Data Protection Intents for Software-Defined Networking

Benjamin E. Ujcich and William H. Sanders
University of Illinois at Urbana-Champaign, USA

5th IEEE International Conference on Network Softwarization (NetSoft 2019)
24-28 June 2019 – Paris, France
Data Protection and Networks

- Data protection regulations are becoming more widespread and require more insight into data use and protection
- EU’s GDPR as example
- How are networks affected?

Network visibility and assurance for GDPR compliance

Since GDPR also restricts cross-border data transfers, it’s important that networking teams understand the country of origin of any particular data, and how that data will traverse the organization’s networks, remaining mindful of which paths it will take and where it will be stored.

To assure and keep track of this information, therefore, businesses will require full visibility across their entire network, including...
A Network View and the Role of Software

Network as **observer**

- All control plane actions **can be seen** by SDN controller → **completeness**

Network as **abstracter**

- SDN controller and apps for reasoning → **bridge semantic gaps**

- Host view:
  - Personal data
  - Data services
  - Network intents
  - Network flow rules
  - Data plane traffic

- Network view:
Approach

- Apply **intent-based networking** concepts to **data protection** with focus on GDPR
- Identify data protection **regulatory requirements** applicable to SDN/IBN
- Identify appropriate abstractions to **bridge semantic gaps**
- Develop an architecture and framework to support **data protection intents**
Personal Data, the GDPR, and the Network

- Data usage requirements
  - Processing, storage, and transmission

- Logging, analysis, and forensics requirements
  - Recordkeeping for demonstration of accountability

- Access control
  - Mechanisms for access control (e.g., network firewalls)

Focus of this work

Prior SDN work
1. Specify host-to-host data plane connection requests for data processing through data protection abstractions.
2. Maintain observance and oversight over all network requests that involve personal data.
3. Log control plane and data plane events to bridge network abstractions and data protection abstractions.
4. Use data protection abstractions to query past events for analysis and forensics.
Architecture

Components:
- Data services
- Data protection intents
- Data protection intent application
- SDN controller

Proof-of-concept in ONOS
Abstractions

Separate concerns and link layers of abstractions to bridge semantic gaps.
Scenario: Data Breach

- Attacker **exfiltrates data** from a private-facing database server via a public-facing Web server
- DPI can **track what data was exfiltrated**
- Useful for **practitioners and regulators**
Scenario: Data Breach

What data were leaked?

Data Protection Intents
- Data
- Lawful bases
- Data purposes
- Data services

Network Intents
- Network resources
- Constraints
- Instructions

Flow Rules
- Device
- Selector
- Treatment
- Timeout

Data Services
Identity Store

APPLICATION PLANE

What intents were seen at time $t$?

User

CONTROL PLANE

What flow rules were seen at time $t$?

APPLICATION PLANE

Data protection intent framework

DATA PLANE

Which hosts were communicating at time $t$?

Network Devices and Hosts

APPLICATION PLANE

Which hosts were communicating at time $t$?

APPLICATION PLANE

Data protection intent framework

DATA PLANE

Which hosts were communicating at time $t$?

Network Devices and Hosts

APPLICATION PLANE

Which hosts were communicating at time $t$?

APPLICATION PLANE

Data protection intent framework

DATA PLANE

Which hosts were communicating at time $t$?

Network Devices and Hosts

APPLICATION PLANE

Which hosts were communicating at time $t$?

APPLICATION PLANE

Data protection intent framework

DATA PLANE

Which hosts were communicating at time $t$?

Network Devices and Hosts

APPLICATION PLANE

Which hosts were communicating at time $t$?

APPLICATION PLANE

Data protection intent framework

DATA PLANE

Which hosts were communicating at time $t$?

Network Devices and Hosts

APPLICATION PLANE

Which hosts were communicating at time $t$?

APPLICATION PLANE

Data protection intent framework

DATA PLANE

Which hosts were communicating at time $t$?

Network Devices and Hosts

APPLICATION PLANE

Which hosts were communicating at time $t$?

APPLICATION PLANE

Data protection intent framework

DATA PLANE

Which hosts were communicating at time $t$?

Network Devices and Hosts

APPLICATION PLANE

Which hosts were communicating at time $t$?

APPLICATION PLANE

Data protection intent framework

DATA PLANE

Which hosts were communicating at time $t$?

Network Devices and Hosts

APPLICATION PLANE

Which hosts were communicating at time $t$?

APPLICATION PLANE

Data protection intent framework

DATA PLANE

Which hosts were communicating at time $t$?

Network Devices and Hosts

APPLICATION PLANE

Which hosts were communicating at time $t$?

APPLICATION PLANE

Data protection intent framework

DATA PLANE

Which hosts were communicating at time $t$?

Network Devices and Hosts

APPLICATION PLANE

Which hosts were communicating at time $t$?

APPLICATION PLANE

Data protection intent framework

DATA PLANE

Which hosts were communicating at time $t$?

Network Devices and Hosts

APPLICATION PLANE

Which hosts were communicating at time $t$?

APPLICATION PLANE

Data protection intent framework

DATA PLANE

Which hosts were communicating at time $t$?

Network Devices and Hosts

APPLICATION PLANE

Which hosts were communicating at time $t$?

APPLICATION PLANE

Data protection intent framework

DATA PLANE

Which hosts were communicating at time $t$?

Network Devices and Hosts

APPLICATION PLANE

Which hosts were communicating at time $t$?

APPLICATION PLANE

Data protection intent framework

DATA PLANE

Which hosts were communicating at time $t$?

Network Devices and Hosts

APPLICATION PLANE

Which hosts were communicating at time $t$?

APPLICATION PLANE

Data protection intent framework

DATA PLANE

Which hosts were communicating at time $t$?

Network Devices and Hosts

APPLICATION PLANE

Which hosts were communicating at time $t$?

APPLICATION PLANE

Data protection intent framework

DATA PLANE

Which hosts were communicating at time $t$?

Network Devices and Hosts

APPLICATION PLANE

Which hosts were communicating at time $t$?

APPLICATION PLANE

Data protection intent framework

DATA PLANE

Which hosts were communicating at time $t$?

Network Devices and Hosts

APPLICATION PLANE

Which hosts were communicating at time $t$?
Future Work

- **Scalability**
  - Distributed GDPR-aware middleware tools
  - Microservice architecture and data processing
- **Reduction of trusted computing base (TCB)**
- **Data protection policies and access control enforcement**
  - Online reference monitor
Conclusion

- New data protection regulations provide challenges and opportunities for SDN
- SDN as an observer and abstracter
- Proposed data protection intent architecture and design for data protection-aware networks
Questions?

- Thanks for listening!
- Authors:
  - **Ben Ujcich**
    Web: [http://ujcich2.web.engr.illinois.edu](http://ujcich2.web.engr.illinois.edu)
    E-mail: ujcich2@illinois.edu
  - **Bill Sanders**
    E-mail: whs@illinois.edu