DIMACS

Center for Discrete Mathematics & Theoretical Computer Science
Founded as a National Science Foundation Science and
Technology Center

CLOUD ACCOUNTABILITY PROJECT

CSA IE IRELAND cloud security alliance℠

CSA UNITED KINGDOM cloud security alliance℠

BIC BUILDING International Cooperation for Trustworthy ICT

International Workshop on Trustworthiness, Accountability and Forensics in the Cloud (TAFC 2013)

Sessions 1-4 reports

Session 1: ACCOUNTABILITY

Reported by: Lenore Zuck, University of Illinois at Chicago (UIC)

Discussion points

What is accountability? Do we need it?
If so then:
Rigorous definition(s)
Does is need to be predictable?
Can it always be defined (multiple sources)
weaker definitions (deterrence?)
Ties to privacy/ethics/contextual
remediation, verifiability, transparency, how to implement/enforce
Is accountability goal or means? If latter, then are there alternatives? Should we focus on it? Does it imply responsibility?

Panel Discussions

- **Point 1:** can accountability always be assigned (is it always well defined)
- **Point 2**: is accountability always important
- **Point 3:** Dealing with loss of data
- **Point 4:** Guaranteeing loss of data

Research areas identified

- New directions in privacy and accountability in face of new technical advancements
- Teasing apart the new from the old
- Definitions of Privacy and Accountability that can be used to gauge compliance with
- Enforcement of policies

Why is International cooperation necessary?

- Self regulations of various privacy laws and seamless merging of those laws for data sharing/transfer/disclosure
- Enforcement of policies *across* borders (including compliance transfers)
- Defining the lines between tech solvable issues and those that are beyond tech solutions

Session 2: Forensics, Evidence and Accountability

Reported by: Nick Papanikolaou, HP Labs, Bristol

Discussion points

- Identifying the artifacts that are useful for investigations across the cloud stack – which artifacts?
- What patterns do we need to look for in executable traces?
- What types of analysis can be carried out at the hardware level?
- Hakim Weatherspoon's example of covert channels
- Spanner for Google – time synchronization across a network

Panel Discussions

•Toolkits for forensics – what are the right tools and how often should they be updated?

•How to build cloud architectures that provide forensic mechanisms?

•What about digital freedoms? Forensic mechanisms have good and bad uses

•Debate about need of chain of custody for legal cases/prosecution

•In practice most cases not taken to court, or penalties not enforceable.

Research areas identified

- Forensics-as-a-Service
- Research into types of evidence for cloud, and how it can be automatically produced
- Graph-based matching for malware detection
- Using network hardware to forensically check compliance to SLAs

Why is International cooperation necessary

- Data centres located worldwide; need ability for law enforcement to work transparently across borders
- Interoperability between standards used by different agencies for forensic data is needed

SESSION 3. TRUST AND CLOUD SECURITY

Reported by: Jim Clarke, Waterford Institute of Technology, Ireland

Discussion points

•Certification, standardization and international convergence issues in cloud security (CIRRUS project), bridging between various activities, initiatives ETSI, CSA, NIST, ENISA, …

•Securing services running over untrusted clouds: the two-tiered trust model via crypto protocols

•Mobile Cloud Computing Paradigm - To augment the capability, capacity and battery time of the mobile devices, computationally intensive and storage demanding jobs should be moved to cloud

•A critical infrastructure network or DoD type network for lightweight devices (e.g. tablets)

•Trust storage controller (TSC) an interpreter for very rich policies.

Panel Discussions

•How does TSC language map to standards? Own interpreter is written.

•TSC deals with transfer of data between providers with a primitive for sending / receiving encrypted data. On both sides, you can make policy checks.

•Dealing with scalability issues when moving from lightweight to more intensive machines. Bootstrap process only happens once and then when that is finished, you have a clean system.

•Crypto protocol for securing services was developed specifically for to obtain the 'dream bound' of corruption resiliency

•Good link between India context and TSC work.

Research areas identified

- Crypto protocols for distributing trust
- Outsourcing to Service Providers and guaranteeing trust via Crypto protocols
- Preparation of semantic data for security parameters for mobile and cloud Security attributes
- Mobile Cloud security features and respective parameters and Security algorithm under different security requirements; Platform Independent Security Architecture
- Trusted Cloud Arch. incl. private cloud deployment and trusted service providers, trusted cloud monitor, access control model for computing services that supports need to know and separation of duties policies, TC-compliant computing services, Lightweight TC-compliant client service endpoints.
- TSC mapping to security and privacy requirements for cloud apps.
- Including legal requirements in the cloud?

Why is International cooperation necessary

- Leverage skill bases of int'l peers e.g crypto expertise, RFID, …
- Good example was from the India context where the government have committed to a mobile government model where all data will be available on mobiles by 2015. The work on crypto, Trusted cloud architecture, and Trust storage controller (TSC) presented all gels very well with this.

SESSION 4: Policy, Ethics AND Int’l cooperation
Reporting by: Karima Boudaoud, Mounib Mekhilef
Trust AND International cooperation, reporting by Aaron Jaggard

Discussion points

- How to design ethical code
- Ethics does not sell but data privacy does
- Which cultural & ethical norms
- EU strengthen individuals’ right to be forgotten :
- Do we have a death of privacy ?
- Stabilize international security architectures
- Cyber security and multi-lateral strategy
- economic security demands robust policy
- Establish international cyber norms
- Intelligent development environment
- Highly effective code re-use & sharing & collaboration
- Good practice -

Panel Discussions

•These will be provided later as there was no time during the workshop.

Research areas identified

- **Philosophy**
- **Mathematics**
  - Computer science
  - Information theory
  - Graph theory
  - Decision theory
  - optimization
  - Simulation/ Predictability
- **Human Sciences**
  - Sociology
  - industrial anthropology
  - Psychology
- **Legal**
  - IPR
  - Laws/regulation
  - Standardisation
- **Business**
  - Model building
  - Operations
  - Information logistics
  - Practices(Good:bad)
  - Lessons learned
  - low investment
  - international trading
- **Policy**
  - education
  - Strategy building
  - Risk & conflict Mngmt
  - Economy
  - incentives
- **Design**
  - User oriented
  - Co/Eco -design
  - Design for X

Why is International cooperation necessary

- **Context**
  - Protectionism
  - Global market
  - lawless lands
  - different priorities
  - Non western-world inc
  - Horizon 2020 coming soon
- **Threads**
  - Co-design as a context
  - Values
  - Needs vs time
  - cultural differences
  - Clock speed
  - Sophistication growing
- **Opportunities**
  - some places "field trial"
  - small markets
  - Closeness to clients
  - Open-ness to change
  - Growing market
  - Lack of:
  - Framework, Roadmap,
  - Body, Coordination
- **Coming Needs**
  - Impacts on large networks
  - Continuity of actions
  - Missing common objective
  - ->Future building
  - Funding planning
  - Sharing experiences