Workshop on Smart Sustainable Cities
Samarkand, Uzbekistan, 1-2 June 2017

Trust in IoT and Its Applications

Gyu Myoung Lee
ITU-T Chair of FG-DPM, WP3/13 Co-chair, Q16/13 and Q4/20 Rapporteur
LJMU UK/ KAIST Korea
gmlee@kaist.ac.kr
Contents

• Introduction
  – Trust in IoT
• Understanding of Trust
  – Trust features
• Key Design Principles and Challenges
• Various Technical Issues
• Use case, emerging technology
• Conclusion
Trust and Knowledge

• Future trust and knowledge infrastructure

ICT is a Basis of Knowledge Society

Potential Risks

Y.3052 – “Overview of trust provisioning in ICT infrastructures and services” Feb. 2017
Increasing Intelligence in IoT

Control and Trust

- Behave intelligently and rationally to
  - **Sense** real-world behaviour
  - **Perceive** the world using information models
  - **Adapt** to different environments and changes
  - **Learn** and **build** knowledge
  - **Act** to control their environments
Barrier to growth of IoT market

Data and Trust

Who are we comfortable sharing personal data from smart devices with?

- 63% Spouse/Significant Other
- 41% Close Friends
- 40% Health Professionals
- 30% Police
- 28% Insurance Companies
- 26% Boss
- 22% Supermarkets
- 14% Ad Companies
- 14% Government

Volume – Data at Rest
Variety – Data in Many Forms
Velocity – Data in Motion
Variability – Data in Change
Veracity – Data in Doubt

Source: 2014 Internet of Things Privacy Infographic
Towards Internet of Value

Data is Value – How to measure Value?

Security, Privacy and Trust

IoPTS – Internet of People, Things & Services

NIST - CPS Framework

Industrial Internet of Things

Trust Management

Trust

Social Capital

Dependability

Security

Privacy

Reliability

Experience

Third-party Opinions

Vulnerabilities

Risks

Threats

Risk Management

People-Centric

System-Centric
Understanding of Trust

Trust of a party A to a party B for a given task S is the measurable belief of A in that B accomplishes S dependably for a specified period P within a particular trust context T (in relation to the task S).

Trust is relative to a specific task (a service). Different trust relationships appear in different business contexts.

The measurement may be absolute (e.g. probability) or relative (e.g. Level of Trust).

This period may be in the past (history), the duration of the service (from now and until end of service), future (a scheduled or forecasted critical time slot), or always.

Dependability is deliberately understood broadly to include availability, reliability, safety, confidentiality, integrity and serviceability.
Social Cyber Physical Trust

Social world
Social Trust

Cyber world
Cyber Trust

Physical world
Physical Trust

ICT infrastructures and services
Everything as a Service

Cyber Objects
Communication
Control
Computing

Social Entities

Trusted ICT applications
E-commerce
Healthcare
Social media
Intelligent transportation
Environment

Social Cyber Physical Trust
Direct Trust vs. Indirect Trust

Indirect Trust (Experience and Third-party Opinions)
- Direct TrustLinks (Trust Context)
- Direct TrustLinks (other Context)
- Global TrustLinks (Trust Context)
- Global TrustLinks (other Context)

Personal Observation as Experience

Experience
Reputation
Global Opinion as Reputation

Direct Trust (Knowledge as Direct Observation)
- P: Reliability
- C: Serviceability (Maintainability)
- S: Safety

Knowledge

- P: Confidentiality
- C: Integrity
- S: Availability

P: Physical
C: Cyber
S: Social
Computational Trust

- **Computational Trust** (Trust Data Management – DIKW Process)
- Social Trust
- Direct Observation (Knowledge)
- System Dependability
- Direct Observation (Knowledge)

**Trust Data Management – DIKW Process**

- **ICT**
- **Computational Trust**
- **Direct Observation (Knowledge)**
- **Social Trust**
- **Experience**
- **Personal Observation**

**Trust**

- **Ability / Capability**
  - Stability
  - Reliability
  - Scalability
  - Safety
  - Robustness

- **Integrity / Honesty**
  - Completeness
  - Accuracy / Correctness
  - Consistency
  - Certainty
  - Recency

- **Benevolence / cooperative**
  - Assurance
  - Availability
  - Credibility
  - Relevance

**Reputation**

**Third Party Information**

**Direct Observation**

**System Dependability**
Key Design Principles

Consider Trust as a Key Component for IoT

- Interactions and relationships among Social/Cyber/Physical worlds
- Ensuring IoT data quality
- Trustable intelligent services based on data convergence and mining
- Trustworthy environment for correct operations
- Enhanced security and privacy
Challenges for Trust in general

1. Understanding of trust
2. Trust relationships
3. Trust management
4. Measure & calculate
5. Decision making
6. Autonomy
7. Constraint environment
8. T-SCPI architecture
9. New business models
10. Standardization

NOTE - T-SCPI: Trustworthy Social-Cyber-Physical Infrastructure

Gyu Myoung Lee, “Challenges for Trustworthy Social-Cyber-Physical Infrastructure,”
ITU Workshop on “Future Trust and Knowledge Infrastructure”, Phase 1, Apr. 2015.
Challenges for Trust in IoT

• Highly interconnected IoT infrastructure
  – A new kind of complex system
• Assuring continuous trustworthiness
  – Trust is situation-specific and trust changes over time
• Data transparency
  – Promote transparency about what data is collected and how it will be processed and handled
• Trust, security and privacy become tightly coupled
  – A unified approach towards trust, security and privacy co-analysis, design, implementation and verification
• The integration of the physical, cyber, and social worlds
  – Social-cyber-physical trust relationships
Technical Issues

• Identification of entities
• Trustworthy data collection and aggregation
• Trustworthy data process and analysis
• Trust modelling and measuring
• Trust computation and trust evaluation/validation
• Dissemination of trust information
• Trust establishment and provisioning
• Trustworthy system lifecycle management
Trust Relationship Model

Legend
- Virtual Social Object
- Cyber Object
- Virtual Physical Object

Individuals Communities
- Social-social Trust relationship
- Social-cyber Trust relationship
- Social-physical Trust relationship

Social Entities
- Cyber-cyber Trust relationship

Stakeholders
- Cyber Trust Component
- Physical Trust Component

Physical Things
Trust Computation Procedure

- **Data** → **Information** → **Knowledge** → **Wisdom**
  - **DIKW Pyramid**
  - **Awareness** → **Understanding** → **Belief** → **Decision**

- **Dependability**
  - High → Low

- **Decision Making**
  - **Reasoning Level of Trust**
  - **Building Trust Knowledge-base**
  - **Formalizing of Semantic Information**
  - **Collecting and Annotating Data**

- **Acquaintance of Trust** → **Trust Computation Processes**
Trust Index

Data from various sources

Trust Attributes
- Qualitative Attributes
- Quantitative Attributes

Trust Indicators
- Subjective Trust Indicators
- Objective Trust Indicators

Objectify
Calculate

Trust Index

Decision

Trustor

Operation
Trustworthy Smart City Crowdsensing

Smart Citizen – collective monitoring of the city

- Smart transportation, smart metering and public safety
  - Benefits to public, business and government
  - Ensuring Trustworthiness
A New Paradigm – Blockchain

“It is a machine for creating trust.”
(Source: The Economist)

• The currency in the IoT is data.
• Revolutionizes how transactions are recorded
  – a decentralized digital ledger that records transactions
  – building trust, reducing costs and accelerating transactions
"Trust is the oxygen which will breathe life into the IoT. Industry needs to show data is safe and that it is properly treated." (source: www.techuk.org.)

Trust is an essential element for value added business models in the IoT.