NOKIA Bell Labs

Cloud Server Geolocating

Presentation at 19th FRUCT conference, Jyväskylä, Finland.

- Leo Hippeläinen, Ian Oliver, Shankar Lal
- Nokia Bell Labs, Security Research Team Espoo, Finland
- leo.hippelainen@nokia-bell-labs.com, leo.hippelainen@aalto.fi

- 2016-11-11

Presentation Topic

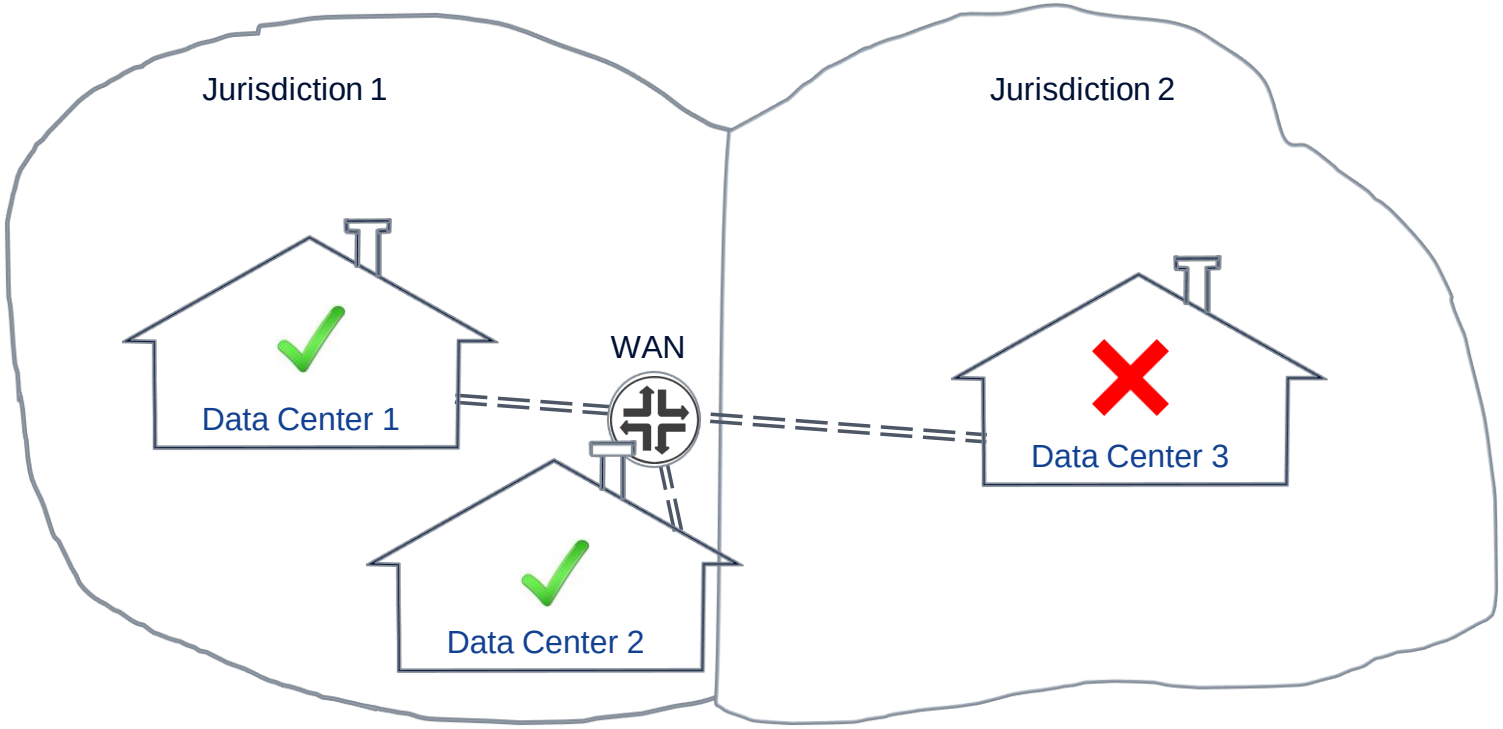
Dependable *geographical location* detection of physical servers belonging to a **computing cloud**.

- Why this deserves attention?
- What can be done about it?

Some Examples of Data Privacy, Residency and Sovereignty Legislations

Region	Laws	Principles
European Union	General Data Protection Regulation (GDPR)	• Privacy is a fundamental right. • Trans border data transfers OK, as long as the involved countries also respect GDPR.
Australia & NZ	The Privacy Amendment Act	• Australian data sender must take reasonable steps to ensure that also the recipient will comply with the Australian Privacy Principles (APP).
Russia	Amendments to the Personal Data Law	• All personal data of Russian citizens must be stored in databases that reside within territory of the Russian Federation. • Personal data can be duplicated to outside Russian borders, as long as Russian personal data laws are followed.
China	No comprehensive personal data protection law, instead scattered provisions. New security law just adopted.	• Unless otherwise agreed or stated in regulations personal information must not be transferred to outside the territory of the People's Republic of China. • Details of the new cyber security law not yet analyzed.
USA	No federal personal data law, but many government policies and regulations	• Legal domain specific laws • HIPAA (health records), PCI DSS (credit cards), etc.

The Data Residency Issue



How can a cloud customer verify that Data Center 3 is not employed?

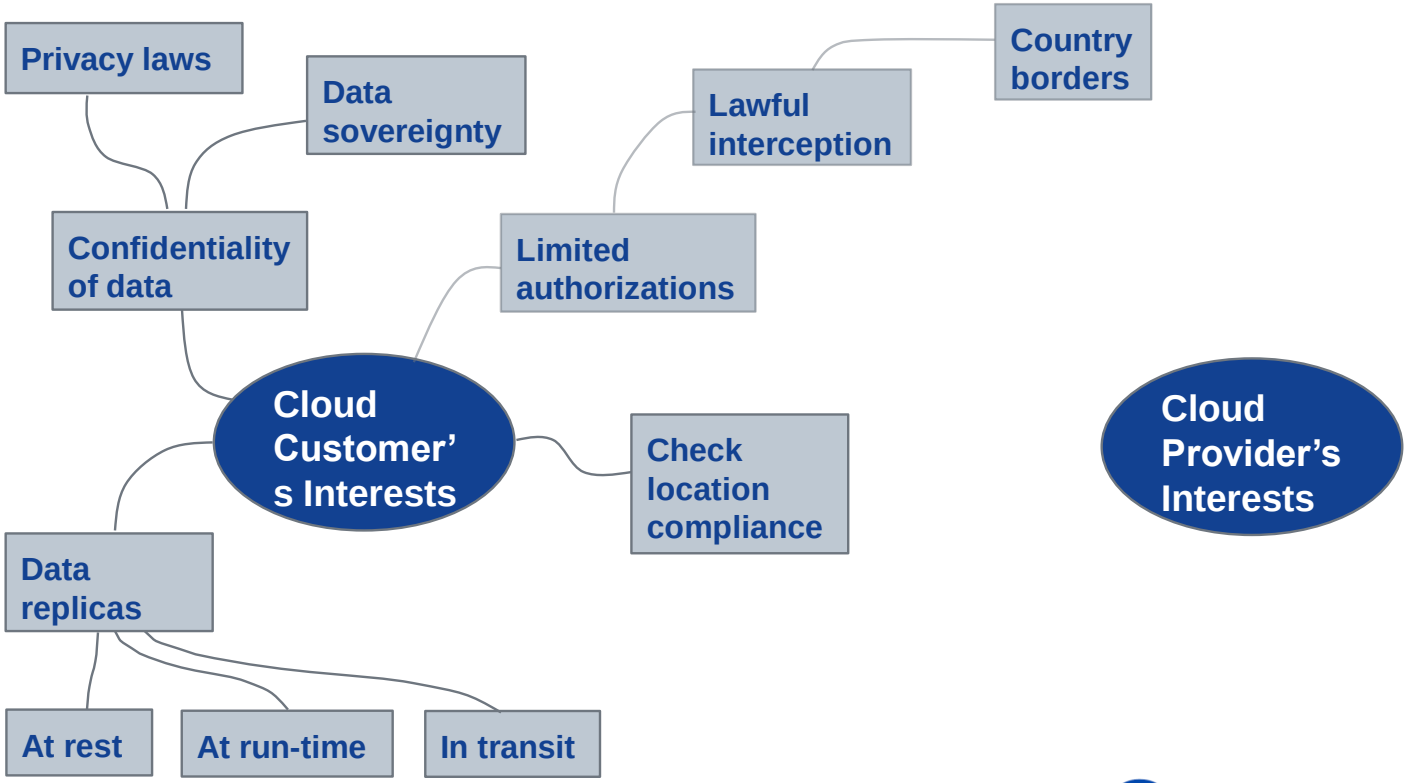
DIMECC Program CYBER TRUST

NOKIA Bell Labs

NOKIA Bell Labs

Analysing the Problem Domain

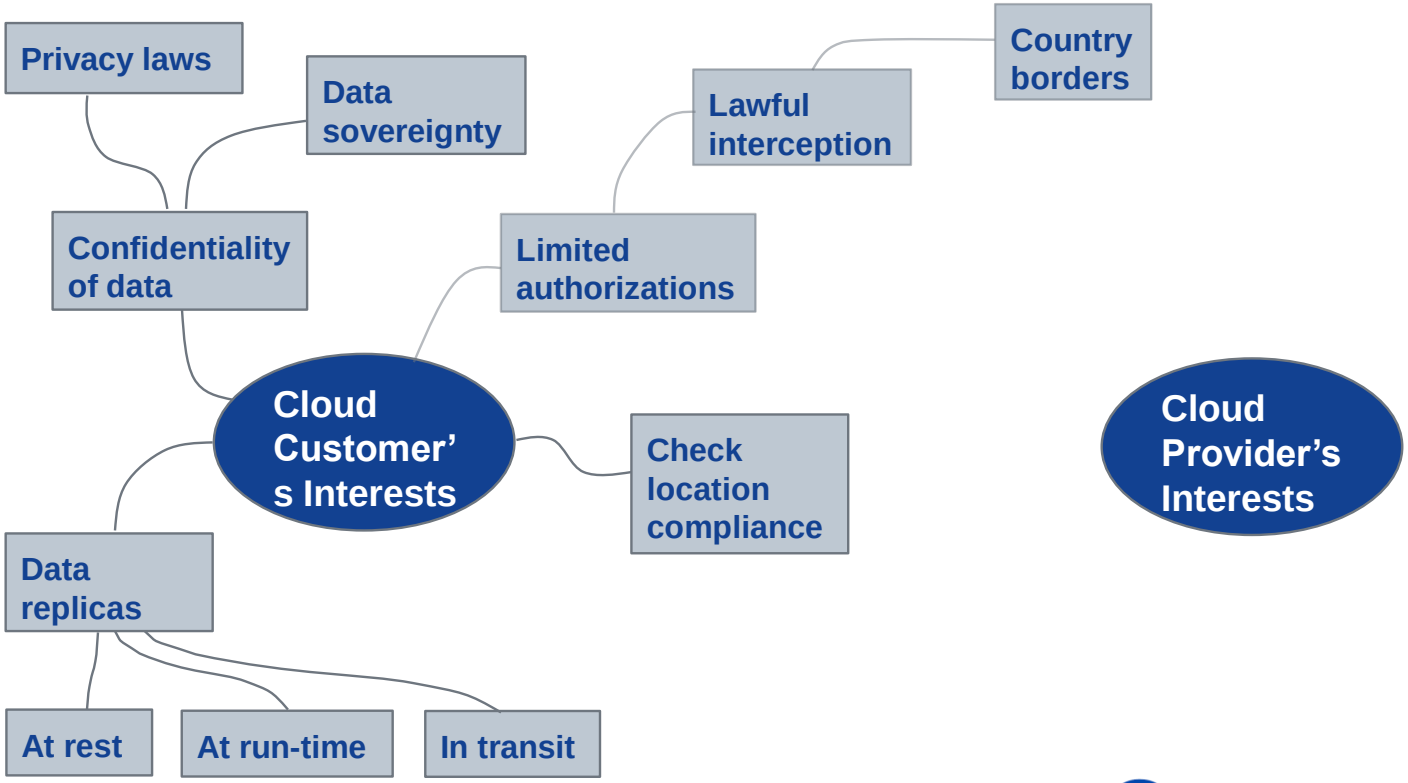
Geographical Trust Interests of Cloud Customer and Cloud Provider



DIMECC Program CYBER TRUST

NOKIA Bell Labs

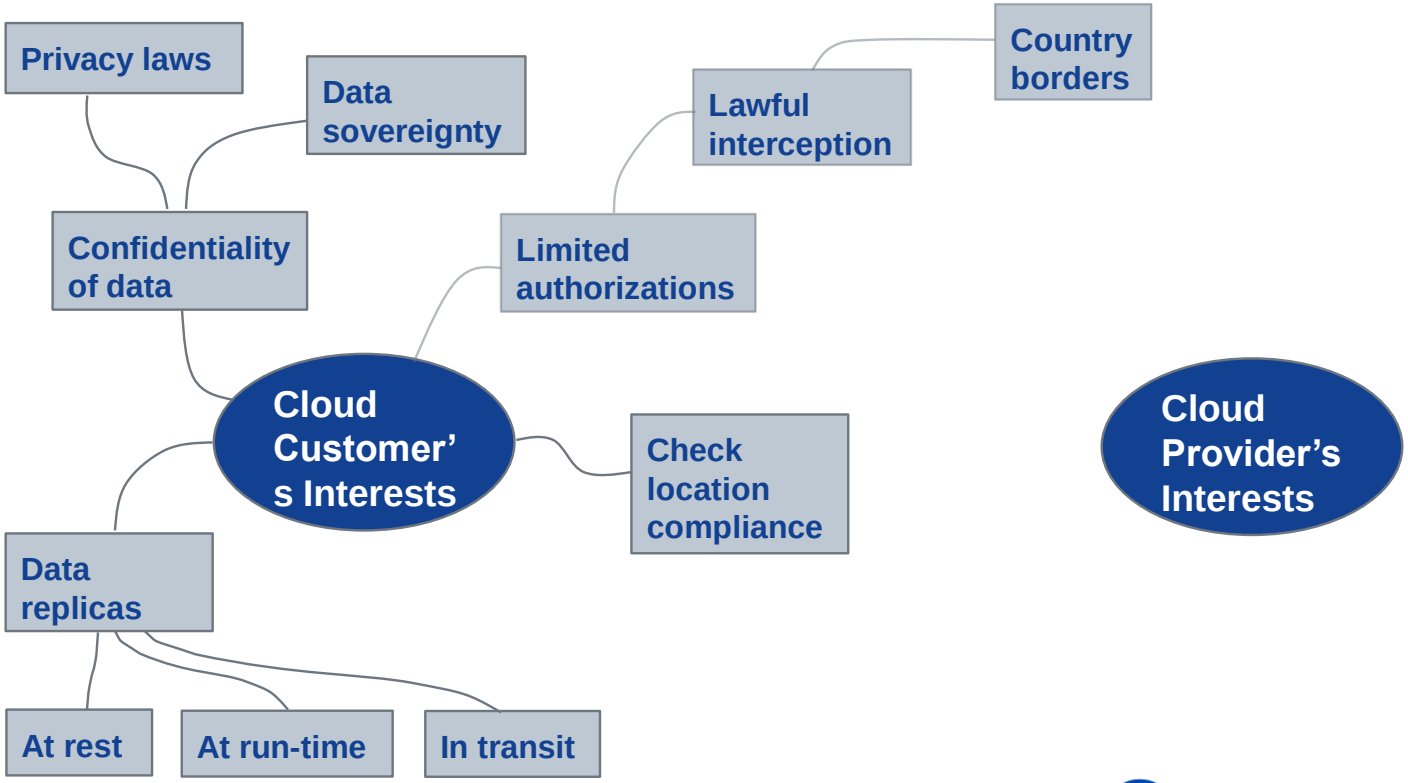
Geographical Trust Interests of Cloud Customer and Cloud Provider



DIMECC Program CYBER TRUST

NOKIA Bell Labs

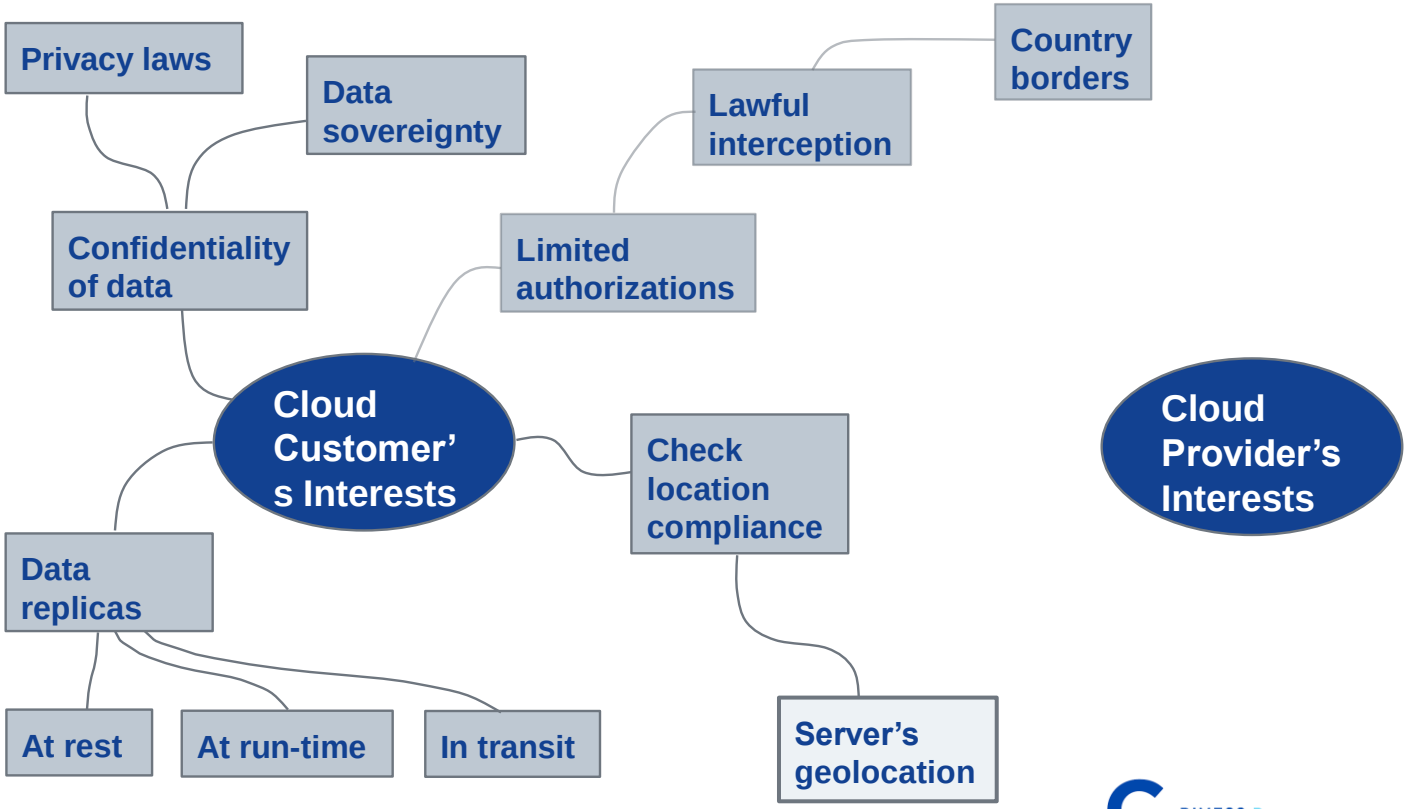
Geographical Trust Interests of Cloud Customer and Cloud Provider



DIMECC Program CYBER TRUST

NOKIA Bell Labs

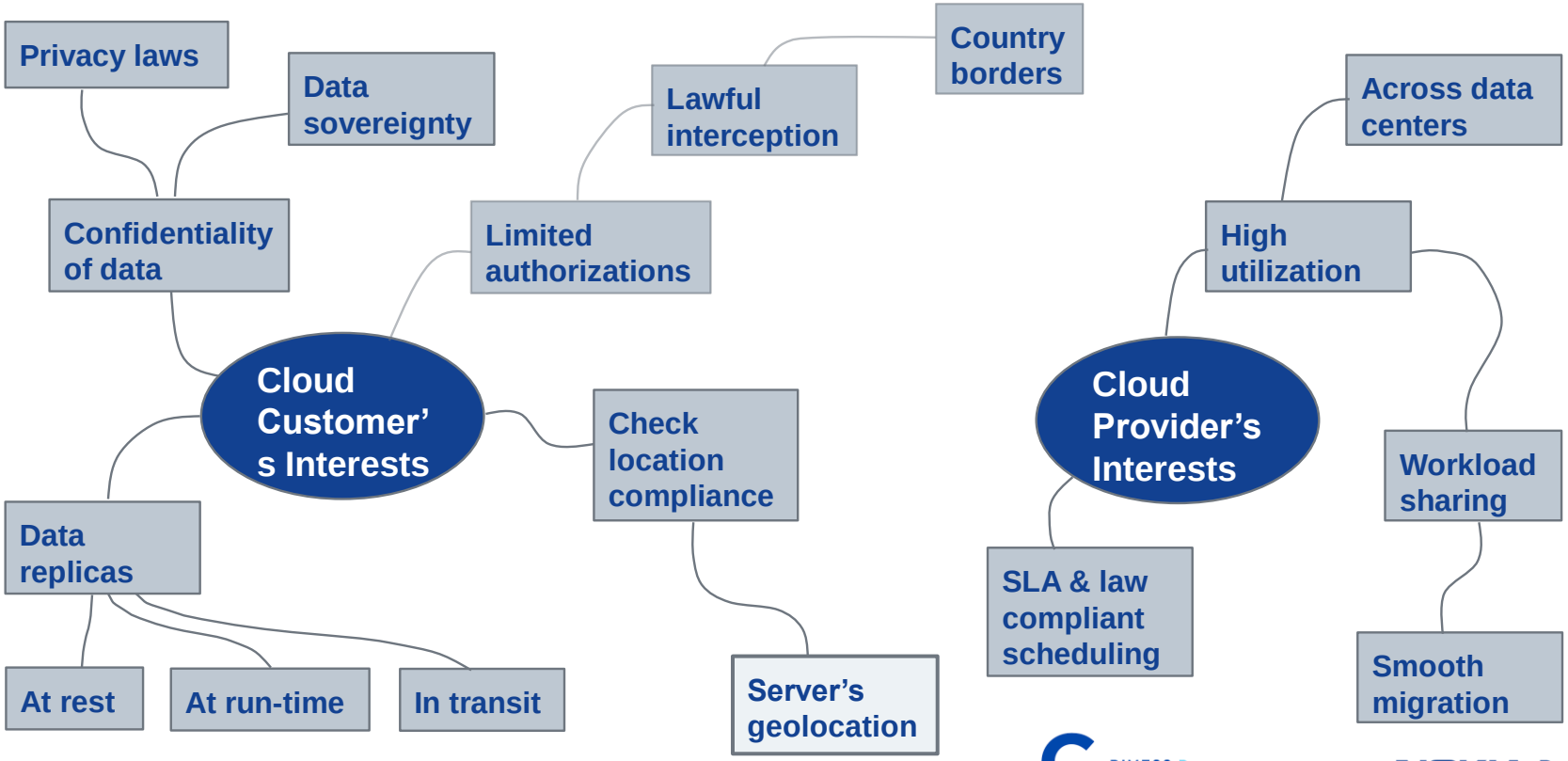
Geographical Trust Interests of Cloud Customer and Cloud Provider



DIMECC Program CYBER TRUST

NOKIA Bell Labs

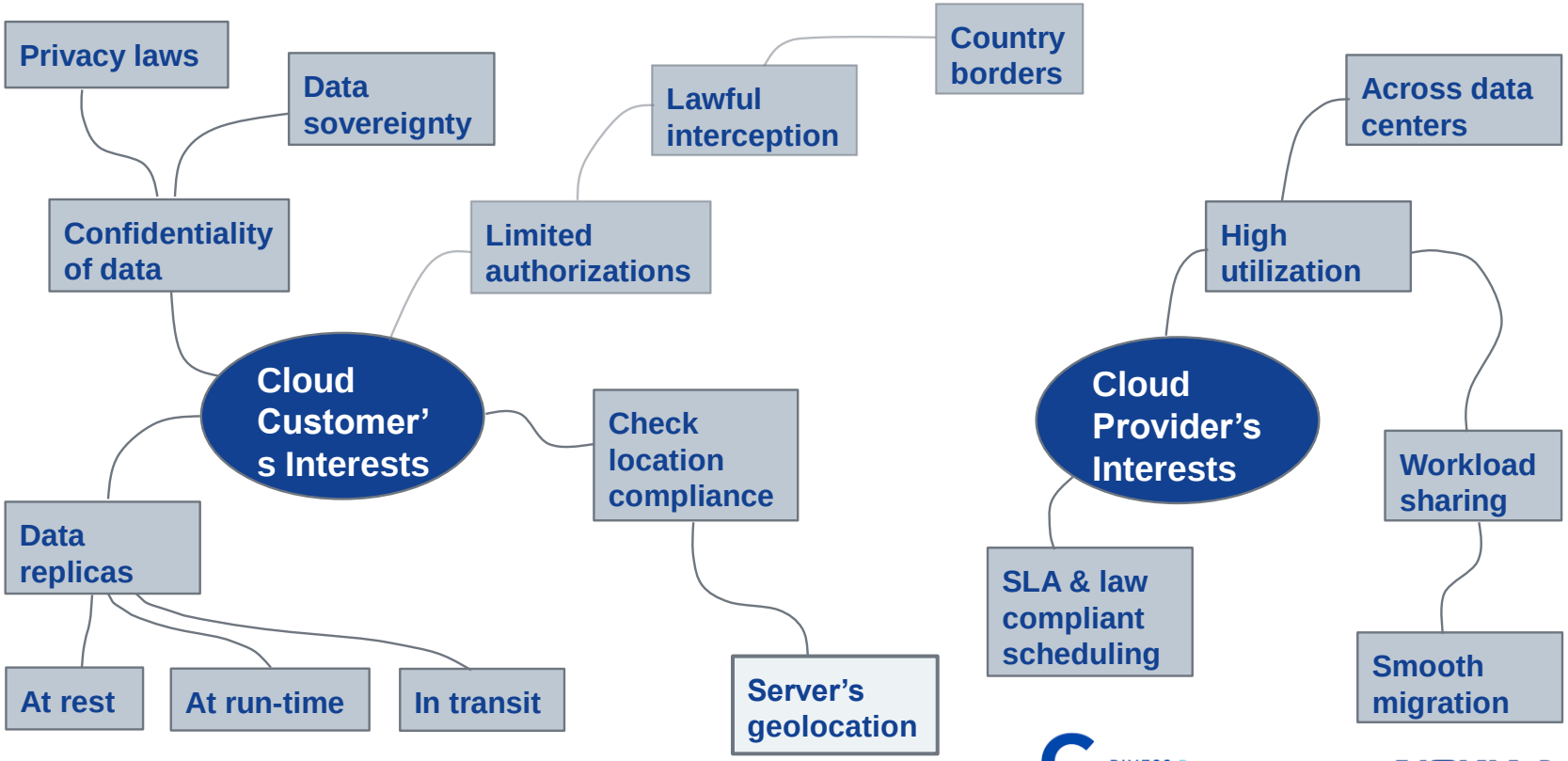
Geographical Trust Interests of Cloud Customer and Cloud Provider



DIMECC Program CYBER TRUST

NOKIA Bell Labs

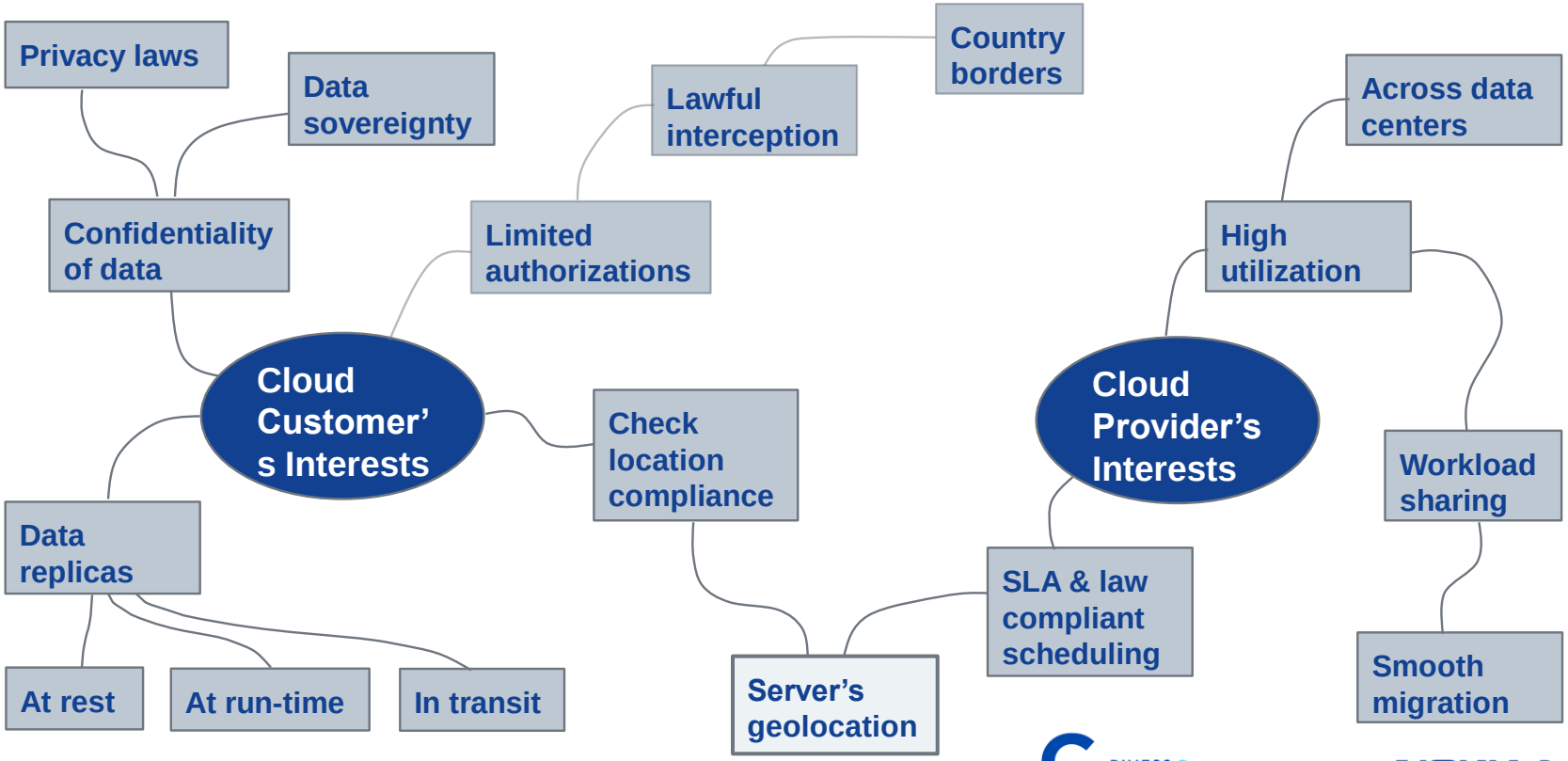
Geographical Trust Interests of Cloud Customer and Cloud Provider



DIMECC Program CYBER TRUST

NOKIA Bell Labs

Geographical Trust Interests of Cloud Customer and Cloud Provider



DIMECC Program CYBER TRUST

NOKIA Bell Labs

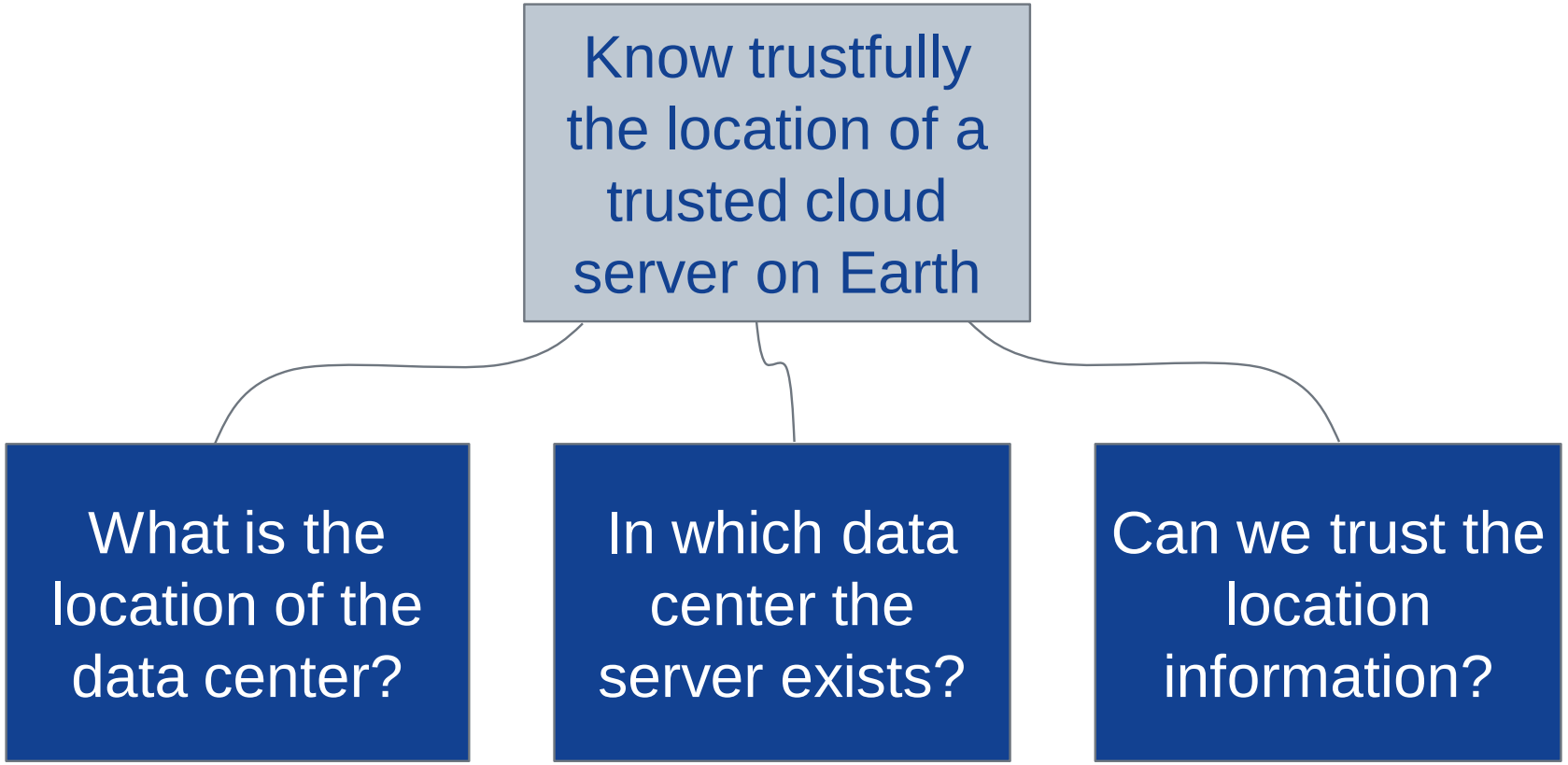
Research Challenges in Providing Geographical Trust

1. Cloud Service **Provider** wants to optimize utilization of server resources and still take into account geographical constraints.
2. Cloud Service **Customer** wants to verify that Cloud Service Provider respects geographical constraints.
3. Service **End User** wants to verify that his data is kept confidential and not copied to uncompliant jurisdictions.
4. External **Auditor** writes an audit report and for that needs to check the locations of cloud servers.
5. Possible geolocation cheating patterns of a dishonest Cloud Service **Provider**.
6. Possible geolocation cheating patterns of a dishonest Cloud Service **Customer**.

NOKIA Bell Labs

Analysing the Solution Domain

Ingredients to Providing Location of a Cloud Server



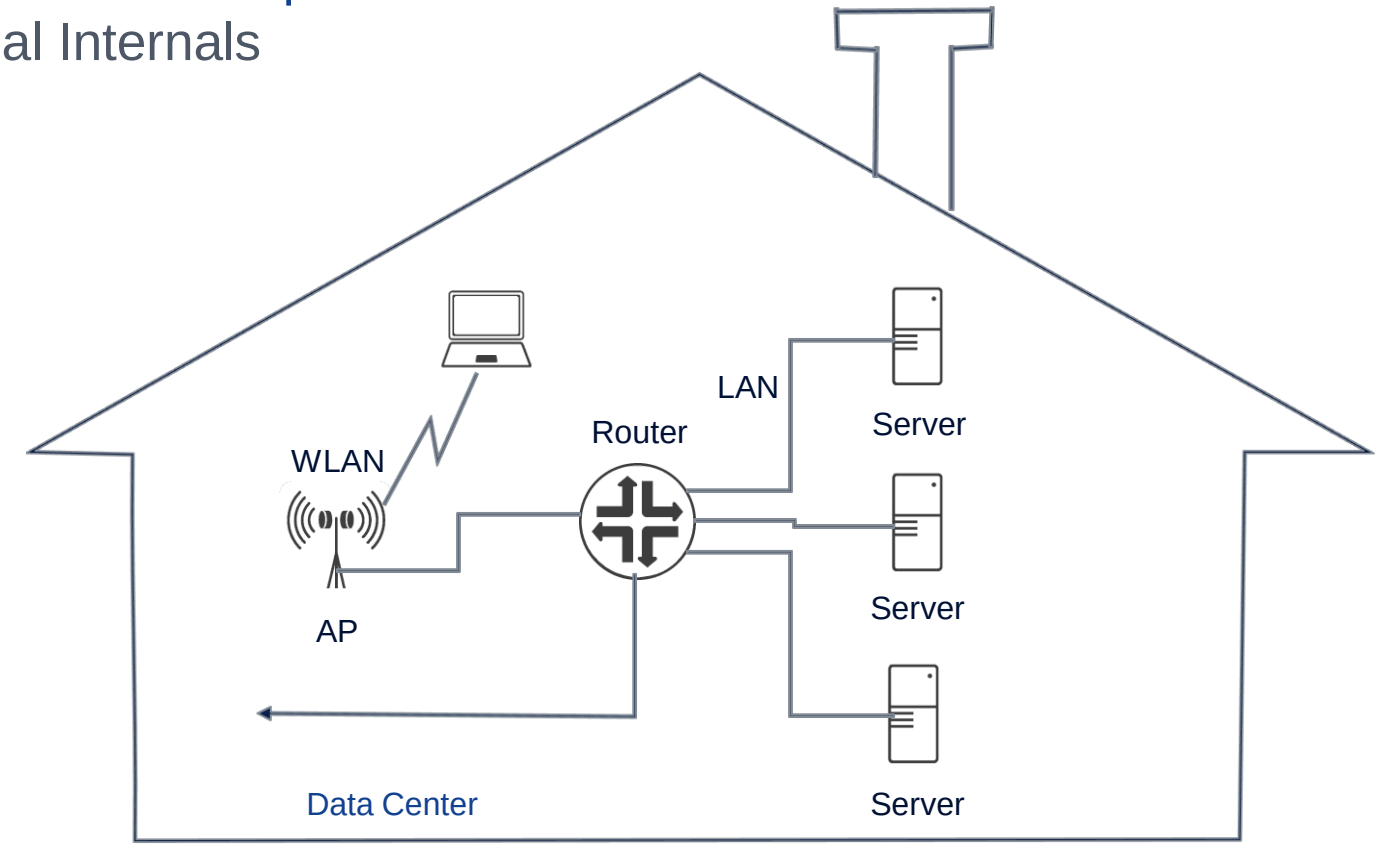
DIMECC Program CYBER TRUST

NOKIA Bell Labs

Assumptions and Requirements
for a Cloud Server Location Detection Solution

• Cost Awareness	Server's price 1K€ .. 10 K€
• Dependability	False positives: 0%
• Node count	>10000 servers per data center
• Radio Signal Propagation	Data center in a Faraday cage
• Auditing	Site visit possible
• Server Identifiers	Unique, e.g. serial number
• Server Mobility	Minimal but can happen
• Geographical Location	Not near jurisdiction border

Data Center Concepts
Essential Internals



Location Detecting Techniques and Algorithms

Incomplete list (but this should contain all essential ones)

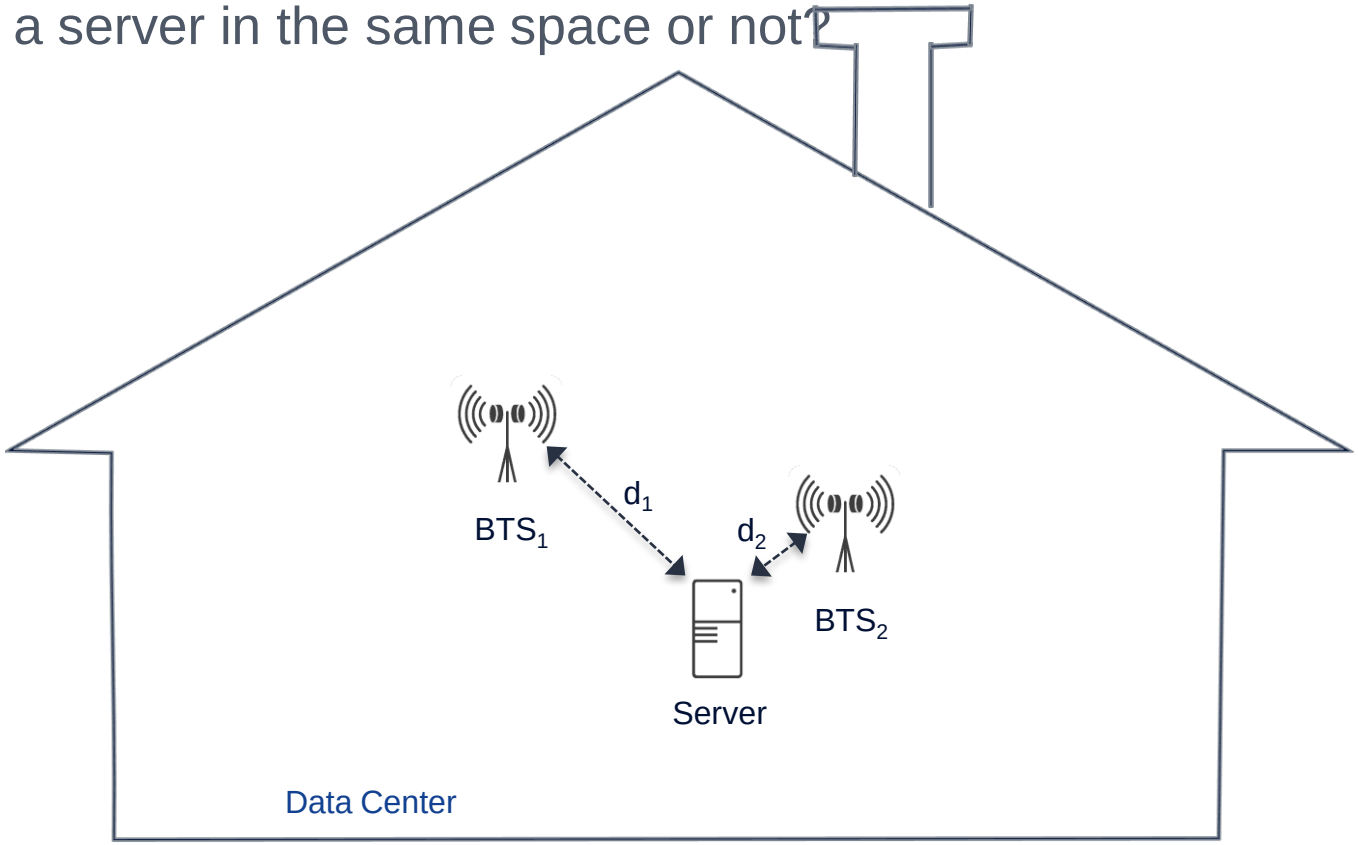
- Proximity to a transceiver ⇦
- Signal strength
- Signal delay
- Signal direction
- Distance-bounding protocols ⇦
- IP address based mapping
- Server naming
- Provisioned location code ⇦
- Visual image
- Network Topology ⇦
- Planetary constants
- Satellite based positioning systems
- Combination techniques
- Attestation service ⇦

DIMECC Program CYBER TRUST

NOKIA Bell Labs

Proximity based Location Detection

Is a server in the same space or not?



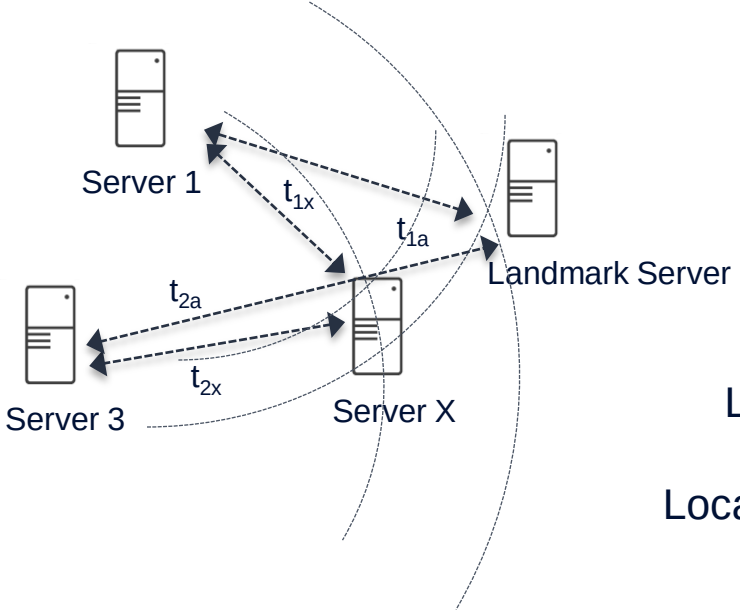
DIMECC Program CYBER TRUST

NOKIA Bell Labs

Round Trip Time with Landmark based Location Detection

Physical distances > 500 km in the Internet

- Distance-Bounding Protocols



Locate data center
or
Locate inside data center

DIMECC Program CYBER TRUST

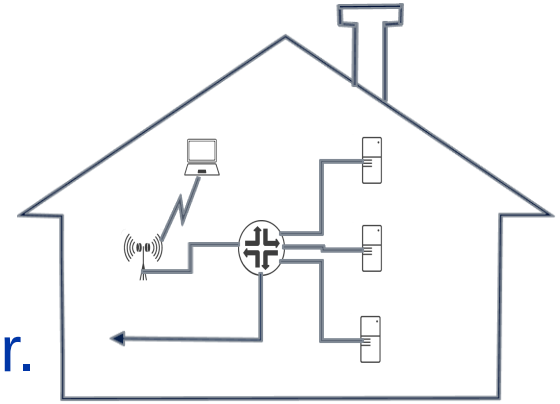
NOKIA Bell Labs

Provisioned Location Code based Location Detection

- Typically location HASH stored to a TPM (Trusted Platform Module) register.
  - or some other HSM (Hardware Security Module).

- Must be provisioned separately for every physical server => extra cost?
- How can we trust that data is correct?

Network Topology based Location Detection



- Servers have wired LAN.
  - Connected to LAN switch or router.
- Network topology can be detected.

- Network topology alone does not provide sufficient evidence.

Attestation Service based Location Detection

- Server’s serial number -> location coordinates.
- Needs a third party trusted server.

- Difficult to maintain the database up-to-date.
- How can we trust that data is correct?

Possible Radio Technologies
for Proximity and Distance Measurements

- RFID
- Bluetooth
- ZigBee
- Wi-Fi
- Cellular

Summary of Radio Signal based Location Detection Techniques

	Cost per server	Cost per reader	Nodes per reader	Range
RFID (active)	<5€	100€ (?)	No limit	
Bluetooth	<5€	20€	7 + 255 (piconet)	
ZigBee	<5€	30€	64000	
Wi-Fi	<5€	50€	2007	
Cellular	20€ (phone + SIM)	1000€ (?)	No limit	

Should run experiments.

Too few nodes per piconet.

Should run experiments.

Too few nodes per AP.

Too expensive, too long range.

Note: Shown prices are only educated guesses.

DIMECC Program CYBER TRUST

NOKIA Bell Labs

Conclusions

- There is need for dependable location detection of physical cloud servers.
- All techniques mentioned here have challenges with locating servers in to a data center site.
- Note: Trusted computing is a precondition to trusted geolocation information.
- Further research work:
  - Combining several locating techniques to increase trust.
  - Identify possible cheating patterns by cloud service providers.
  - Detect location of data and its replicas.

NOKIA Bell Labs