PRI: Privacy Preserving Inspection of Encrypted Network Traffic

Liron Schiff Stefan Schmid

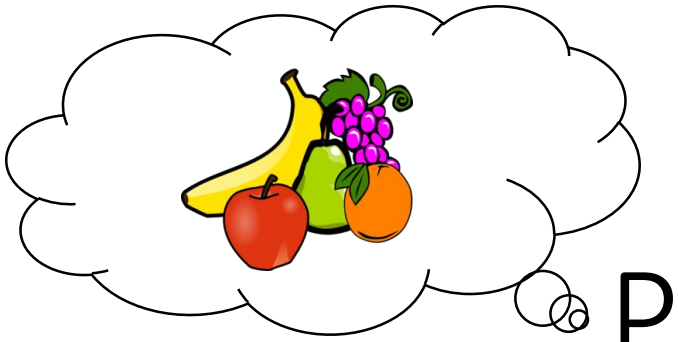
Tel Aviv Uni, IL Aalborg Uni, DK

PRI: Privacy Preserving Inspection of Encrypted Network Traffic

on Schiff Stefan Schmid

viv Uni, IL Aalborg Uni, DK

A contradiction already in the title? Insider threat detection is hard: privacy-preserving even harder?? Or legal???



PRI: Privacy Preserving Inspection of Encrypted Network Traffic

Liron Schiff Stefan Schmid

Tel Aviv Uni, IL Aalborg Uni, DK

The Broader Context: Decoupling Trust in Network Security

- Computer networks: **critical infrastructure**
  - Enterprise, datacenter, transport network
- Problem: Users need to trust many „roles“…
  - The sysadmin
  - The network operator / ISP
  - The infrastructure provider (e.g., optical splicing)
  - The hardware / vendor
- … as soon as the packet leaves the network card

The Broader Context: Decoupling Trust in Network Security

- Computer networks: **critical infrastructure**
  - Enterprise, datacenter, transport network
- Prob ny „roles“…
  - The sysadmin
  - The network operator / ISP
  - The infrastructure provider (e.g., optical splicing)
  - The hardware / vendor
- … as soon as the packet leaves the network card

Our approach: identify, decouple, isolate roles (often with focus on SDN).

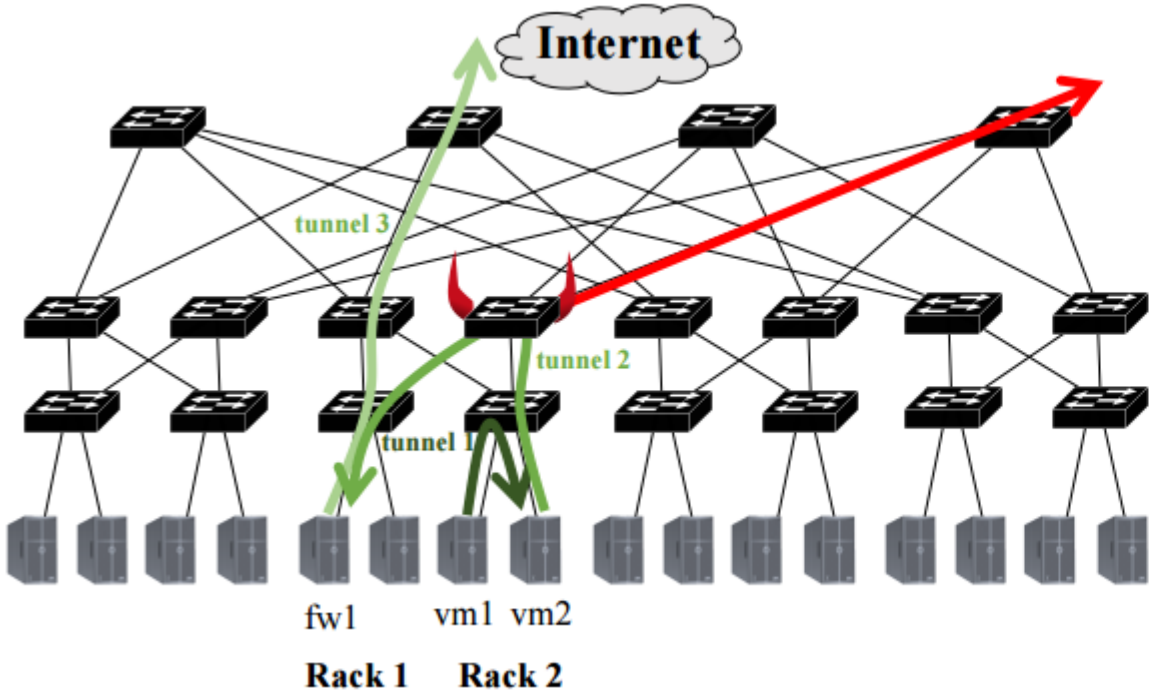
We are asking: Is it possible to reduce trust…

- … in infrastructure, hardware, vendor?
- … in operator and software (e.g., ISP, SDN controller)?
- … in administrator?

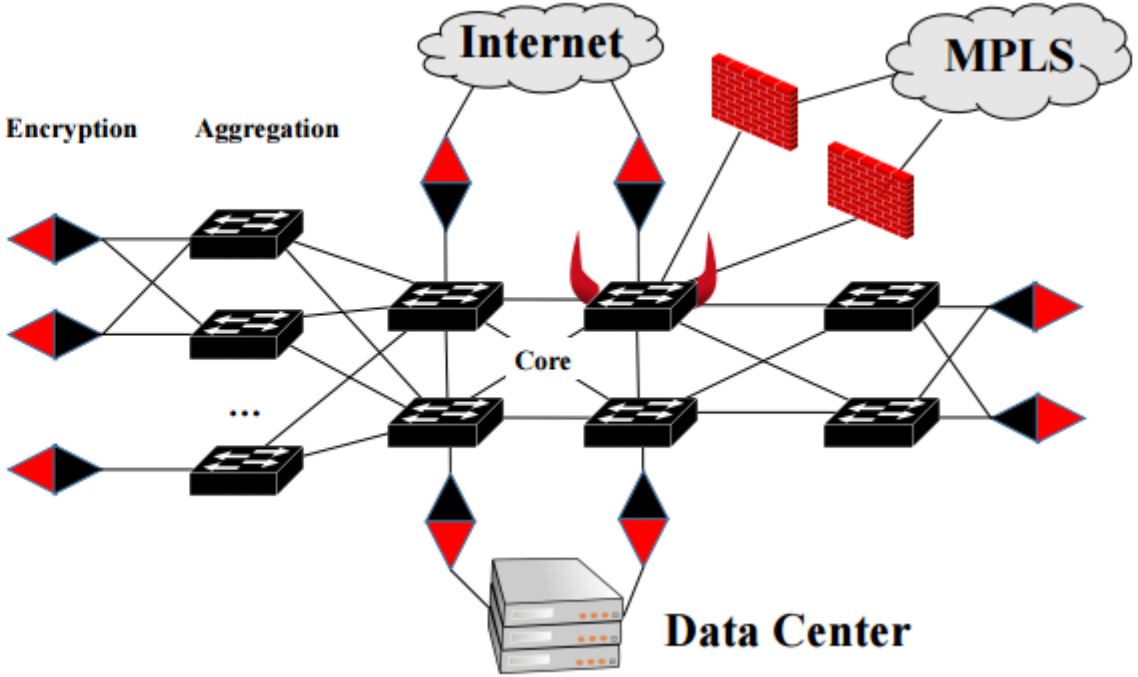
Example 1: Untrusted Routing Infrastructure

- An actual **problem**: hardware backdoors, hacked routers, hardware dealt with underground, …
- E.g., government networks: cannot afford manufacturing trusted hardware
- Possible vulnerabilities: Malicious routers may mirror and exfiltrate traffic, generate new flows, modify flows
- No easy solution: Sampling, Traceroute, etc.: fails in the presence of malicious routers

Exploits 1: Untrusted Routing Infrastructure



Exfiltration

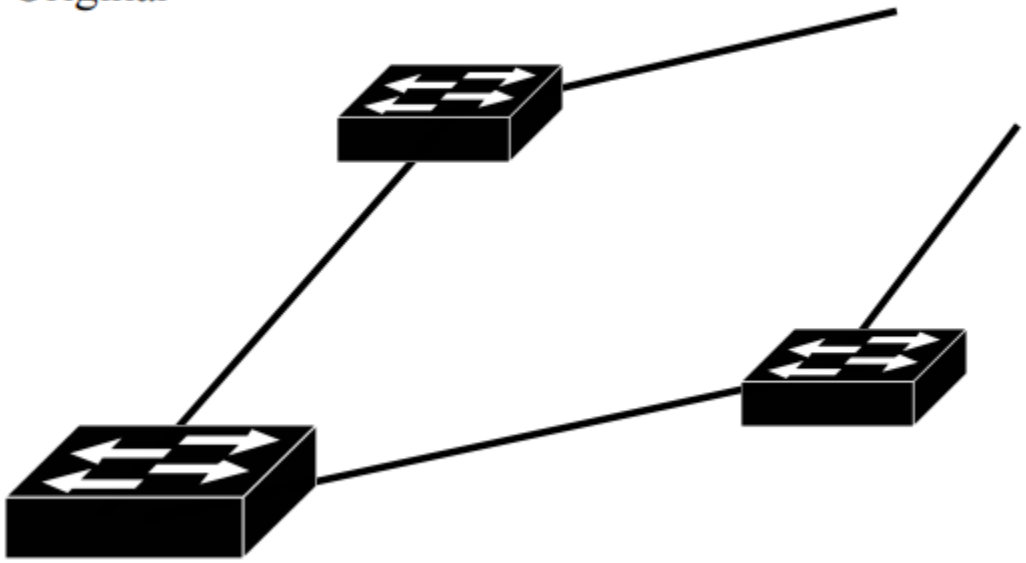


DoS

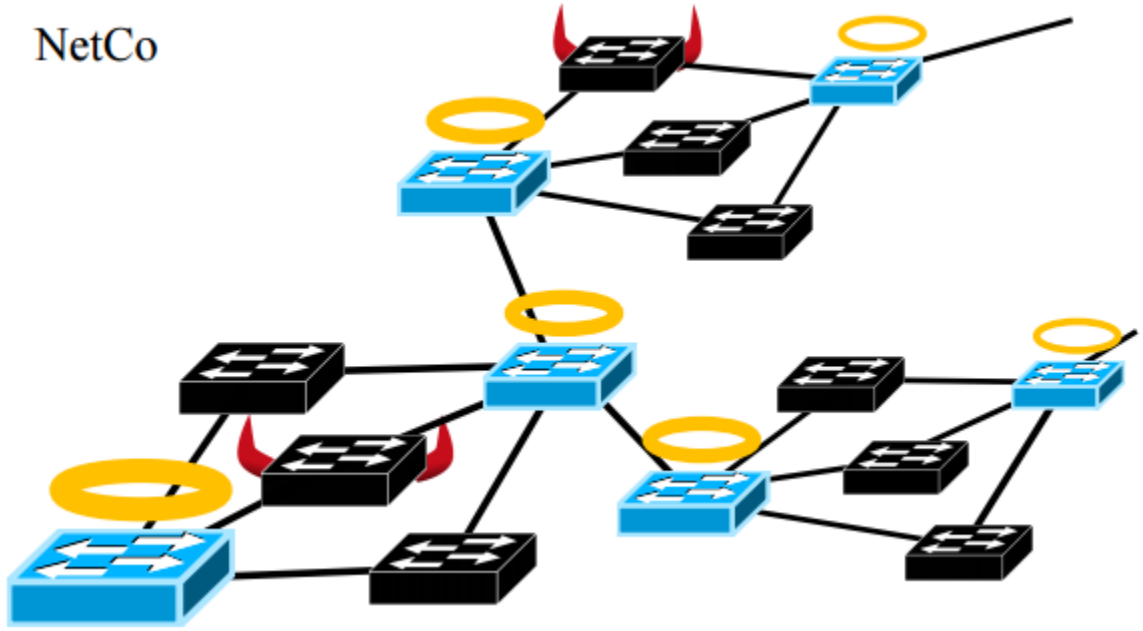
Idea: Leverage Hardware Heterogeneity

NetCo: „Robust Combiner“ for Networks

Original



NetCo



[NetCo: Reliable Routing With Unreliable Routers]
Anja Feldmann et al.IEEE/IFIP DSN Workshop on Dependability Issues on SDN and NFV (**DISN**), Toulouse, France, June 2016.

Problem 2: Untrusted Operator

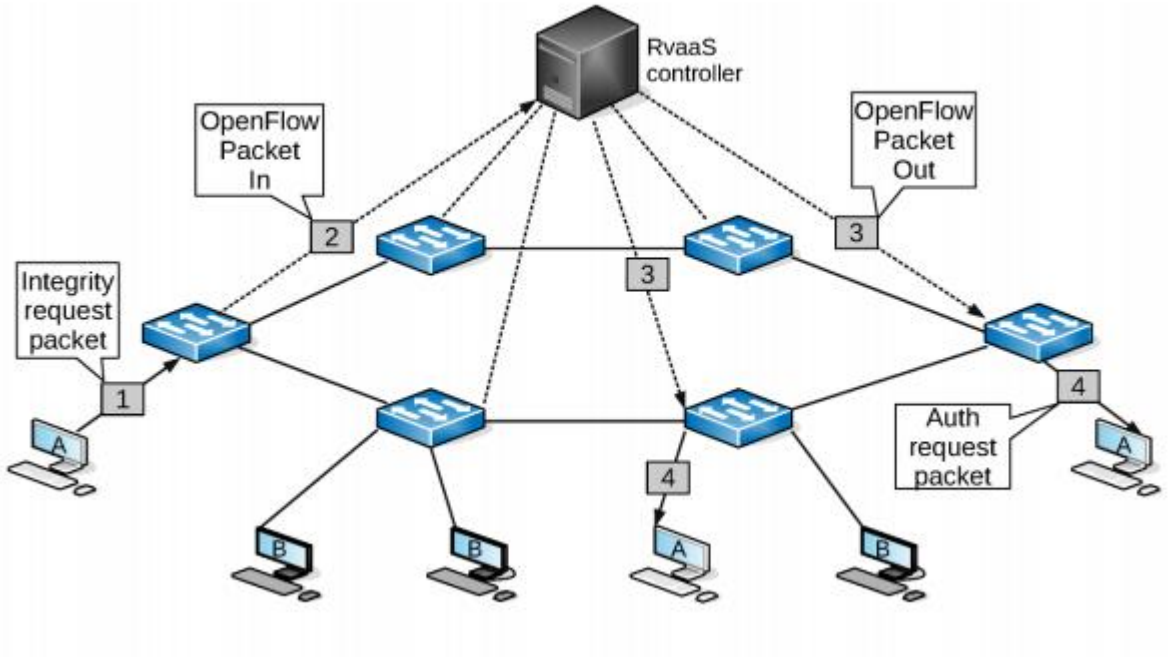
- Decouple operator role: Problem even with trusted infrastructure
  - Hacked operator…
  - … or SDN controller under **cyber attack**
  - **…** may simply **install rules to exfiltrate** / mirror traffic
- How can clients and users verify that the routes installed for them are correct?
  - E.g., „set of end points reached from packets leaving my network card?“
  - E.g., „countries visited by packets leaving network card?“
  - E.g., „are bandwidth sharing rules max-min-fair?“
- Traceroute cumbersome
  - Too many possibilities (all possible headers?)
  - Malicious endpoints will not respond
  - Configuration rules preventing a response
  - etc.

RVaaS: Routing-Verification-as-a-Service

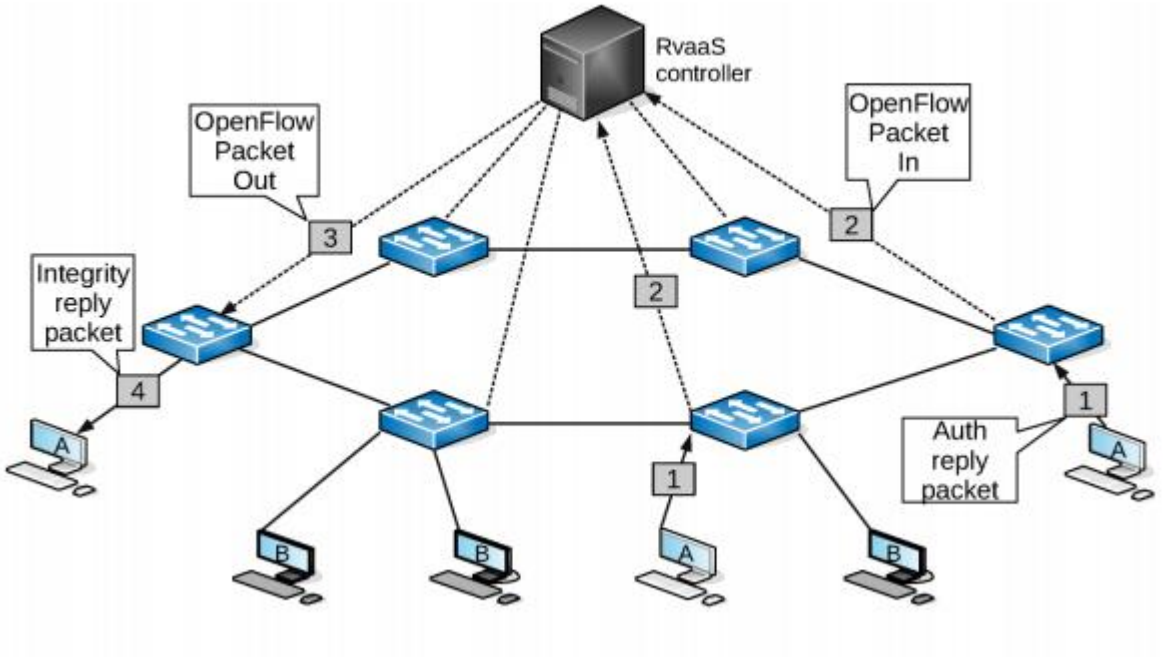
- Idea: In SDN, possible to **offer an „independent“ query API**
  - Add 2nd controller (on secure server) with reliable channels to switches
  - Can maintain view of network configuration…
  - … by subscribing to OpenFlow switch events
  - Receives all packet-in and FlowMod commands!

- SDN controller performs logical and physical checks
  - Logical check for internal config: E.g., Header Space Analysis / NetKAT
  - Physical for attachment points: Who is really behind this port? (PacketOuts and **authenticated response** by actual endpoints)

RVaaS: Routing-Verification-as-a-Service



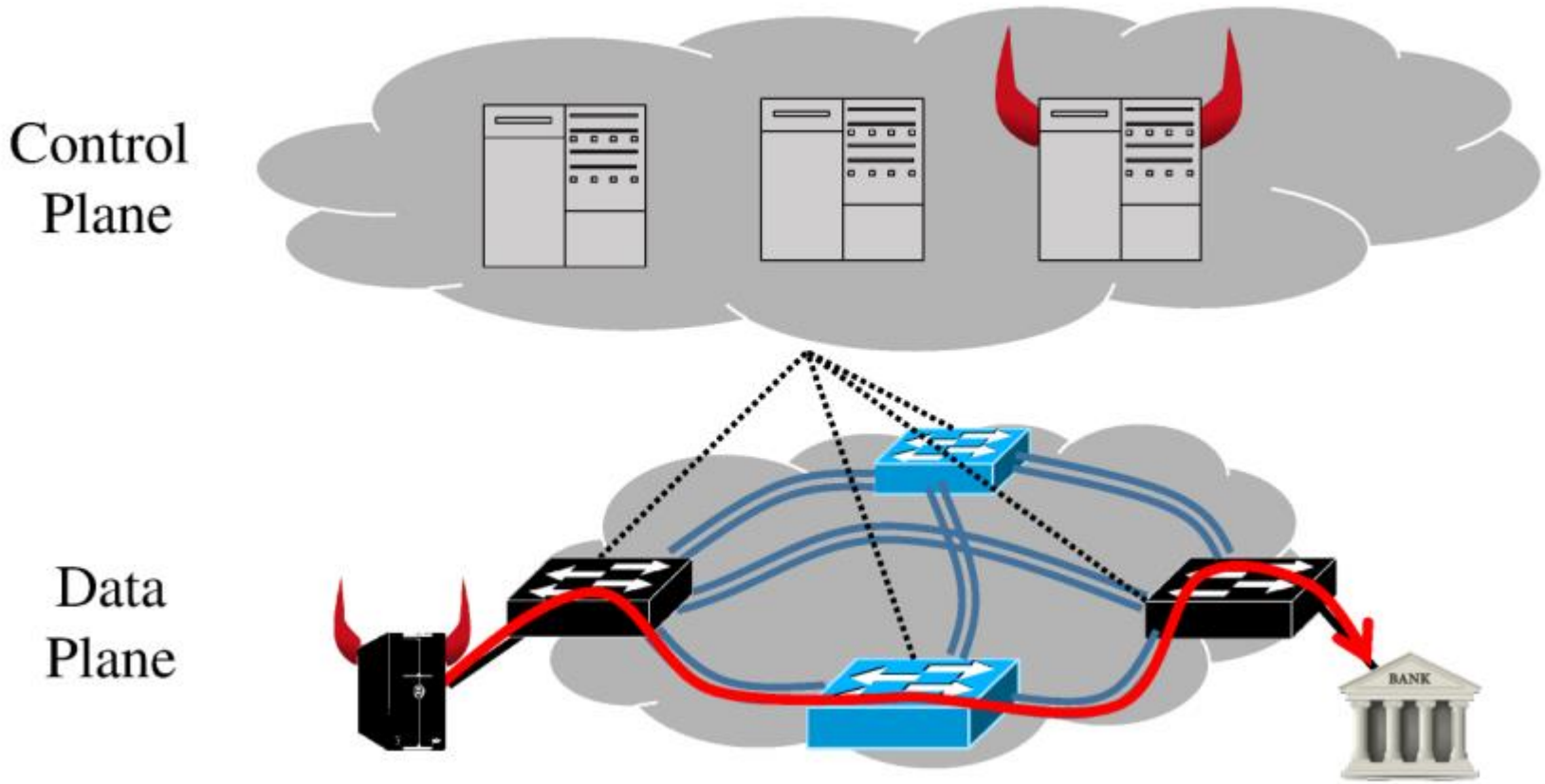
Client makes **integrity request** to RVaaS controller. RVaaS analyzes the request and then dispatches Auth request packets to relevant clients (PacketOut).



Relevant clients send Auth reply packets back to RVaaS. RVaaS collects replies and sends them back to the requesting client.

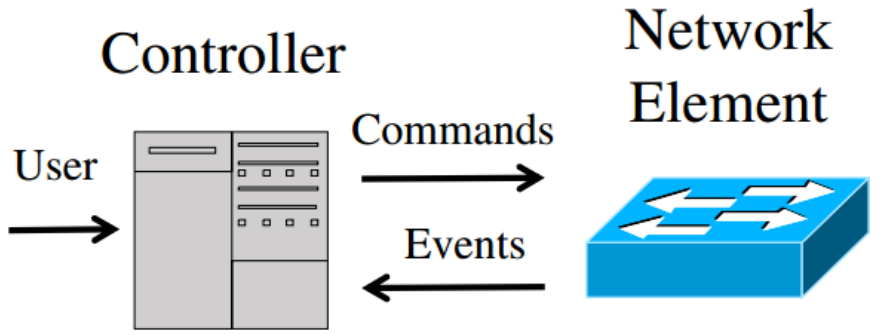
Routing-Verification-as-a-Service (RVaaS): Trustworthy Routing Despite Insecure Providers
Liron Schiff, Kashyap Thimmaraju, and Stefan Schmid.
IEEE/IFIP DSN Workshop on Dependability Issues on SDN and NFV (**DISN**), Toulouse, France, June 2016.

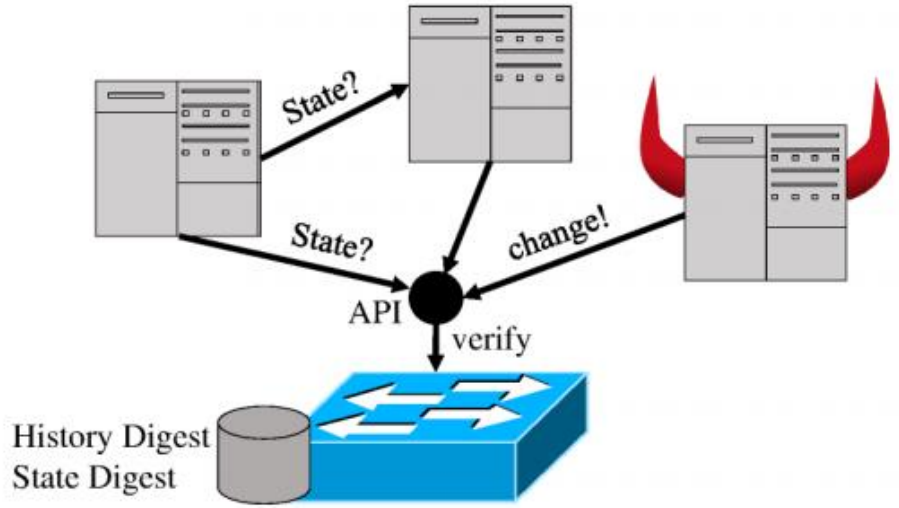
The Malicious Administrator Problem



The Malicious Administrator Problem

- Introduced by Perrig et al.: *Fleet* relies on signed commands and threshold crypto objects (majority)
- However, suffers from late or incomplete information, as well as replay attacks
- Our solution: Need history and state!





Study the past if you would define the future: Implementing Secure Multi-Party SDN Updates
Liron Schiff and Stefan Schmid.
IEEE International Conference on Software Science, Technology and Engineering (**SwSTE**), June 2016..

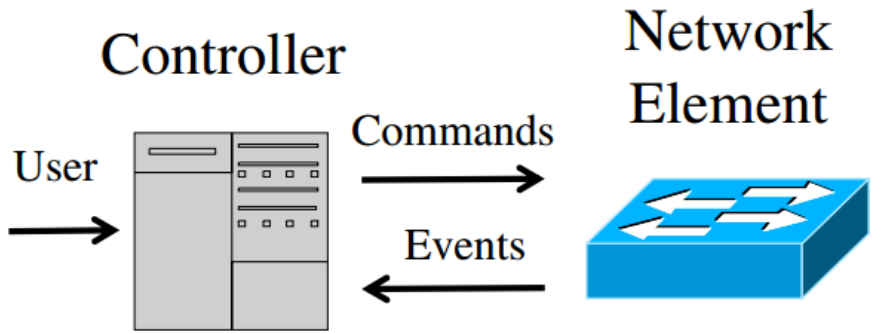
The Malicious Administrator Problem

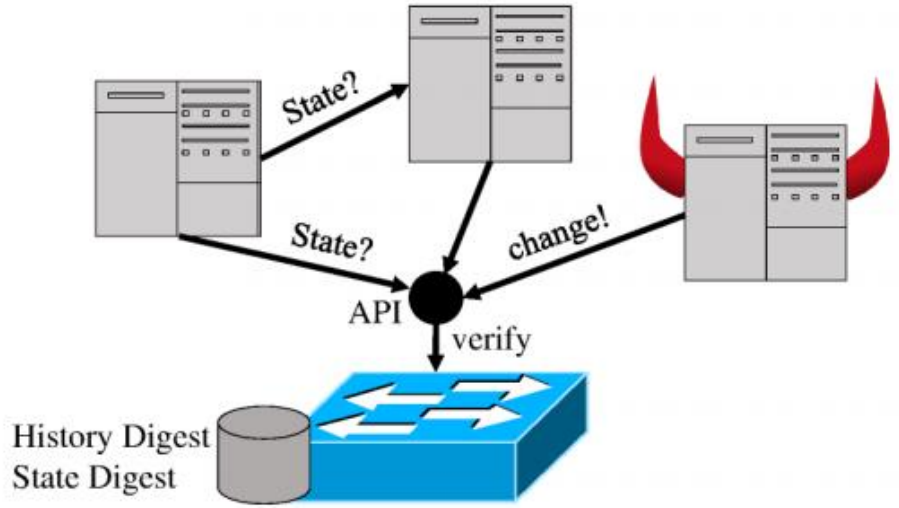
- Introduced by Perrig et
  Fleet
  com
  cryp

This talk: also motivated by untrustworthy administrator, but with focus on privacy (spying administrator)

- However, suffers from late or incomplete information, as well as replay attacks

- Our solution: Need history and state!



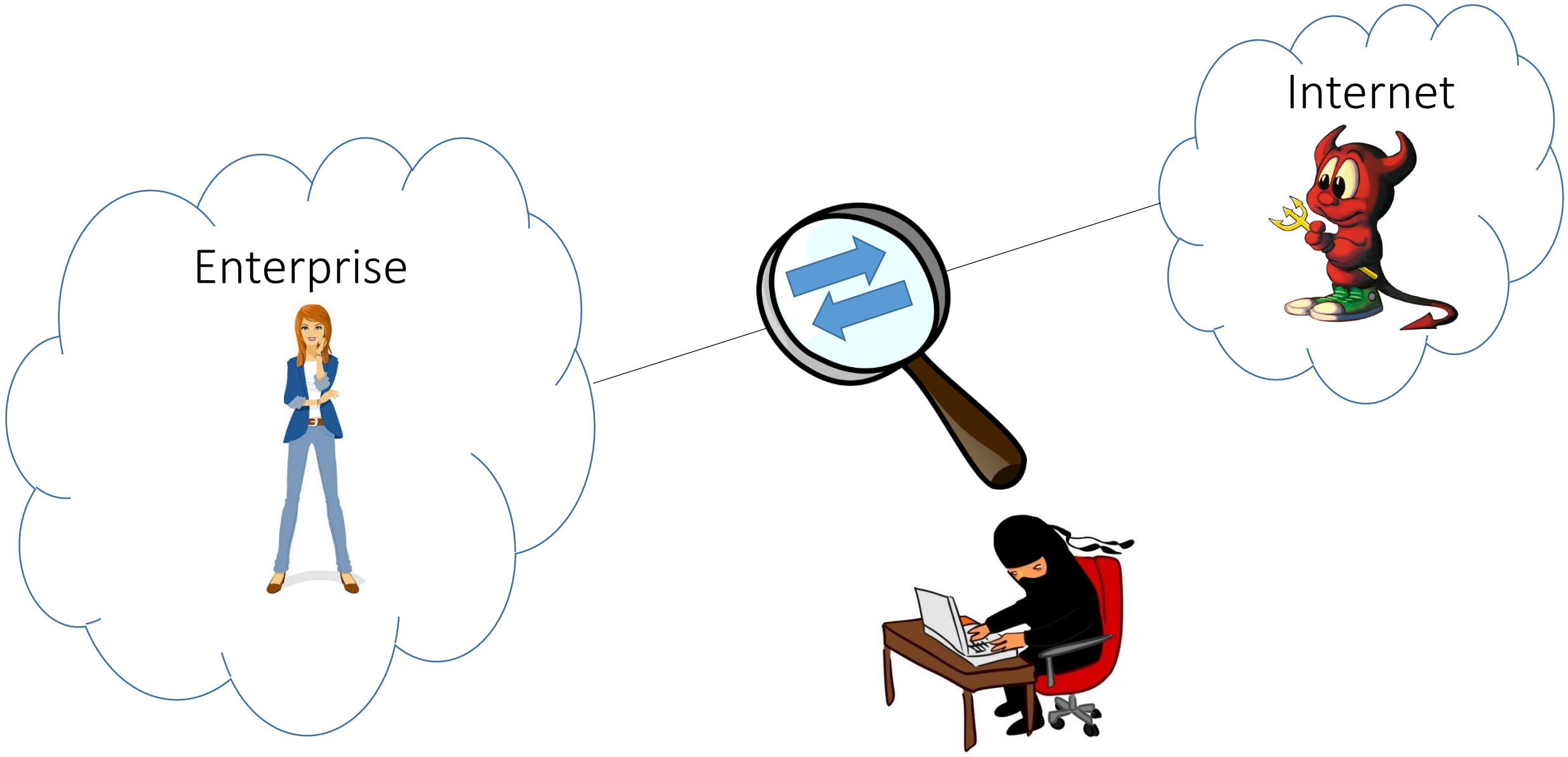


Study the past if you would define the future: Implementing Secure Multi-Party SDN Updates
Liron Schiff and Stefan Schmid.
IEEE International Conference on Software Science, Technology and Engineering (**SwSTE**), June 2016..

Traffic Inspection vs Privacy

- Traffic inspection: vital component of many security solutions (including IDS/IPS systems)
- ***Outbound:*** e.g., prevent exfiltration / leak of confidential insider information, search for watermarks
- ***Inbound:*** e.g., block malicious traffic before entering, parental filtering

Setup for now: Enterprise



Setup for now: E

Attacker: «Let's introduce malicious code, then perform cyber-attack!»

Employee: «I want perforamnce, security but also privacy! And maybe exfiltrate some confidential insider infos...»

Sysadmin: «Provide security and availability! But how?! Also, want to spy a bit on the employees…»

Internet

Enterprise

Conflicting Goals?

Employees want their traffic to be confidential (at least the uncritial parts)!

vs

Sysadmin wants to detect threats

Solution today favors admin…

Proxy = Man-in-the-Middle

Enterprise

Internet

Solution today favors admin…

As we will see, employee is not the only role which may have privacy concerns with this architecture!

roxy = Man-in-the-Middle

Enterprise

Internet

Alternatives?

- **Homomorphic encryption:** A general solution to process confidential information. But how to apply here? And what about efficiency?

- **BlindBox** (SIGCOMM 2015): Network function over encrypted traffic, but limited to exact match and overhead (tokenization)

- **PRI**: this paper

PRI: Supported Roles

- **Administrators**
  - Goal: ensure availability and security, detect insider threats
  - Prevent leakage of sensitive insider information
  - Prevent malicious traffic from outside
  - In addition to up-to-date security rules (maybe outsourced), add organization-specific Data Leak Prevention (DLP) rules
- **Employees/Users**
  - Wants high communication performance
  - Profits from a secure environment
  - Desires privacy

PRI: Supported Roles

- **Administrators**
  - Goal: ensure availability and security, detect insider threats
  - Prevent leakage of sensitive insider information
  - Prevent malicious traffic from outside
  - In addition to up-to-date security rules (maybe outsourced), add organization-specific Data Leak Prevention (DLP) rules

- **Employees/Users**
  - Wants high communication performance
  - Profits from a secure environment
  - Desires privacy

- **Rules Provider**
  - Specialized into high-quality configurations
  - Configuration for a traffic inspection system
  - Wants its rule to **stay confidential**! (for **effectiveness and profit**…)

PRI: Supported Roles

- **Administrators**
  - Goal: ensure availability and security, detect insider threats
  - Prevent leakage of sensitive insider information
  - Prevent malicious traffic from outside
  - In addition to up-to-date security rules (maybe outsourced), add organization-specific Data Leak Prevention (DLP) rules

→ **Effective inspection**

- **Employees/Users**
  - Wants high communication performance
  - Profits from a secure environment
  - Desires privacy

→ **Privacy-Preserving Inspection**

- **Rules Provider**
  - Specialized into high-quality configurations
  - Configuration for a traffic inspection system
  - Wants its rule to stay confidential! (for effectiveness and profit…)

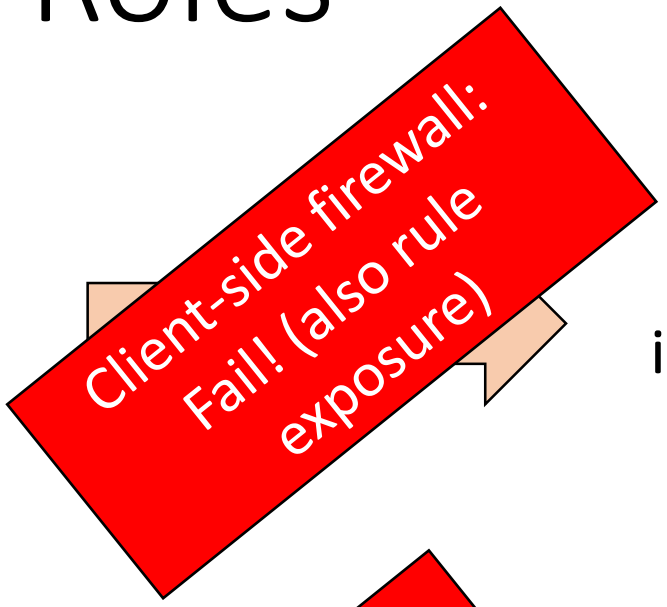
→ **Confidentiality of Rules**

PRI: Supported Roles

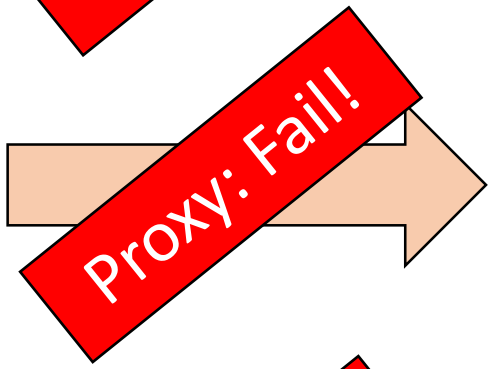
- **Administrators**
  - Goal: ensure availability and security, detect insider threats
  - Prevent leakage of sensitive insider information
  - Prevent malicious traffic from outside
  - In addition to up-to-date security rules (maybe outsourced), add organization-specific Data Leak Prevention (DLP) rules

- **Employees/Users**
  - Wants high communication performance
  - Profits from a secure environment
  - Desires privacy

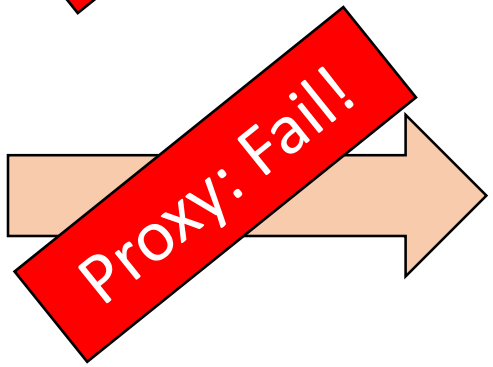
- **Rules Provider**
  - Specialized into high-quality configurations
  - Configuration for a traffic inspection system
  - Wants its rule to stay confidential! (for effectiveness and profit…)



Effective inspection



Privacy-Preserving Inspection



Confidentiality of Rules

PRI: Based on Trusted Hardware

- Trusted hardware: much attention e.g., for cloud computing, less for computer networks
- Intel SGX (as well as AMD equivalence) offers CPU instructions to applications to **manage private regions of code and data**: Application runs in **enclave**
- Before being built, enclave code and data is free for inspection and analysis
- Application can **prove its identity** to a remote party (**attestation**)
- Application can also request an **enclave-specific key** that it can use to protect keys and data that it wishes to store outside the enclave

PRI: Based on Trusted Hardware

- Trusted hardware: much attention e.g., for cloud computing, less for computer networks
- Intel SGX (
  manage pr
- Before bei
- Application can **prove its identity** to a remote party (**attestation**)
- Application can also request an **enclave-specific key** that it can use to protect keys and data that it wishes to store outside the enclave

Interesting technology for secure and efficient cloud computing.
But what about computer networks? A topic with potential: #routers = #middleobxes (DPI, proxy, cache, NAT, WAN optimizer, …)!

PRI: Based on Trusted Hardware

- Trusted hardware: much attention e.g., for cloud computing, less for computer networks
- Intel SGX (
  manage pr
- Before bei
- keys and data that it wishes to store outside the enclave

Interesting technology for secure and efficient cloud computing.
But what about computer networks? A topic with potential: #routers = #middleobxes (DPI, proxy, cache, NAT, WAN optimizer, …)!

Importance of security for middleboxes further increases as they are outsourced to third parties (clouds, ISPs, NFV providers), in context of Network Function Virtualization: losing control to less trustworthy domains

PRI: Deoupling with trusted hardware

configure

Internet

Enterprise

confirm fairness

PRI

add DLP rules

PRI: Deoupling with trusted hardware

key

configure

Internet

Enterprise

confirm fairness

key

PRI

key

add DLP rules

PRI: Deoupling with trusted hardware

key

configure

Internet

Enterprise

confirm fairness

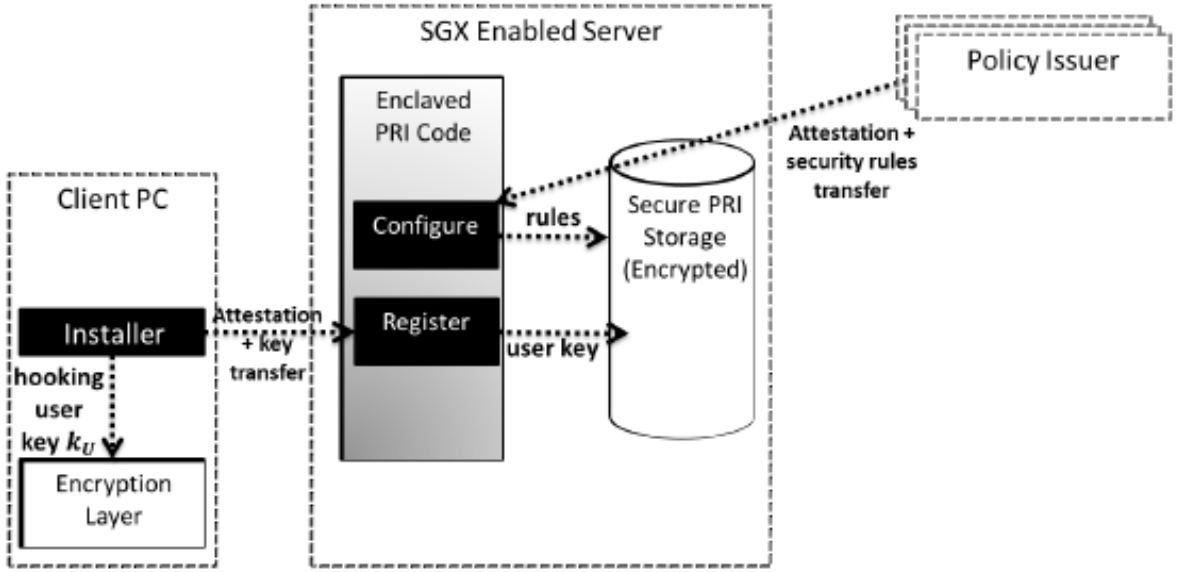
PRI

Traffic Transparent!

key

add DLP rules

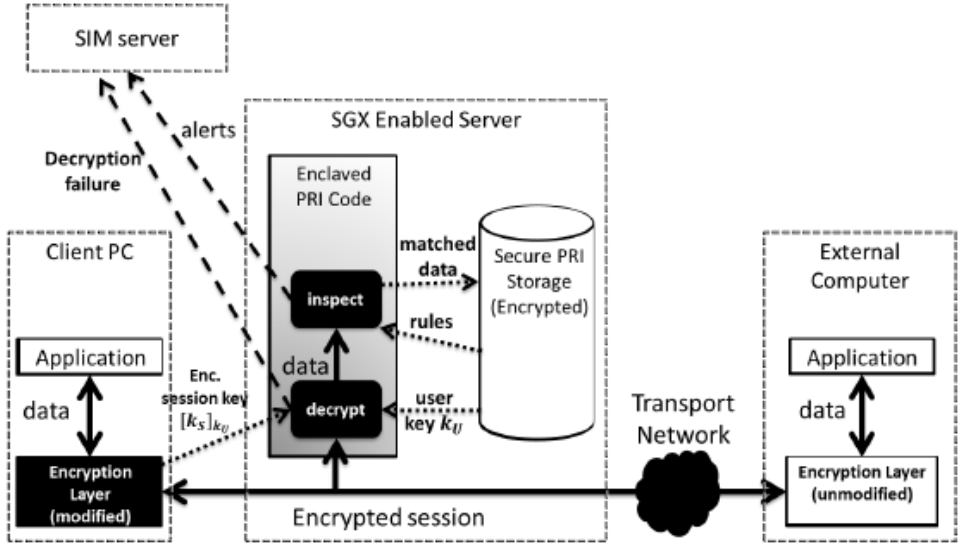
Details: Configuration and Alerts



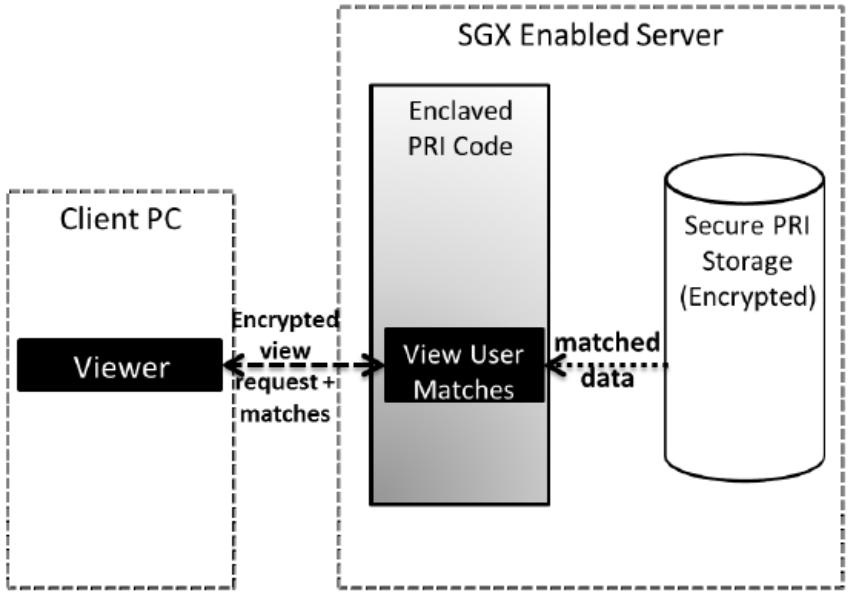
PRI process can be configured to inspect user traffic according to **security rules inserted by the policy issuer**.

Keys and rules are **stored safely** in the PRI storage.

PRI can then inspect user session using the key sent by the agent. **Matches are saved** in a secured storage and **alerts** are sent to the corporate SIM server.

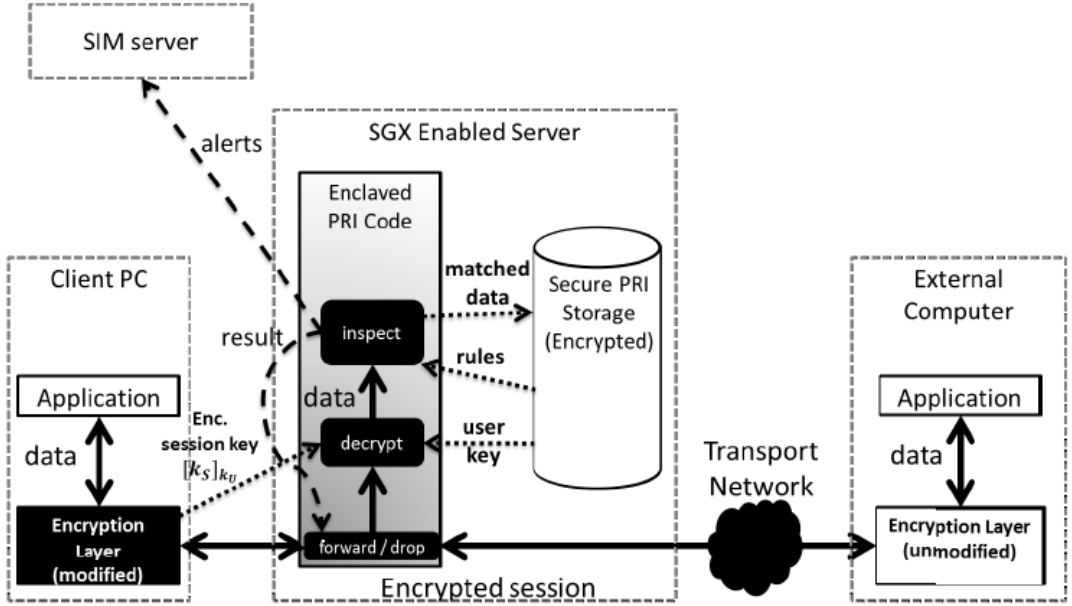


Details: Verification



PRI includes a **special viewer app** which allows users to **verify that matching** rules are not abused to violate confidentiality of their traffic.

Of course, PRI can also be used for **prevention** not only detection: depending on the result of the inspection, it is decided whether traffic should be forwarded or dropped.



Further Potential Applications

- **Privacy-Preserving Detection of Insider Threats**
  - Challenging: IDS for insider threats?? How to configure IDS?!
  - Recent progress, e.g., watermarking
  - Moreover: PRI is more general, e.g., supports machine-learning

- **Network Outsourcing**
  - Trend to **outsource cyber security logic** or entire network admin to external company
  - In PRI terminology: **external company operates PRI server**

- **Anti-Terror Intelligence**
  - Delicate topic related to privacy: national security
  - With PRI: **Government provides rules** and publishes them in aggregated form
  - **Attestation to citizens**: rules are installed properly and did not leak information
  - What has been matched is revealed to users only with a delay, attacker cannot react

Conclusion

- Dependencies and roles not well-understood in many networked systems today: untrusted hardware, untrusted operator, untrusted administrator, untrusted SDN controller
- Our approach: decoupling! Gives opportunities for new roles, e.g., rule provider!
- Privacy preserving traffic inspection: not impossible!
- Interesting use cases: enterprise, insider threats, outsourced security, anti-terror intelligence
- PRI touches two larger questions:
  - How to reduce trust in computer networks?
  - Applications for secure hardware in computer networks?

Backup

		Use Case		
		Enterprise Security and Insiders	**Outsourced Security**	**Anti-Terror Intelligence**
Entities	Clients	employees	enterprise	civilians / web hosts
	PRI Operators	admins	external	ISPs
	Rule Providers	admins + external	external	governments

		Architecture			
		Proxy	**Client-Side Firewall**	**BlindBox [25]**	**PRI**
Privacy	user exposure	middlebox	no	no	no (enclaved)
	rules exposure	middlebox	endpoint	middlebox	no (enclaved)
Effectiveness	inspection guarantee	yes	no	no	yes
	supports rules	any	any	exact match only	any
Overhead	computation	en-&decryption	none	tokenization & encryption	decryption
	communication	none	none	a stream of tokens	one packet