Evidence-Based Trust Reasoning

Jingwei Huang and David M. Nicol

ENGINEERING AT ILLINOIS
INFORMATIONTRUST INSTITUTE

TRUST AND CYBERSECURITY

- Trust is a necessary component for cybersecurity.
- In cyberspace, entities rely on each other w.r.t. security, privacy, trustworthiness of services, and trustworthiness of information.
- When a party needs to "trust" another in an interaction this "trust" frequently becomes a vulnerability.
- To mitigate this vulnerability, we need to understand that trust and handle it in a scientific way.
- **Objective**: develop evidence-based trust reasoning, as a part for developing computational theory of trust.
- Use cloud privacy as a driving application.

WHAT IS TRUST?

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

CIA TRIAD OF TRUST EVIDENCE

- Identify visible aspects for evidence
  - **Consistency (C)**, for integrity, including behavior history, compliance to standards;
  - **Intension (I),** for goodwill, -- e.g. readability of terms;
  - **Ability (A),** equivalent to competence.

EVIDENCE-BASED TRUST REASONING

- Identify expectation space
- Identify evidence space
- Use Belief Networks for inferring beliefs in expectation from available pieces of evidence through CIA triad

$$pr(S_k|E_1 \wedge E_2 \ldots \wedge E_m) = \sum_{c_k, i_k, a_k, e_{m+1}, \ldots, e_n} (pr(S_k|c_k, i_k, a_k) \times pr(c_k|E_1 \wedge \ldots \wedge E_m, e_{m+1}, \ldots, e_n) \times pr(i_k|E_1 \wedge \ldots \wedge E_m, e_{m+1}, \ldots, e_n) \times pr(a_k|E_1 \wedge \ldots \wedge E_m, e_{m+1}, \ldots, e_n) \times pr(E_1 \wedge \ldots \wedge E_m, e_{m+1}, \ldots, e_n)),$$

EXTENDED BELIEF NETWORKS

- Evidence is incomplete and uncertain
- Need to consider uncertainty due to incomplete information
- Extend BN model to accommodate this need
- Each node (variable) has three truth values:
  true (T), false(F), unknown(U)
- Belief distribution over T, F, U
- Equivalent to an interval of belief degrees
- Construct extended BN from traditional BN

$$pr(C|R, ?SIH) = min\{pr(C|R, SIH), pr(C|R, \neg SIH)\}$$
$$pr(\neg C|R, ?SIH) = min\{pr(\neg C|R, SIH), pr(\neg C|R, \neg SIH)\}$$
$$pr(?C|R, ?SIH) = 1 - pr(C|R, ?SIH) - pr(\neg C|R, ?SIH).$$

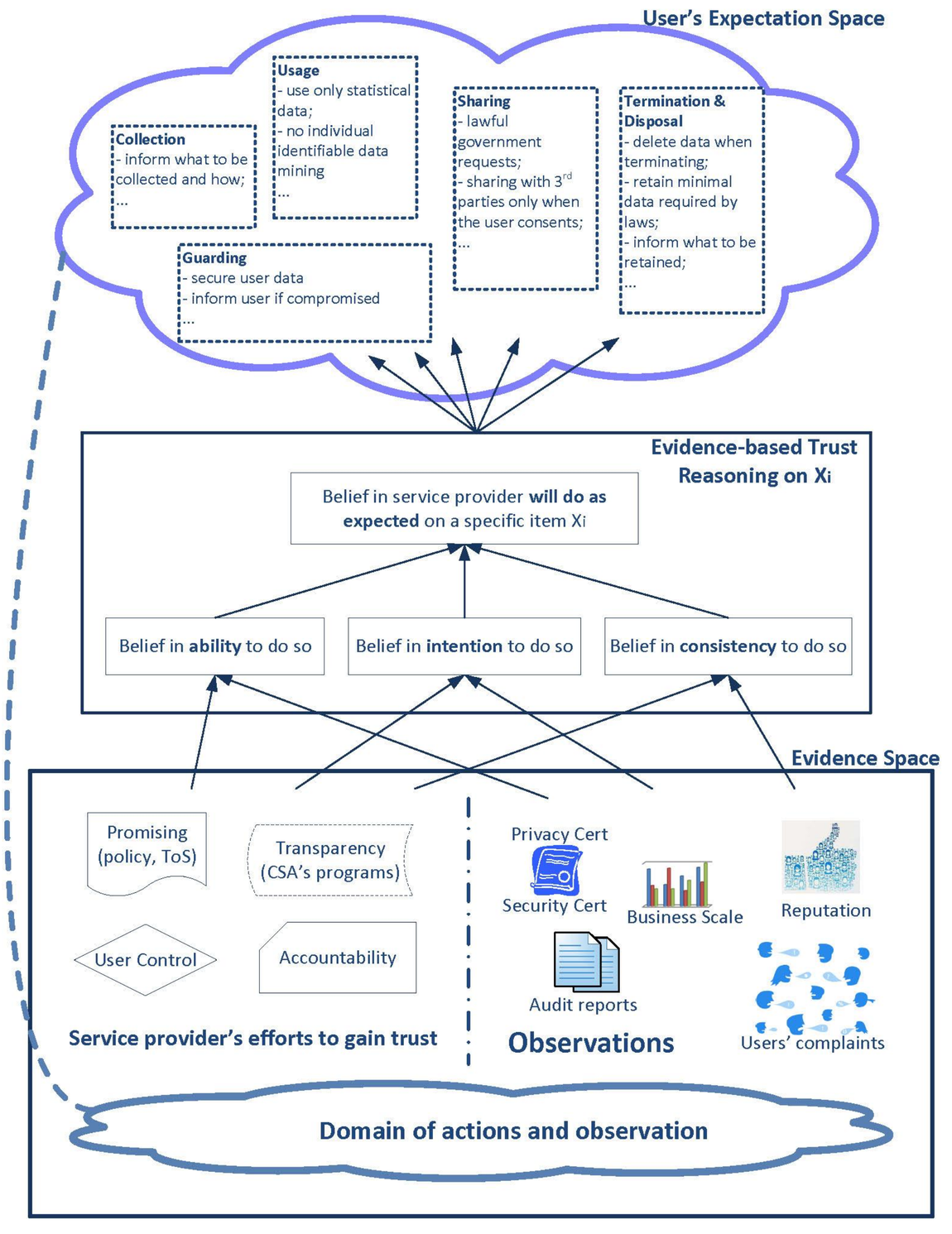
REFERENCES

J. Huang and D. Nicol, Evidence-based trust reasoning on privacy protection in cloud computing, 2014.
J. Huang and D. Nicol, A formal-semantics-based calculus of trust, IEEE IC, 2010

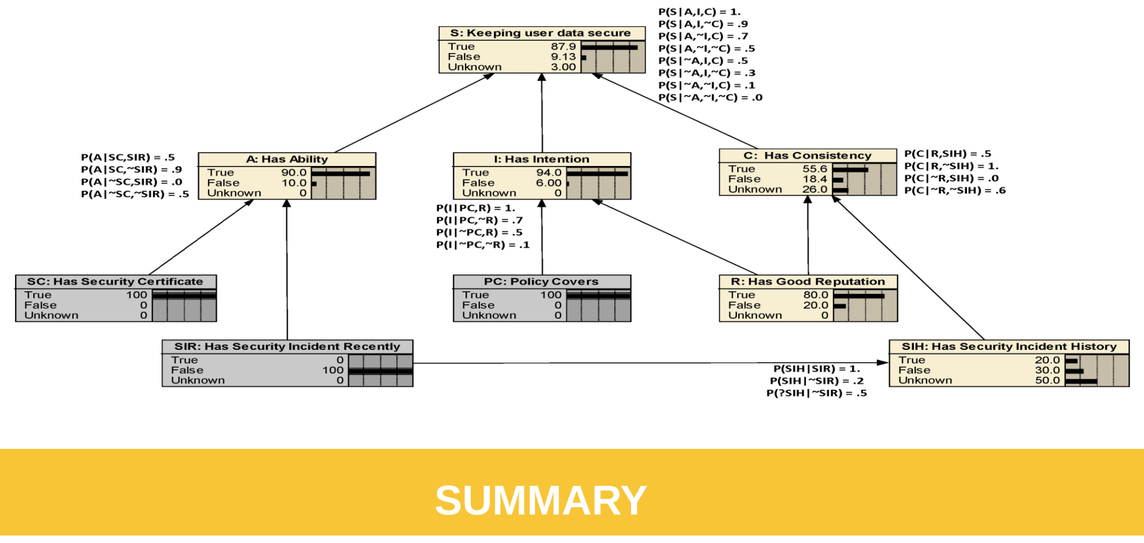
EXPECTATION ON CLOUD PRIVACY PROTECTION

- **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" (Westin 1967)
- Extend Solove's taxonomy of privacy (2006) into the context of Cloud Computing,
- Construct **domain of expectation** (or Expectation Space)

A FRAMEWORK



EXAMPLE



SUMMARY

- With respect to Science of Security, we are aiming at developing a computational theory of trust.
- We constructed a framework for evidence-based trust reasoning, using extended Belief Networks.
- A new component to our formal-semantics-based calculus of trust (2010), to enable inferring trust from evidence.