

IdTrust 2009, NIST, April 14-16, 2009

---

## A Calculus of Trust and Its Application to PKI and Identity Management

Jingwei Huang & David M. Nicol\*

Information Trust Institute

\*Department of Electrical and Computer Engineering

University of Illinois at Urbana-Champaign

{jingwei,nicol}@iti.uiuc.edu



1

## Outline

---

1. Motivation
2. Trust conceptualization
3. Trust formalization / Formal semantics
4. A formal semantics based calculus of trust
5. Quantifying risk associated with trust in PKI
6. Discussion and Concluding remarks



2

## Specific Motivation (to IdM &PKI)

---

- ❑ Trust is a foundation for IdM and PKI
  - ❑ Ten risks in PKI (Ellison&Schneier,2000)
  - ❑ Incident: VeriSign, cert for Microsoft
  - ❑ “Who do we trust, and for what?” [Ellison&Schneier,2000]
- ❑ Current PKI trust models
  - Assume -- each certificate has the same level of risk
  - Evaluate risk -- the longer a certification path is, the higher risk is
  - Focus on:
    - **Structure of PKI (e.g. hierarchical, mesh, bridge)**
    - **Certification path discovery (to find shortest one)**
- ❑ Question: **How to quantify the risk associated with trust in PKI?**



3

## General Motivation

---

- ❑ On the Web, people need to interact with “strangers”.
- Trust becomes a crucial problem!
- **How can we make trust judgment on the entities we don't know (or are not familiar with)?**



4

## Methodology

---

- Our approach of trust modeling
  - Abstract concepts of trust from social studies
  - Formalize in logic
  - Extend logical model of trust to uncertainty model
  - Apply in real domain and make further improvement
  
- Principles to follow:
  - Semantics consistency
  - Common sense consistency
  - simplicity



5

## Outline

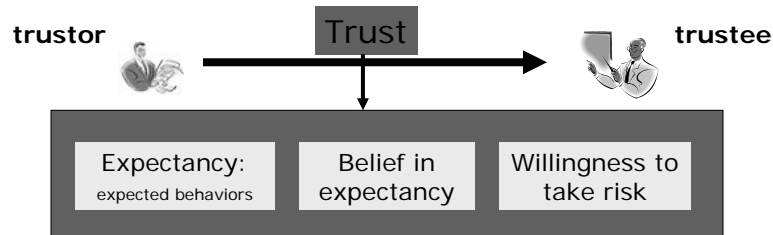
---

1. Motivation
2. Trust conceptualization
3. Trust formalization / Formal semantics
4. A formal semantics based calculus of trust
5. Quantifying risk associated with trust in PKI
6. Discussion and Concluding remarks



6

## Our View of Trust



- Trust is a **mental state** comprising:
  - (1) **expectancy**
  - (2) **belief** – expected behaviours to be true
  - (3) **willingness to take risk** for that belief



7

## Trust in Belief / Performance

- 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
- Trust is context-dependent  
e.g. trust a physician in healthcare but not in finance



8

## Outline

---

1. Motivation
2. Trust conceptualization
3. Trust formalization / Formal semantics
4. A formal semantics based calculus of trust
5. Quantifying risk associated with trust in PKI
6. Discussion and Concluding remarks



9

## Formal Semantics of Trust

---

- Uses a logical language of situation calculus.
- We develop uncertain trust model, based on a simplified version
  - Simplifies notation
  - The obtained results remain true for the full version of logic model.



10

## Two Types of Trust

---

- $trust\_p(d,e,x,k)$  (*trust in performance*)  
--- “Trustor  $d$  trusts trustee  $e$  on a thing  $x$  made by  $e$  in context  $k$ ”
  
- $trust\_b(d,e,x,k)$  (*trust in belief*)  
--- “Trustor  $d$  trusts trustee  $e$  on trustee’s belief  $x$  in context  $k$ ”



11

## Other Notation

---

- Distrust
  - $distrust\_p(d,e,x,k) \iff$   
( $madeBy(x,e,k) \rightarrow believe(d, k \sim \rightarrow neg(x))$ )
  
  - $distrust\_b(d,e,x,k) \iff$   
( $believe(e,k \sim \rightarrow x) \rightarrow believe(d, k \sim \rightarrow neg(x))$ )



12

## Trust Reasoning

---

- **Trust in belief is transitive**

$trust\_b(a,b,x,k) \ \& \ trust\_b(b,c,x,k) \ \rightarrow$   
 $trust\_b(a,c,x,k)$

- **Propagation of trust in performance via trust in belief**

$trust\_b(a,b,x,k) \ \& \ trust\_p(b,c,x,k) \ \rightarrow$   
 $trust\_p(a,c,x,k)$



13

## Outline

---

1. Motivation
2. Trust conceptualization
3. Trust formalization / Formal semantics
4. A formal semantics based calculus of trust
5. Quantifying risk associated with trust in PKI
6. Discussion and Concluding remarks



14

## Formal Semantics of Uncertainty in Trust

---

- Trust is not binary
- Using probability logic [Hajek, 2001], we define:
  - **Degree of trust in performance**  
 $td\_p(d,e,x,k) = pr(believe(d,x) | madeBy(x,e,k) \& beTrue(k) )$   
The sample space based on history of interactions
  - **Degree of trust in belief**  
 $td\_b(d,e,x,k) = pr(believe(d,x) | believe(e,x) \& beTrue(k) )$
  - Degree of distrust defined similarly



15

## Measurement of Uncertainty

---

Trust degree is measured by the fraction of successful encounters

$$td = n/m, \quad dtd = l/m; \quad n + l \leq m$$

$m$  – total encounters

$n$  – successful encounters;

$l$  – negative encounters.

- General form  
 $td = \sum(i=1, \dots, m; ep(i))/m,$   
 $dtd = \sum(i=1, \dots, m; en(i))/m$



16

## More on Uncertainty

---

- ❑ Not all encounters need to yield 'positive' or 'negative' as result
- ❑ Cognitively there are three mental states:
  - believed
  - disbelieved
  - undecidable.
- ❑ We model multiple sources of uncertainty:
  - **Randomness**, inaccuracy, complexity, **incomplete information**
- ❑ Uncertainty is represented as probability distribution (*td, dtd, ud*) or simply (*td, dtd*).



17

## Trust Calculation in Trust Networks

---

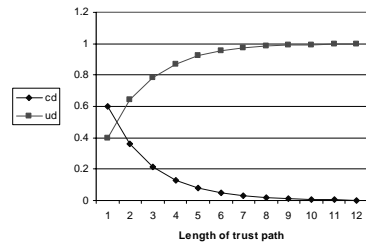
- ❑ A trust network is a directed graph, comprising a set of nodes – entities, and edges – trust relationships
  - A subset of a social network
- ❑ Calculation of trust from a trustor to a trustee though trusted friends in a network?
- ❑ Two basic operators:
  - **Sequence aggregation**: to aggregate trust in a chain
  - **Parallel aggregation**: to aggregate trust in parallel structure



18

## 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 defining  $td$ ,  $dtd$ , and  $cd = td+dtd$ 
  - $cd$  is “degree of certainty”

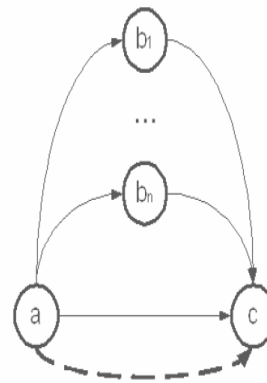


19



## Parallel Aggregation

- Combine independent trust paths.
- Use sequence aggregation on paths. e.g.
 
$$td(a,bi,c) = td(a,bi) * td(bi,c) + dtd(a,bi) * dtd(bi,c)$$
- Aggregated trust degree of trust weighted average  
 e.g. aggregated trust from  $a$  to  $c$ ,
 
$$td(a,c)' = \frac{[m(a,c) * td(a,c) + m(b1,c) * td(a,b1,c) + \dots + m(bn,c) * td(a,bn,c)]}{[m(a,c) + m(b1,c) + \dots + m(bn,c)]}$$



- Direct trust relationship
- - -→ Aggregated (indirect) trust relationship



- Path weight proportional to # encounters

20

## Outline

---

1. Motivation
2. Trust conceptualization
3. Trust formalization / Formal semantics
4. A formal semantics based calculus of trust
5. Quantifying risk associated with trust in PKI
6. Discussion and Concluding remarks



21

## Trust in PKI

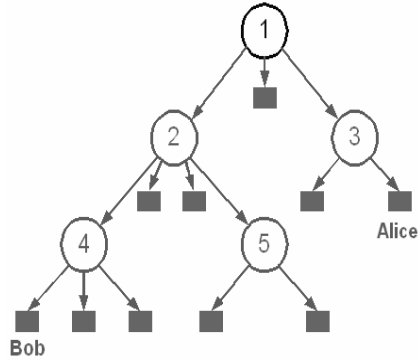
---

- Motivating question:
  - How to quantify the risk associated with trust in PKI?
- **uncertainty** is represented as **probability distribution** on <believed, disbelieved, unknown>
- Apply the calculus of trust to quantifying risk associated with trust in PKI



22

## Trust Evaluation in Hierarchical PKI

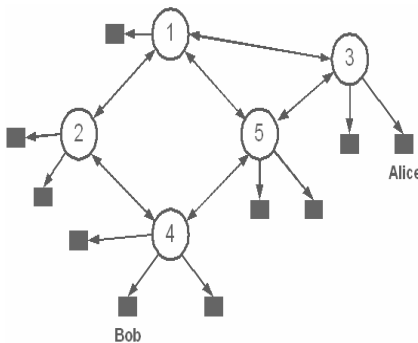


- Chain of trust:  
 Alice – CA3 – CA1 – CA2 - CA4  
 $tr^b(A, CA3, pk.validity) = (1, 0, 0)$   
 $tr^b(CA3, CA1, pk.validity) = (0.98, 0.01, 0.01)$   
 $tr^b(CA1, CA2, pk.validity) = (0.92, 0.02, 0.06)$   
 $tr^p(CA2, CA4, pk.validity) = (0.96, 0.01, 0.03)$
- By sequence aggregation  
 $tr^b(A, CA4, pk.validity) = (0.866, 0.037, 0.097)$



23

## 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  
 $tr^b(A, CA4, pk.validity) = (0.866, 0.037, 0.097)$
- Assume path 2:  
 $tr^b(CA3, CA5, pk.validity) = (0.65, 0.35, 0.1)$   
 $tr^b(CA5, CA4, pk.validity) = (0.75, 0.00, 0.25)$   
 then  
 $tr^b(A, CA4, pk.validity) = (0.488, 0.188, 0.324)$

- For using **one-path certification**, the shortest certification path may not be the most trustworthy path;
- In practice, if the shortest path has unacceptable level of trust, another path with high enough level of trust needs to be found



24

## 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

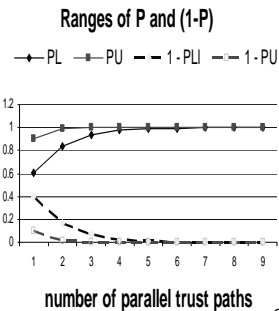
$$td_i \leq p_i \leq td_i + ud_i.$$

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

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

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

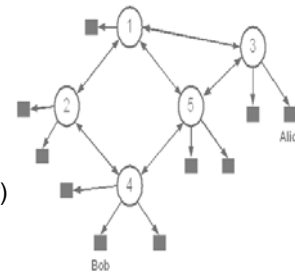
- So, the probability of multiple independent certification paths being compromised,  $1-p$ , decreases exponentially
- In general, multiple independent trust paths significantly increase trustworthiness and certainty



25

## Example

- By path-1: CA3-CA1-CA2-CA4  
 $\text{tr}^b(\text{CA3}, \text{CA4}, \text{pk. validity}) = (0.866, 0.037, 0.097)$
- 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  $\text{tr}^b(\text{CA3}, \text{CA4}, \text{pk. validity}) = (0.488, 0.188, 0.324)$
- 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  $[0.488, 0.812]$ .



26

## Outline

---

1. Motivation
2. Trust conceptualization
3. Trust formalization / Formal semantics
4. A formal semantics based calculus of trust
5. Quantifying risk associated with trust in PKI
6. Discussion and Concluding remarks



27

## Concluding Remarks

---

- **The semantics of trust needs to be defined explicitly and accurately.**
  - To avoid misuse of trust
  - To understand trust deeper
  - To answer questions about trust clearer and more accurate
  - To make model design clearer
- Our research shows:
  - ***Trust in belief* is transitive; *trust in performance* is not, but through trust in belief it can propagate in a social network.**
  - **With the growth of the length of a trust path, trust along the path decreases multiplicatively;**
  - **Multiple independent trust paths significantly increase the trustworthiness and certainty.**



28

## Next...

---

- Use quantified risk as heuristics for certificate path discovery
- We are looking for industrial partners to put it into practice :)



29

---

*Thank you !*

&

**Questions ?**



30