Doctoral Dissertation
Doctoral Program in Computer Engineering (29th cycle)

Modelling and Analysis of Network Security Policies

Fulvio Valenza

Supervisor: Prof. Antonio Lioy
Co-Supervisor: Ing. Cataldo Basile
Scenario

Introduction

Large-sized Networks:

- hundreds of nodes
- different security technologies
- many network services
- policy-based management

Modelling and Analysis of Network Security Policies

Fulvio Valenza
• specification of security policies requires several technical details
  • security properties, protocols, cipher-suites and timeouts

• security administrators’ (hard) tasks: write correct policies and avoid network errors
  • e.g. blocking legitimate traffic or sending insecure data

The literature confirms¹:

× 60% of security breaches and breakdowns are attributable to administrators’ responsibilities

¹Data breach investigation 2016
PhD Objectives

1. Deep investigation on the limitations of the current state of the art on network security policies
2. Improvements of the analysis of policy types less addressed in the literature (i.e. communication protection policy)
3. Definition of a unified model for policy analysis
Network Security Policy

Communication Protection Policy

Unified Model for Policy Analysis
• **policy**: *a set of rules to administer, manage, and control access to network resources*

• **policy rule**: *a set of actions to a set of conditions - where the conditions determine whether the actions are performed*

• **network security policy**: *a policy that specify the security requirements of network communications*
  - e.g., forward, filter, translate, protect and monitoring network traffic

### packet filter policy

<table>
<thead>
<tr>
<th>src_IP</th>
<th>src_Port</th>
<th>dst_IP</th>
<th>dst_Port</th>
<th>protocol</th>
<th>action</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.*</td>
<td>0-1024</td>
<td>192.168.3.*</td>
<td>0-1024</td>
<td>TCP</td>
<td>allow</td>
</tr>
</tbody>
</table>
Research Topics

Network Security Policy

- **Policy Analysis**: process to analyze and check some properties against a set of policies
  - *Anomaly Analysis, Reachability Analysis, Policy Comparison*

- **Anomaly Analysis** checks the policy specification to prevent errors, conflicts and sub-optimization (i.e. *anomalies*) in the network
• **Conflicts** are triggered when the effect of one security policy is influenced or altered by another one
  - e.g., the actions of two rules contradict each other

• **Errors** occur when the enforcement of the policy actions fails
  - e.g., a mismatch between the policy actions and the device capabilities

• **Sub-optimizations** arise when other more efficient policy implementations are available
  - e.g., redundant rules are present in policy specification
Filtering

- Several works mostly related to packet filters
- Few works on stateful and application firewalls

Communication protection policy

- Few works in literature and only on IPsec policy anomalies
- No policy analysis over many technologies (e.g. TLS vs SSH)

Other

- Few and limited works on other policy types
- No analysis among different policy types
PhD Contributions

Network Security Policy

Modelling and Analysis of Network Security Policies

Fulvio Valenza
Network Security Policy

Communication Protection Policy

Unified Model for Policy Analysis
Communication Protection Policy

- specify the security requirements to apply on a communication
- difficult to manage
  - enforced by several security controls
  - use different protocols at different layers of the OSI stack
    - e.g. IPsec, TLS, SSH, WS-Security

× incorrect implementations produce faulty and redundant configurations, leading information disclosure, violations of the users’ privacy, monetary losses, etc
• **Channel** is a directional data exchange between two entities at a specific ISO/OSI layer

• **Secure channel** is a channel with some security properties
  - e.g., header integrity, payload integrity and (payload) confidentiality

• **Communication** is all directional data exchanges between nodes
  - a communication is a set of several channels

• **Policy Implementation (PI)** is a formal representation of a channel
  - a communication is represented by a set of PIs
Policy Implementation

Communication Protection Policy

\[ i = (s, d, t, C, S, G) \]

- represent the **source** and **destination** of the channel

  data link layer ↔ layer 2 addresses  
  network layer ↔ IP addresses  
  session layer ↔ port numbers  
  application layer ↔ URIs
Policy Implementation

Communication Protection Policy

\[ i = (s, d, t, C, S, G) \]

- the requested security **technology**
  - data link layer ↔ WPA2 and MACsec
  - network layer ↔ IPsec
  - session layer ↔ TLS and SSH
  - application layer ↔ WS-Security
  - NULL
Policy Implementation

Communication Protection Policy

\[ i = (s, d, t, C, S, G) \]

- the requested **security coefficients**
  \[ C = (c^h, c^p, c^c) \]
  - non-negative values to indicate a required security level for a specific property
    - i.e. confidentiality, header and payload integrity
  - estimated by the administrators based on some metrics
    - key length, encryption/hash algorithms, cipher mode

\[ \text{if } t = NULL \implies C = (0, 0, 0) \]
Policy Implementation

Communication Protection Policy

\[ i = (s, d, t, C, S, G) \]

- a set of network fields \textit{(selectors)} to identify the traffic to protect
  - e.g. IPsec packet headers

\[ S = (ip_{src}, ip_{dst}, p_{src}, p_{dst}, proto) \]
\[ i = (s, d, t, C, S, G) \]

- the list of the *gateways* involved in the communication
Example

Communication Protection Policy

Modelling and Analysis of Network Security Policies

Fulvio Valenza
Anomalies

- Insecure communications
- Unfeasible communications
- Potential errors
- Suboptimal implementations
- Suboptimal walks
Anomalies

Insecure communications
- Inadequacy
  - Monitorability
  - Skewed channel
  - Asymmetric channel
- Skewed channel
- Asymmetric channel
- Non-enforceability
- Out of place
- Filtered
- L2
- Shadowing
- Exception
- Correlation
- Affinity
- Contradiction
- Redundancy
- Inclusion
- Superfluous
- Internal loop
- Alternative path
- Cyclic path

Unfeasible communications

Potential errors

Suboptimal implementations

Suboptimal walks

“An **insecure communication** occurs when the communication security level is lower than the expected one”
Anomalies

Insecure communications

Unfeasible communications

Non-enforceability
Out of place
Filtered
L2

Potential errors

Suboptimal implementations

Suboptimal walks

“An unfeasible communication is a communication that cannot be established because of a hard misconfiguration”
Anomalies

Communication Protection Policy

Insecure communications

Unfeasible communications

Potential errors

Suboptimal implementations

Suboptimal walks

Shadowing
Exception
Correlation
Affinity
Contradiction

“A potential error occurs where the original intent of administrators is unclear and is required a thorough human inspection”
Anomalies

Communication Protection Policy

Insecure communications

Unfeasible communications

Potential errors

Suboptimal implementations

Suboptimal walks

Redundancy
Inclusion
Superfluous
Internal loop

“A suboptimal implementation arises when extra PIs can decrease the network throughput by producing some overhead in nodes”
Anomalies

- Insecure communications
- Unfeasible communications
- Potential errors
- Suboptimal implementations
- Suboptimal walks

“A group of PIs can produce a suboptimal walk when the path taken by the data is unnecessarily long”
Anomalies

Insecure communications
- Inadequacy
- Monitorability
- Skewed channel
- Asymmetric channel

Unfeasible communications
- Non-enforceability
- Out of place
- Filtered
- L2
- Shadowing
- Exception
- Correlation
- Affinity
- Contradiction
- Redundancy

Potential errors
- Inclusion
- Superfluous
- Internal loop
- Alternative path
- Cyclic path

Suboptimal implementations

Suboptimal walks
a monitorability anomaly is when some nodes at the channel junctions can “see” the exchanged data
Skewed channel anomaly

- A **skewed channel anomaly** is when a wrong tunnel overlapping removes the confidentiality in a part of the communication.

\[ g_{c3} \rightarrow g_{c1} \rightarrow g_{a1} \]

\[ \rightarrow \text{Double tunnel} \]
\[ \rightarrow \text{Single tunnel} \]
\[ \rightarrow \text{No tunnel} \]

\[ ^1 \text{Al-Shaer et al. “Modeling and Verification of IPSec and VPN Security Policies”} \]
Filtered anomaly

- a **filtered anomaly** is when the packets of a channel are dropped by a firewall that lies on the path between source and destination
  - external info: the filtering policy
Contradiction anomaly

Potential error
- Shadowing
- Exception
- Correlation
- Affinity
- Contradiction

- a **contradiction anomaly** is when two PIs respectively express that the same communication should be protected and unprotected
a **superfluous anomaly** is when a tunnel encapsulates other tunnels with a higher security level
Anomaly analysis

1. **algebraic model**
   - based on First Order Logic (FOL) formulas
     - one formula for each anomaly to check

2. **multi-graph representation**
   - a user-friendly representation of the anomalies
     - based on multi-graph theory
### Algebraic model

#### Communication Protection Policy

- **Filtered**

\[ A_{fi}(i_1) \iff \exists e : e \in G_1 \land F_e(i_1) = true \]

- **Skewed**

\[ A_{sk}(i_1, i_2) \iff s_1 \in S_2 | ip_{src} \times psr_{c} \times \ldots \land (|G_1^* \cap G_2^*) \geq 2 \land \]
\[ \land (G_2^* \setminus G_1^* \neq 0) \land c_1^c > 0 \land c_2^c > 0 \land i_1 \neq i_2 \]

- **Superfluous**

\[ A_{su}(i_1) \iff \not\exists i_k : s_k \in S_1 | ip_{src} \times psr_{c} \times \ldots \land G_k^* \supset G_1^* \land C_k \prec C_1 \]
end-to-end

Multi-graph representation

Communication Protection Policy

Modelling and Analysis of Network Security Policies

Fulvio Valenza
Multi-graph representation

Communication Protection Policy

Modelling and Analysis of Network Security Policies

Fulvio Valenza
Multi-graph representation

Communication Protection Policy

Modelling and Analysis of Network Security Policies
Fulvio Valenza
Multi-graph representation

Communication Protection Policy

skewed channel anomaly

IPsec: \((c_{c1}, *, s_{c1}, *, \ldots)\)

\((3, 3, 3)\)

browser

web\(_1\)

Modelling and Analysis of Network Security Policies

Fulvio Valenza
Multi-graph representation

filtered anomaly

browser

Modelling and Analysis of Network Security Policies
Fulvio Valenza
Model validation

1. **Model usefulness**
   - an empirical assessment with 30 different subjects

2. **Model feasibility**
   - testing of a implementation prototype
Empirical assessment

Communication Protection Policy

subjects
- recruiting a set of 30 administrators
  - split into 3 categories of experience (high, medium, low)

questionnaire
- translate five high-level CPPs into a set of PIs
- no limits on the time and number of PIs

results
- all the anomaly types have been introduced by the administrators when configuring the CPPs
- the number of anomalies decrease when administrator expertise grows
Implementation and Testing

Communication Protection Policy

- Java-based prototype relying on:
  - an ontology-centric core (OWL)
  - a powerful rule-based language (SWRL)

- All tests are executed on my workstation
  - 16 GB RAM
  - an Intel i7@2.4 GHz processor
  - running on Windows 10
Modelling and Analysis of Network Security Policies

Fulvio Valenza
Content

Unified Model for Policy Analysis

Network Security Policy

Communication Protection Policy

Unified Model for Policy Analysis
Define a unified model for policy analysis able to:

1. represent network security policies of different domains
   - filtering, transformation and communication policies

2. detect intra- and inter-domain anomalies
   - current literature limits its analysis to a single domain

3. extend the capabilities of policy analysis
   - detect any irregular network conditions and events that an administrator wants to monitor
     - i.e., no errors and conflicts
Inter-domain anomaly example

- a CPP is defined to *encrypt all traffic sent to the Internet*
- a filtering policy is configured to *drop all the encrypted traffic*
The Unified Model for Policy Analysis (UMPA) is composed of five elements:

- network fields
- policy actions
- policy implementations
- detection rules
- policy anomalies
network fields

- identify the traffic flows or the events an administrator wants to manage through a set of actions
  - e.g., packet headers, network node ID, traffic label, ...

policy actions

- represent either the action performed by a network node, the parameters and information that characterize that action
  - e.g., firewall’s “deny” or “allow”, algorithms, protocols, ..
Policy Implementations

- the formal definition of policy rule
- a sequential set of *network fields* \((n)\) and *policy actions* \((a)\):

\[
pi_i = (n_{i1}, n_{i2}, ..., n_{in}, a_{i1}, a_{i2}, ..., a_{in})
\]

- e.g., *packet filtering policy*

\[
pi_{fp} = (f, r, ip_{src}, ip_{dst}, t, p_{src}, p_{dst}, a)
\]
Relations $\mathcal{R}$:

- **equivalence**: $n_i$ and $n_j$ are equivalent if they have the same value
  \[ n_{i1} = 1.1.*.*, \quad n_{j1} = 1.1.*.* \rightarrow n_{i1} = n_{j1} \]

- **disjointness**: $n_i$ and $n_j$ are disjoint if they do not share any value
  \[ n_{i1} = [1,75], \quad n_{j1} = [100,50] \rightarrow n_{i1} \perp n_{j1} \]

- **dominance**: $n_i$ dominates $n_j$, if $n_i$ is a generalization of $n_j$
  \[ n_{i1} = 1.1.*.*, \quad n_{j1} = 1.1.1.* \rightarrow n_{i1} \succ n_{j1} \]

- **correlation**: $n_i$ and $n_j$ are correlated if they share some values, but none of them dominates the other
  \[ n_{i1} = [1,75], \quad n_{j1} = [50,100] \rightarrow n_{i1} \sim n_{j1} \]

- **non-disjointness** $n_i \not\perp n_j$: if $n_i$ and $n_j$ are not disjoint, they can be equivalent, correlated or one can dominate the other
Detection Rules

- set of conditions applied on fields and actions of one or more PIs
  - expressed using Horn clauses
    \[ C_1 \land C_2 \land \ldots \land C_n \implies I \]

\[ C_i := (n_{ik} \mathcal{R}_1 n_{ih}) \lor (n_{ik} \mathcal{R}_2 n_{jh}) \lor (n_{ik} \mathcal{R}_3 n_{jk}) \lor (a_{ik} \mathcal{R}_4 a_{ih}) \lor (a_{ik} \mathcal{R}_5 a_{jh}) \lor (a_{ik} \mathcal{R}_n a_{jk}) \lor \ldots \]

Anomaly

- arises when all the conditions are satisfied
  - e.g., *Intra-Firewall Shadowing anomaly*
    \[ f_i = f_j \land r_j \triangleright r_i \land ip_{src_i} \succeq ip_{src_j} \land t_i \triangleright t_j \land ip_{dst_i} \succeq ip_{dst_j} \land p_{src_i} \succeq p_{src_j} \land p_{dst_i} \succeq p_{dst_j} \land a_i \neq a_j \implies \text{Intra-Shadowing}(p_{i_i}, p_{i_j}) \]
Model validation

Validation of the capability of UMPA model by using:

1. three types of policy
   - packet filtering
   - communication protection
   - traffic flow (novel)

2. rule detection of
   - well-know intra-domain anomalies
   - new types of intra- and inter-domain anomalies

---

2Al-Shaer et al. “Discovery of policy anomalies in distributed firewalls”


## Contributions

- ✔ deep literature review on policy types and analysis approaches
- ✔ definition of inter-technology and inter-domain anomalies
- ✔ application anomaly analysis on communication protection policy
- ✔ formalization of a unified model for policy analysis
Future works

1. extend the expressiveness and capabilities of the UMPA model
   - improvements with policy reachability and reconciliation

2. integrate the policy anomaly analysis in NFV and SDN
   - policy analysis over Service Function Chains
<table>
<thead>
<tr>
<th>Policy Type</th>
<th>Papers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy refinement</td>
<td>NETSOFT2015, CSP2015, TON</td>
</tr>
<tr>
<td>Policy comparison</td>
<td>MIST2016, JOWUA2017</td>
</tr>
<tr>
<td>Policy reachability</td>
<td>CAEE2017</td>
</tr>
<tr>
<td>Others</td>
<td>SPRO2015, WFCS2017</td>
</tr>
</tbody>
</table>

**Accepted** | **Review** | **Conference** | **Journal** | **Book chapter**
Thanks for your attention!