Trust and Security Seminar, March 18, 2009

Trust: Concepts, Formal Semantics, Quantification and Application

Jingwei Huang
Information Trust Institute
University of Illinois at Urbana-Champaign

Outline

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

Motivation

- Web/Internet has become:
  - decentralized information / knowledge repositories,
  - global electronic markets,
  - a platform of distributed computing.
- ➔ People need to interact with “strangers”.
- ➔ Trust becomes a crucial problem!

“On the Internet, nobody knows you’re dog.”

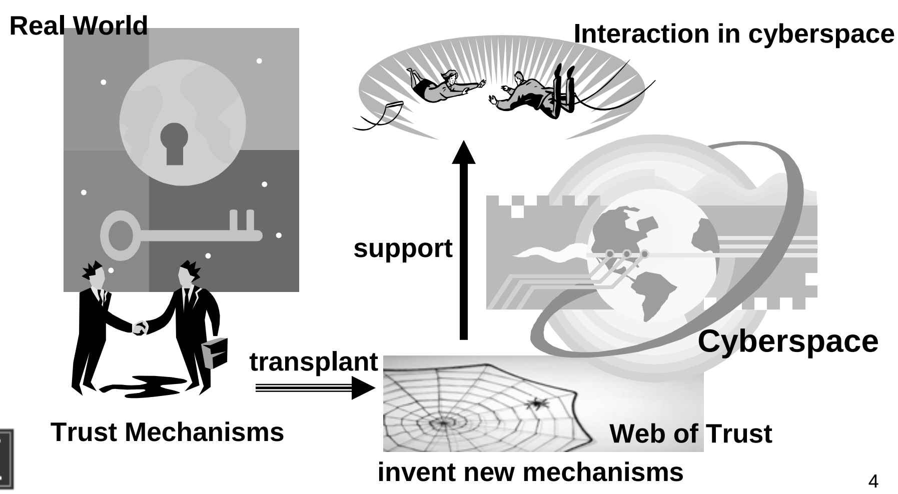
– Peter Steiner

“On the Internet, everyone can tell you’re dog, but nobody knows whether you’re likely to bite.”

-- David Nicol

➔ **How can we make trust judgment on the entities we are not familiar (don’t know)?**

Motivation (2)



Methodology

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

Outline

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

What Does Trust Mean?

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

  -– widely cited.
- Rousseau etc. (1998): “Trust, as the willingness to be vulnerable under condition of risk and interdependence, is a psychological state”.

7

What Does Trust Mean?

- Fukuyama(1995): “trust is the expectation that arises within a community of regular, honest, and cooperative behavior, based on commonly shared norms”
- Economists’ view [Zucker1986]: “implicit contracting”
- Gambetta (1988): Trust is a subject probability. Trust is fragile due to limited knowledge and foresight, and uncertainty of trustee’s behaviors.
- Blomqvist (1997), from different discipline perspectives, presented “many faces of trust”.
- McKnight(2001) gives a topology of trust, based on 65 definitions.

8

Spectrum of Trust

- Deutsch (1962) defined trust as a choice possibly leading to a beneficial outcome or a harmful outcome of higher strength, which outcome occurs dependent on the behavior of another 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 /unusual cases
- Lewis&Weigert (2001) presented trust in two dimensions:

RATIONALITY \ EMOTIONALITY	High	Low	Virtually Absent
High	Ideological Trust	Cognitive Trust	Rational Prediction
Low	Emotional Trust	Mundane, Routine Trust	Probable Anticipation
Virtually Absent	Faith	Fate	Uncertainty, Panic

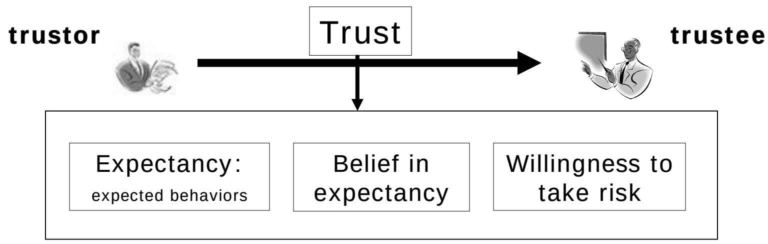
9

Major concepts gained:

- Trust is a psychological state.
- Trust has three aspects: expectancy, belief, and willingness to be vulnerable.
- Trust is based upon trustee's characteristics of competency, goodwill (benevolence) and integrity (predictability);
- (Minimally, trust is based on trustor's vision on the stable and predictable behaviors of trustee; such vision may be gained by familiarity or certain social mechanisms such as laws.)
- Trustor does not have control on trustee's behavior.
- Trust is associated with **risk**.

10

Our View of Trust



- Trust is a **mental state** comprising:

  (1) **expectancy**: the trustor expects a specific behavior of the trustee, (such as providing valid information or effectively performing cooperative actions);

  (2) **belief**: the trustor believes that the expected behavior occurs, based on evidence of the trustee's competence and goodwill; and

  (3) **willingness to take risk**: the trustor is willing to take risks for (or be vulnerable to) that belief.

11

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

12

Contexts of Trust

- **Trust is context-dependent**
- Context of trustee
  - Context of creating a piece of information
  - Context of performing an action
- Context of trustor
  - Context of expectancy
    - Context to use the information
    - Context in which trustor needs the action from trustee
  - Context of willingness (the situation to make trust decision)
- These two contexts may be in the same situation, but trustor and trustee usually have different utilities regarding the expectancy.

  e.g. in situation “take taxi to airport”, passenger’s utility and driver’s utility are different.

13

Outline

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

14

A Big Picture of Trust Modeling

Classify by the approaches to Trust

- **Process-based trust** (inter-individual trust, direct trust): trust is built up in the process of interaction.
  - Most of social studies,
    e.g. Rotter(1967), Deutsch(1962) – trust in cooperation
  - Marsh (1994) trust among agents
  - Mui (2002) – model encounters as Bernoulli trials
- **Reputation-based trust**: trust degree is represented by reputation level in a social network
  - Amazon, eBay [Resnick, 2002]
  - Kleinberg (1999): authorities, hubs; PageRank; EigenTrust

15

A Big Picture of Trust Modeling

- **Relational Trust:** derived indirect trust through trusted friends in a social network
  - Golbeck et al (2002, 2005), extended FOAF
  - Yu et al (2000)
  - Josang et al (2006), uncertainty notation b+d+u =1
- **System Trust**: trust in the function of a system [Luhmann, 1973]

  many manifestations:
  - Professional-based [Barber,1983]
  - Characteristic based [Zucke,1986]
  - Attribute-based [Johnston et al, 1998]
  - Institutional based [Zucke,1986]
  - Regularity-based [Minsky, 2003]

16

Research Issues in Trust Modeling

- Should trust be represented explicitly or just be used pragmatically (implicitly, tightly combined or mixed with application)?
- Does a trust model need formally defined semantics of trust?
- Is trust transitive or not? What type of trust transitive? Why?
- What is an effective notation for uncertainty of trust?
  - Need to discern distrust and untrust
  - Untrust is the state of uncertainty due to lack of knowledge to make judgment

17

Why we need formal semantics?

- **To avoid misuse of trust**
  - Calculation of trust needs to use trust data/models distributed on the web and specified by different people;
  - Without explicitly and accurately defined semantics, trust is easy to be misused, especially in such distributed computing.
- **To have better Knowledge about trust**
  - To separate trust modeling from application
  - For clearance in model design
  - For generalization and knowledge evolution
  - For better application

18

Formal Semantics of Trust

- A formal semantics of trust has been defined as ontology [Huang, 2007],
  - Based on formalization of belief in Epistemic Logic, and using a logical language of situation calculus.
  - An ontology is an explicit and formal specification of concepts.
- We develop uncertain trust model, based on a simplified version in FOL
  - To avoid complex notation
  - The obtained results remain true for the original logic model.

Trust in Performance

- *trust_p(d,e,x,k)*

  represents *trust in performance* relationship --- “Trustor *d* trusts trustee *e* on a thing *x* made by *e* in context *k*”
- Definition: in a given context *k*, if thing x is made by e, then d believes it.

  trust_p(d,e,x,k) <=>

  (madeBy(x,e,k) -> believe(d, k~>x))

  x: information created by *e*, or “commitment” of performance made by *e*, represented as a reified proposition (a term).

  k : context, represented as a reified proposition.

  ~> is a function mimicking logical implication.
- *believe(d, k) & believe(d, k~>x) -> believe(d, x).*

Trust in Belief

- *trust_b(d,e,x,k)*
  represent *trust in belief* relationship --- "Trustor *d* trusts trustee *e* on trustee's belief *x* in context *k*"
- Defination: *d* believes what *e* believes in the given context *k*.
  trust_b(d,e,x,k) <=>
  (believe(e,k ~>x) -> believe(d, k~>x))

21

Other Notation

- Distrust
  - *distrust_p(d,e,x,k) <=>*
    (madeBy(x,e,k) -> believe(d, k~> neg(x)))
  - *distrust_b(d,e,x,k) <=>*
    (believe(e,k ~>x) -> believe(d, k~> neg(x)))
- General form – trust in everything in a given context, rather than a specific thing *x*
  - *trust_p(d,e,k) <=> (forall x) trust_p(d,e,x,k)*
  - *trust_b(d,e,k) <=> (forall x) trust_b(d,e,x,k)*

22

Trust Reasoning

- Rule 1
  madeBy(x,e,k) & trust_p(d,e,x,k) -> believe(d, k~>x)
- Rule 2
  believe(e, k~>x) & trust_b(d,e,x,k) -> believe(d, k~>x)
- Rule 3: ***Trust in belief* is transitive**
  trust_b(a,b,x,k) & trust_b(b,c,x,k) -> trust_b(a,c,x,k)
- Rule 4: ***Trust in performance* is not, but though *trust in belief*, *trust in performance* can propagate**
  trust_b(a,b,x,k) & trust_p(b,c,x,k) -> trust_p(a,c,x,k)
- Rule 5: Rules 3 and 4 are also true in general form of trust relationship
  trust_b(a,b,k) & trust_b(b,c,k) -> trust_b(a,c,k)
  trust_b(a,b,k) & trust_p(b,c,k) -> trust_p(a,c,k)
  - **By rules 3,4,5, trust can propagate in a social network!**

23

Outline

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

24

Uncertain Trust

- Usually, a trust relationship is not completely trust or completely distrust.
- Based on semantics of trust defined in logic, by 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 is the event set in which ***madeBy(x,e,k) & beTrue(k)*** is true.
  - 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 -- ***pr(believe(d,neg(x) | …)***

Measurement of Uncertain Trust

- Practically, trust degree is measured by the rate of successful encounters

  td = n/m, ***dtd = l/m; n + l <= m***

  m – **total encounters**, in which the condition in the conditional probability is true;

  n – **successful encounters**, in which both the consequence and condition in the conditional probability are true;

  l – **negative encounters**.
- General form

  td = sum(i=1,…,m; e_p(i))/m,

  dtd = sum(i=1,…,m; e_n(i))/m

  e_p(i) in [0,1]: **positive degree of encounter i**

  e_n(i) in [0,1]: **negative degree of encounter i**

  e_p(i) + e_n(i) <= 1
- Extended versions:
  - Each encounter has different utility
  - Utility may change with time

Further Discussion on Uncertainty

- Why ***td + dtd <= 1*** ?
- Practically, a trustor may have difficulty to rate an encounter as positive or negative, due to insufficient information
- Cognitively, regarding belief, there are three mental states:
  - believe
  - disbelieve
  - "undecidable" , unable to determine to believe or disbelieve x, due to insufficient information.
- Here, we meet multiple sources of uncertainty:
  - **Randomness**, inaccuracy, complexity, **incomplete information**
- Uncertainty is represented as probability distribution over three mental states
  - Definition: uncertainty degree

    ud = 1 - td - dtd
  - An uncertain trust relationship is denoted as

    (td, dtd, ud) or simply *(td, dtd).*

27

Trust Calculation in a Network

- A trust network is a directed graph, nodes – entities, edges – trust relationships
- Given a trust network, how to evaluate the aggregated degree of trust from a trustor to a trustee?
- Two basic issues:
  - Evaluation of trust in a chain – **sequence aggregation**
  - Evaluation of trust in parallel structure – **parallel aggregation**

28

Sequence Aggregation

- Given that *a* trusts *b*, *b* trusts *c*, how much *a* trusts *c*?
- From the formal definitions, we derived and proved the following theorem:

  (1) td(a,c) = td(a,b)*td(b,c) + dtd(a,b)*dtd(b,c)

  (2) dtd(a,c) = td(a,b)*dtd(b,c) + dtd(a,b)*td(b,c)

  (3) let cd = td + dtd, then

  cd(a,c) = cd(a,b)*cd(b,c)

29

Discussion - sequence

- By this theorem, with the growth of the length of a trust path, the degree of certainty (trust and distrust) of the aggregated trust decreases exponentially.
- Sequence trust aggregation is associative
  - so the order of aggregation doesn't matter.
- Most uncertain trust opinion (ud =1; td=dtd =0)
  - zero element in aggregation
  - equivalent to no trust relationship
  - block a trust path

30

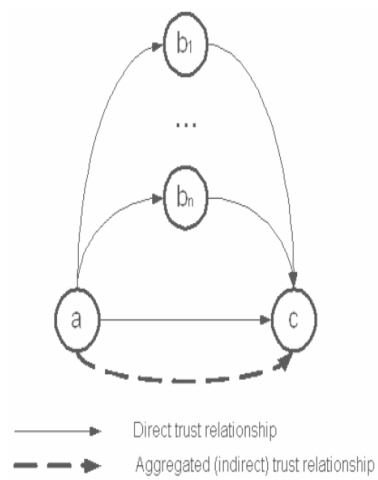
Parallel Aggregation

- Given *a* directly trusts *c* with s(a,c) encounters, *a* (directly or indirectly) trusts (in belief) *b1, …, bn*, and *b1,…,bn* trust *c* with encounters *s(b1,c),…,s(bn,c)*, how much *a* trusts *c*?
- Aggregated trust, td(a,c)':

  td(a,c)' =

  *[s(a,c)*td(a,c)*
  *+s(b1,c)*td(a,b1,c) + …*
  *+s(bn,c)*td(a,bn,c)]*
  / [s(a,c)+s(b1,c)+…+s(bn,c)]
- By sequence aggregation, indirect trust of *a* to c via bi is:

  *td(a,bi,c)= td(a,bi)*td(bi,c)*
  *+dtd(a,bi)*dtd(bi,c)*



31

Discussion - parallel

- Trust evolves
  - with more experience of interaction,
  - and with new information from trusted peers.
- Parallel trust aggregation reflects this feature.
  - *a* has direct trust relationship with *c*, <td(a,c),dtd(a,c)>
  - when *a* obtains from trusted friends *b1,…,bn* about their trust relationships with c, --- the new information,
  - *a* revises its trust to *c*, by using parallel aggregation, and has revised trust relationship *<td(a,c)', dtd(a,c)'>*
- In parallel aggregation, the opinion based on bigger number of samples is count more.

32

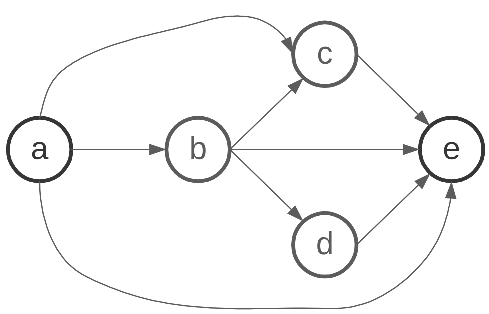
Evaluating Trust in a Network

- Given a trust network (acycle directed graph), how to calculate overall trust from *a* to *z?*
- Trust network *TN = (E,A)*; *E* – set of entities; *A* – set of edges representing trust relationships <*td,dtd*>
- aggregate(a,z,TN){

    (1) find B, the set of entities having direct trust to z;
    (2) for each b in B, if a has single trust path to b,
        <td(a,b), dtd(a,b)> = sequence-aggr(a,b,TN);
        else, if *a* has multiple independent trust path to b,
            <td(a,b), dtd(a,b)> = parallel-aggr(a,b,TN);
        else, <td(a,b), dtd(a,b)> = aggregate(a,b,TN);
    (3) return <td(a,c),dtd(a,c)> = parellel-aggr(a,z,B)

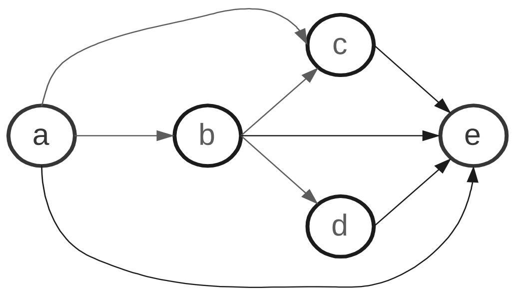
}

Example



- Apply algorithm *aggregate(a,e,TN)* to the trust network

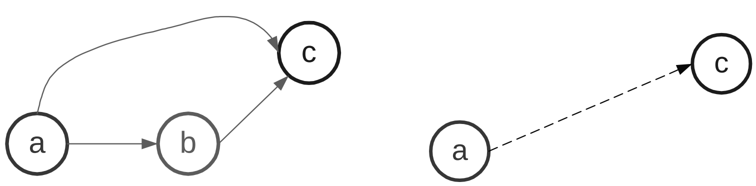
Example



- Find e’ neighbors set B = {a,b,c,d}
- Check each node in B

35

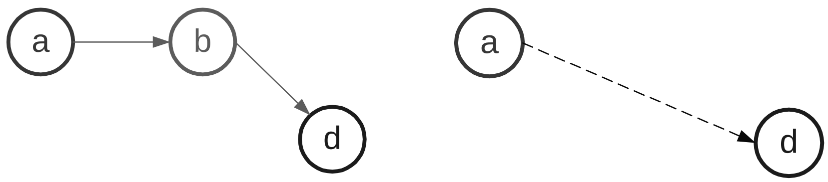
Example



- For *C*
  - Apply algorithm parallel-*aggr(a,c,TN)* to the sub-network
  - <td(a,c),dtd(a,c)> = parallel-*aggr(a,c,TN)*

36

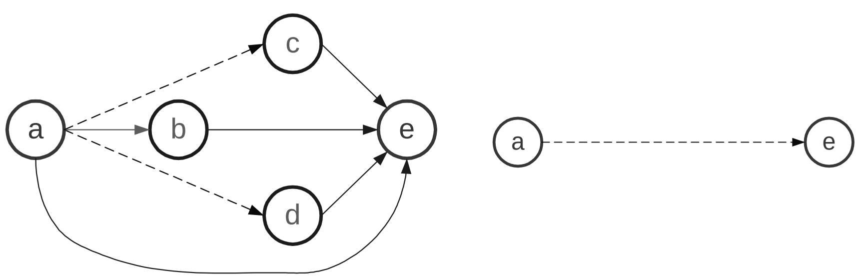
Example



- For *d*
  - Apply sequence-*aggr(a,d,TN)*
  - *<td(a,d),dtd(a,d)>* = *sequence-aggr(a,d,TN)*

37

Example



- Now *a* has independent trust paths to every entities in B
- apply parallel-*aggr(a,e,TN)*
- *<td(a,e),dtd(a,e)>* = *parallel-aggr(a,e,TN)*

38

Outline

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

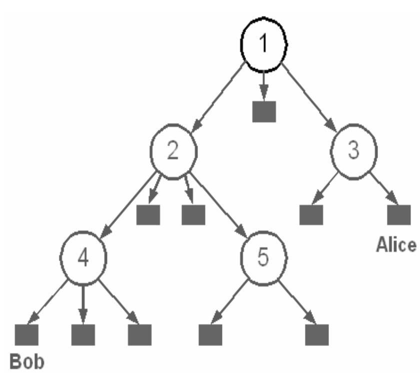
Trust in PKI

- Trust is major risk factor in PKI
  - Ten risks in PKI[Ellison&Schneier,2000]
    - Key compromised for its limited "theft lifetime"
    - Failure in maintaining CRL
  - Incident: VeriSign issued an impostor two digital certification associated with Microsoft
  - "Who do we trust, and for what?" [Ellison&Schneier,2000]

PKI Trust Models

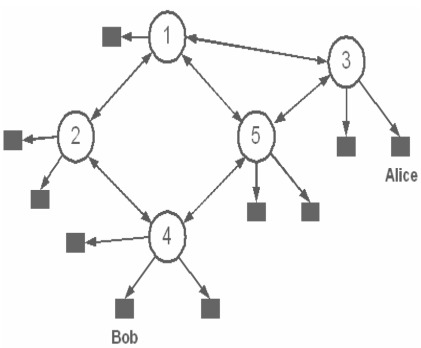
- Assume
  - Each certificate has the same level of risk
- Risk evaluation criterion
  - The longer a certification path is, the higher risk is
- Focus on
  - Structure of PKI (e.g. hierarchical, mesh, bridge)
  - Certification path building (to find shortest one)
- Question: How to quantify the risk associated with trust in PKI?

Trust Evaluation in Hierarchical PKI



- Chain of trust:
  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)

Trust Evaluation in Mesh PKI

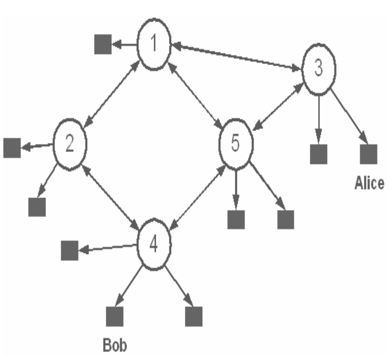


- Multiple chains of trust exist
  1. Alice-CA3-CA1-CA2-CA4
  2. Alice-CA3-CA5-CA4
- Assume path1 the same as before
  tr^b(A,CA4,pk.validity)
  =(0.866, 0.037, 0.097)
- Assume path 2:
  tr^b(CA3,CA5,pk.validity)
  =(0.65, 0.35, 0.1)
  tr^b(CA5,CA4,pk.validity)
  =(0.75, 0.00, 0.25)
  then
  tr^b(A,CA4,pk.validity)
  =(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

43

What is the risk level in multiple independent paths?



- By path: CA3-CA1-CA2-CA4
  tr^b(CA3,CA4,pk.validity)
  =(0.866, 0.037, 0.097)
- The probability of path-1 being valid,
  p1 in [0.866, 0.963]
  0.963 = td+ud = 0.866+0.097
- By path: CA3-CA5-CA4
  tr^b(CA3,CA4,pk.validity)
  =(0.488, 0.188, 0.324)
- The probability of path-2 being valid,
  p2 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].

44

Multiple Independent Trust Paths

- Assume path i having aggregated trust level *(td, dtd, ud)*
- 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 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 invalid, 1-p, decreases exponentially
- In general, **multiple independent trust paths increase trustworthiness and certainty**

45

Concluding Remarks

- In order to avoid misuse of trust, also to make model design clear, the semantics of trust needs to be defined explicitly and accurately.
- Our research shows:
  - ***Trust in belief* is transitive; *trust in performance* is not, but via trust in belief it can propagate in a network.**
  - **With the growth of the length of a trust path, trust along the path decreases exponentially;**
  - **Multiple independent trust paths significantly increase the trustworthiness and certainty.**

46

Thank you !

&

Questions ?

Contact information:
Jingwei Huang,
CSL 349
jingwei@iti.uiuc.edu