POLITECNICO DI TORINO

Dipartimento di Automatica e Informatica

PhD in Computer and Control Engineering

XXIX cycle

Advisor

prof. Antonio Lioy

PhD Candidate: *Fulvio Valenza*

Anomaly Analysis in Network Security Policy

Introduction

Nowadays, computers have a pervasive presence in all our daily activities. The current technological trend is to reduce human intervention and to provide human beings adequate instruments that can be used for decision-making purposes. This is particularly important in areas where human lives, high economic costs and security in general are at stake. The final target is to lessen the human fallibility. Protecting a networked IT infrastructure, guaranteeing user privacy, and securing communications are important facets of this technological evolution. For a human being is very difficult (if not actually impossible) to envision the whole configuration of large networked systems and implement it without errors and with an adequate number of protections. As several studies have proven, the human factor is the main cause of network misconfiguration. Anomalies in the security configurations may result in serious breaches and network vulnerability causing problems such as blocking legitimate traffic, permitting unwanted traffic and sending insecure data.

Therefore, the overall goal of the PhD research activity is the analysis of issues related to the network security policies in order to avoid policy anomalies.

Research Outcome

Policy Anomaly Analysis is designed to identify potential errors, conflict and redundancy among policy rules. In literature, several works and techniques have been proposed to identify anomalies, however the research is mainly concentrated on Intra- and Inter-policy analysis. The *Intra-Policy* analysis identifies any anomaly in the rules of a single policy, while the *Inter-Policy* analysis identifies anomalies in rules of a set of interconnected policies.

However, the complexity of real systems is not self-contained, as each network security control may affect the behavior of other controls in the same network.

For this reason, we propose an innovative anomaly analysis for network security policy based on two new classes of policy anomaly: inter-technology and inter-domain.

The *Inter-Technology Policy Analysis* identifies any anomaly in a set of policies of different security communication technologies (e.g. IPsec, TLS, SSH). For instance, when an IPsec tunnel encapsulates other TLS tunnels, the external tunnel is a redundant level of protection.

The *Inter-Domain Anomaly Policy Analysis* identifies anomalies in a set of policies of different security policy domains. This is the case of a firewall that blocks some encrypted communication channels created by a VPN functionalities, which generates an inter-domain anomaly between the filtering domain (i.e., firewall) and the communication-protection one (i.e., VPN).

In summary, the research outcome of this work is to present a unified and complete analysis for detecting network policies anomaly, in order to avoid erroneous and unexpected network behaviors.

Inter-Technology Analysis in CPP

Communication protection policies (CPPs) specify how to protect the network communications. Their correct deployment is crucial in several areas, such as protection of intellectual properties, and confidentiality of financial or corporate data (like credit card numbers). CPP specification simply requires the definition of the communication end-points to protect, seldom the security properties to ensure (e.g., confidentiality and data integrity), and, seldom if ever, hints about the technology to adopt.

Therefore, the refinement of CPPs is challenging since an administrator, or a tool mimicking his behaviour, must automatically infer and has to choose several technical details among several alternatives, such as the security protocol (e.g., SSL/TLS, SSH or S-FTP), the cipher-suite and the time-outs. Anomalies in the refinement process can lead to incorrect or suboptimal implementations, that in turn affect the overall security, decrease the network throughput and increase the costs.

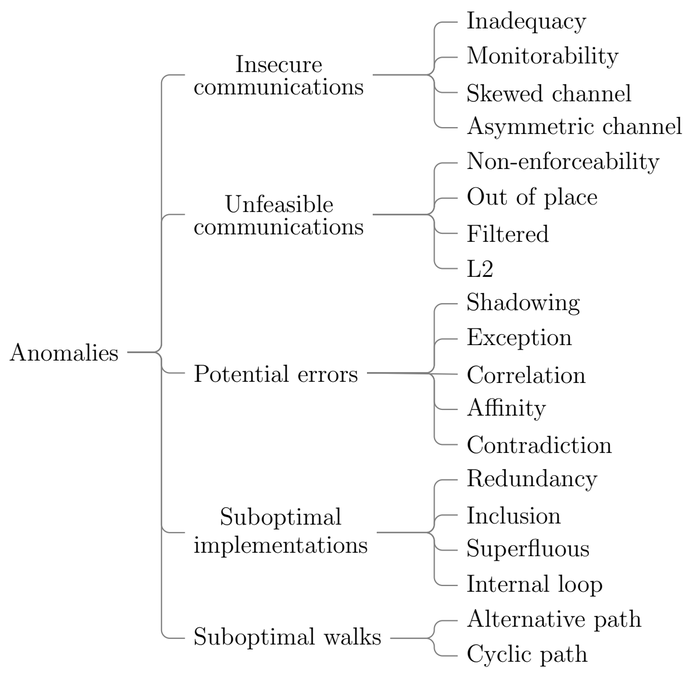

Figure 1: *Policy Anomalies in CPP.*

We propose in [1], a novel classification of CPP anomalies (Figure 1) and a formal model, which is able to detect anomalies among policy implementations relying on technologies that work at different network layers.

In this model, a Policy implementation i is a tuple:

$$i = (s, d, t, C, S, G)$$

The field s and d respectively represent the channel source and destination; t is the adopted security technology; C is an ordered set of coefficients that indicate the required security levels; S is a tuple of selectors used to identify the traffic that needs to be protected; G is the list of the gateways involved in the communication.

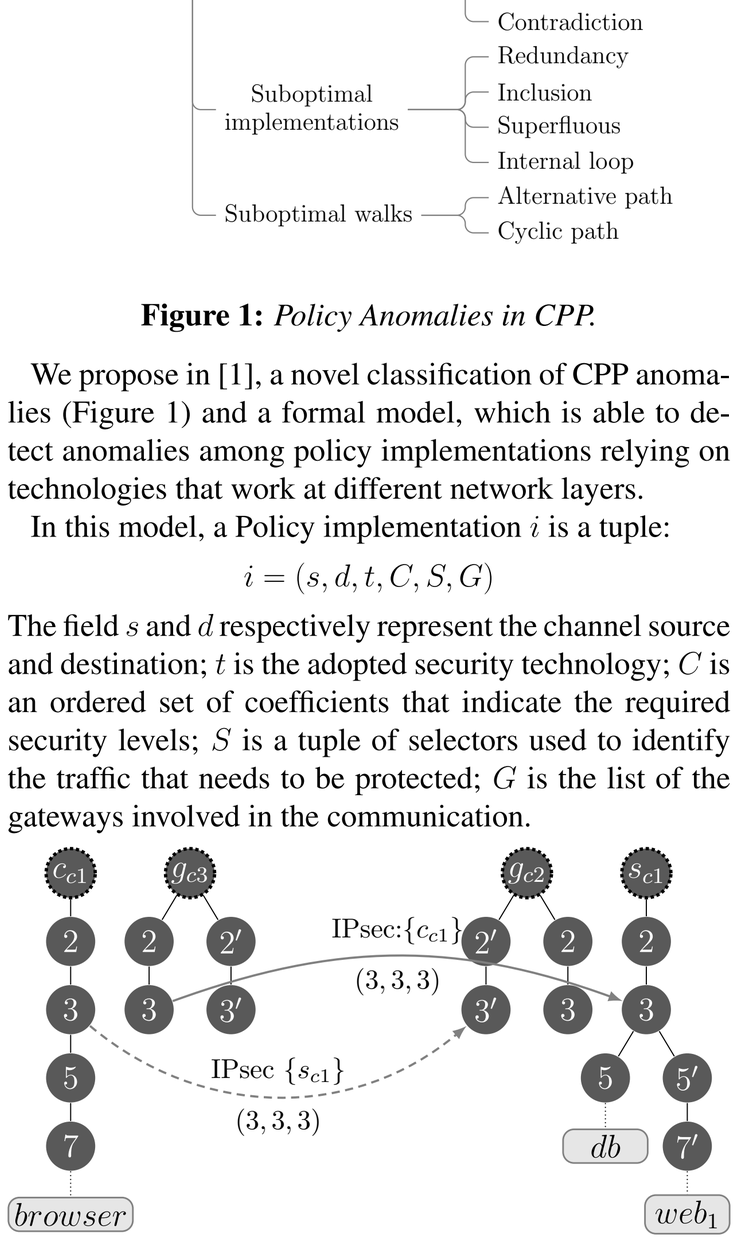

Figure 2: *Graphical representation of skewed channel.*

Aiming for a model that also has practical relevance, we have investigated the possibility of a user friendly representation of these anomalies. It is evident that logical formulas are not easily usable by administrators. By means of this view, we can depict secure communications by connecting network nodes to form a multi-graph. The obvious advantage of such representation is that it allows a network administrator to visualize the communications at a glance, intuitively identify the anomalies, and immediately see the consequences and the proper reactions. For example, Figure 2 shows an *skewed channel* anomaly between two Policy Implementations.

In summary, our approach can be used to inter-technology analysis that find incompatibilities, redundancies and severe errors among policy implementations that use security technologies working at different ISO/OSI layers and with different security properties.

Inter-Domain Policy Analysis

Visualized networks are becoming more and more complex systems to manage for administrators, due to the number and type of services available. For this reason, it is indispensable to help the administrators by supporting, in a general analysis framework, different types of functions (e.g., firewalls, content filters, channel protection devices, logging, monitoring, and so on) and their interactions. Thanks to its usefulness, a detection policy anomalies can be define in different application domains (e.g. filtering, data protection, parental control).

A unified model for detecting *inter-* and *intra-domain* policy anomalies has been presented in [2], with the aim of avoiding erroneous and unexpected network behaviours. The proposed model is a generalization of the model used in the policy analysis of CPPs [1].

The unified analysis model is composed of four sets, that are: *network fields*, *policy actions*, *Policy Implementations*, and *detection rules*.

The *network fields* and *policy actions* are atomic elements that identify condition and action of a policy.

Policy Implementations (*PIs*), are data-structures to pinpoint in a formal and abstract way the policy rules enforced by a network node for a certain domain. Actually, a *PI* has a different set of network fields and policy actions, based on the domain where the *PI* is defined.

$$pi_i = (n_{i1}, n_{i2}, ..., n_{in}, a_{i1}, a_{i2}, ..., a_{in})$$

The *detection rules* are a set of conditions that distinguish the possible anomalies among *PIs*. In the proposed model, the detection rules are based on the First Order Logic (FOL) and are expressed using the Horn clauses.

$$C_1 \wedge C_2 \wedge \cdots \wedge C_n \Rightarrow A$$

The results of the inter-domain policy analysis allow administrators to have a precise insight on the various configuration implemented for each domain, their relations and the possibility of resolving anomalies, thus increasing the overall security and performance of a network.

Bibliography

[1] F. Valenza, C.Basile, D.Canavese and A.Lioy "Classification and analysis of communication protection policy anomalies," Submitted to: IEEE/ACM Transactions on Networking "

[2] F. Valenza, S. Spinoso, C. Basile, R. Sisto, and A. Lioy, "A formal model of network policy analysis," in First International Forum on Research and Technologies for Society and Industry, September 2015, pp. 516–522,