Two waves of concern about trust

- Frequency of word “trust” appearing in published books;
- Generated by using Google ngram viewer
“On the Internet, nobody knows you’re a dog.”
-- Peter Steiner

“On the Internet, everyone can tell you’re a dog, but nobody knows whether you’re likely to bite.”
-- David Nicol
Cybersecurity and Trust

- Trust is a necessary component of cybersecurity
  - In cyberspace, **one party typically relies on other parties** w.r.t. security, privacy, trustworthiness of information, and trustworthiness of services.
  - When a party needs to “trust” others, this “trust” frequently becomes a vulnerability.
  - To mitigate this vulnerability, we must handle trust in a scientific way.
- Towards *Science of Security*, we are aiming at developing a computational theory of trust.

Overarching Research Questions

- “Trust” has been intensively used in Internet-based systems and applications. But,
  - What does trust mean precisely?
  - What properties does trust have?
  - How should we quantify trust and reason about trust?
  - What are mechanisms to facilitate trust in a decentralized open network?
• Introduction
• **Conceptualization of trust**
• Formal semantics of trust
• Calculus of trust
  – Quantification of trust
  – Trust propagation in network
  – Evidence-based trust reasoning
  – Trust-based decision making
• Trust in PKIs
• Trust in Cloud Computing
• Future Research Perspectives
What is trust? (1)

- Oxford dictionary: "firm belief in the reliability, truth, ability, or strength of someone or something".

- Deutsch (1962) defined trust as confidence on a trusting choice possibly leading to either a beneficial outcome or a harmful outcome of higher strength, which outcome occurs dependent on the behavior of the trusted individual.
  
  A trusting choice maybe based upon:
  - "confidence" – most common case, also most relevant
  - "conformity" / "virtue" – associated with social mechanisms
  - "innocence", "faith", "despair", "gambling", ...
    -- blind / irrational

What is trust? (2)

- Rotter (1967): “an expectancy held by an individual or a group that the word, promise, verbal or written statement of another individual or group can be relied on.”

- Luhmann (1979): “confidence in one’s expectations”

- Zucker (1986): Economists’ view -- “implicit contracting”

- Gambetta (1988): Trust is a subject probability. Trust is fragile due to limited knowledge and foresight, and uncertainty of trustee’s behaviors.

- Fukuyama (1995): “trust is the expectation that arises within a community of regular, honest, and cooperative behavior, based on commonly shared norms”
What is trust? (3)

• Mayer et al. (1995): “the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party”.

• Rousseau et al. (1998): “Trust, as the willingness to be vulnerable under condition of risk and interdependence, is a psychological state”.

Our view of trust

• Trust is a mental state, consisting of:
  — Expectation, trustor expects a specific thing from trustee;
  — Belief in that expectation, based on evidence of competence, goodwill, and integrity;
  — Willingness to take risk for that belief.

• Key features
  — Trusted party is out of trustor’s control
  — Trusted party’s behavior is predictable, based on some evidence
  — Trust is associated with risk and uncertainties
  — Trust is context-dependent
Outline

• Introduction
• Conceptualization of trust
• Formal semantics of trust
• Calculus of trust
  – Quantification of trust
  – Trust propagation in network
  – Evidence-based trust reasoning
  – Trust-based decision making
• Trust in PKIs
• Trust in Cloud Computing
• Future Research Perspectives

Formal Semantics of Trust

• A formal semantics of trust is defined as ontology [Huang&Fox2006, Huang2007],
  – Using logical language of Situation Calculus.
  – An ontology is a shared, explicit and formal specification of concepts.
• Further development: a modal logic model of trust (KD45-T) [Huang etal 2013]
  – Define semantics of trust, based on KD45
  – KD45 is a modal logic system for belief [Fagin etal 1995]
Two Basic Types of Trust

By different expectancy, two fundamental types of trust can be identified:

- **Trust in performance**
  - Trust what trustee performs in a context
  - e.g. trust ftd.com to deliver a bouquet as ordered.

- **Trust in belief**
  - Trust what trustee believes in a context
  - e.g. trust the opinion of a wine expert regarding the quality of wine products

Epistemic Logic

- Kripke (1962) structure and “Possible World Semantics”

  \[ M = (\mathbb{S}, \pi, R_1, R_2, \ldots, R_n) \]
  \[ \pi : \mathbb{S} \rightarrow (\Phi \rightarrow \{\text{true, false}\}) \]
  \[ R_i \subseteq \mathbb{S} \times \mathbb{S} \]

  \[ (M, s) \models K_i \varphi \iff (M, t) \models \varphi, \text{ for all } t \text{ such that } (s, t) \in R_i \]

- S5 – logic system for knowledge
  - Axiom P: all propositional tautologies;
  - Axiom K: \( K_i (p \supset q) \supset (K_i p \supset K_i q) \)
  - Rule MP (Modus Ponens)
  - Rule N (Necessitation): if \( \vdash p \), then \( \vdash K_i p \)
  - Axiom T: \( K_i p \supset p \)
  - Axiom 4 (Positive Introspection): \( K_i p \supset K_i K_i p \)
  - Axiom 5 (Negative Introspection): \( K_i p \supset K_i \neg K_i p \)

- KD45 – logic system for belief
  - Knowledge must be true; belief may not.
  - S5 without axiom T, plus axiom D
  - Axiom D: \( \neg B_i (p \land \neg p) \)

- KD45 is sound and complete w.r.t. its Kripke semantics structure.
  [Halpern and Moses 1992]
KD45-T: Axioms and Rules

• **Axiom 1:** $T_{i,j}^b \varphi \equiv B_j \varphi \supset B_i \varphi$.
• **Axiom 2:** $T_{i,j}^p \tau(p) \equiv \text{made}_j(p) \supset B_i \tau(p)$.
• **Axiom 3:** $\kappa B_i \varphi \equiv B_i \kappa \supset B_i \varphi$.
• **Axiom 4:** $\kappa T_{i,j}^b \varphi \equiv \kappa B_j \varphi \supset \kappa B_i \varphi$.
• **Axiom 5:** $\tau(c) T_{i,j}^b \tau(p) \equiv \text{made}_j(p, c) \supset \tau(c) B_i \tau(p)$.
• **Rule 1:** $\text{if } \vdash B_i B_i \varphi, \text{ then } \vdash B_i \varphi$.
• **Rule 2:** $\text{if } \vdash B_i (\kappa B_i \varphi), \text{ then } \vdash \kappa B_i \varphi$.
• **Rule 3:** $\text{if } \vdash B_i (\kappa T_{i,j}^b \varphi) \text{ and } \vdash B_i (\kappa B_j \varphi), \text{ then } \vdash \kappa B_i \varphi$.
• **Rule 4:** $\text{if } \vdash B_i (\tau(c) T_{i,j}^p \tau(p)) \text{ and } \vdash B_i \text{made}_j(p, c), \text{ then } \vdash \tau(c) B_i \tau(p)$.
• **Rule 5:** $\text{if } \vdash B_i (\kappa T_{i,j}^b \varphi) \text{ and } \vdash B_i (\kappa T_{j,k}^b \varphi), \text{ then } \vdash B_i (\kappa T_{i,k}^b \varphi)$.
• **Rule 6:** $\text{if } \vdash B_i (\tau(c) T_{i,j}^b \tau(p)) \text{ and } \vdash B_i (\tau(c) T_{j,k}^p \tau(p)), \text{ then } \vdash B_i (\tau(c) T_{i,k}^p \tau(p))$.

Properties

• KD-45-T is sound and complete w.r.t. its Kripke semantics structure.
• **Trust-in-belief relation is transitive**
  \[ \kappa T_{i,j}^b \varphi \land \kappa T_{j,k}^b \varphi \supset \kappa T_{i,k}^b \varphi; \]
• **Trust-in-performance relation is propagatable through trust-in-belief relation**
  \[ \kappa T_{i,j}^b \varphi \land \kappa T_{j,k}^p \varphi \supset \kappa T_{i,k}^p \varphi. \]
Trust Propagates in Trust Networks

- A Trust Network is a subset of a social network, consisting of trust relations.
  - Agent i believes a trust relation – e.g. $B_i(\kappa T^{b}_{j,k} \varphi)$
  - Agent i holds a trust relation – e.g. $B_i(\kappa T^{b}_{i,j} \varphi)$

- Reasoning about trust relations
  
  \[ B_i(\kappa T^{b}_{i,j} \varphi) \land B_i(\kappa T^{b}_{j,k} \varphi) \supset B_i(\kappa T^{b}_{i,k} \varphi) \]
  
  \[ B_i(\kappa T^{b}_{i,j} \varphi) \land B_i(\kappa T^{p}_{j,k} \varphi) \supset B_i(\kappa T^{p}_{i,k} \varphi) \]

- Reasoning about beliefs in others’ trust relations, by rule 3
  
  \[ B_i B_j(\kappa T^{b}_{j,k} \varphi) \land B_i(T^{b}_{i,j}(\kappa T^{b}_{j,k} \varphi)) \supset B_i(\kappa T^{b}_{j,k} \varphi) \]

Is Trust Transitive or Not?

- Argument of Christianson&Harbison (1997)
- “i trusts j” is defined as conjunction of
  - “if i believes j says x, then i believes j believes x”
    - Called “trust in honesty”
  - “if i believes j believes x, then i believes x”
    - Called “trust in competence”
  - A simplified definition from BAN logic [BAN1990].

- Given agent i believes that
  “i trusts j” and “j trust k” and “k says x”,
  try to prove: “i believes x” (thus “i trusts k”)

- Since there is no way to prove “i believes j says x”,
  the target goal cannot be proved.
Is Trust Transitive or Not? (2)

- The definitions of trust matters
- Difference in definitions
  - “trust in competence”: $B_i B_j X \rightarrow B_i X$
  - In KD45-T:
    - Agent $i$ holds “trust in belief” relation, $B_i (B_j X \rightarrow B_i X)$
    - $B_i B_j X \rightarrow B_i X$ is derivable from $B_i (B_j X \rightarrow B_i X)$!
    - Separate trust relation (real logical relation of trust) from holding a trust relation;
    - Discern trust-in-belief ($B_j X \rightarrow B_i X$) and trust-in-performance ($m_{ade}(p) \rightarrow B_i \tau(p)$, $X=\tau(p)$)
    - “trust in honesty” is not generally true, so not an axiom.
  - Better explanation of what is “transitive trust” and why trust propagates in social networks.

Key Points

- Trust = Expectation
  + belief in the expectation
  + willingness to take risk for that belief
- Trust-in-belief relation is transitive
- Trust-in-performance relation is propagatable through trust-in-belief relation

J. Huang, M. Fox, M. Gruninger (2013), A formal semantics of trust, EIL research paper, University of Toronto.
Outline

• Introduction
• Conceptualization of trust
• Formal semantics of trust
  • Calculus of trust
    – Quantification of trust
    – Trust propagation in network
    – Evidence-based trust reasoning
    – Trust-based decision making
• Trust in PKIs
• Trust in Cloud Computing
• Future Research Perspectives

Formal-Semantics-based Calculus of Trust

• Trust has uncertainty
• We developed an uncertain trust model,
  – to quantify trust, characterizing uncertainties in trust
  – to calculate trust
• Based on a simplified version of formal semantics
  – Simplifies notation
  – The obtained results remain true for the full version of logic model.
Trust Notation

- **trust in belief**: $\text{trust}_b(d,e,x,k)$
  - “Trustor $d$ trusts trustee $e$ on trustee’s belief $x$ in context $k$”
  
  $\text{trust}_b(d,e,x,k) \iff (\text{believe}(e,k \sim x) \rightarrow \text{believe}(d, k \sim x))$

- **trust in performance**: $\text{trust}_p(d,e,x,k)$
  - “Trustor $d$ trusts trustee $e$ on a thing $x$ made by $e$ in context $k$”
  
  $\text{trust}_p(d,e,x,k) \iff (\text{madeBy}(x,e,k) \rightarrow \text{believe}(d, k \sim x))$

Formal Semantics of Uncertainty in Trust

- Using probability logic [Hajek, 2001], we define:
  - Degree of trust in performance
    
    $\text{td}_p(d,e,x,k) = \text{pr} (\text{believe}(d,x) | \text{madeBy}(x,e,k) \& \text{beTrue}(k))$

    The sample space based on history of interactions

  - Degree of trust in belief
    
    $\text{td}_b(d,e,x,k) = \text{pr} (\text{believe}(d,x) | \text{believe}(e,x) \& \text{beTrue}(k))$

  - Degree of distrust defined similarly
Quantify Trust

• Trust degree is measured by the fraction of successful encounters
  \[ td = \frac{n}{m}, \quad dtd = \frac{l}{m}; \quad n + l \leq m \]
  \[ m \] – total number of interactions
  \[ n \] – number of interactions with positive outcomes;
  \[ l \] – number of interactions with negative outcomes;
  \[ (m - n - l) \] number of interactions with unknown outcomes.

  \[ utd = \frac{(m - n - l)}{m} = 1 - td - dtd \]

• General form
  \[ td = \frac{\sum_{i=1,\ldots,m} ep(i)}{m}, \]
  \[ dtd = \frac{\sum_{i=1,\ldots,m} en(i)}{m} \]

Quantify Trust (2)

• Not all encounters need to yield ‘positive’ or ‘negative’ as result
• Cognitively there are three mental states:
  – believed
  – disbeliefed
  – Undecidable/unknown.
• We model multiple sources of uncertainty:
  – Randomness
  – incomplete information
• Uncertainty is represented as probability distribution
  \((td, dtd, ud)\) or simply \((td, dtd)\).
Outline

• Introduction
• Conceptualization of trust
• Formal semantics of trust
• Calculus of trust
  — Quantification of trust
  — Trust propagation in network
  — Evidence-based trust reasoning
  — Trust-based decision making
• Trust in PKIs
• Trust in Cloud Computing
• Future Research Perspectives

Trust Calculation in Trust Networks

• A trust network is a directed graph, comprising a set of nodes – entities, and edges – trust relationships
  — A subset of a social network

• Calculation of trust from a trustor to a trustee though trusted friends in a network?

• Two basic operators:
  — Sequence aggregation: to aggregate trust in a chain
  — Parallel aggregation: to aggregate trust in parallel structure
Sequence Aggregation

When \( a \) trusts \( b \) (in belief), and \( b \) trusts \( c \) (in either belief or performance), how much does \( a \) trust \( c \)?

For simpler notation, we omit subscripts \( b \) (for trust in belief) and \( p \) (for trust in performance).

From the formal definitions, we derived and proved a theorem:

1. \( td(a,c) = td(a,b) \cdot td(b,c) + dtd(a,b) \cdot dtd(b,c) \)
2. \( dtd(a,c) = td(a,b) \cdot dtd(b,c) + dtd(a,b) \cdot td(b,c) \)
3. Let \( cd = td + dtd \), then \( cd(a,c) = cd(a,b) \cdot cd(b,c) \)

cd is “degree of certainty”

Parallel Aggregation

- Combine independent trust paths.
- Use sequence aggregation on paths.
  e.g. \( td(a,bi,c) = td(a,bi) \cdot td(bi,c) + dtd(a,bi) \cdot dtd(bi,c) \)
- Aggregated trust degree of trust weighted average
  e.g. aggregated trust from \( a \) to \( c \),
  \[
  td(a,c)' = \frac{[m(a,c) \cdot td(a,c)] + m(b1,c) \cdot td(a,b1,c) + \ldots + m(bn,c) \cdot td(a,bn,c)]}{[m(a,c) + m(b1,c) + \ldots + m(bn,c)]}
  \]
- Path weight proportional to # encounters
Trust Evaluation in Hierarchical PKI

- Chain of trust:
  Alice – CA3 – CA1 – CA2 - CA4
  \[ t_{\text{chain}}^b(A, CA3, pk\_validity) = (1, 0, 0) \]
  \[ t_{\text{chain}}^b(CA3, CA1, pk\_validity) = (0.98, 0.01, 0.01) \]
  \[ t_{\text{chain}}^b(CA1, CA2, pk\_validity) = (0.92, 0.02, 0.06) \]
  \[ t_{\text{chain}}^p(CA2, CA4, pk\_validity) = (0.96, 0.01, 0.03) \]

- By sequence aggregation
  \[ t_{\text{sequence}}^b(A, CA4, pk\_validity) = (0.866, 0.037, 0.097) \]

Trust Evaluation in Web PKI

- Multiple chains of trust exist
  1. Alice-CA3-CA1-CA2-CA4
  2. Alice-CA3-CA5-CA4

- Assume path 1 the same as before
  \[ t_{\text{path}}^b(A, CA4, pk\_validity) = (0.866, 0.037, 0.097) \]

- Assume path 2:
  \[ t_{\text{path}}^b(CA3, CA5, pk\_validity) = (0.65, 0.35, 0.1) \]
  \[ t_{\text{path}}^b(CA5, CA4, pk\_validity) = (0.75, 0.00, 0.25) \]
  then
  \[ t_{\text{path}}^b(A, CA4, pk\_validity) = (0.488, 0.188, 0.324) \]

- For using one-path certification, the shortest certification path may not be the most trustworthy path;
- In practice, if the shortest path has an unacceptable level of trust, another path with high enough level of trust needs to be found
Risk in Multiple Independent Trust Paths

- If use multiple independent paths for certification, What is the risk level?
- Assume path $i$ having aggregated trust level $(td_i, dtd_i, ud_i)$
- Let $p_i$ be the probability of certification path $i$ being valid, then

$$td_i \leq p_i \leq td_i + ud_i.$$ 

- The probability of at least one of $n$ paths being valid will be:

$$p = 1 - \prod_{i=1}^{n} (1 - p_i)$$

$$1 - \prod_{i=1}^{n} (1 - td_i) \leq p \leq 1 - \prod_{i=1}^{n} (1 - (td_i + ud_i)).$$

- So, the probability of multiple independent certification paths being compromised, $1-p$, decreases exponentially
- In general, multiple independent trust paths significantly increase trustworthiness and certainty

Example

- By path-1: CA3-CA1-CA2-CA4
  $tr^b(\text{CA3,CA4,pk.validity}) = (0.866, 0.037, 0.097)$
  The probability of path-1 being valid, $p_1$ in $[0.866, 0.963]$
  $0.963 = td + ud = 0.866 + 0.097$

- By path-2: CA3-CA5-CA4
  $tr^b(\text{CA3,CA4,pk.validity}) = (0.488, 0.188, 0.324)$
  The probability of path-2 being valid, $p_2$ in $[0.488, 0.812]$

- Evaluate the probability ($p$) of at least one path being valid:
  lower bound: $1-(1-0.866)(1-0.488) = 0.931$
  upper bound: $1-(1-0.963)(1-0.812) = 0.993$
  so, $p$ in $[0.931, 0.993]$, which is much more certain and trustworthy than any single-path validation, $[0.866, 0.963]$ and $[0.488, 0.812]$. 
Outline

• Introduction
• Conceptualization of trust
• Formal semantics of trust
• Calculus of trust
  – Quantification of trust
  – Trust propagation in network
  – Evidence-based trust reasoning
  – Trust-based decision making
• Trust in PKIs
• Trust in Cloud Computing
• Future Research Perspectives

Evidence-Based Trust Reasoning

• Use “trust in privacy protection in cloud computing”, as driving application
• Warren & Brandeis (1890) gave the first concept of privacy -- “right to be alone”, when addressing privacy threat posed by portable cameras.
• Westin (1967): Privacy is “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others”.
• What’s your expectation on cloud privacy?
• Domain of Expectation, about how a cloud service provider handles cloud users’ data, extending Solove’s taxonomy of privacy
  – Data collection
  – Data usage
  – Data guarding
  – Data situation informing
  – Data dissemination
  – Data termination and disposal.
Inferring Belief from Evidence

User's Expectation Space

Belief in service provider will do as expected on a specific item
Belief in ability to do so
Belief in intention to do so
Belief in consistency to do so

Evidence-based Trust Reasoning on X

Evidence Space

Promising (policy, ToS)
Transparency (CIA’s programs)
Privacy Cert
Security Cert
Business Scale
Depo
Audit reports
Utility Complaints

Service provider's efforts to gain trust
Domain of actions and observation

Extended Belief Networks

• Evidence is incomplete and uncertain
• Need to address this type of uncertainty
• Extend BN model to accommodate this need.

\[
\begin{align*}
pr(C|R, SIH) &= \min\{pr(C|R, SIH), pr(C|R, \neg SIH)\} \\
pr(\neg C|R, SIH) &= \min\{pr(\neg C|R, SIH), pr(\neg C|R, \neg SIH)\} \\
pr(C|R, \neg SIH) &= 1 - pr(C|R, SIH) - pr(\neg C|R, SIH).
\end{align*}
\]

\[
\min\{pr(C|R, SIH), pr(C|R, \neg SIH)\} \leq pr(C|R) \leq \max\{pr(C|R, SIH), pr(C|R, \neg SIH)\}
\]
Key Points

- Trust degree decreases exponentially along a chain a trust;
- Multiple independent trust paths significantly increase trustworthiness and certainty (uncertainty decreases exponentially).
- Trust can be derived from evidence of CIA (ability, intention, consistency).

J. Huang and D. Nicol (2009), A calculus of trust and its application in PKI and identity management, IdTrust’09, pp.23-37, ACM-DL
http://dl.acm.org/citation.cfm?id=1527017.1527021

http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=5477411

J. Huang and D. M. Nicol. Evidence-Based Trust Reasoning, HotSoS'2014

Outline

- Introduction
- Conceptualization of trust
- Formal semantics of trust
- Calculus of trust
  - Quantification of trust
  - Trust propagation in network
  - Evidence-based trust reasoning
    - Trust-based decision making
- Trust in PKIs
- Trust in Cloud Computing
- Future Research Perspectives
Trust-based Decision Making

Outline

• Introduction
• Conceptualization of trust
• Formal semantics of trust
• Calculus of trust
  – Quantification of trust
  – Trust propagation in network
  – Evidence-based trust reasoning
  – Trust-based decision making

• Trust in PKIs
• Trust in Cloud Computing
• Future Research Perspectives
PKI Trust: Scenario

Questions

- Any problem with this chain of validation?
- Is this chain of key certs sufficient to allow Alice to believe Bob’s public key being Kb?
What does a key cert say?

- IETF RFC 5280, IETF3647, ...
- Key cert structure
  - Basic: \{Id, K\}
  - “extension” fields
    - Certification policy (CP)
    - Policy mapping
    - Key usage
    - ...
- Types of key certs
  - End entity certs, issued to end users
  - CA certs, issued to CAs
    - End CA certs, issued to CAs only issuing end-entity certs
    - Full CA certs, issued to CAs issuing CA certs

PKI Trust Examination: Implicit Trust

- Semantics of key certs
  1. Assertion of binding key with Id;
  2. The assertion is made under the technical and management standards specified in the CP;
  3. (for CA certs) trust subject CA conforming to the specified CP;
  4. (for full CA certs) trust subject CA’s belief that downstream CAs conforms to the CP;
  5. (for full CA certs) trust subject CA’s performance on policy comparing and equivalence assertion;
  6. (for full CA certs) trust subject CA’s belief on policy equivalence assertions in downstream.

- Implicit trust / assumptions
  - 3 is never specified in IETF RFCs
  - 4,5,6 is implicitly assumed in “certification path validation logic”
Trust Mechanism used in PKIs

- Certification Authorities as intermediated entities in a trust path;

- **Policy based trust**
  - If a CA conforms to a trusted policy, then this CA’s operations are secure;
  - If a CA conforms to a trusted policy, then this CA’s key cert can be believed;
  - If a CA conforms to a trusted policy, then this CA’s assertion that this policy is equivalent to another policy can be believed.

- Rich semantics of certificates
  - Trust relations need to be specified explicitly

---

Policy-based trust:
believe a CA conforms to policy P, then trust the CA w.r.t. issuing valid key certs

A simplified view of policy-based trust reasoning
Outline

- Introduction
- Conceptualization of trust
- Formal semantics of trust
- Calculus of trust
  - Quantification of trust
  - Trust propagation in network
  - Evidence-based trust reasoning
  - Trust-based decision making
- Trust in PKIs
- Trust in Cloud Computing
- Future Research Perspectives

Trust Mechanisms for Cloud Computing

- Reputation-based trust
- SLA verification based trust
- Cloud transparency mechanisms (CSA’s STAR)
  - Cloud Controls Matrix (CCM)
  - Consensus Assessments Initiative Questionnaire (CAIQ)
  - CloudTrust Protocol (CTP)
- Trust as a service
  - RSA: Cloud Trust Authority (CTA)
- Formal accreditation, audit, and standards
  - ISO/IEC 27000 (intnl. information security management standard)
  - ISSE16 / SAS70; ISAE3402 (Int. Standard on Assurance Engagements)
- Evidence-based trust
- Policy-based trust
Trust Chains in cloud


Concerned Attributes of Trustworthiness

- Resilience
- Confidentiality
- Integrity
- Privacy
- Safety
- Maintainability
- Availability
- Reliability

Malicious attacks
Non-malicious faults
A New Great Wave of Computing

- Future Internet
  - Internet of Things
  - Internet of Information
  - Internet of People
  - Internet of Services

- Big Data

An Integrated Cyber-Physical World

- Future Internet will lead to numerous novel Cyber-Physical-Human Smart Systems,
  - e.g. smart manufacturing, smart supply chain, smart hospitals, smart homes, smart cities
- Security, privacy, and trust will be critical success factors for novel CPH smart system applications.
Challenging Issues

- Smart things and systems “know” their users much more than traditional products.
- The collection of big data from different sources poses great privacy, security, and safety issues.
- How will the society accommodate the new technologies?
  - Emerged new technologies frequently challenge the boundary of privacy, ...
  - New social norms, rules, laws ...
- We need extend/revise existing trust mechanisms and invent new trust mechanisms for a secure & trustworthy Cyber-Physical-Human smart society?

Challenging Issues

- Many different stakeholders involved in a smart product; each has their policies on security, privacy, intellectual rights, business interests, ...
  - E.g. end-users; service provider; manufacturers and designers of the product and its components
- What trust management mechanisms we can use for representing, reasoning, negotiating, validating the policies, respecting each party’s rights?
- How do we evaluate the trustworthiness of a complex smart system?
  - A complex smart product consisting of a large number of smart components, e.g. airplane
Building Trust for Future Internet Society

- In Future Internet society, entities will further rely on other parties with respect to privacy, security, safety, trustworthiness of information and trustworthiness of services.
- It is critical
  - to understand those trust assumptions explicitly;
  - to manage trust in a scientific way;
  - to create new societal and technical trust mechanisms for facilitating a better Cyber-Physical-Human Smart Planet.

Questions?
jingwei@illinois.edu
References

- F. B. SCHNEIDER. 2013. "Blueprint for a Science of Cyber-security". Talk at UIUC.