:

- Some work as a single client application or a collection of ad hoc tools, e.g. those products in the mentioned Remote Tools category.
- Some lack change tracking and auditing functions, e.g. One most popular configuration tool is the Really Awesome New Cisco Configuration Differ (RANCID) [7], which just backups changes to the revision control system.
- All don't emphasize enforced Access Control policies.
- All lack the ability to ensure adherence to those standards and policies for device configuration management.
- Lack relevant solutions for some use cases and requirements in the enterprise-wide network, e.g.
  - Unauthorized modification on network devices due to shared passwords
  - Configuration inconsistency due to different users logging on at the same time on the same device
  - Changes by maintenance personnel from the equipment supplier

Based on our evaluation of surveyed products, our proposed method will provide a novel and more advanced solution for NCMS, including enforced access control policies for the network device, user and policy management to ensure continuous network security.

III. System Model

The target of our NCMS system is to establish and enforce enterprise-wide access control policies for device and user operation. From the perspective of network topology, the system is working as a bastion host, or a controllable Secure Access Gateway to the network devices, and all types of user device operations are managed by NCMS system. The user is authenticated by the system through following the system-managed procedures and policies. This policy prevents unplanned changes from different individuals that can lead to security holes or misconfigurations.

A. System Architecture

The present system model will become more fully understood from the following figures and their descriptions.

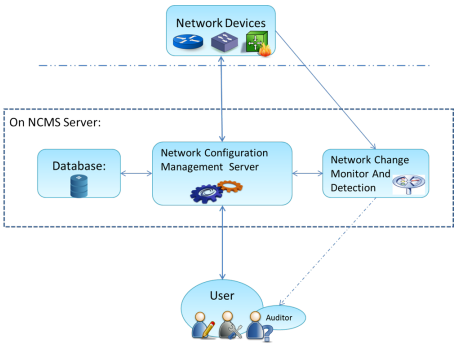

Fig. 1. The architecture of Network Configuration Management System (NCMS)

Figure 1 shows the complete architecture of Network Configuration Management System with the proposed method. There are five components in the proposed system.

1) **User with roles**

There are the different role users in the NCMS system, including basic operator role, device manager role, and system administrator role. Users access the system portal using a client interface of NCMS (e.g. web browser). NCMS system delegates these user operations to the network devices.

2) **Network Devices**

Network devices are devices that its configurations are managed by our NCMS system, such as routers, switches, and firewalls from varied vendors such as Cisco, Juniper, and Check Point. In our system, the network devices are isolated from the user, and the user cannot operate on devices directly. For the configuration operations on the network devices, there is only the connection between the network device and the NCMS server, and using access control setting in the device and network security technology to control network access and prevent unauthorized access from any nodes outside the NCMS communication channel.

3) **Database**

The database is part of the system. Network device configuration management requires centralized data storage outside of the device. The management data belonging to the configuration system are stored in the database. The type of data includes user, device, configuration, access control policy, log, etc.

4) **Network Configuration Management Server**

This is the main part of our NCMS system. Details are described as mentioned data management modules and execution and control type modules in the following subsection.

5) **Network Change Monitor and Detection on Server**

There is one-way communication channel from the network device to the network change monitor and detection part in the NCMS system. The monitor processes the notifications from the device and performs consistency checking with the Network Configuration Management Server. Users with the system auditor role can perform audit work on the result from monitor and detection module.

The core of the Network Configuration Management System (NCMS) is the Network Configuration Management Server responsible for configuring network devices. It performs various functions like creation processing, configuration operations, security check, and audit.

1) **Creation**

- Create user profiles and assign access control policy to IT staff in charge of managing configuration change, e.g., Access Control roles of manager, operator, auditor, and system administrator.
- Create representations of the network devices that are managed by the system.

2) **Configuration**

- Online backup, restoration, and update of configuration to the network device.
- Using the database for configuration backup, storage, and version control, and log function for audit.

3) **Verification**

- When the configuration on the device is changed, the Network Configuration Monitor and Detection (NCMD) will be notified and generate a real-time notification to the server.
- The server's auditor checks the configuration changes for any unwarranted part, in which case it sends an alert to management for a manual check.

B. System Modules

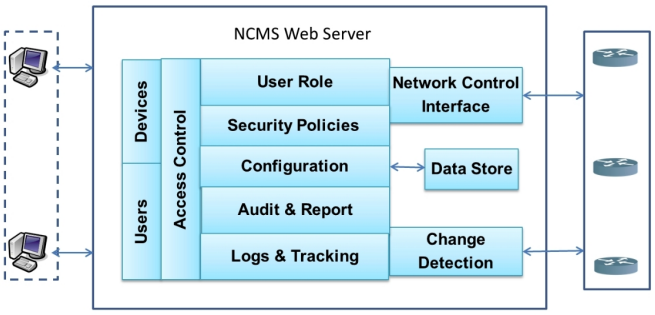

Fig. 2. The interface and main modules of NCMS

Figure 2 shows the interface and main modules of proposed NCMS. There are two types of modules on the Network Configuration Management System. One type concerns data management, while the other type concerns execution and control.

The data management modules include:

Role management module: A typical user is a person with a specialized responsibility: for example, a network manager who is in charge of a network group; a configuration manager who is in charge of the configuration management procedures

and policies; network engineers who are responsible for developing and maintaining the configurations on network device; the security manager/auditor, who validates the correctness of the configurations and ensures proper changes have been made as planned and authorized for the network engineer or operation staff. The functions offered by this module concern various functions about roles, such as add roles, list roles, delete roles, etc.

User management module: According to user roles and policies, the network manager role or system administrator role needs to create user profiles and assign access control policy to staff who are in charge of managing configuration change. User data are stored in the database and used by other modules. The functions offered by this module include list users, add users, delete users, etc.

Device management module: This module is for network device resources. The configuration manager role or administrator role creates the network device data and groups devices, as well as performing initial setup and management of network devices and setting up the protocol for transport of configurations. The device data are stored in database and used by the other modules. The device functions include list device, add device, etc.

User and Device associated module: This module defines the link between the user and specific devices list or device groups that permit authorization of access to network resources.

Configuration management module: This module handles the configuration data of network devices. The functions include configuration related operations such as list, add, delete, edit, compare, and version control functions.

Log module: The user actions are logged into the database. This module provides the management and query functions for log record so as to facilitate inquiries on user actions.

The following are the main modules of the system execution and control section.

User login and authentication control module: This module manages the user authentication request made from a web browser.

Configuration operation module: The network engineer role uses the client interface to login and access the system for configuration purposes, enabling access of the following functions: configuration download, configuration upload, create a new configuration, etc. The user follows the system service interface to sends the operation request to the server, then server delegates the operations to the network device through the network device interface control.

Network device interface control module: The system provides a uniform network device configuration interface to the user, irrespective of the device vendor. This module defines detailed access protocols (Telnet, SSH, SNMP, etc.) for transport of configurations to perform operations on different models of network devices.

Change monitor and detection module: This module implements an event-driven, nonintrusive network change detection and control method. Once the configuration of a device is changed, then a security notification is automatically sent to the change monitor server. Network devices can be configured to send Syslog messages or SNMP (Simple Network Management Protocol) traps whenever they are modified.

Audit and report module: The auditor uses this module to check this configuration changes if there is unwarranted configuration change. In this case, the system sends an internal notification, alert, or email message to the security manager or auditor for a deeper check.

We proposed a vendor-neutral multi-protocol controllable security configuration management system that meets the following essential network and configuration capabilities:

- **Rich functions for device configuration management:** The system should provide simple, intuitive options in the user interface to carry out various configuration operations such as configuration retrieval; viewing, editing and uploading configurations back to the device; establishing a documented network configuration change management process; and providing configuration secure storage and version control.
- **A centralized view and management for the multi-vendor network:** The system should provide an intuitive centralized view interface with support for the multi-vendor network devices. Network engineers will have a common system to record and access configuration information for every network device.
- **A uniform network device configuration interface:** Deploying and managing new configurations for different devices requires a lot of manual effort and time. A uniform configuration interface allows more accurate and manageable device configurations, changes and deployments.

IV. System Analysis and Our Solutions

In this section, we give detailed system analysis of the proposed method. The proposed system that provides the novelty method for Enforcing Access Control Policies on NCMS will provide a novel and complete solution, including enforced access control policies for complete network, device, user and policy management to ensure continuous network security.

A. Threat Model

Existing other Network Configuration Management (NCM) products mainly focus on the network and configuration management fields but lack the fully comprehensive capabilities that prevent unauthorized modification of network configurations in the enterprise-wide network. For example, the following these special situations that actually occur, but no relevant solution given in those products.

- Inside attack or unauthorized changes on network devices prone to happen. e.g. shared passwords for network devices
- Configuration inconsistency, e.g. different users log on at the same time on the same device

- Loss of critical information in documents for changes history. e.g. modification by ad-hoc network tools
- Lack of validation and auditing difficulties. e.g. changes by maintenance personnel from the equipment supplier
- Lack the fully comprehensive capabilities to ensure enforced policies.

One important fact that needs to be faced is many enterprises have established standards and policies for equipment configuration but lack the ability to ensure adherence to those standards. This case can lead to security holes or misconfigurations. Therefore,how to build a system for preventing unauthorized modification of network configurations that establishes and enforces enterprise-wide Access Control policies for device and user management? It is the key issue that we must focus on and try to solve.

B. Our Solutions

Two methods are helpful in eliminating bad network configurations: enforced access control for device and user operation, and adoption of effective configuration management techniques. The present paper claims that the proposed solution is combining these two aspects, an effective Network Configuration Management System (NCMS) with the enforced Access Control policies and Centralized management method to provide an interface for the configuration management of internal network devices and leads to better network resiliency, security, and scalability.

The enhancement of security features is one of the biggest differences between our proposed system and other NCM systems. Others mainly focus on the network and configuration part and lack the fully comprehensive capabilities that prevent unauthorized modification of network configurations in the enterprise-wide network. We provide the corresponding following claimed methods which are mainly focused on the security. These methods cover the entire lifecycle of device configuration management, preventing unauthorized modification of network configurations.

1) **Enforcement of compliance with policies via centralized control and bastion host solution:** To prevent unauthorized changes or configuration drift, the first target and a core concept of the proposed system is to establish and enforce enterprise-wide access control policies for device and user operation via centralized control. The proposed method or solution is separating network devices from user operations, and from the perspective of network topology, the system is working as a bastion host [9], or a controllable Secure Access Gateway to the network devices. The user is authenticated by the system through following the system-managed procedures and policies. The system server delegates the user operation requests to the network devices through the backbone protocol. This policy prevents unplanned changes from different individuals that can lead to security holes or misconfigurations. And this proposed method focuses on the operation and configuration management of network device; this is quite different from the normal hardening bastion hosts for the internal network, so it has little impact on existing network.
2) **Controlling network access and preventing unauthorized access:** In order to achieve the first solution that separates network devices from user operations and the system is working as a bastion host, we are using strong device protection and network security technologies to control network access and prevent unauthorized access. The detailed access information of network devices includes settings such as user account, access protocol, and Access Control List (ACL). These access settings on network device are managed by our proposed system; without correct password or proper ACL permission, the user cannot operate on devices directly. Aside from Access Control setting at specific devices, there are also other ways, such as using proper network firewall policies, to prevent unauthorized access from any nodes outside our NCMS communication channel.
3) **Applying Role-based access control and action audits:** Our proposed system provides a unified access portal and security management for multi-user access. Roles and permissions can be securely delegated to individuals. The system provides the management ability to assign users to roles, to associate roles with devices, and to allocate granular permissions to perform actions on associated devices, to identify involved personnel along with their responsibilities, in order to prevent unauthorized changes and approve genuine changes; the user actions for devices are logged into system database, and the system provides the management and query functions for log record so as to facilitate inquiries on user actions. With centralized control and bastion host solution, our proposed system also prevents this situation, which is different users operate on the same device at the same time, this causes device operation conflict and configuration version cannot be unified management, which is a problem faced in the other existing NCMS.
4) **Enables real-time policy enforcement of configuration changes and security check:** The system archives a real-time, nonintrusive network change detection and control method. Once the configuration of a device is changed, a security notification is automatically sent for audit. We designed the Application Program Interface (API) in the system to call other tools to analyze, validate and certify the device configuration file. It audits the security of network devices and automatically discovers policy violations based on the device configurations.
5) **Ability to quickly and safely restore to a trusted state:** The system provides change tracking and reporting to ensure proper changes have been made as planned and authorized, enabling a complete record of the 'who', 'what' and 'when' of configuration changes. The system also can immediately roll the device back to a previous configuration if results are unsatisfactory or any unauthorized changes are found. Without this

capability, engineers would have to spend critical time on searching for a stable configuration and manually reconfiguring devices.

C. Technological Innovations

The following novelties or features are designed into our proposed effective Network Configuration Management System (NCMS) with the enforced Access Control policies and Centralized management method to provide an interface for the configuration management of internal network devices:

- The enhancement of security features is one of the biggest differences between our proposed system and other NCMS systems.
- Fully comprehensive capabilities that prevent unauthorized modification of network configurations in the enterprise-wide network.
- Not only establish standards and policies for equipment configuration but also, more importantly, have the ability to ensure adherence to those standards.
  - Enforce enterprise-wide access control policies for device and user operation via centralized control and Bastion host solution
- Provide relevant solutions for some special use cases and requirements in the enterprise-wide network:
  - Prevent unauthorized modification on network devices due to shared passwords
  - Prevent configuration inconsistency due to different users operate at the same time on the same device
  - Prevent changes by maintenance personnel from the equipment supplier

V. Implementation

We have built a global Controllable Secure Configuration Management System (CSCMS) based on our proposed solution on NCMS and multiple feedbacks from our industry collaborator. CSCMS is presented as a web application accessible through a web browser. It provides a range of services and communicates with other entities, making more contributions on the controllable security and access control methods to our industry collaborator network system.

The prototype of CSCMS was implemented with Java Platform, Enterprise Edition (Java EE) and several technologies. The server side is based on Spring Web MVC framework, which provides a Model-View-Controller architecture for web applications. On the client-side, the Graphical User Interface of the system web front was created using Bootstrap web framework from Twitter. This web framework is compatible with the most common browsers, including their mobile versions. Its responsive design adapts to different screen resolutions.

VI. Conclusion

Configuration of large-scale networks is difficult and error-prone. Misconfigurations known as vulnerabilities are a major cause of network outages and security problems. In this paper, we present an effective Network Configuration Management System (NCMS) with the enforced Access Control policies and centralized management method to provide a controllable security access interface for the configuration management of internal network devices and leads to better network resiliency, security, and scalability.

Acknowledgment

This work was supported by the National Research Foundation (NRF), Prime Minister's Office, Singapore, under its National Cybersecurity R&D Programme (Award No. NRF2014NCR-NCR001-31) and administered by the National Cybersecurity R&D Directorate. The special thanks are also given to SMRT Trains Ltd for providing domain knowledge and technical support.

References

[1] Juniper, "Whats Behind Network Downtime? Proactive Steps to Reduce Human Error and Improve Availability of Networks," Juniper Networks White Paper, 2008.

[2] IBM, "IBM Security Services 2013 Cyber Security Intelligence Index: Analysis of cyber security attack and incident data from IBMs worldwide security operations," IBM Global Technology Services, 2013.

[3] J. Pescatore, "Taxonomy of Software Vulnerabilities," Gartner Research, 2003.

[4] Z. Kerravala, "As the Value of Enterprise Networks Escalates, So Does the Need for Configuration Management." The Yankee Group, Jan 2004.

[5] D. Curtis, "MarketScope for Network Configuration and Change Management," Gartner, Oct 2011.

[6] M. Gabdurahmanov, "Analysis and Evaluation of Network Management Solutions : A Comparison of Network Management Solutions Suitable for Networks with 2,500+ Devices," KTH ROYAL INSTITUTE OF TECHNOLOGY, June 2016.

[7] S. Networks, "RANCID - Really Awesome New Cisco confIg Differ," Shrubbery Networks.

[8] D. Genkov, "Software System for Configuration Management of Networking Devices," in *IJRET: International Journal of Research in Engineering and Technology, Volume: 03 Special Issue: 17*, Dec 2014, pp. 46–50.

[9] T. Jenkins, "GSEC Version 1.2e - Hardening Bastion Hosts," SANS Institute, 2001.