Evidence-Based Trust Reasoning

Jingwei Huang and David Nicol (UIUC)

- Trust is a necessary component of cybersecurity
- When a party needs to “trust” others, this **“trust” frequently becomes a vulnerability**.
- To mitigate this vulnerability, we must handle that trust in a scientific way.

What is trust?

- Many definitions …
- Trust is defined as 3 elements:
  - **Expectation**, trustor expects a specific thing from trustee
  - **Belief** in that expectation
  - **Willingness to take risk** for that belief.

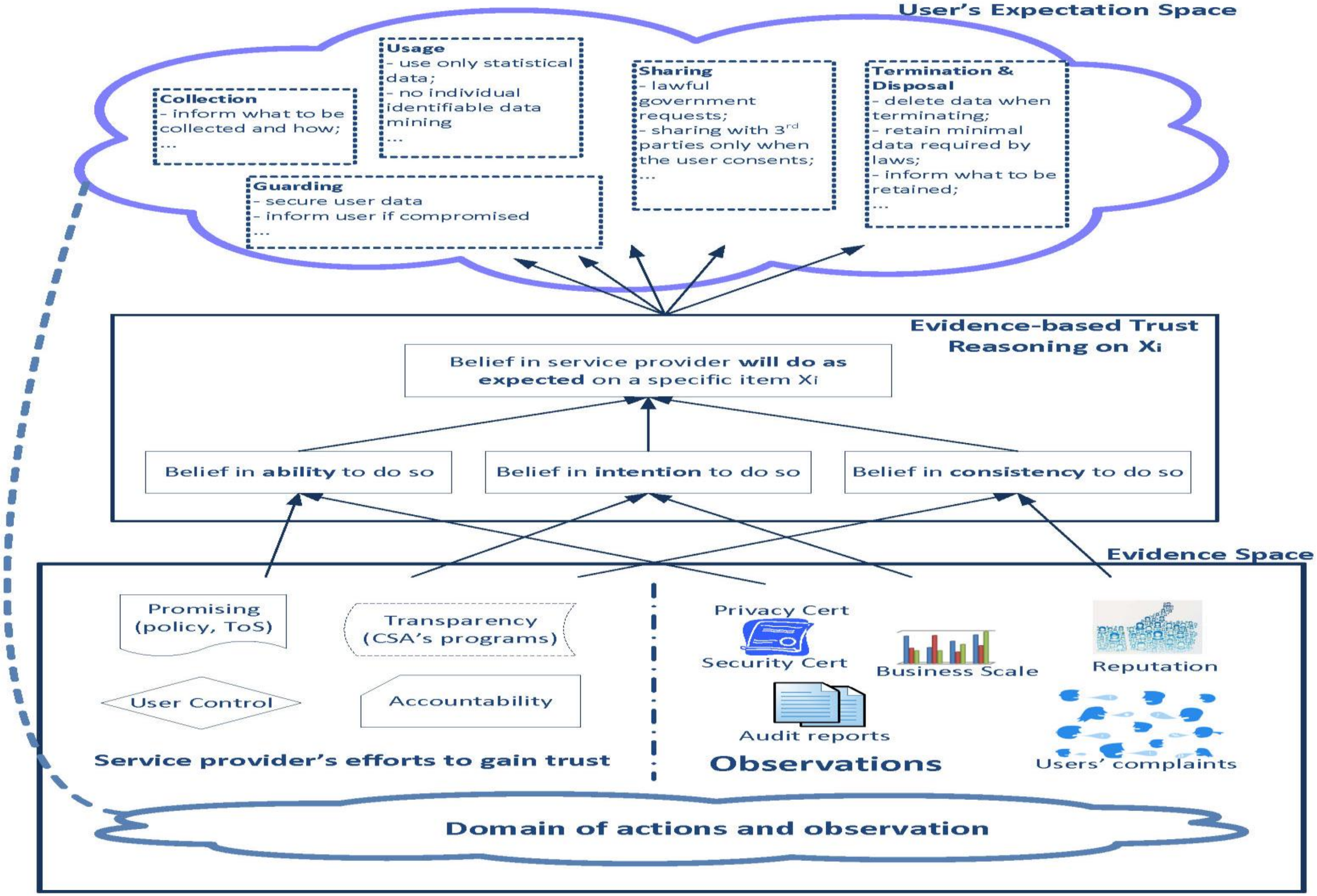
- Belief is based on evidence about trustee on
  - **Consistency (C)** -> integrity
  - **Intension (I)** -> goodwill
  - **Ability (A),** or competence

(CIA triad of trust evidence)

What’s your **Expectation** on cloud privacy?

- Trust in privacy protection in cloud computing
- [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”.
- **Domain of Expectation**, about how a cloud service provider handles cloud users’ data
  - Data collection
  - Data usage
  - Data guarding
  - Data situation informing
  - Data dissemination
  - Data termination and disposal.

Inferring Belief from Evidence



User's Expectation Space

Collection
- inform what to be collected and how;
...

Usage
- use only statistical data;
- no individual identifiable data mining
...

Sharing
- lawful government requests;
- sharing with 3rd parties only when the user consents;
...

Termination & Disposal
- delete data when terminating;
- retain minimal data required by laws;
- inform what to be retained;
...

Guarding
- secure user data
- inform user if compromised
...

Evidence-based Trust Reasoning on Xi

Belief in service provider **will do as expected** on a specific item Xi

Belief in **ability** to do so

Belief in **intention** to do so

Belief in **consistency** to do so

Evidence Space

Promising (policy, ToS)

Transparency (CSA's programs)

User Control

Accountability

Service provider's efforts to gain trust

Privacy Cert

Security Cert

Business Scale

Reputation

Audit reports

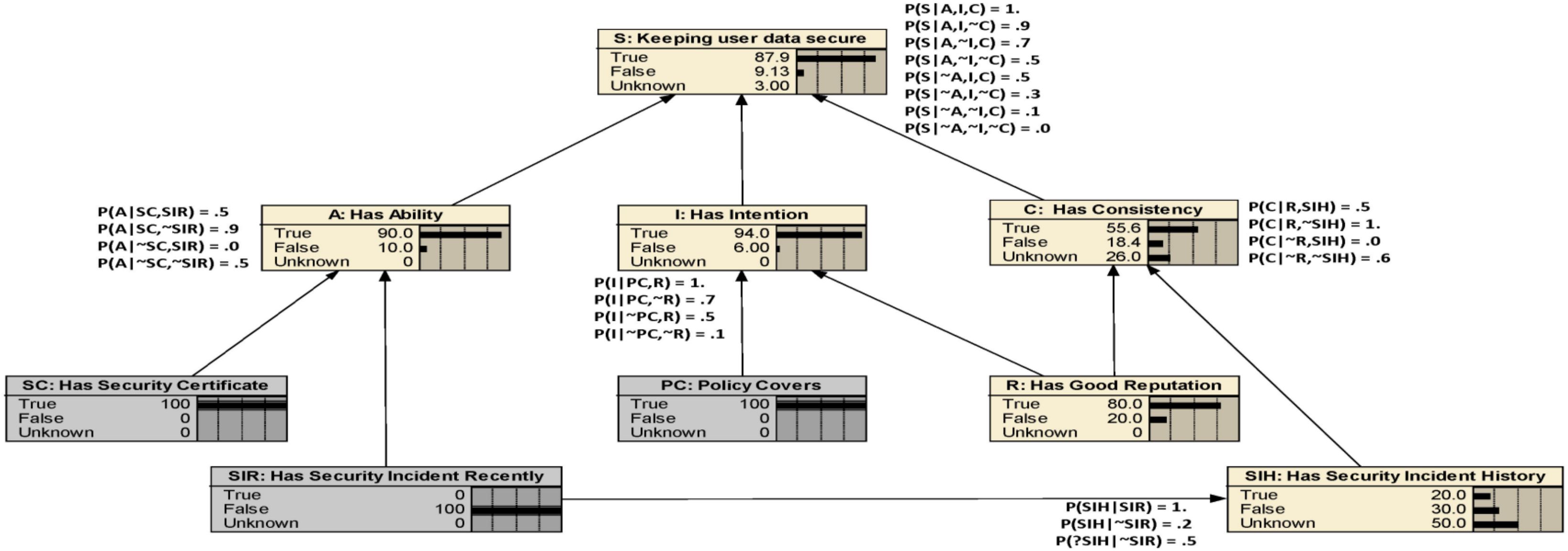
Users' complaints

Observations

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.



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

$$min\{pr(C|R,SIH), pr(C|R,\neg SIH)\} \leq pr(C|R) \leq max\{pr(C|R,SIH), pr(C|R,\neg SIH)\}$$

Summary

- We constructed a framework for evidence-based trust reasoning
- A new component of our formal-semantics-based calculus of trust
- An effort for building a computational theory of trust, towards Science of Security.

Please stop by and discuss :-)

Thank you!