Chapter 7
State Model Diagrams:
A Universal, Model Driven Method for Network System Configuration and Management

S. P. Maj
Edith Cowan University, Australia

ABSTRACT
The Internet is an integral part of business communications, however it was based on open standards without due regard to security issues consequently security threats are not only persistent but also increasing. The Computer Security Institute (CSI) 2007 reported a doubling of average annual loss by US companies. There are three primary network security threats: policy, technology, and configuration. This chapter is primarily concerned with the configuration and management of network devices. There are a number of different network management tools currently available, however typically it is problematic to concurrently display configuration data from devices and protocols whilst maintaining a navigational context. This chapter demonstrates how the State Model Diagram method is not only a universal model-driven network tool but also useful for the configuration and management of complex security protocols and devices.

NETWORK DEVICE CONFIGURATION AND MANAGEMENT
Configuring devices, even for routine end users applications such as Internet Explorer, may be problematic (Furnell, 2007) (Furnell, 2005). This problem is exacerbated for dedicated devices such as firewalls which are not only complex devices within themselves but also difficult to configure. Configuring a firewall is considered to be of paramount importance (Rubin, 1997). A firewall employs directional; rule based stateful packet analysis for inbound and outbound packets. According to Bartal,

This is a crucial task ... The bottom line, however, is that the security of the whole intranet depends upon the exact content of the rule-base, with no level of abstraction available. Since the syntax

DOI: 10.4018/978-1-61520-837-1.ch007
and semantics of the rules and their ordering depend upon the firewall product/vendor, this is akin to the dark ages of software, where programs were written in assembly language so that the programmer had to know all the idiosyncrasies of the target processor. (Bartal, Mayer, Nissim, & Wool, 2004)

Firewall configuration is via either a text based Command Line Interface (CLI) or a Graphical User Interface (GUI). The syntactic and semantic complexities of the Cisco PIX firewall CLI have, to some extent, been progressively addressed. Check Point can be configured using either the GUI or the INSPECT language. The INSPECT language is a powerful but complex low level-language. The Check Point GUI is designed to address the problems associated with configuring directional, rule-based filtering. However, according to Wool direction-based filtering remains problematic,

Most firewall vendors (exemplified by Cisco and Lucent) seem to be unaware of the usability issues related to direction-based filtering. These vendors simply expose the raw and confusing direction based filtering functionality to the firewall administrator. A notable exception is Check Point. In order to avoid the usability problem, Check Point chooses to keep its management interface simple, and hide the direction-based filtering functionality in such a way that most users are essentially unable to use it. (Wool, 2004)

In effect the human factor is a significant aspect of security. According to Shultz security is primarily a people issue and hence a usability problem, ‘People, for example, are almost invariably involved in installing, configuring and maintaining technology, something that leaves ample opportunity for human error that can result in exposures that can allow those who are intent on evil doing to bypass or defeat this technology.’ (Shultz, 2005)

Based on a heuristic evaluation method Nielsen developed criteria for a successful human interface (Nielsen & Molich, 1990), (Nielsen). These criteria may be used to evaluate security related interfaces (Furnell, 2007). To address issues specific to interfaces for security purposes Johnston proposed criteria for a security Human Computer Interface (HCI-S) (Johnston, Eloff, & Labuschagne, 2003). HCI-S criteria are defined as: convey features; visibility of system status; learnability; aesthetic and minimalist design; errors; satisfaction and trust. Despite advances in GUI development, administrators continue to use the CLI (Takayama, 2006).

The problems associated with security device management are further exacerbated by the need to configure, integrate and manage a wide range of heterogeneous technologies such as routers, and switches. Van den Akker (van den Akker, 2001) makes the point, ‘Other security breaches caused by user error can be attributed to the complexity of modern systems. Users must be able to used and clearly understand the system in order to use it effectively.’ Wireless technologies may be especially problematic. According to Solms, ‘Insecure wireless networks can cause very serious risks to companies, and before installing any such networks, all these risks must be identified, evaluated, and based on the results, the necessary counter measures must be installed to secure the network.’ (Solms & Marais, 2004).

Commercial Network Management Tools

There are a range of both simple and more advanced Windows and Linux based tools for manually testing network connectivity that include: ping, traceroute, whois, nslookup, dig, netsat and nbstat, all of which are typically based on the text-based Command Line Interface (CLI) with associated pull down menus. The syslog protocol allows network devices to automatically send unacknowledged notification messages to event
Related Content

[www.igi-global.com/chapter/cloud-software-testing-environment-dependable/72239?camid=4v1a](www.igi-global.com/chapter/cloud-software-testing-environment-dependable/72239?camid=4v1a)

A Look Behind Conceptual Modeling Constructs in Information System Analysis and Design
[www.igi-global.com/article/look-behind-conceptual-modeling-constructs/40954?camid=4v1a](www.igi-global.com/article/look-behind-conceptual-modeling-constructs/40954?camid=4v1a)

Integrated Software Testing Learning Environment for Training Senior-Level Computer Science Students
[www.igi-global.com/chapter/integrated-software-testing-learning-environment/29601?camid=4v1a](www.igi-global.com/chapter/integrated-software-testing-learning-environment/29601?camid=4v1a)

Risk-Based Privacy-Aware Information Disclosure
[www.igi-global.com/article/risk-based-privacy-aware-information-disclosure/136467?camid=4v1a](www.igi-global.com/article/risk-based-privacy-aware-information-disclosure/136467?camid=4v1a)