Using Hierarchical Change Mining to Manage Network Security Policy Evolution

Gabriel A. Weaver, Nick Foti, Sergey Bratus,
Dan Rockmore, and Sean W. Smith

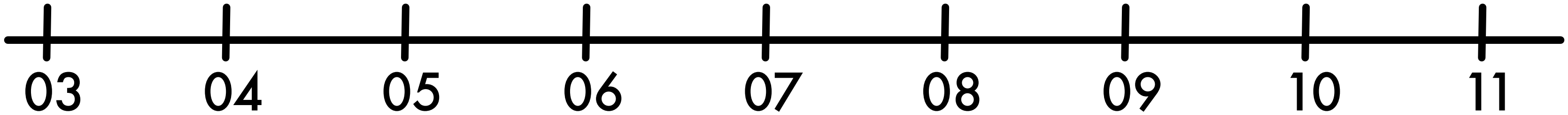
Presented by Gabriel A. Weaver
Dartmouth College

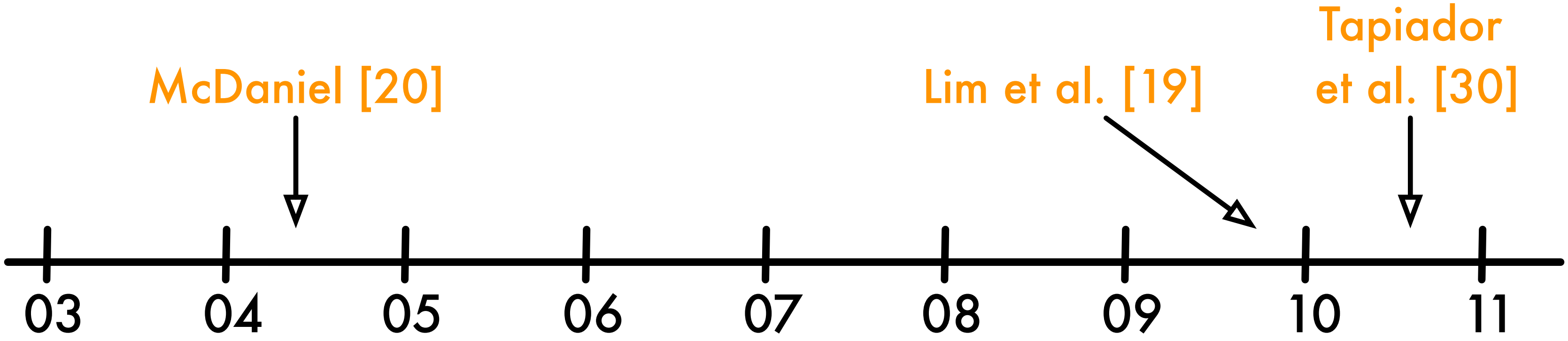
Network services change and evolve. Therefore managing security requires us to manage security policy evolution.

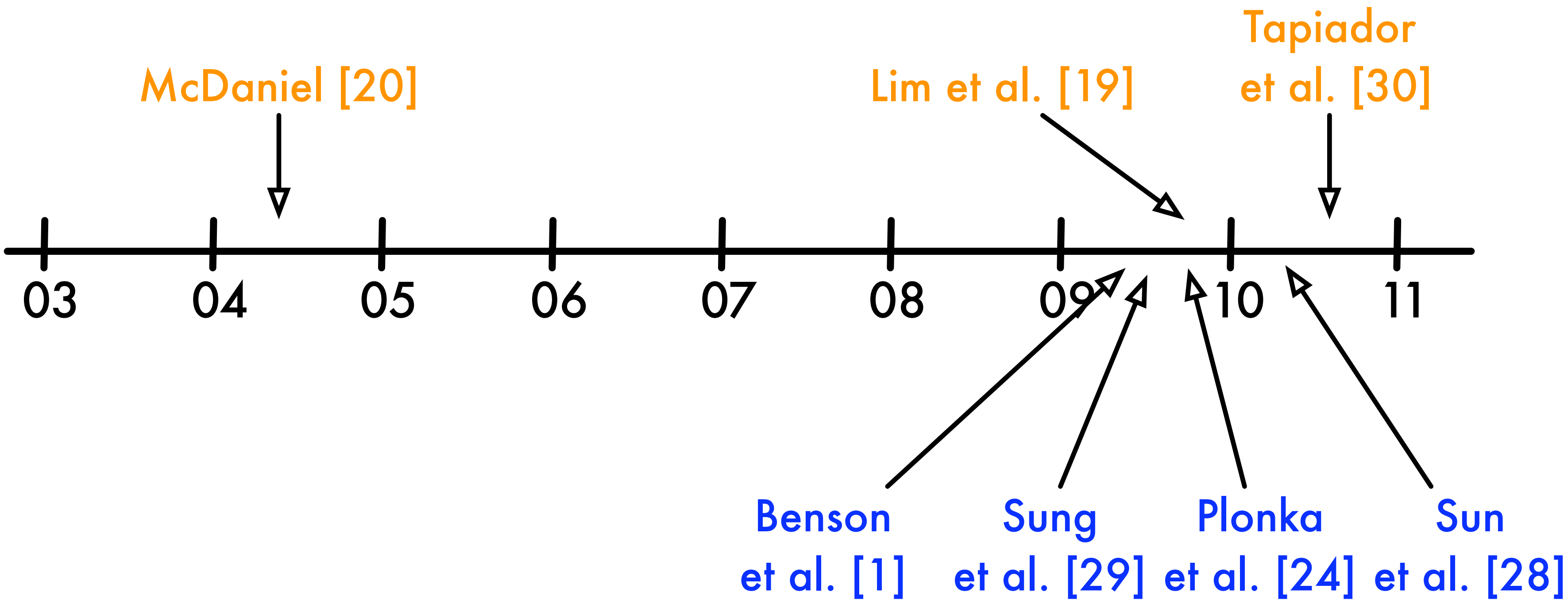
Case 1: If practitioners don't change policies as services change, systems are vulnerable.

Case 2: If practitioners make changes to the policy as services change, then errors may be accidentally introduced.

Before this paper, little research had been done on the general problem of security policy evolution.


03
04
05
06
07
08
09
10
11


McDaniel [20]
Lim et al. [19]
Tapiador et al. [30]
03
04
05
06
07
08
09
10
11


Tapiador
et al. [30]
McDaniel [20]
Lim et al. [19]
03
04
05
06
07
08
09
10
11
Benson
et al. [1]
Sung
et al. [29]
Plonka
et al. [24]
Sun
et al. [28]

We recognize that security policies are hierarchically-structured texts.

We propose a general method to mine changes within these structures.

Outline

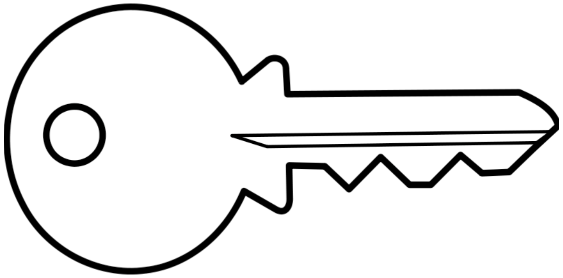
Two real-world examples

- security policy evolution problem
- hierarchical policy structure
- current approach, our approach & initial results

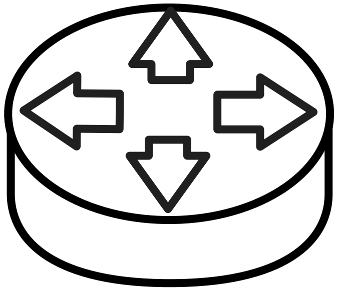
Conclude

Outline

Two real-world examples

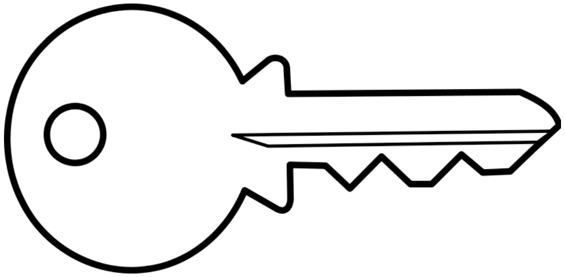


Identity Management



Switch/Router Configuration

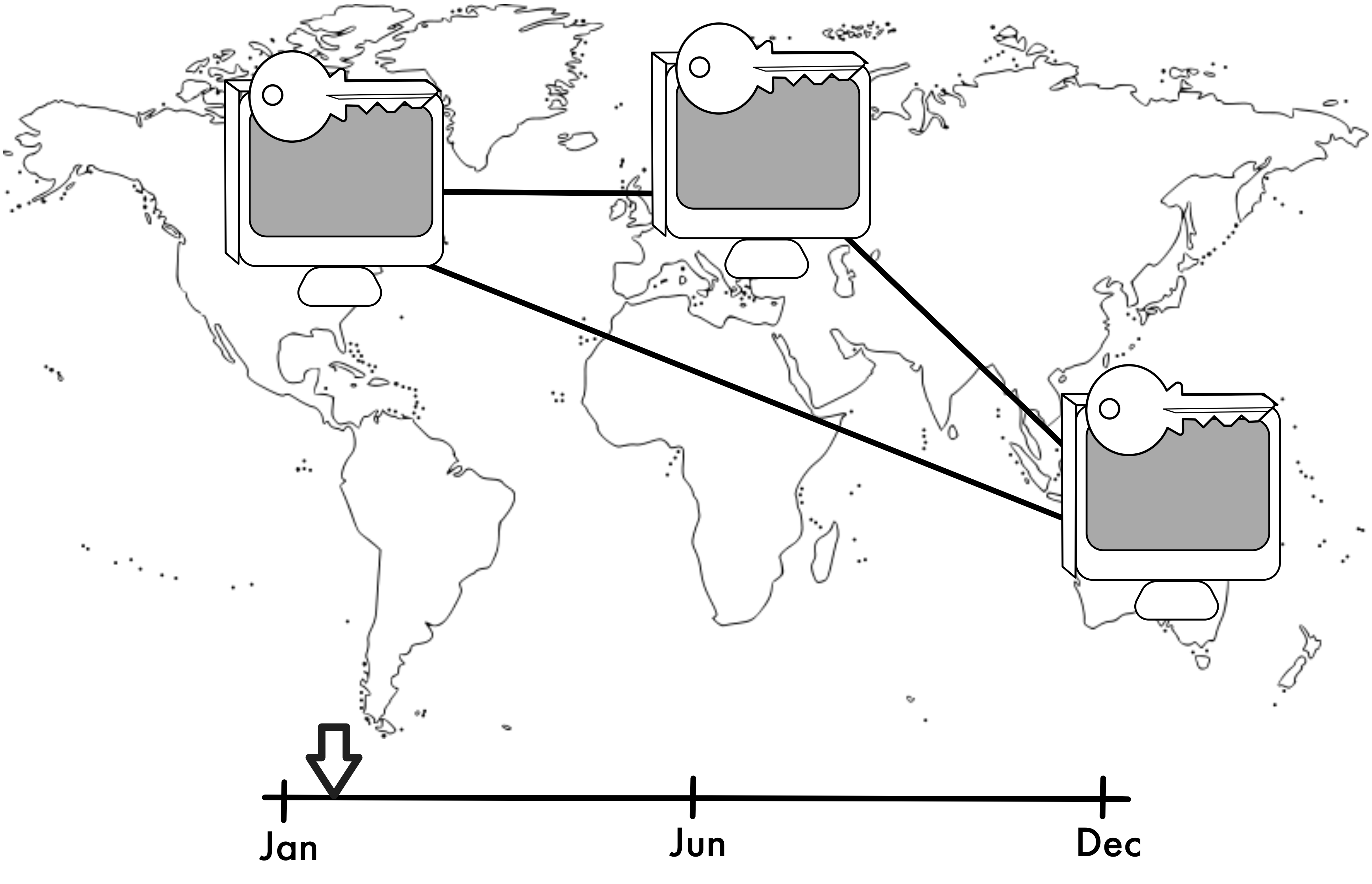
Conclude



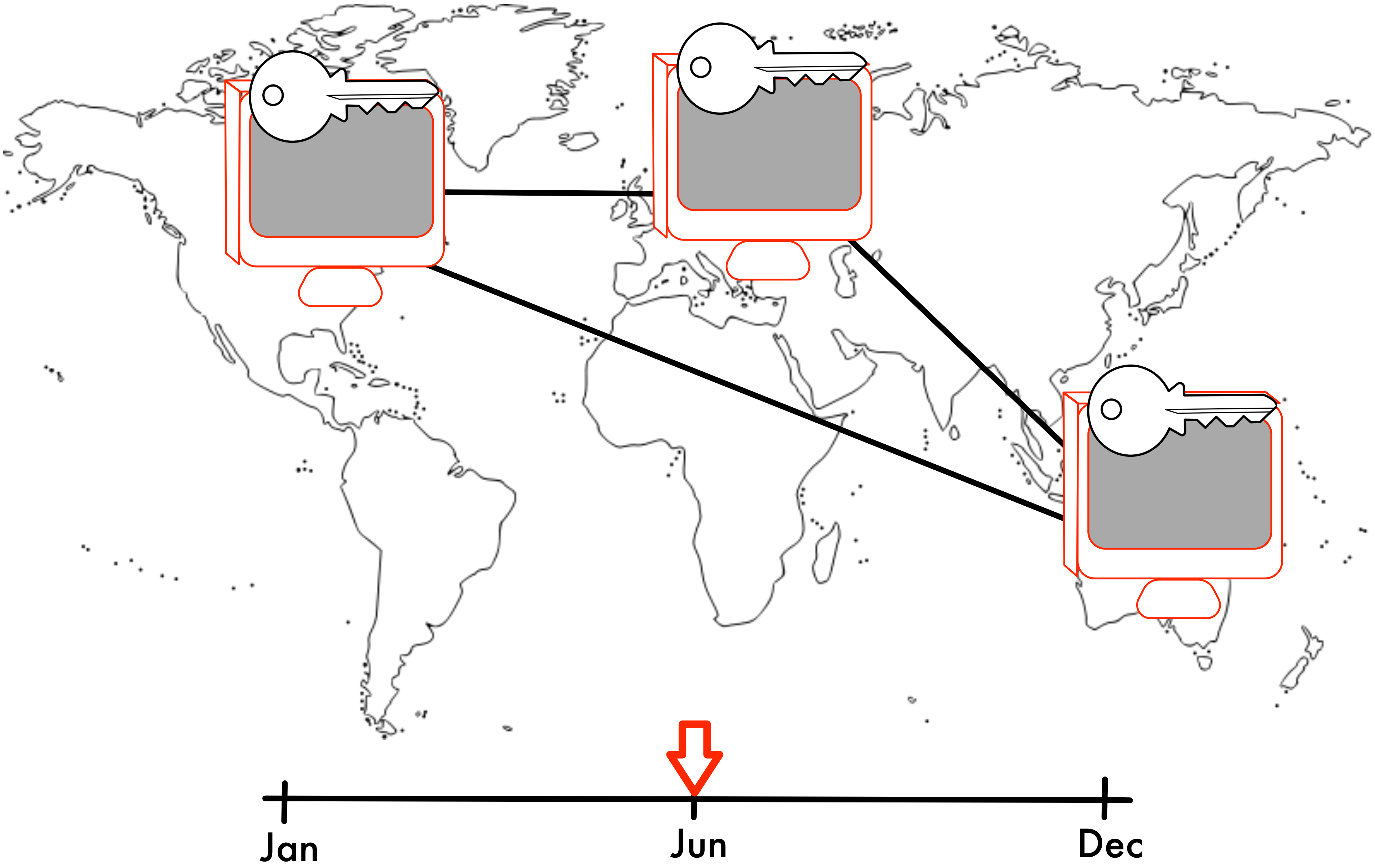
Identity Management

Changelogs insufficient

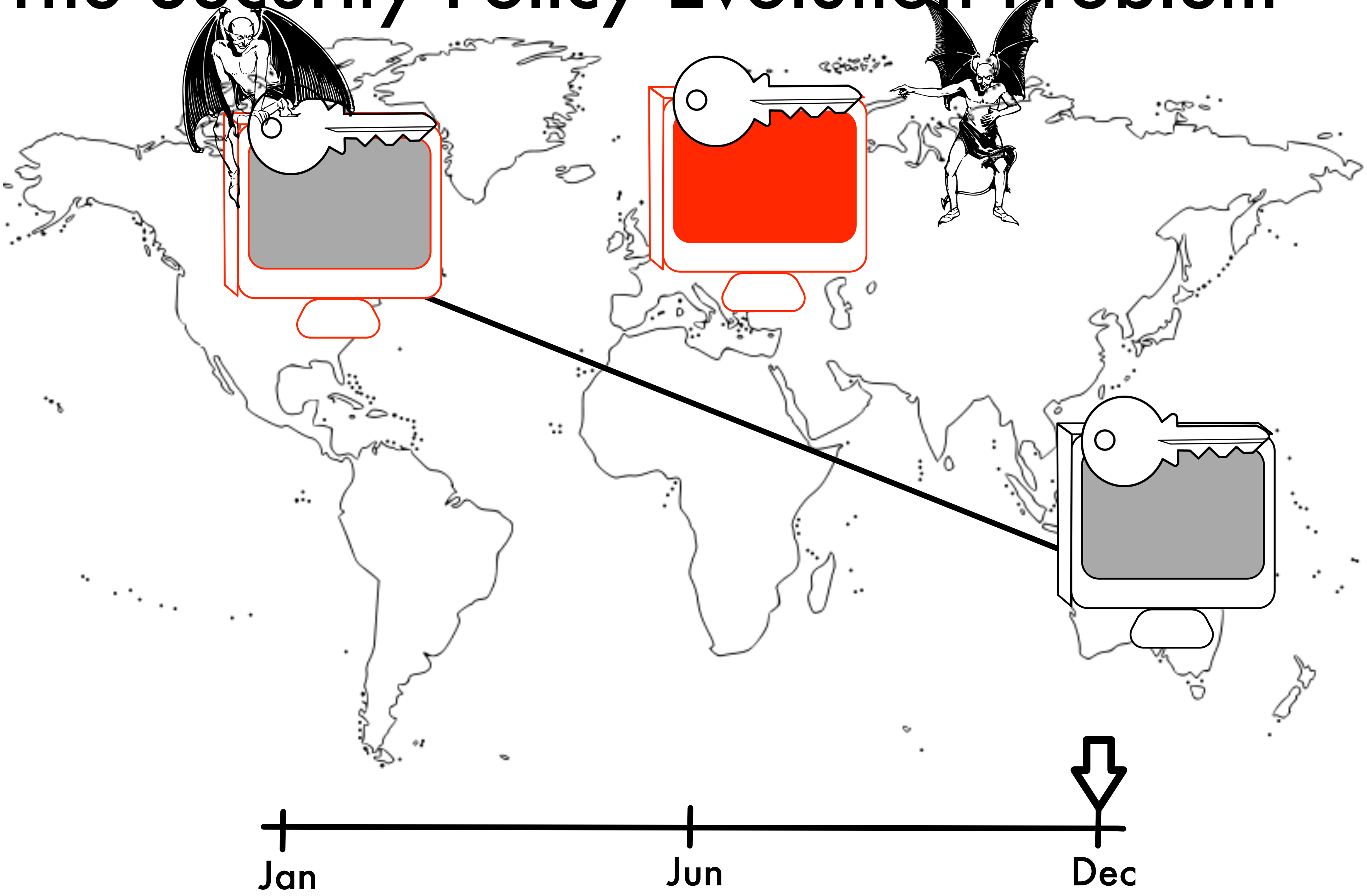
The Security Policy Evolution Problem



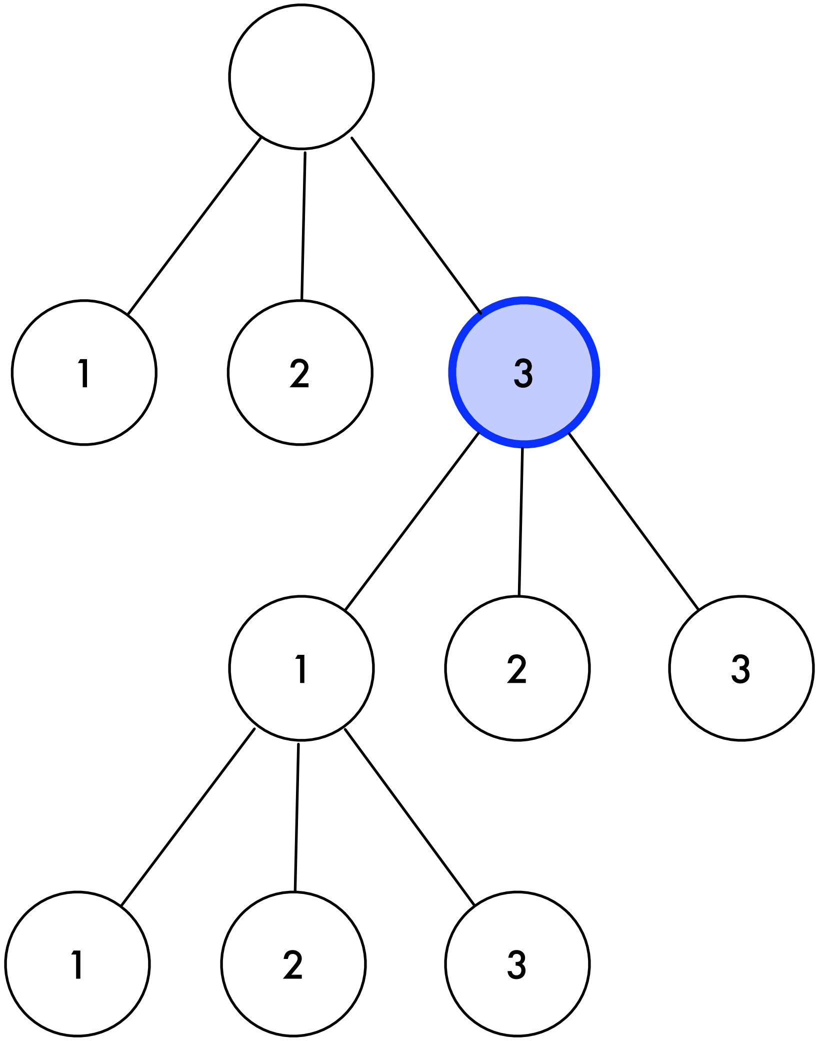
The Security Policy Evolution Problem



The Security Policy Evolution Problem



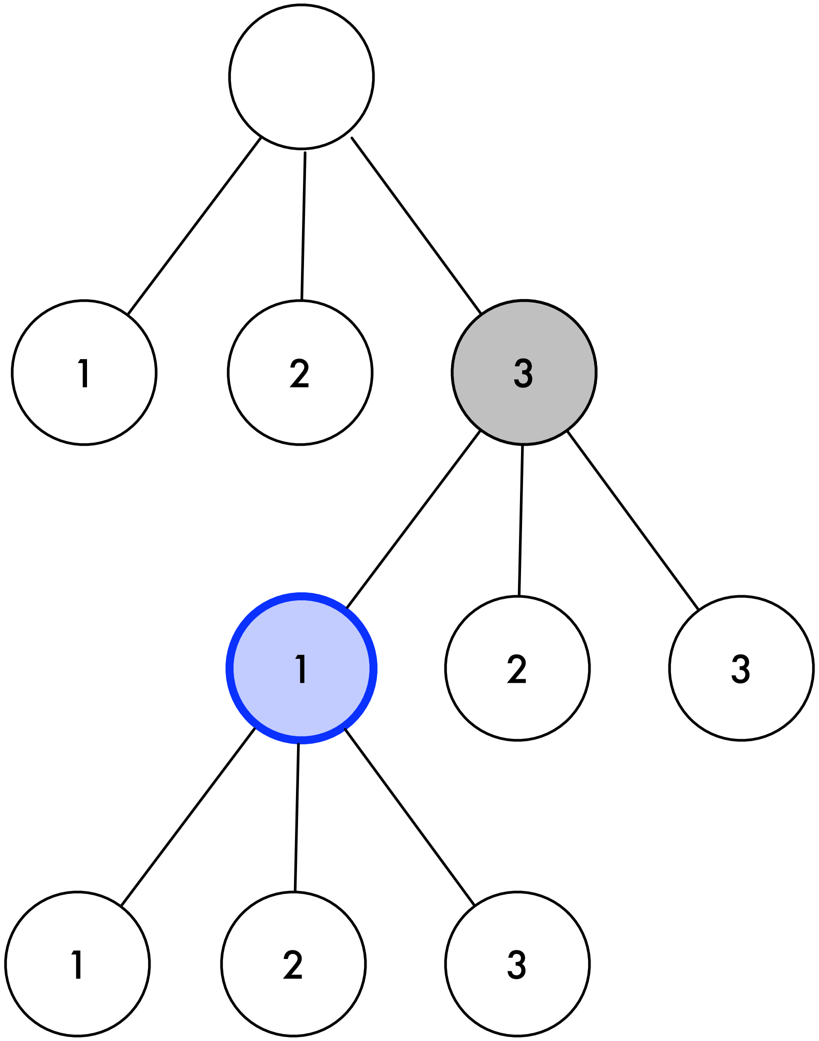
Hierarchical Policy Structure: RFC 3647



3 Identification and Authentication

SDG version 1.5.1

Hierarchical Policy Structure: RFC 3647

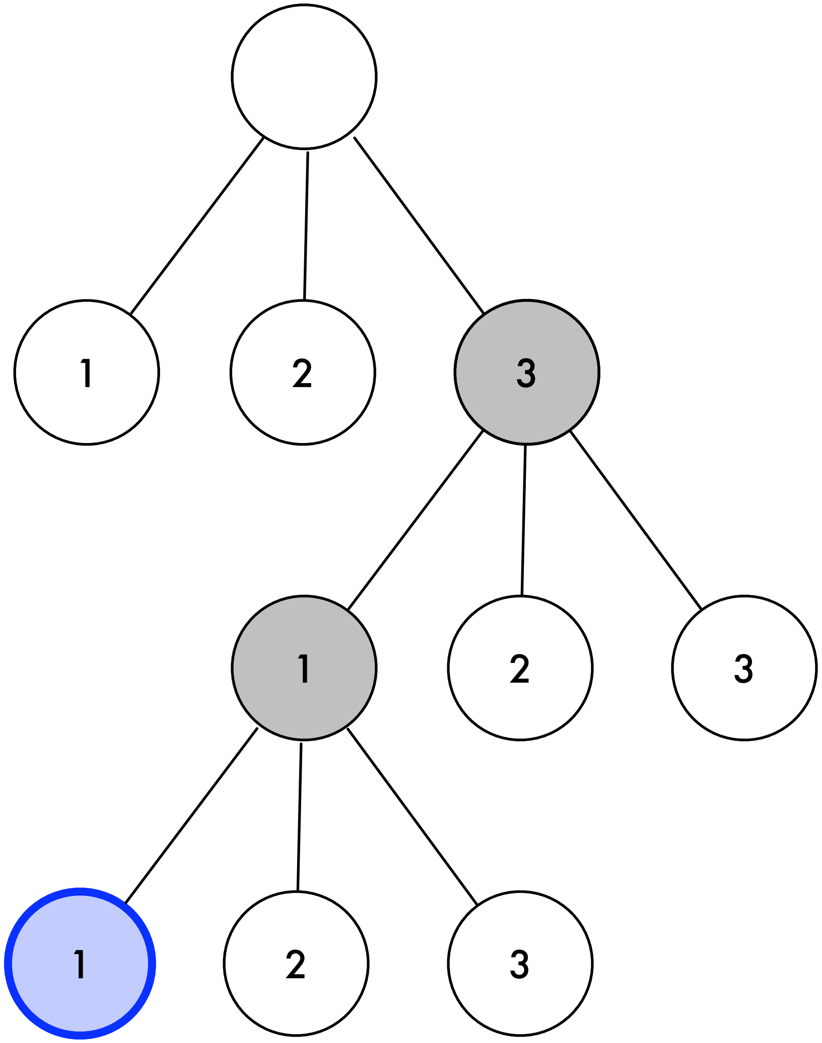


3 Identification and Authentication

3.1 Initial Registration

SDG version 1.5.1

Hierarchical Policy Structure: RFC 3647



3 Identification and Authentication

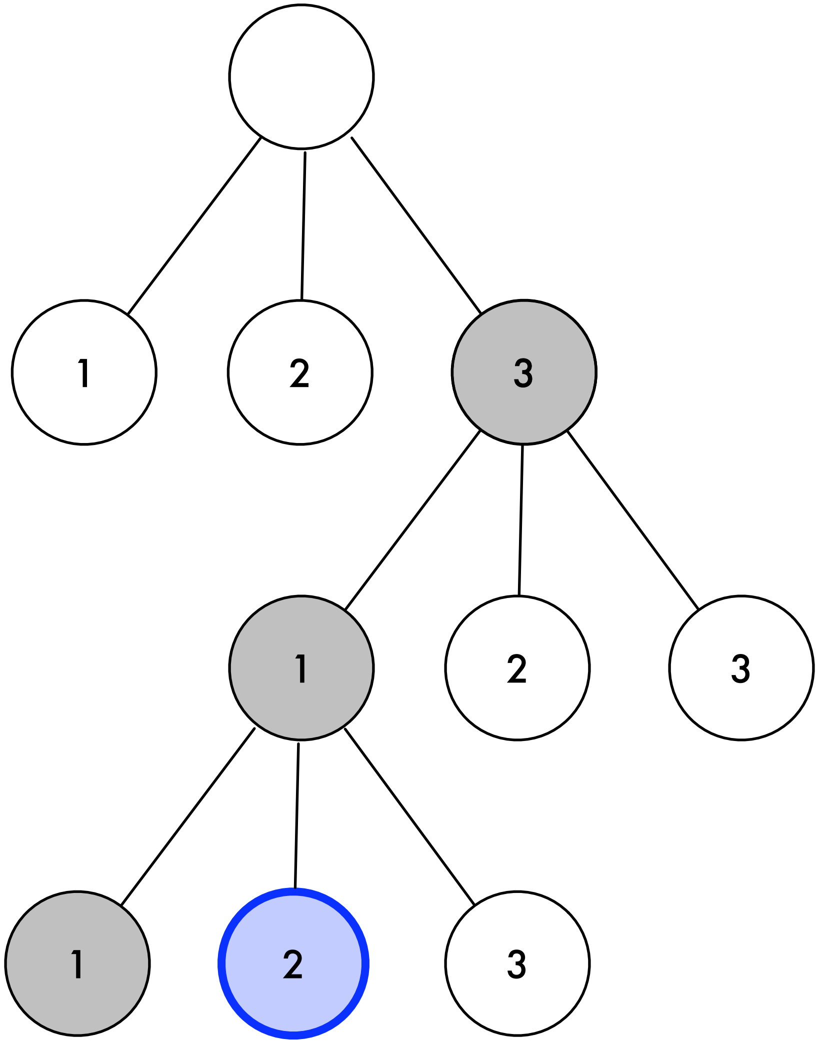
3.1 Initial Registration

3.1.1 Types of Names

The subject name is...

SDG version 1.5.1

Hierarchical Policy Structure: RFC 3647



3 Identification and Authentication

3.1 Initial Registration

3.1.1 Types of Names

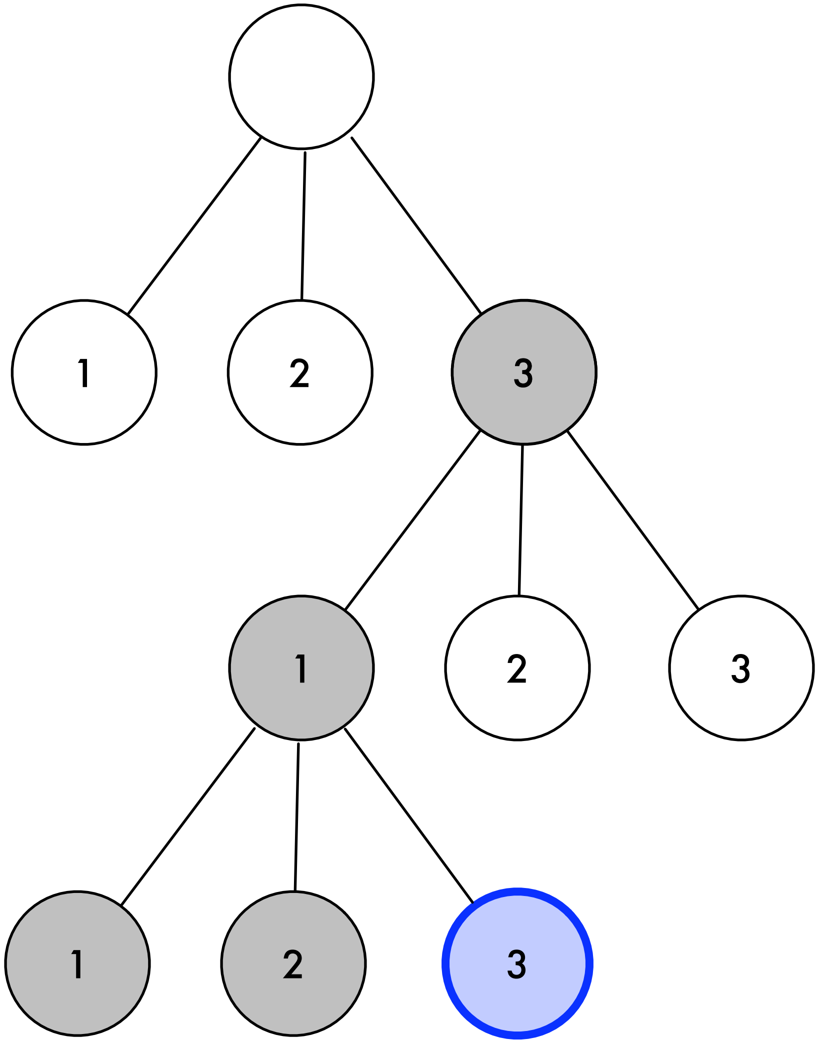
The subject name is...

3.1.2 Name Meanings

The subject name...

SDG version 1.5.1

Hierarchical Policy Structure: RFC 3647



3 Identification and Authentication

3.1 Initial Registration

3.1.1 Types of Names

The subject name is...

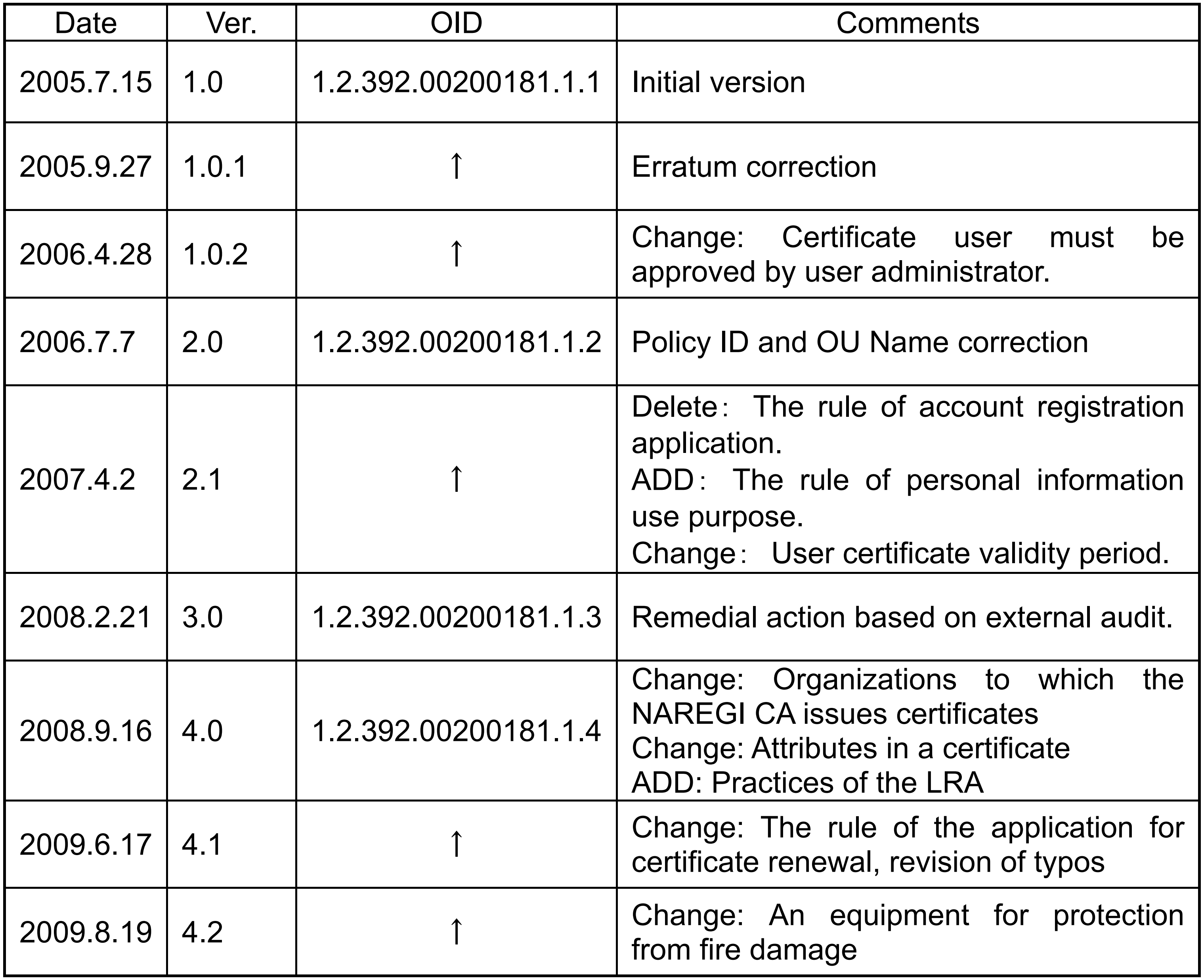
3.1.2 Name Meanings

The subject name...

3.1.3 Rules for Interpreting Name Forms

SDG version 1.5.1

Current Solution: Changelogs



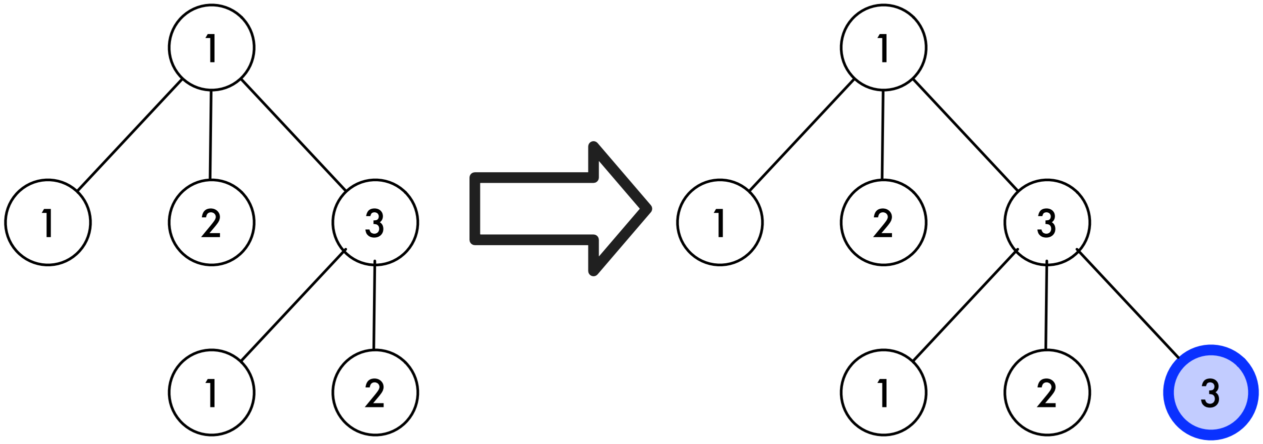
Date	Ver.	OID	Comments
2005.7.15	1.0	1.2.392.00200181.1.1	Initial version
2005.9.27	1.0.1	↑	Erratum correction
2006.4.28	1.0.2	↑	Change: Certificate user must be approved by user administrator.
2006.7.7	2.0	1.2.392.00200181.1.2	Policy ID and OU Name correction
2007.4.2	2.1	↑	Delete： The rule of account registration application. ADD： The rule of personal information use purpose. Change： User certificate validity period.
2008.2.21	3.0	1.2.392.00200181.1.3	Remedial action based on external audit.
2008.9.16	4.0	1.2.392.00200181.1.4	Change: Organizations to which the NAREGI CA issues certificates Change: Attributes in a certificate ADD: Practices of the LRA
2009.6.17	4.1	↑	Change: The rule of the application for certificate renewal, revision of typos
2009.8.19	4.2	↑	Change: An equipment for protection from fire damage

Current Solution: Changelogs

Date	Ver.	OID	Comments
2005.7.15	1.0	1.2.392.00200181.1.1	Initial version
2005.9.27	1.0.1	↑	Erratum correction
2006.4.28	1.0.2	↑	Change: Certificate user must be approved by user administrator.
2006.7.7	2.0	1.2.392.00200181.1.2	Policy ID and OU Name correction
2007.4.2	2.1		Delete： The rule of account registration application. ADD： The rule of personal information use purpose. Change： User certificate validity period.
2008.2.21	3.0	200181.1.3	Remedial action based on external audit.
2008.9.16	4.0	1.2.392.00200181.1.4	Change: Organizations to which the NAREGI CA issues certificates Change: Attributes in a certificate ADD: Practices of the LRA
2009.6.17	4.1	↑	Change: The rule of the application for certificate renewal, revision of typos
2009.8.19	4.2	↑	Change: An equipment for protection from fire damage

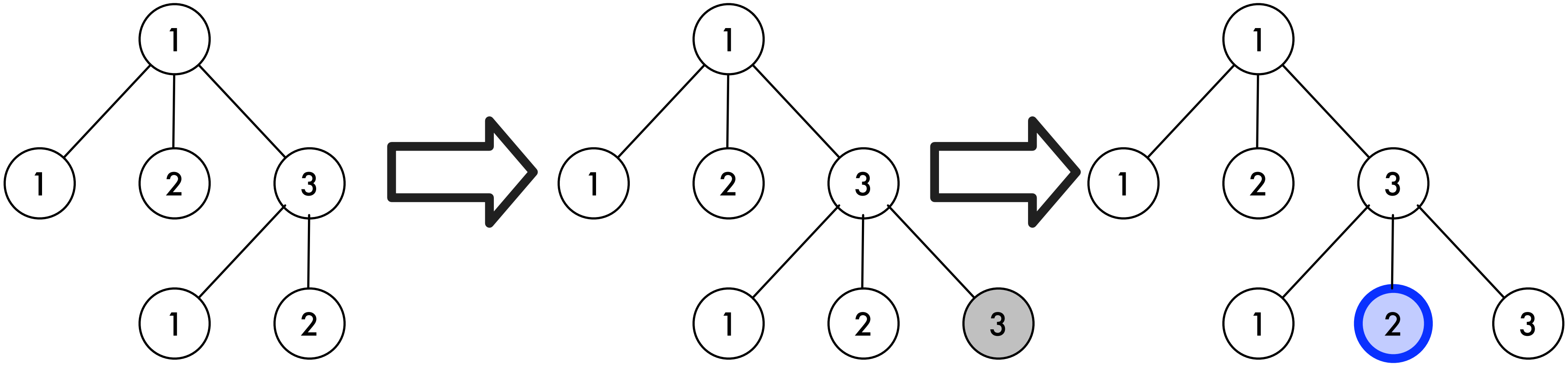
Delete
ADD
Change

Our Approach: Edit Distance



Tree Edit Distance = 1
"Added Section 1.3.3"

Our Approach: Edit Distance



Word Edit Distance > 0
"Added description to Section 1.3.2"

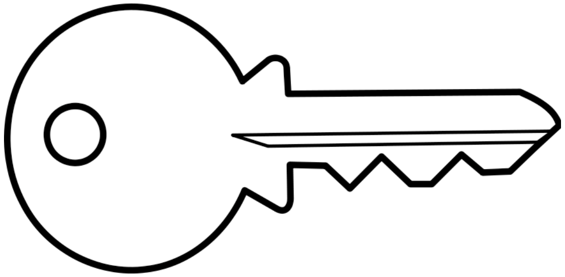
Initial Results

Reference	Description	wordED	treeED
SDG. 1_5_1:6.1.1	In Sec 6.1.1, added more description	12	0
AIST. 1_1:1.4.3	Added Section 1.4.3	21	1
IUCC. 1_5:4.6.1	Changed 4.6.1 to add logging of ...	0	0

Initial Results: Changelogs are Insufficient

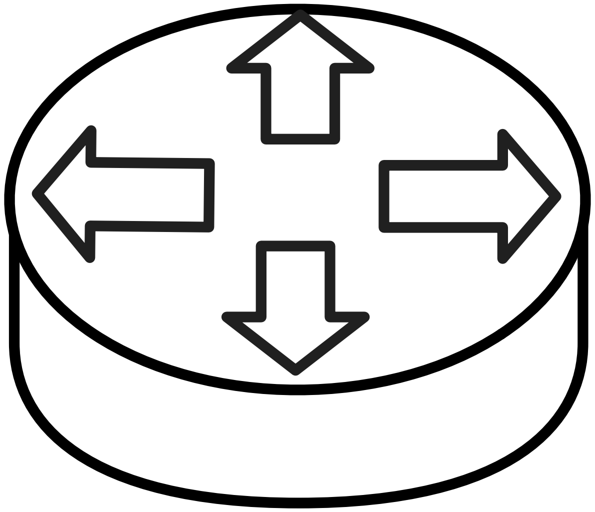
Reference	Description	wordED	treeED
SDG. 1_5_1:6.1.1	In Sec 6.1.1, added more description	12	0
AIST. 1_1:1.4.3	Added Section 1.4.3	21	1
IUCC. 1_5:4.6.1	Changed 4.6.1 to add logging of ...	0	0

Out of 178 reported changes,
9 never actually occurred!



Identity Management

Changelogs insufficient

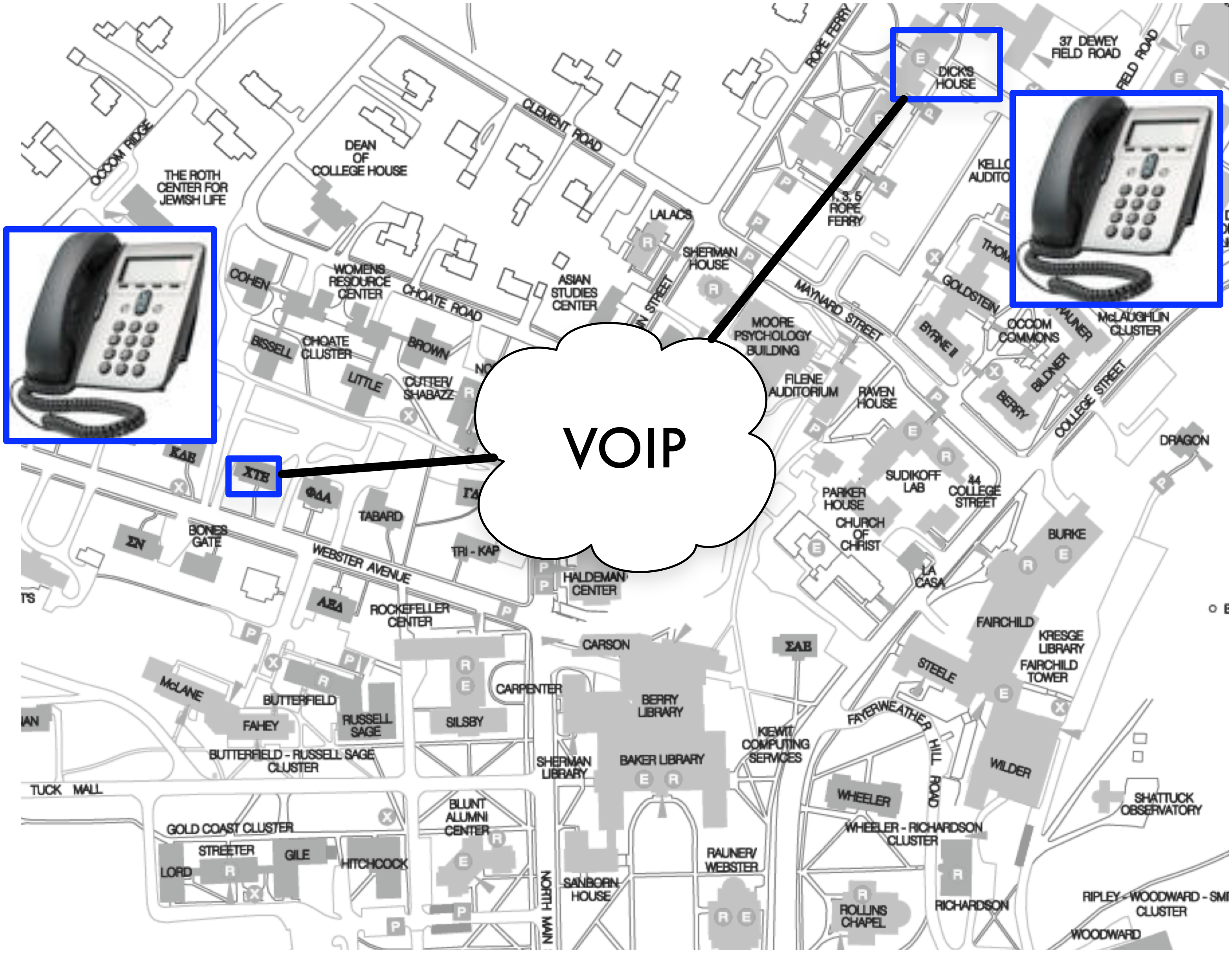


Switch/Router Configuration

Hierarchical Diffing

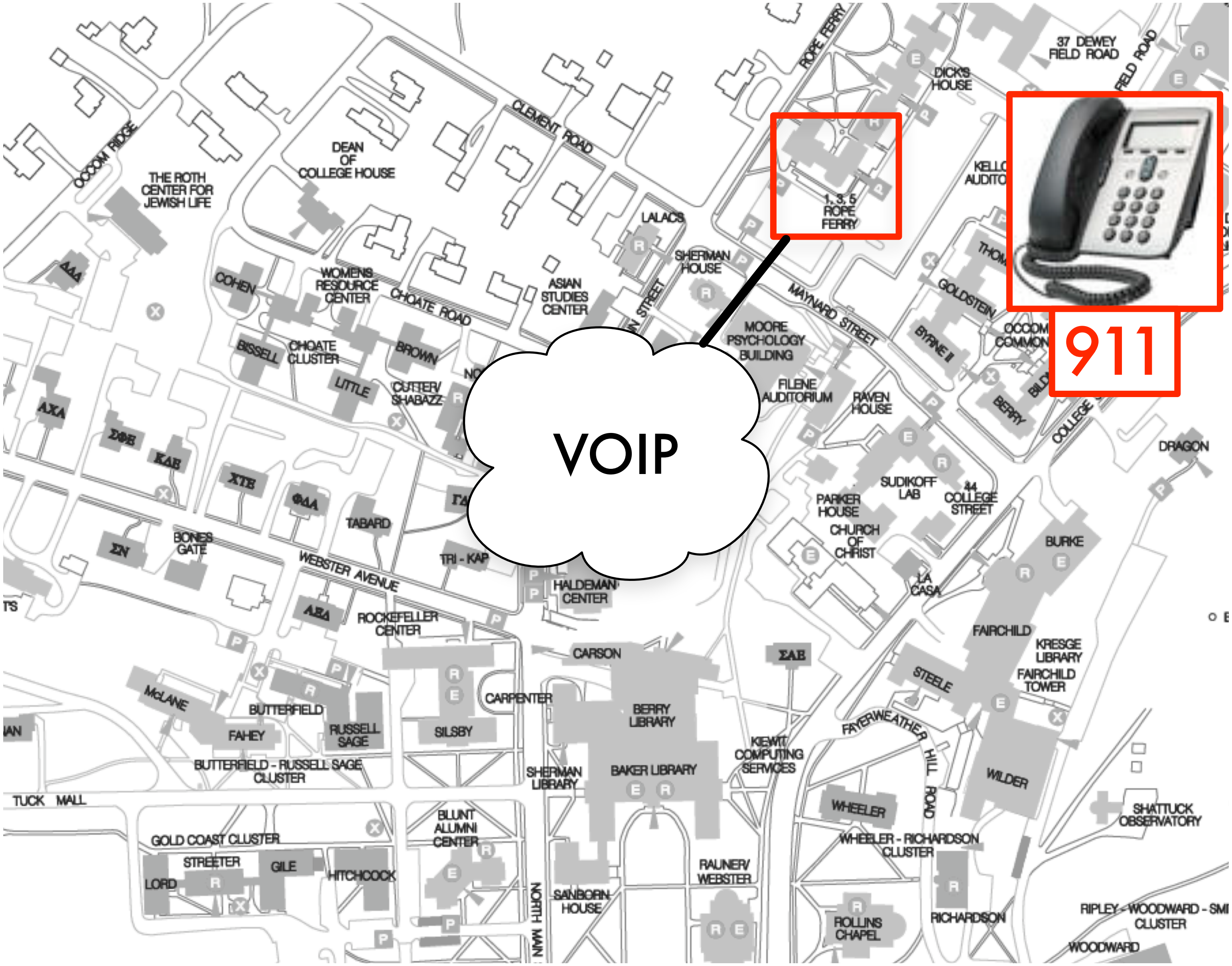
Change Querying

The Security Policy Evolution Problem

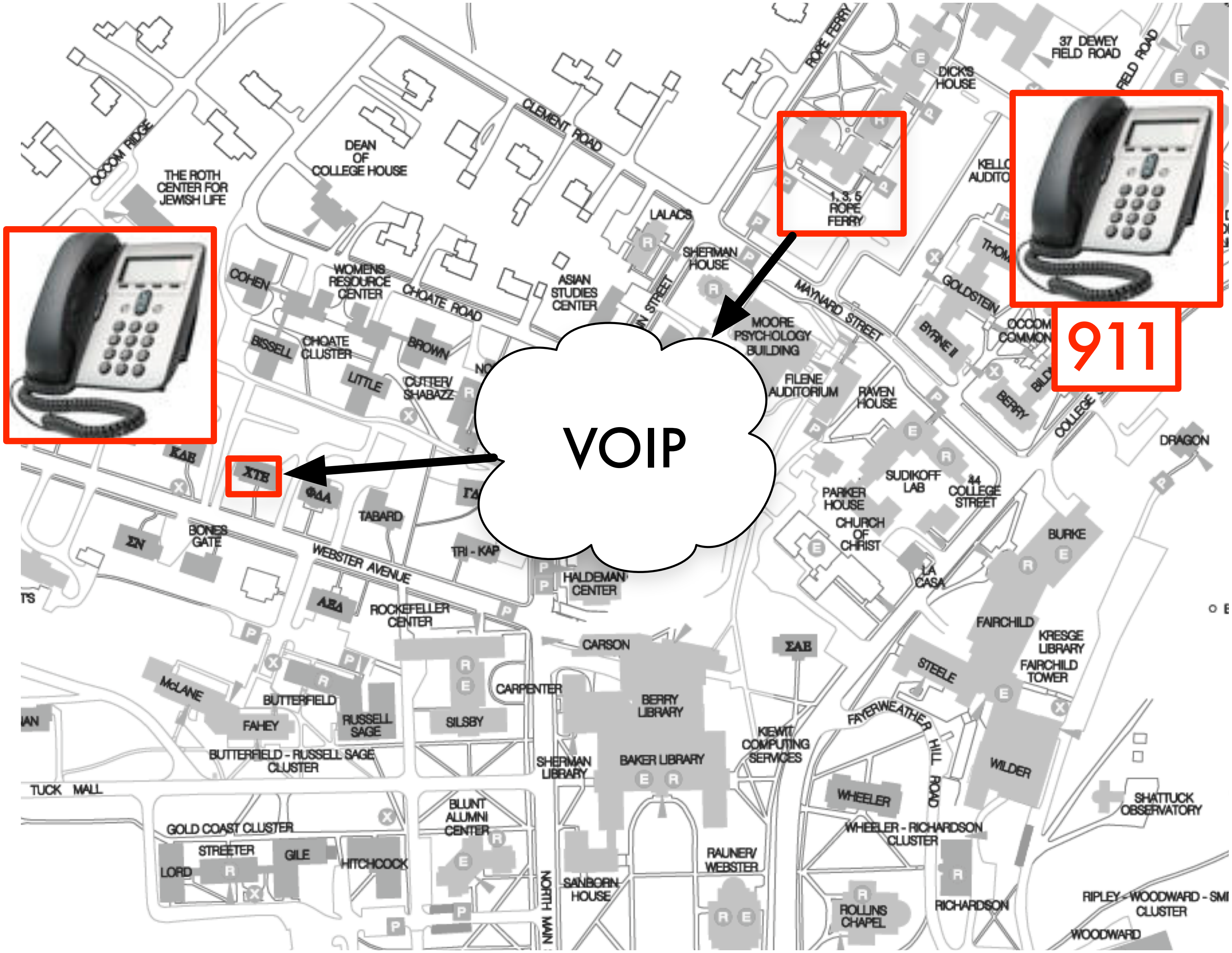


VOIP

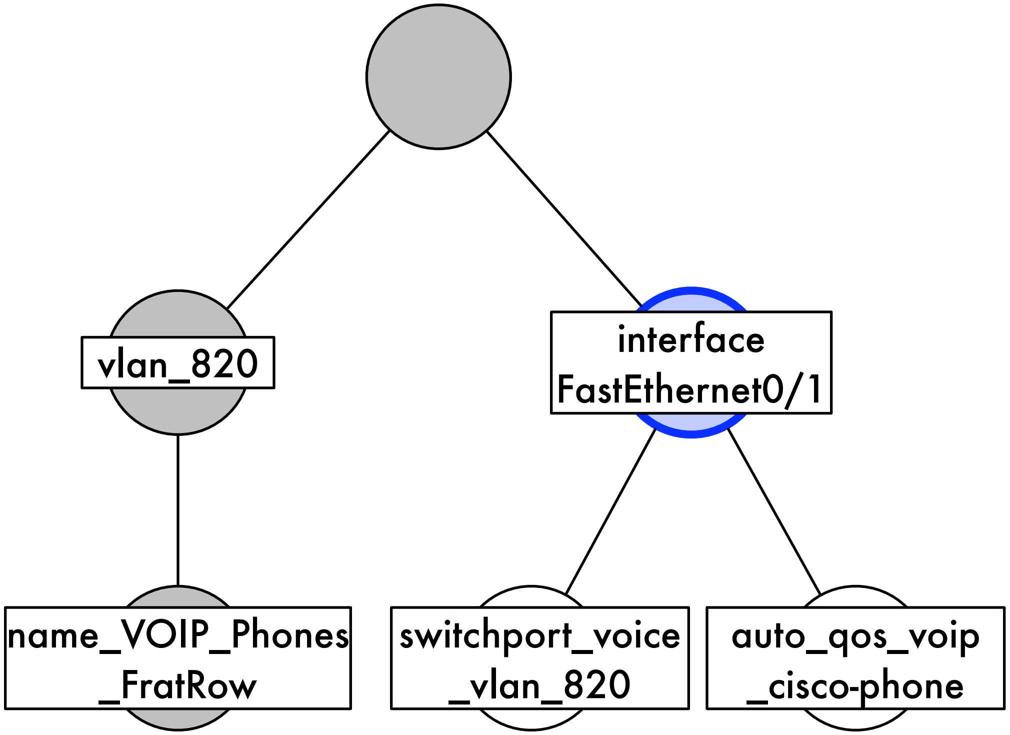
The Security Policy Evolution Problem



The Security Policy Evolution Problem



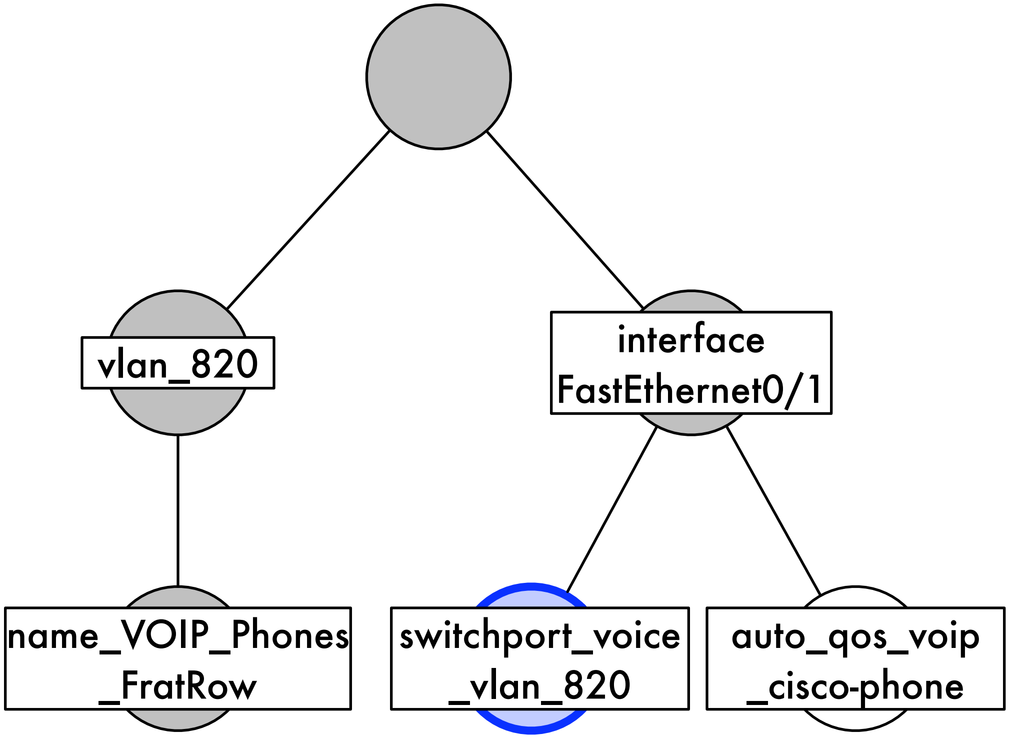
Hierarchical Policy Structure: Cisco IOS


vlan_820
interface FastEthernet0/1
name_VOIP_Phones _FratRow
switchport_voice _vlan_820
auto_qos_voip _cisco-phone

```
!
vlan 820
  name VOIP_Phones_FratRow
!
interface FastEthernet0/1
```

kappa-theta version 1.3

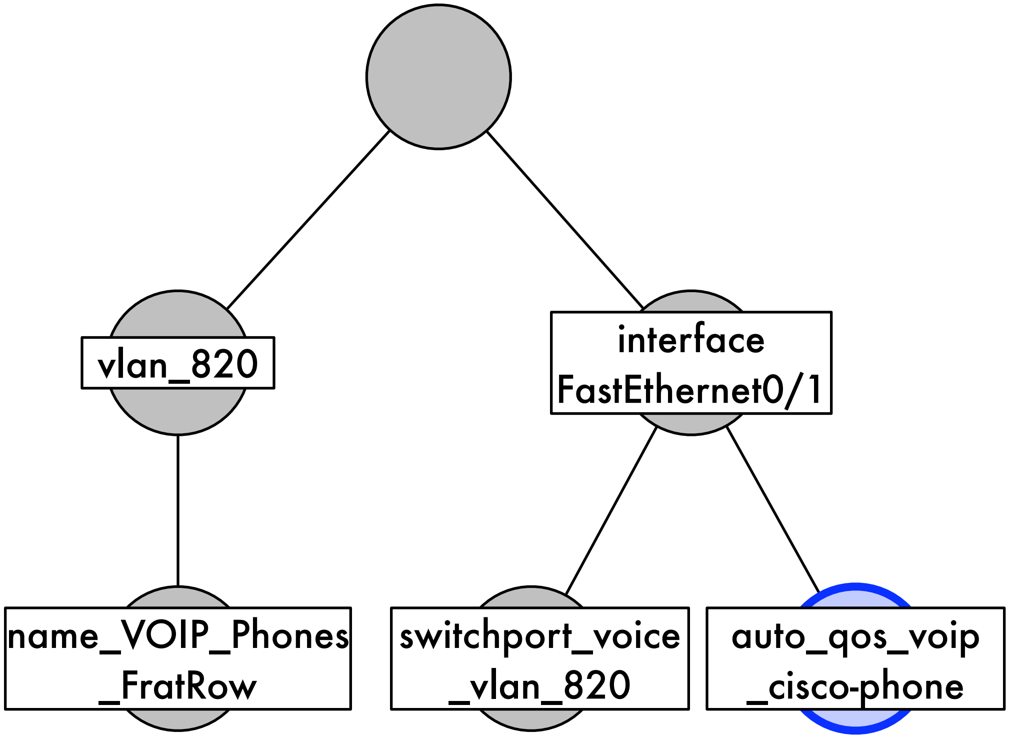
Hierarchical Policy Structure: Cisco IOS


vlan_820
interface FastEthernet0/1
name_VOIP_Phones _FratRow
switchport_voice _vlan_820
auto_qos_voip _cisco-phone

```
!
vlan 820
  name VOIP_Phones_FratRow
!
interface FastEthernet0/1
  switchport voice vlan 820
```

kappa-theta version 1.3

Hierarchical Policy Structure: Cisco IOS


vlan_820
interface FastEthernet0/1
name_VOIP_Phones _FratRow
switchport_voice _vlan_820
auto_qos_voip _cisco-phone

```
!
vlan 820
  name VOIP_Phones_FratRow
!
interface FastEthernet0/1
  switchport voice vlan 820
  auto qos voip cisco-phone
!
```

kappa-theta version 1.3

Current Practitioner Solution: Really Awesome New Cisco Config Differ (RANCID)

```
diff -u kappa-theta1.3 kappa-theta1.4
@@ -107,6 +109,13 @@
  switchport voice vlan 820
+ switchport port-security maximum 1 vlan voice
+ switchport port-security mac-address beef.feed.face vlan voice
  auto qos voip cisco-phone
```

Current Solutions Don't Leverage Hierarchical Structure of CiscoIOS

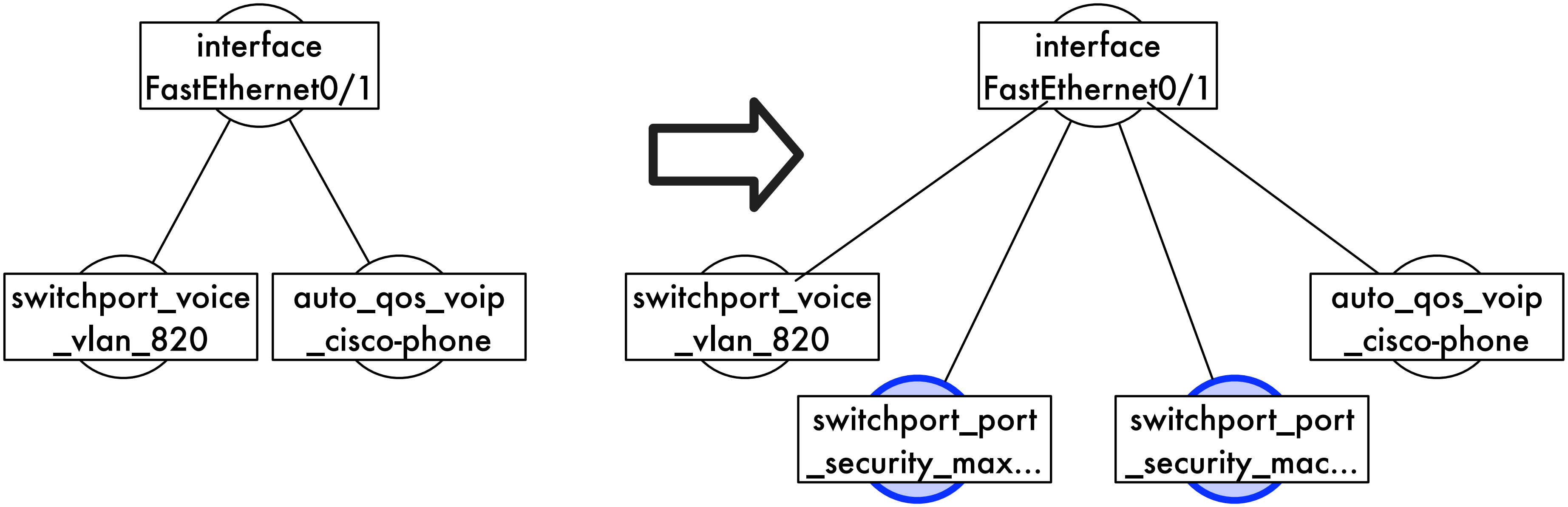
RANCID:

```
diff -u kappa-theta1.3 kappa-theta1.4
@@ -107,6 +109,13 @@
```

Plonka et al.: LOC, file counts, stanzas

Sung et al.: superblocks

Our Approach: Edit Distance


interface FastEthernet0/1
switchport_voice _vlan_820
auto_qos_voip _cisco-phone
interface FastEthernet0/1
switchport_voice _vlan_820
switchport_port _security_max...
switchport_port _security_mac...
auto_qos_voip _cisco-phone

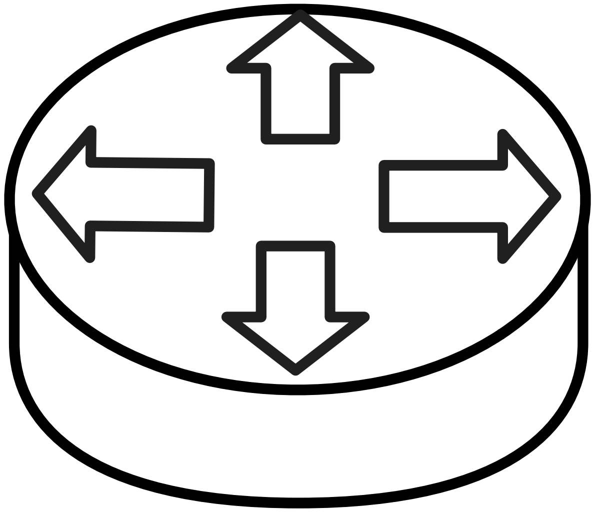
Tree Edit Distance = 2

Initial Results

Reference	Total treeED	Hits
/root/interface*	1542	80
global	304	278
/root/vlan*	28	25
/root/ip*	18	18
/root/logging*	0	0
/root/bridge*	0	0

Hierarchical Querying

Reference	Total treeED	Hits
/root/interface*	1542/628	80/628
/root/interface*/switchport*	247	247
/root/interface_FastEthernet0_8 /switchport*	17	17
/root/interface_FastEthernet0_8 /switchport_voice*	2	2

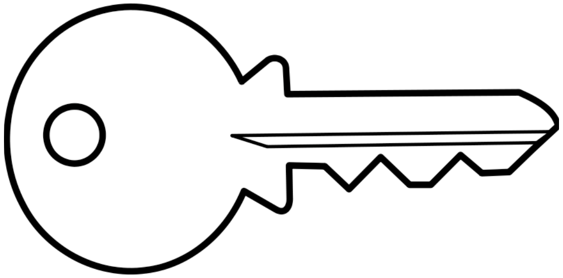


Switch/Router Configuration

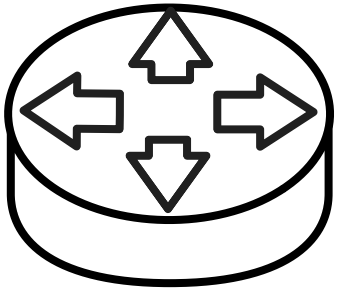
Hierarchical Diffing
Change Querying

Outline

Two real-world examples



Identity Management



Switch/Router Configuration

Conclude

1 Security policies must be changed and synchronized in order to maintain security.

2 We can model many of policies as hierarchically-structured texts.

3 We propose a unified methodology to detect and manage change.

Thank You!
Questions?

Gabriel A. Weaver
gabriel.a.weaver@dartmouth.edu

IGTF Data: http://pkipolicy.appspot.com/