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

<table>
<thead>
<tr>
<th>Region</th>
<th>Laws</th>
<th>Principles</th>
</tr>
</thead>
</table>
| **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?
Analysing the Problem Domain
Geographical Trust Interests of Cloud Customer and Cloud Provider

**Cloud Customer's Interests**
- Data replicas
  - At rest
  - At run-time
  - In transit
- Confidentiality of data
- Data sovereignty
- Limited authorizations
- Lawful interception
- Check location compliance

**Cloud Provider's Interests**
- Limited authorizations
- Lawful interception
- Country borders
- Data sovereignty
- Privacy laws
- Confidentiality of data

© 2016 Nokia
Geographical Trust Interests of Cloud Customer and Cloud Provider

Cloud Customer’s Interests
- Data replicas
  - At rest
  - At run-time
  - In transit
- Confidentiality of data
- Privacy laws
- Data sovereignty

Cloud Provider’s Interests
- Limited authorizations
- Lawful interception
- Country borders
- Check location compliance
- Data sovereignty

Confidentiality
Privacy laws
Data sovereignty
Cloud Customer’s Interests
Data replicas
At rest
At run-time
In transit

Cloud Provider’s Interests
Limited authorizations
Lawful interception
Country borders
Check location compliance
Data sovereignty
Geographical Trust Interests of Cloud Customer and Cloud Provider

Cloud Customer’s Interests
- Privacy laws
- Confidentiality of data
- Data replicas
- At rest
- At run-time
- In transit
- Lawful interception
- Limited authorizations
- Check location compliance

Cloud Provider’s Interests
- Data sovereignty
- Country borders
- Lawful interception
- Limited authorizations
- Lawful interception
- Check location compliance

Confidentiality

Privacy laws

Country borders
Geographical Trust Interests of Cloud Customer and Cloud Provider

Cloud Customer’s Interests:
- Data replicas
  - At rest
  - At run-time
  - In transit
- Confidentiality of data
- Privacy laws
- Lawful interception
- Data sovereignty

Cloud Provider’s Interests:
- Limited authorizations
- Lawful interception
- Check location compliance
- Server’s geolocation
- Country borders

Confidentiality of data
Geographical Trust Interests of Cloud Customer and Cloud Provider

Cloud Customer’s Interests

- Data replicas
  - At rest
  - At run-time
  - In transit
- Confidentiality of data
- Limited authorizations
- Lawful interception
- Server’s geolocation

Cloud Provider’s Interests

- Country borders
- Across data centers
- High utilization
- Workload sharing
- Smooth migration
- SLA & law compliant scheduling
- Check location compliance
- Limited authorizations
- Lawful interception
- Server’s geolocation
Geographical Trust Interests of Cloud Customer and Cloud Provider

Cloud Customer’ s Interests
- Data replicas
  - At rest
  - At run-time
  - In transit
- Confidentiality of data
- Limited authorizations
- Lawful interception
- Check location compliance
- Server’s geolocation

Cloud Provider’s Interests
- Across data centers
- High utilization
- Workload sharing
- Smooth migration
- Limited authorizations
- Lawful interception
- Country borders
- SLA & law compliant scheduling
- Server’s geolocation
- Server’s geolocation

Privacy laws
- Data sovereignty
- Data sovereignty
- Data sovereignty
- Data sovereignty
Geographical Trust Interests of Cloud Customer and Cloud Provider

Cloud Customer’ s Interests
- Data sovereignty
- Limited authorizations
- Check location compliance
- Server’s geolocation
- Data replicas
  - At rest
  - At run-time
  - In transit

Cloud Provider’s Interests
- Lawful interception
- Country borders
- Across data centers
- High utilization
- Workload sharing
- Smooth migration
- SLA & law compliant scheduling
- Limited authorizations
- Server’s geolocation
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**.
Analysing the Solution Domain
Ingredients to Providing Location of a Cloud Server

Know trustfully the location of a trusted cloud server on Earth

What is the location of the data center?

In which data center the server exists?

Can we trust the location information?
Assumptions and Requirements for a Cloud Server Location Detection Solution

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Acceptance Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost Awareness</td>
<td>Server’s price 1K€ .. 10 K€</td>
</tr>
<tr>
<td>Dependability</td>
<td>False positives: 0%</td>
</tr>
<tr>
<td>Node count</td>
<td>&gt;10000 servers per data center</td>
</tr>
<tr>
<td>Radio Signal Propagation</td>
<td>Data center in a Faraday cage</td>
</tr>
<tr>
<td>Auditing</td>
<td>Site visit possible</td>
</tr>
<tr>
<td>Server Identifiers</td>
<td>Unique, e.g. serial number</td>
</tr>
<tr>
<td>Server Mobility</td>
<td>Minimal but can happen</td>
</tr>
<tr>
<td>Geographical Location</td>
<td>Not near jurisdiction border</td>
</tr>
</tbody>
</table>
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
Proximity based Location Detection
Is a server in the same space or not?
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
• 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
<table>
<thead>
<tr>
<th></th>
<th>Cost per server</th>
<th>Cost per reader</th>
<th>Nodes per reader</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFID (active)</td>
<td>&lt;5€</td>
<td>100€ (?)</td>
<td>No limit</td>
<td>500 m</td>
</tr>
<tr>
<td>Bluetooth</td>
<td>&lt;5€</td>
<td>20€</td>
<td>7 + 255 (piconet)</td>
<td>400 m (BT5) + MESH</td>
</tr>
<tr>
<td>ZigBee</td>
<td>&lt;5€</td>
<td>30€</td>
<td>64000</td>
<td>MESH</td>
</tr>
<tr>
<td>Wi-Fi</td>
<td>&lt;5€</td>
<td>50€</td>
<td>2007</td>
<td>MESH</td>
</tr>
<tr>
<td>Cellular</td>
<td>20€ (phone + SIM)</td>
<td>1000€ (?)</td>
<td>No limit</td>
<td>Too expensive, too long range</td>
</tr>
</tbody>
</table>

Note: Shown prices are only educated guesses.
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.