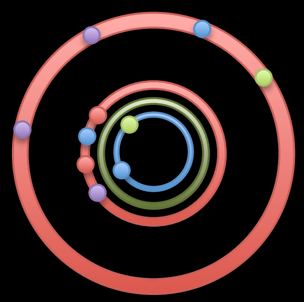


The Solar Trust Model

Aerospace Technical Talk

Dr. Michael Clifford

March 20th, 2017

Presentation Outline

Introduction

Defining Trust

Problems with Other Trust Models

How the Solar Trust Model Works (Overview)

Securely Mapping and Maintaining the Trust Network

Path Evaluation

Computational Scalability

How the STM Addresses Problems with Other Trust Models

Future Work

Contributions and Questions

About This Talk

- This talk is about my Ph.D. work:

  School: UC Davis (Computer Security Lab), 2012
  Advisor: Professor Matt Bishop
  Committee: Matt Bishop, Karl Levitt, Sean Peisert

- Due to time limitations, I will only cover a subset of this work

- This talk is NOT related to my current research or employer

Solar Trust Model History

- Initially developed during an internship with Aerospace (TCSD) in 1997
- Collaboration with Charles Lavine (TCSD) and Matt Bishop (UC Davis)
- Developed to allow communication between users of different PKIs
- Resulted in 4 published papers, MS Thesis, Ph.D. Dissertation

Dissertation Research Plan

Plan

1. Formalization of the Solar Trust Model

2. Ensuring the model's resilience against implementation attacks through proofs and modifications

3. Development of a theoretical framework for identity and anonymity

4. Development new classes of identity and anonymity attacks and countermeasures

Result

Exploration of identity within the Solar Trust Model led to new discoveries on relative anonymity and identity, and to 7 new classes of identity and anonymity attacks

Presentation Outline

Introduction

Defining Trust

Problems with Other Trust Models

How the Solar Trust Model Works (Overview)

Securely Mapping and Maintaining the Trust Network

Path Evaluation

Computational Scalability

How the STM Addresses Problems with Other Trust Models

Future Work

Contributions and Questions

What is Trust?

The degree of confidence that an observing entity has that another entity will meet a particular set of requirements

Example:

How trustworthy is a message from a specific sender, given the perspective of the recipient?

Examples of Trust Problems

1. How much can sensor data be trusted?
2. How much can you trust data from arbitrary sources?
3. Can a system of systems trust the behavior of its own components?
4. How should data from potentially untrustworthy sources be evaluated?
5. Data from two sources conflicts. Which should be trusted more?

Presentation Outline

Introduction

Defining Trust

Problems with Other Trust Models

How the Solar Trust Model Works (Overview)

Securely Mapping and Maintaining the Trust Network

Path Evaluation

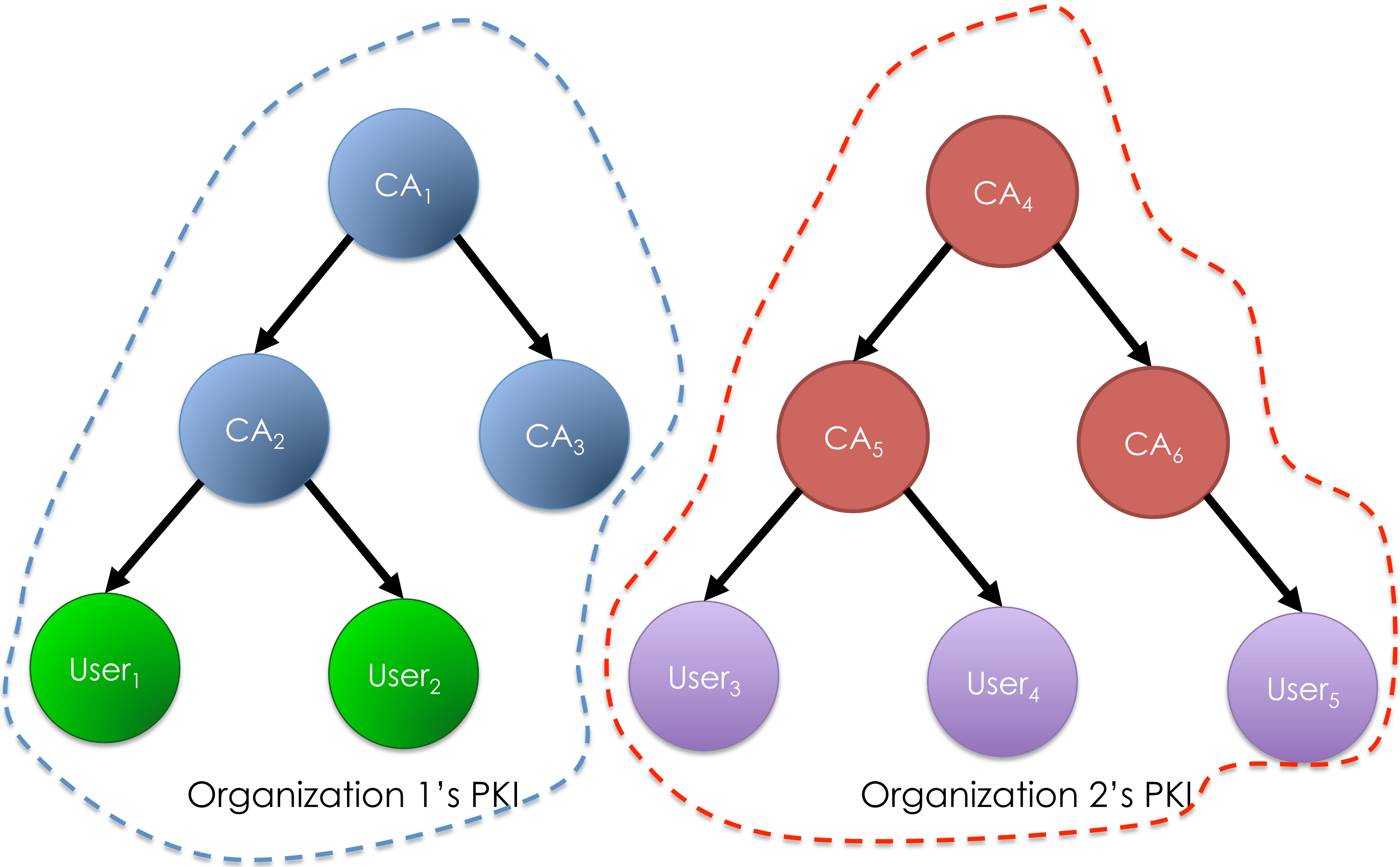
Computational Scalability

How the STM Addresses Problems with Other Trust Models

Future Work

Contributions and Questions

Interoperability

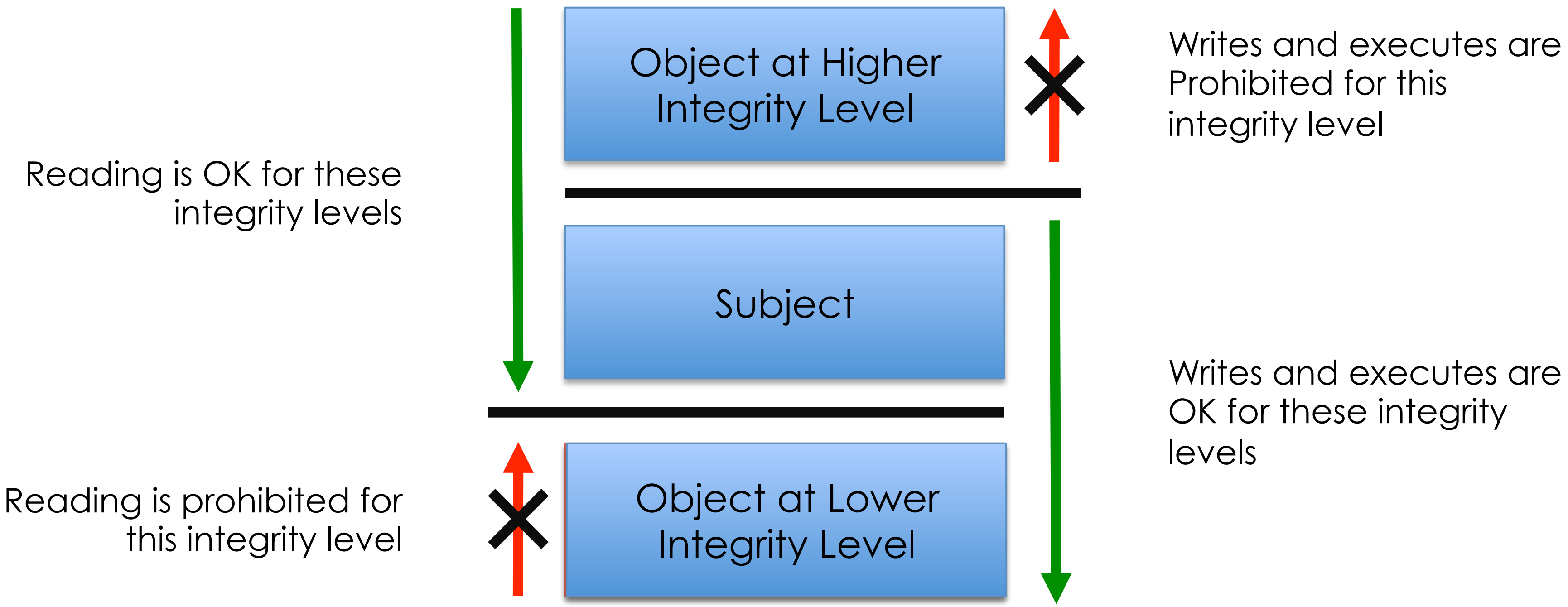


A tale of two PKIs

The Interoperability Problem

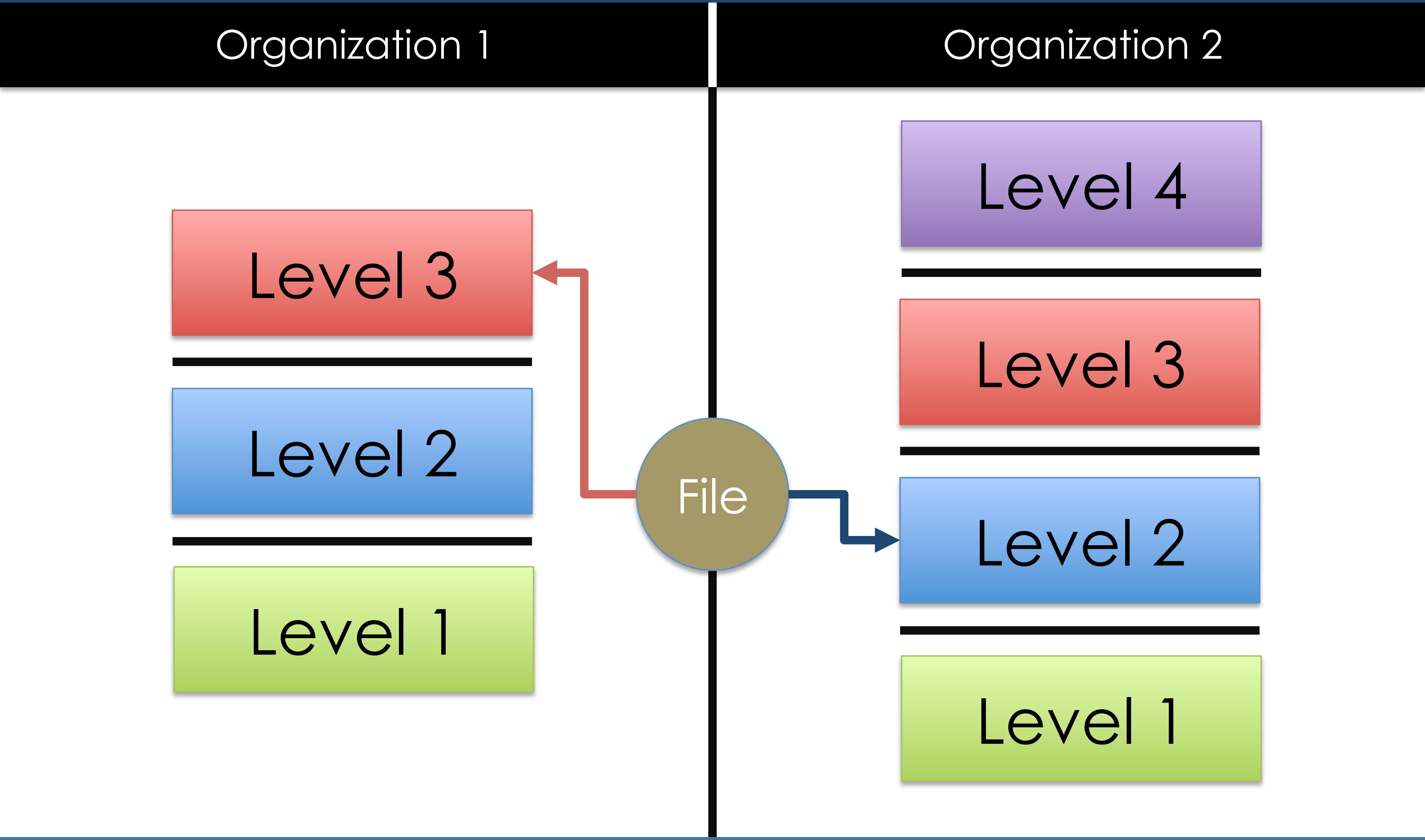
- Unrelated organizations do not share common authentication or trust policies
- Organizational, cultural, and political boundaries prevent mutual acceptance
- Diminishes interoperability between commercial, civil and military organizations

Scalability



Biba Integrity Model - No reads down, no writes up

The Scalability Problem



Different organizations may not agree on integrity levels and object assignments

The Scalability Problem

Many trust models do not scale beyond individuals or organizations

Context

Would you rather fly on a plane with flight control software written by:

1. An experienced programmer
2. An auto mechanic

Context

What if the programmer had never written flight control software before?

Context

Who would you trust to fix your car?

1. An experienced programmer
2. An auto mechanic

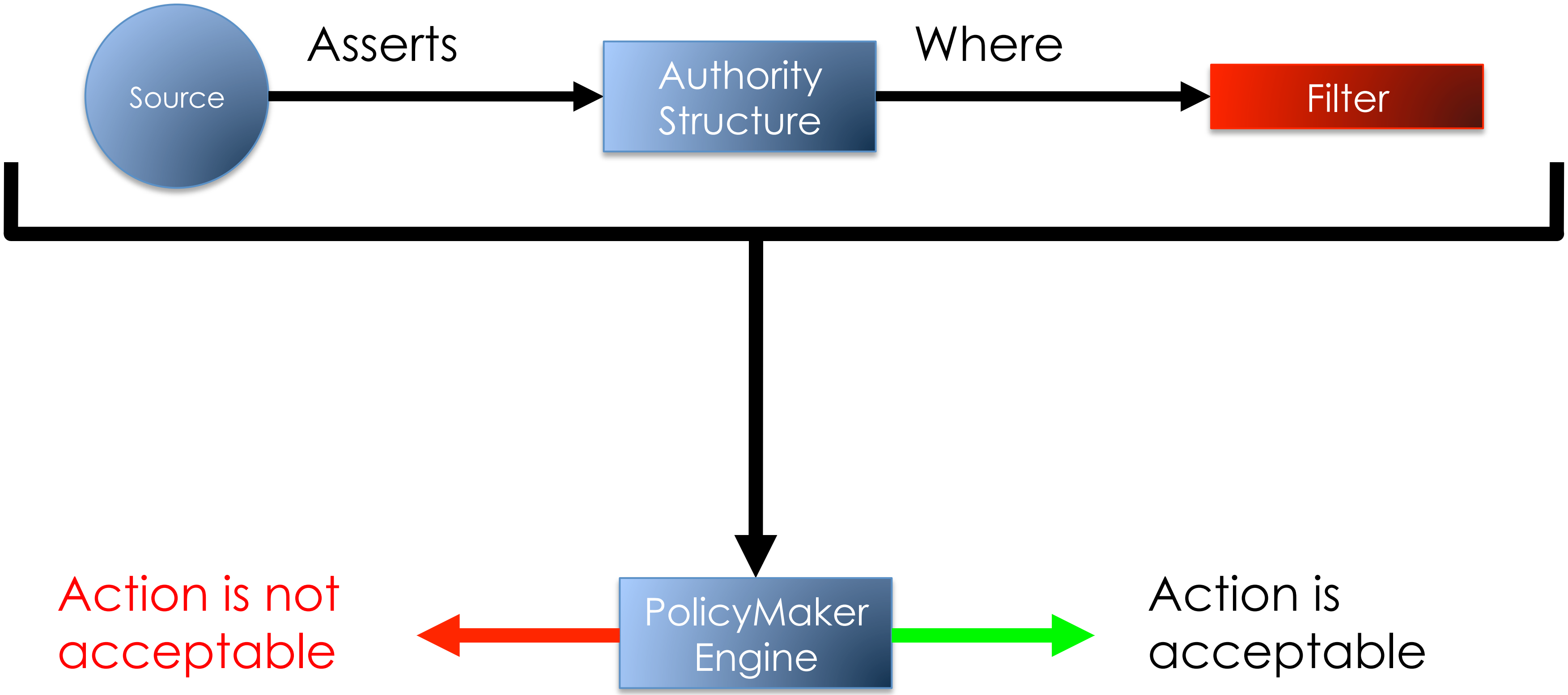
The Context Problem

- Authentication and trust mechanisms do not take context or experience into account

- Trust judgments may not be appropriate to the situation

- Individual needs and experiences are not taken into account

The Relativity Problem



PolicyMaker outputs binary trust decisions, but trust is not binary

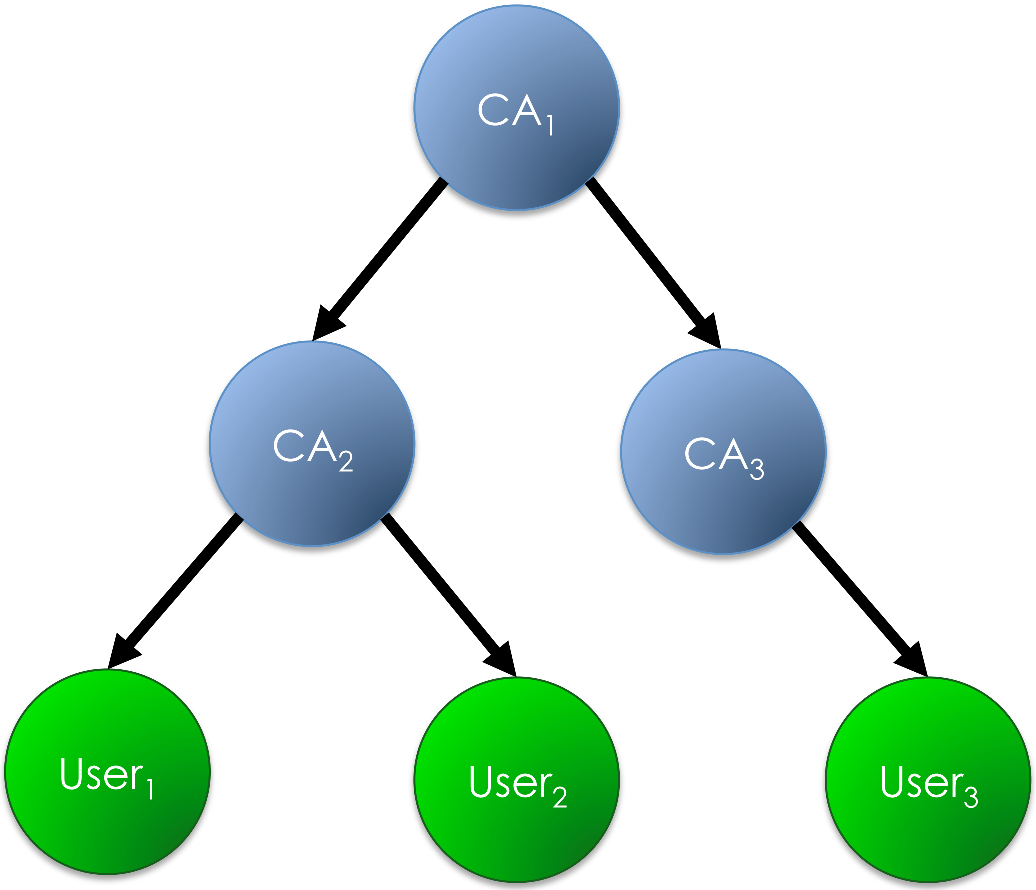
The Relativity Problem

- Many trust models output binary trust decisions:

  You are trusted or you are not

- Real world trust is often relative – something is more or less trusted than something else in a given context

Transitivity

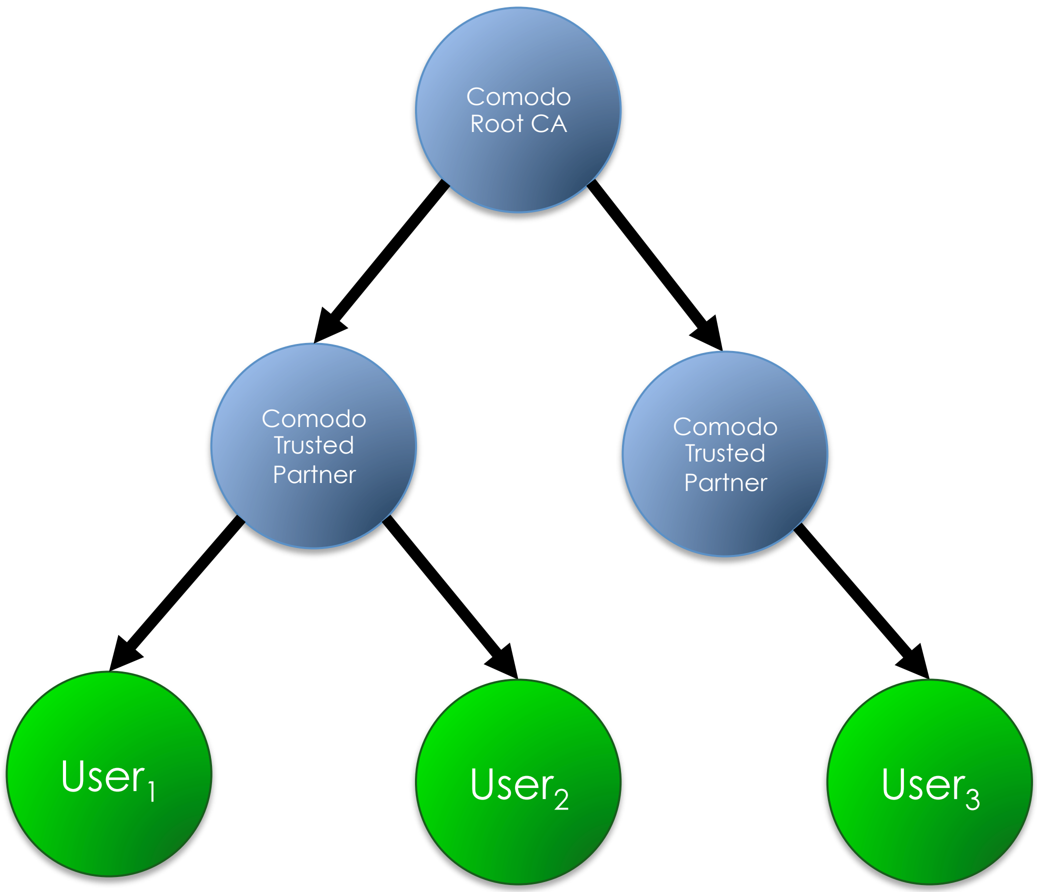


PKIs use transitive trust

The Transitivity Problem

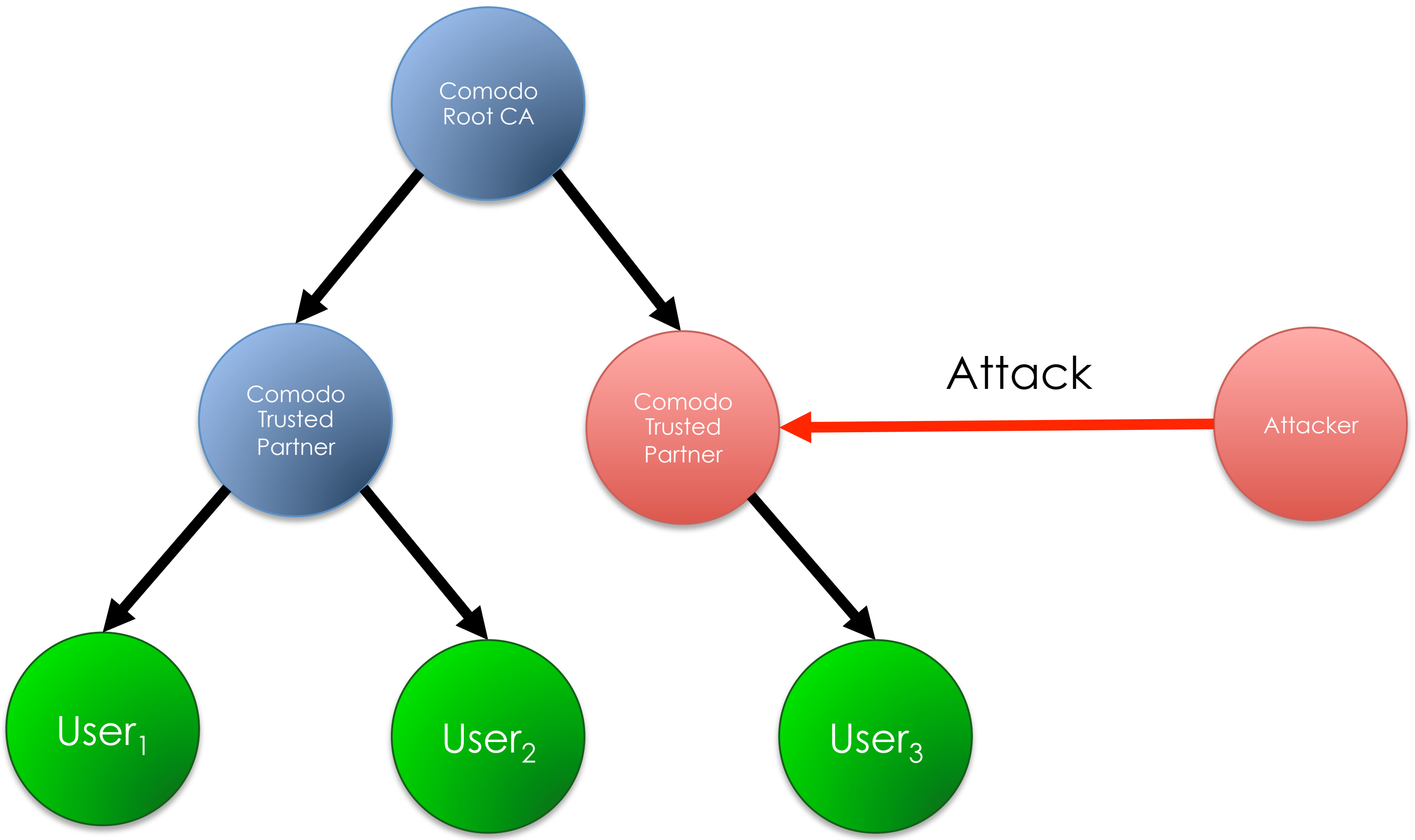
- Many trust models assume that trust is transitive:
- If Alice trusts Bob and Bob trusts Charlie, then Alice must trust Charlie
- Trust in the real world is almost never transitive

Centralized Trust



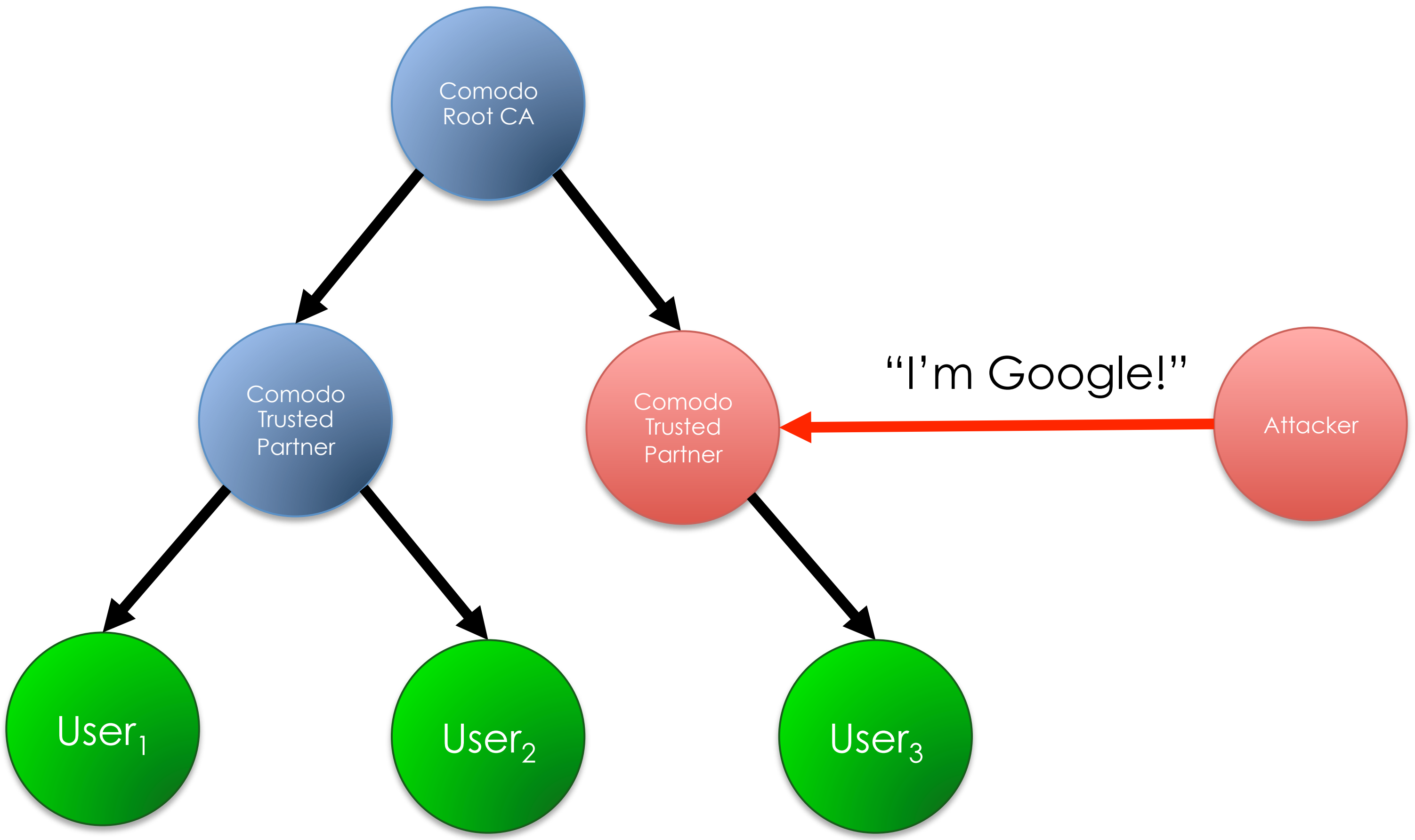
The root CA Comodo was trusted by all major browsers

Centralized Trust



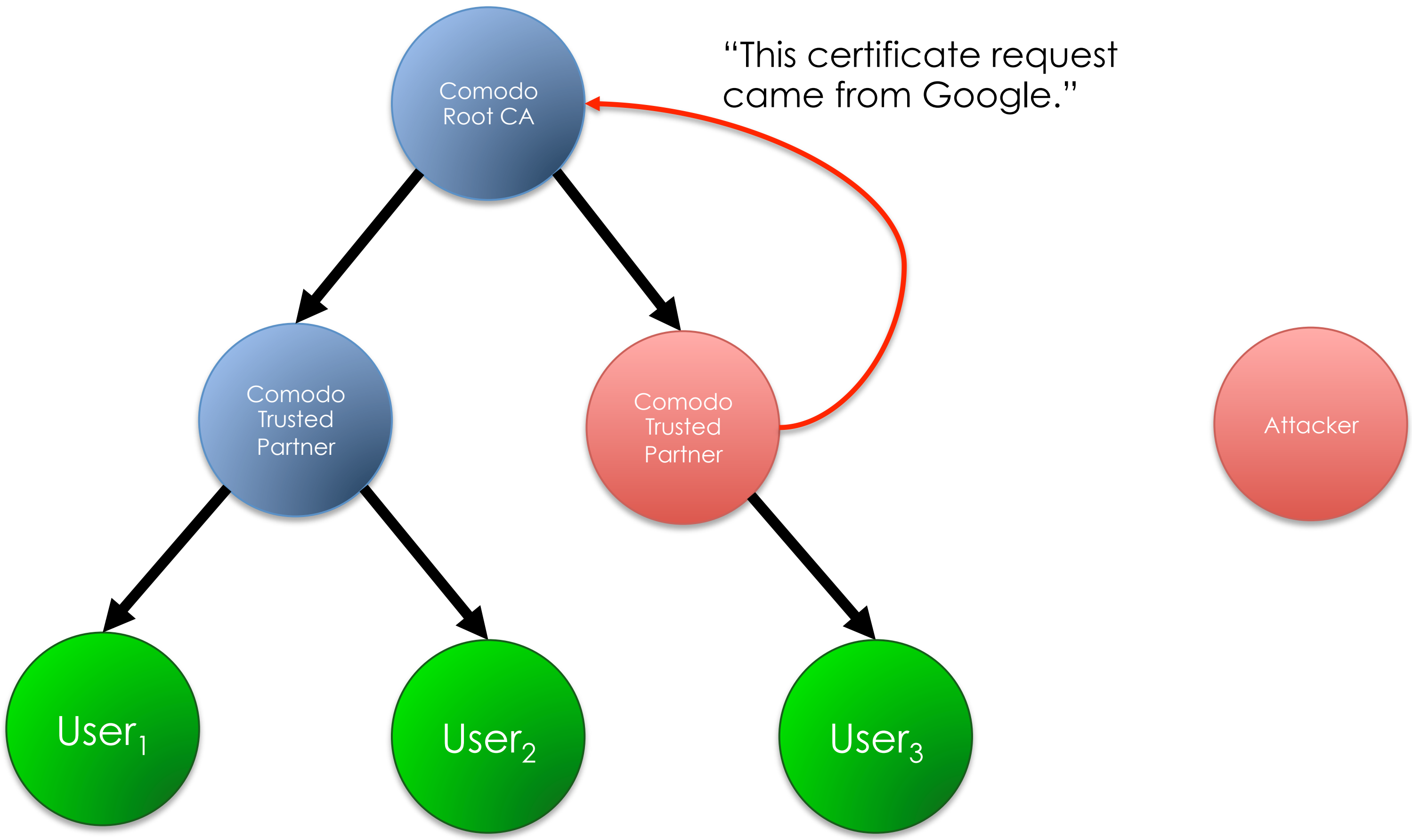
The Comodo Attack

Centralized Trust



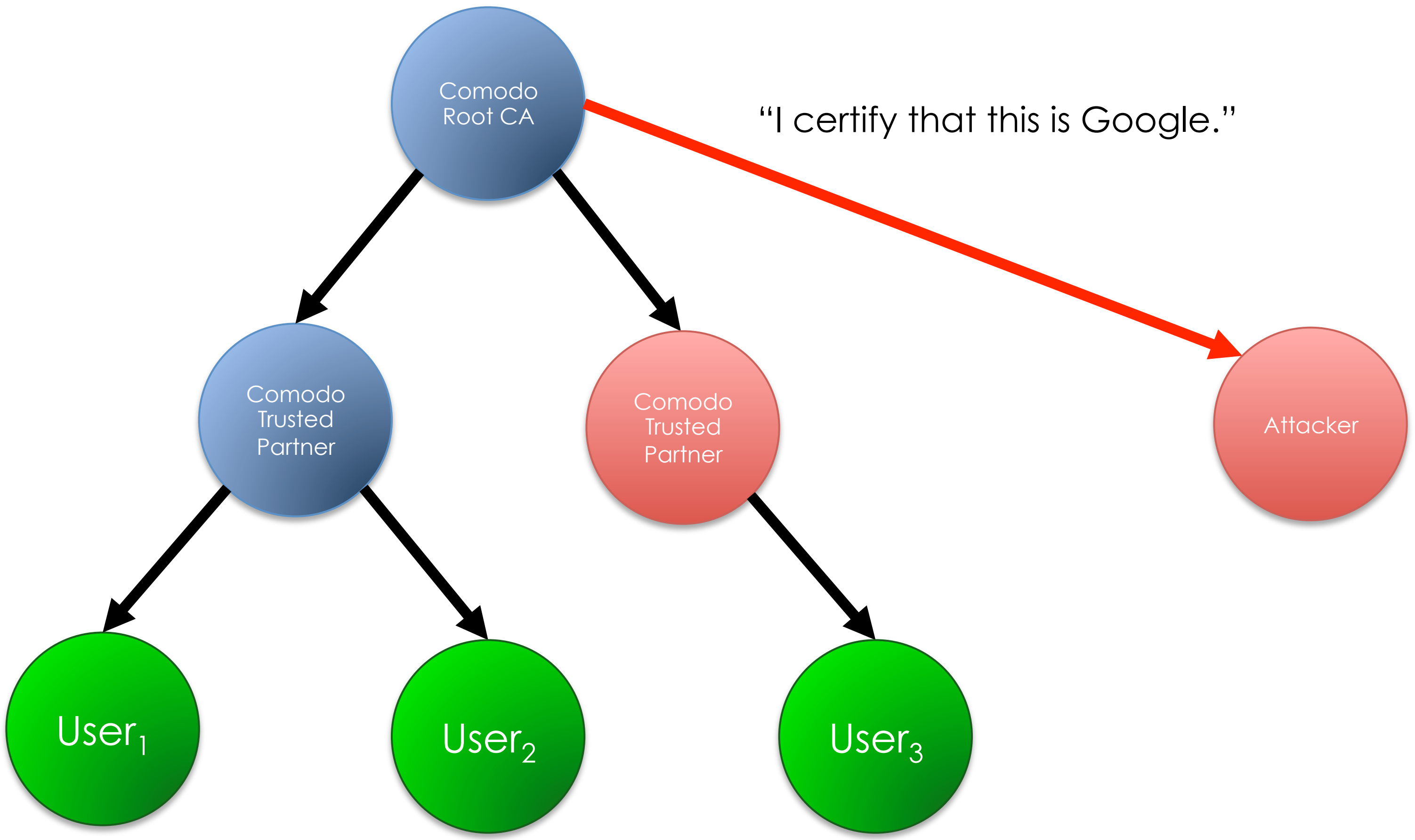
The Comodo Attack

Centralized Trust



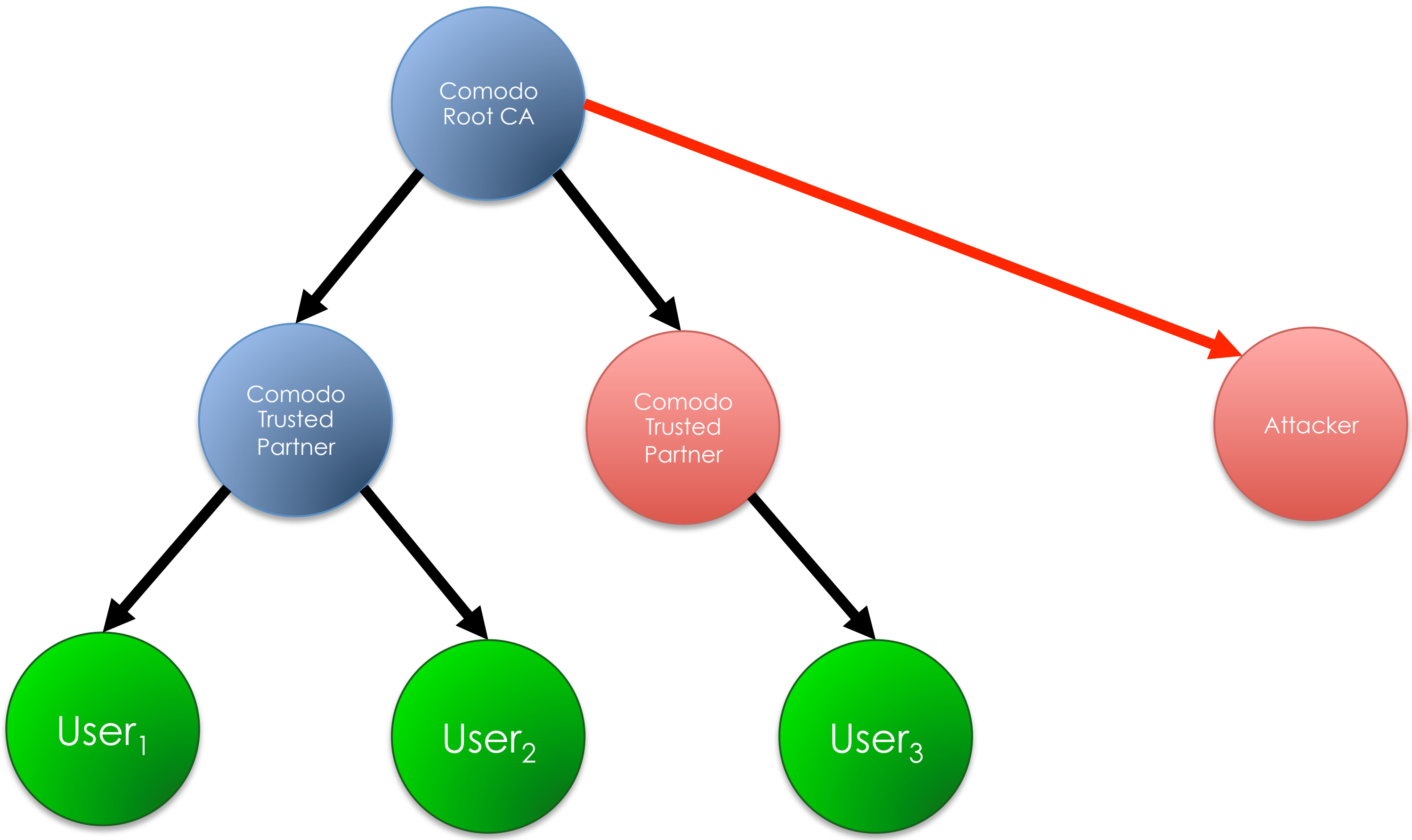
The Comodo Attack

Centralized Trust



The Comodo Attack

Centralized Trust



"I'm Google."

The Comodo Attack

The Centralized Trust Problem

- Some trust models rely on a central trust authority
- Single point of failure

Presentation Outline

Introduction

Defining Trust

Problems with Other Trust Models

How the Solar Trust Model Works (Overview)

Securely Mapping and Maintaining the Trust Network

Path Evaluation

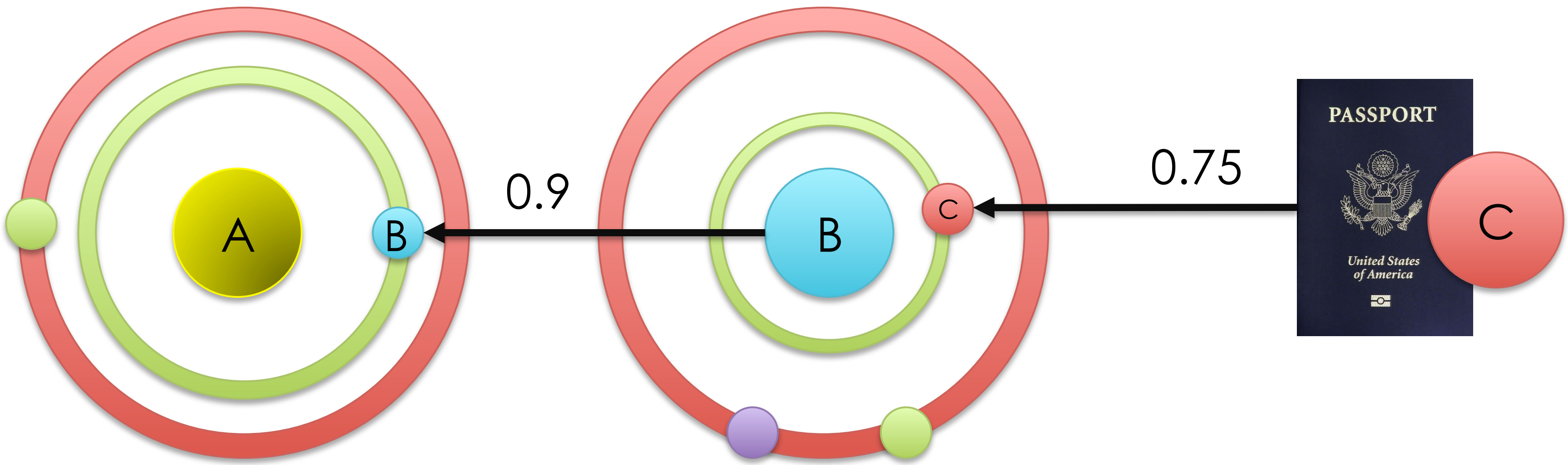
Computational Scalability

How the STM Addresses Problems with Other Trust Models

Future Work

Contributions and Questions

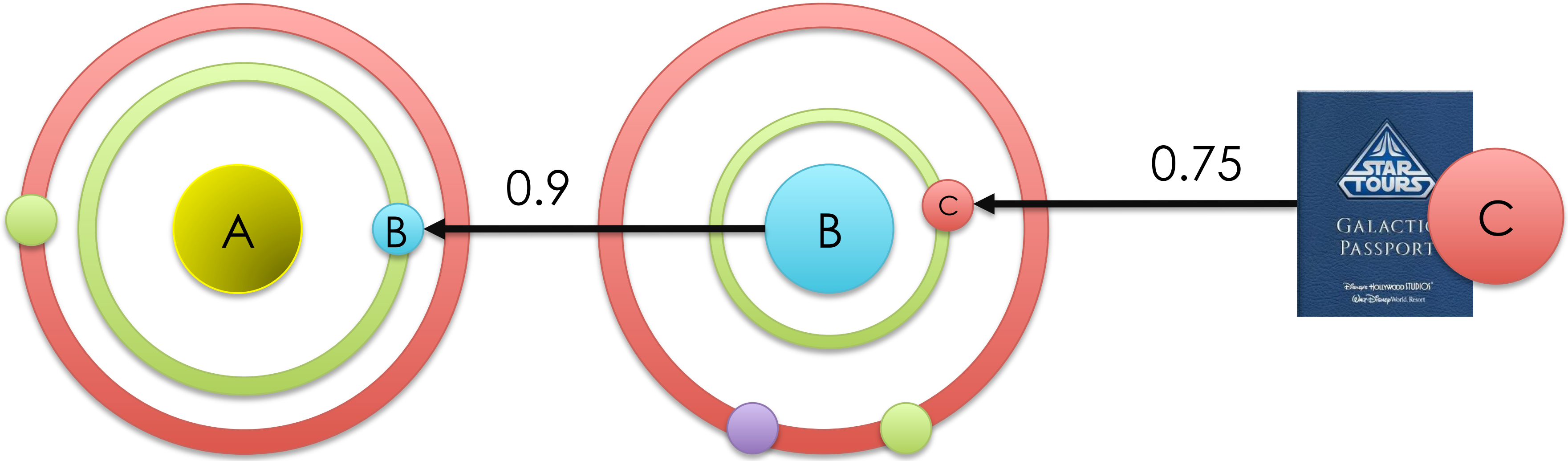
Example



Initially, A trusts B to validate passports

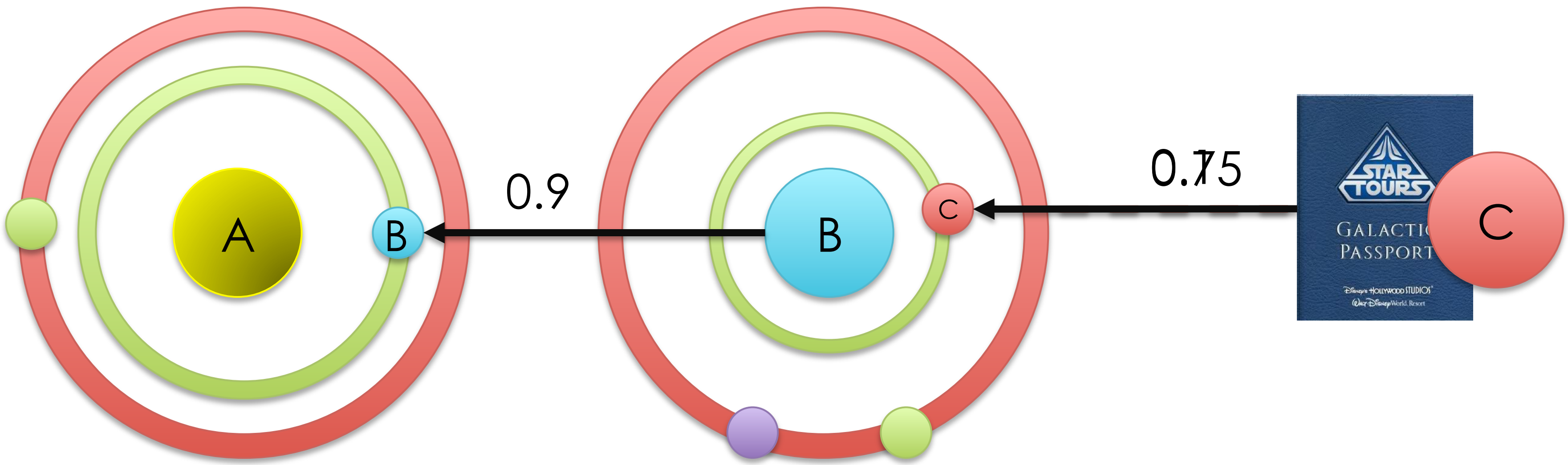
B places C's passport in orbit 0.75

Example



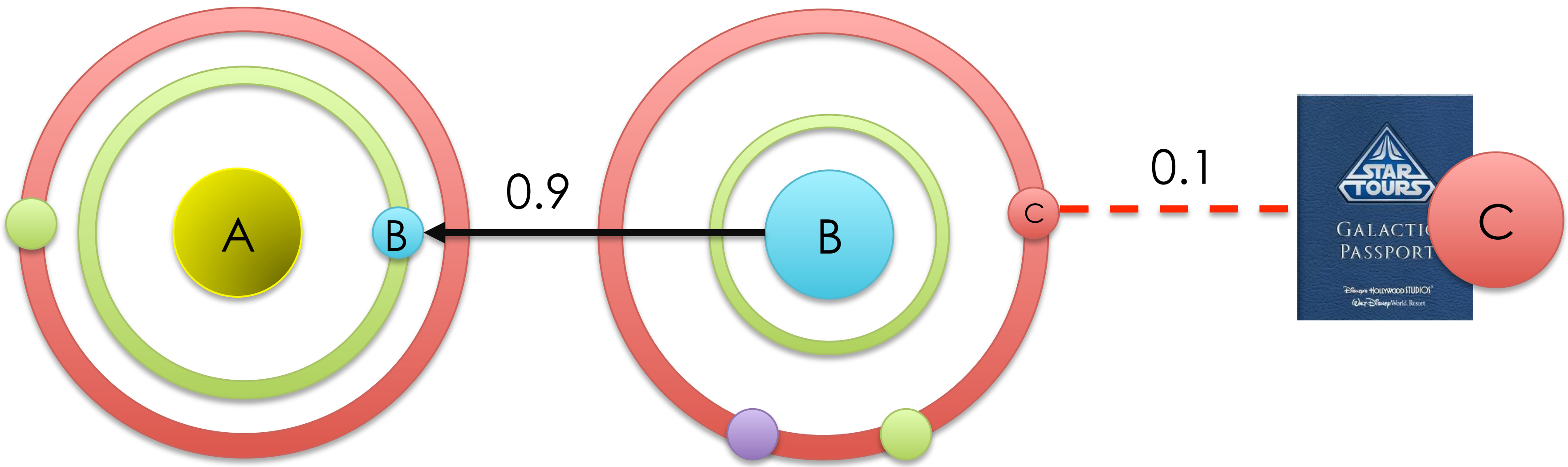
C shows B a fake passport

Example



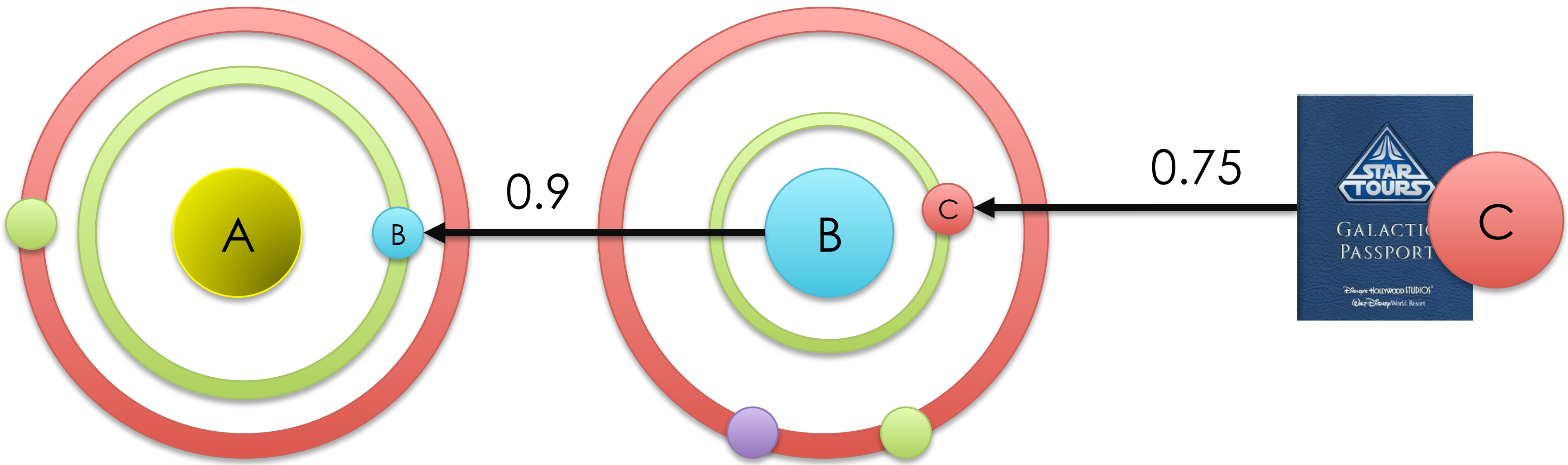
If B detects it, B reduces its trust in passports shown by C, possibly rendering them untrusted

Example



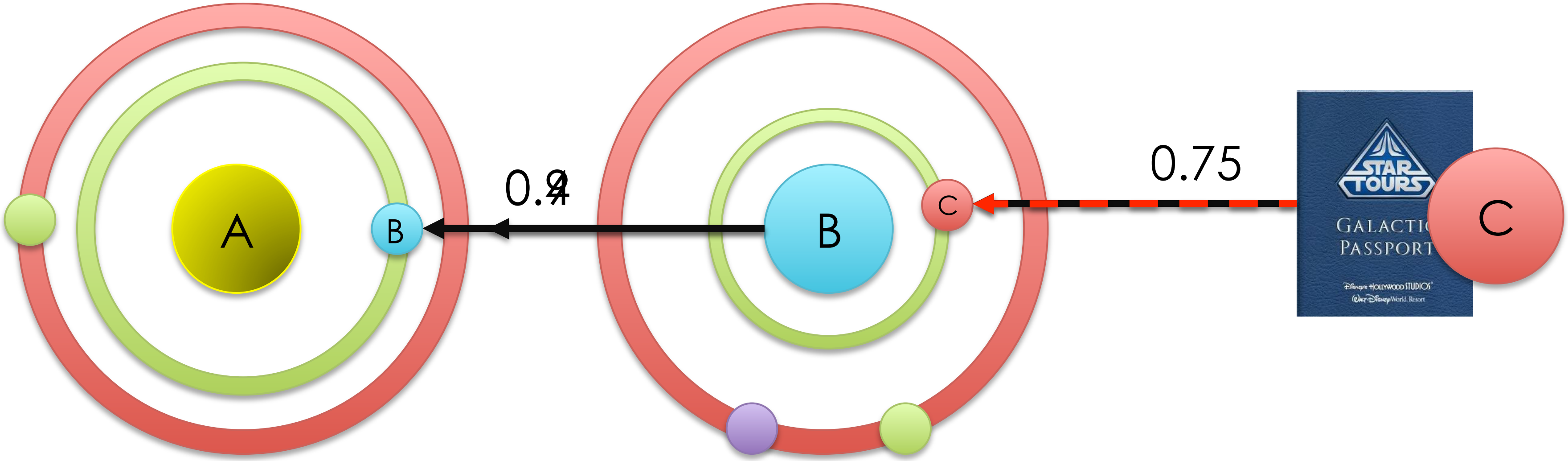
A no longer has a path to C, so C's passport is untrusted by A

Example



If B does not detect it, A's experience with C's passport won't match B's recommendation

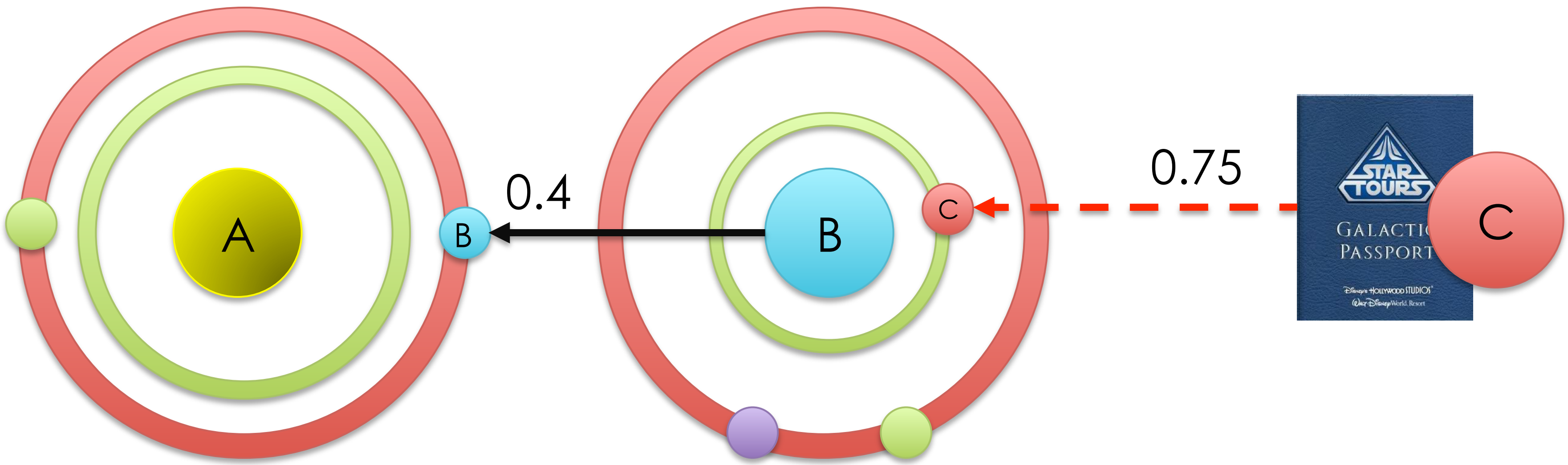
Example



A reduces its trust in B, possibly causing A to no longer trust C

36

Example



Eventually, C's reputation may force it off of the network

Entities

An entity is something in the Solar Trust Model

Trust

Trust(Observing Entity, Observed Entity, Context) = Degree of Trust

Trust is relative

The degree of confidence that someone has that something will meet a particular set of criteria.

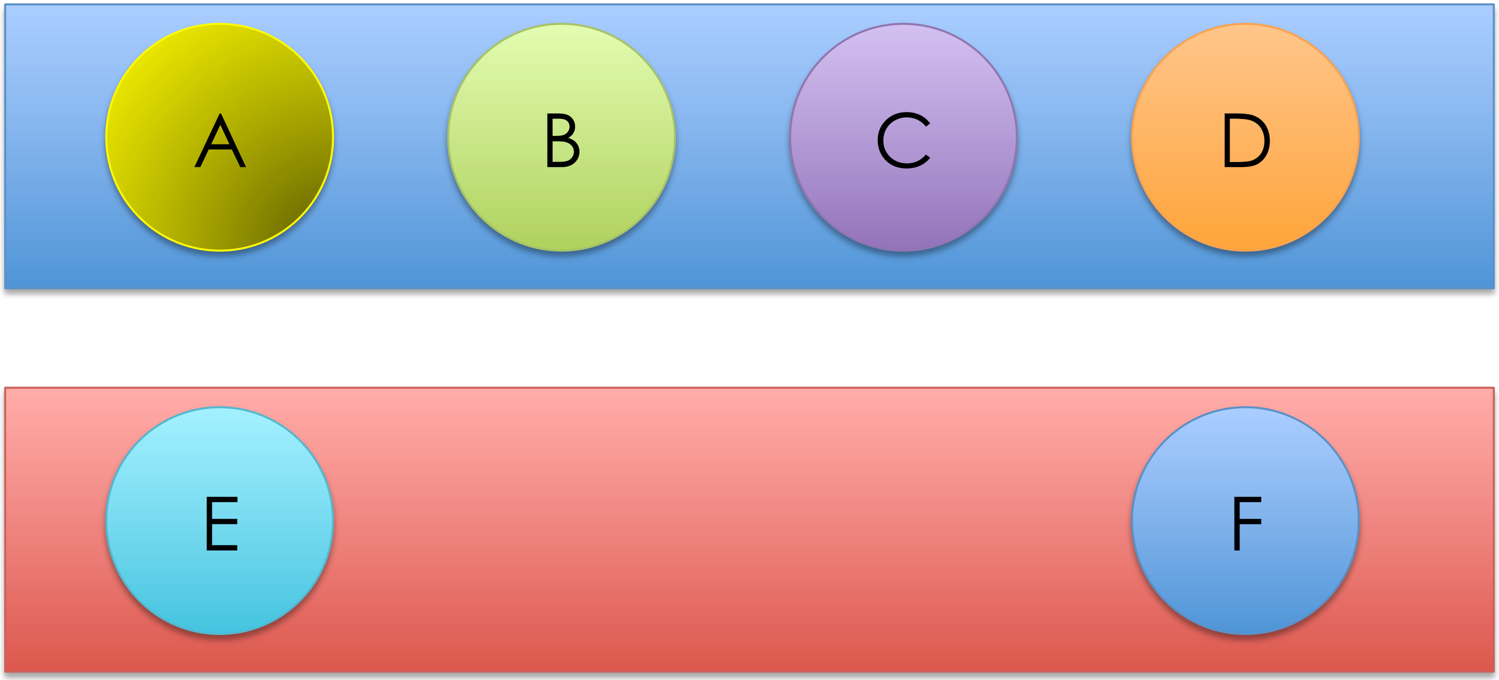
Context

- The set of information used in making a trust judgment
- A set of constraints on the applicability of the scope of that trust judgment
- Analogous to an agent's environment in machine learning

Solar Trust Server (STS)

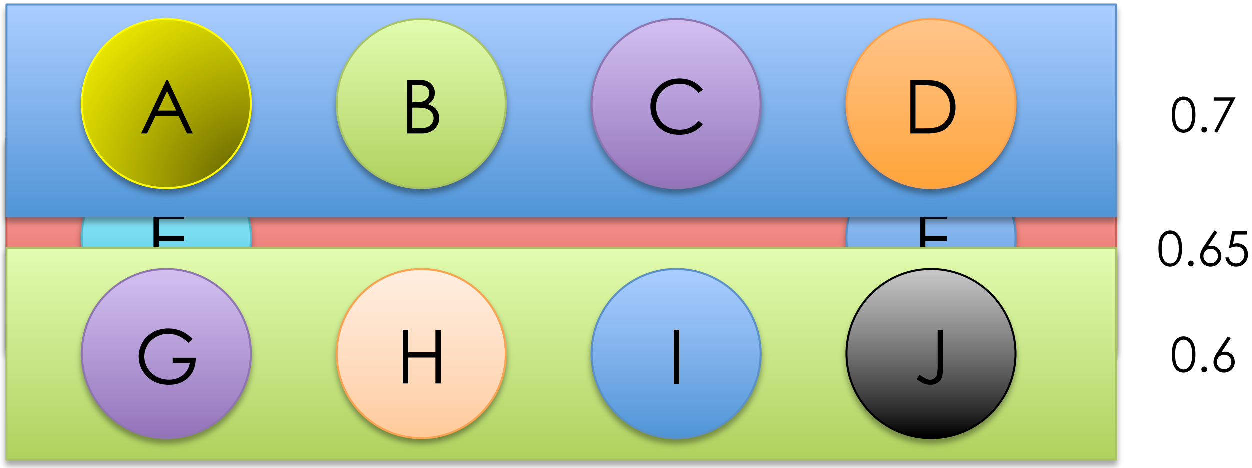
A server that acts as a proxy for a user and implements their trust policies

Trust Levels



Disjoint sets of objects that are trusted to the same degree in the same context

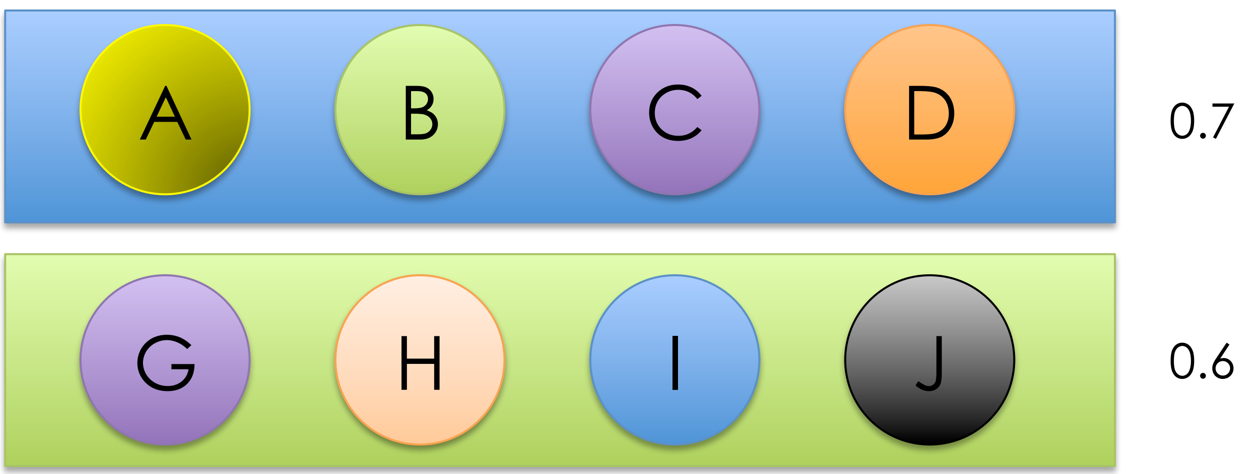
Dense Trust Levels



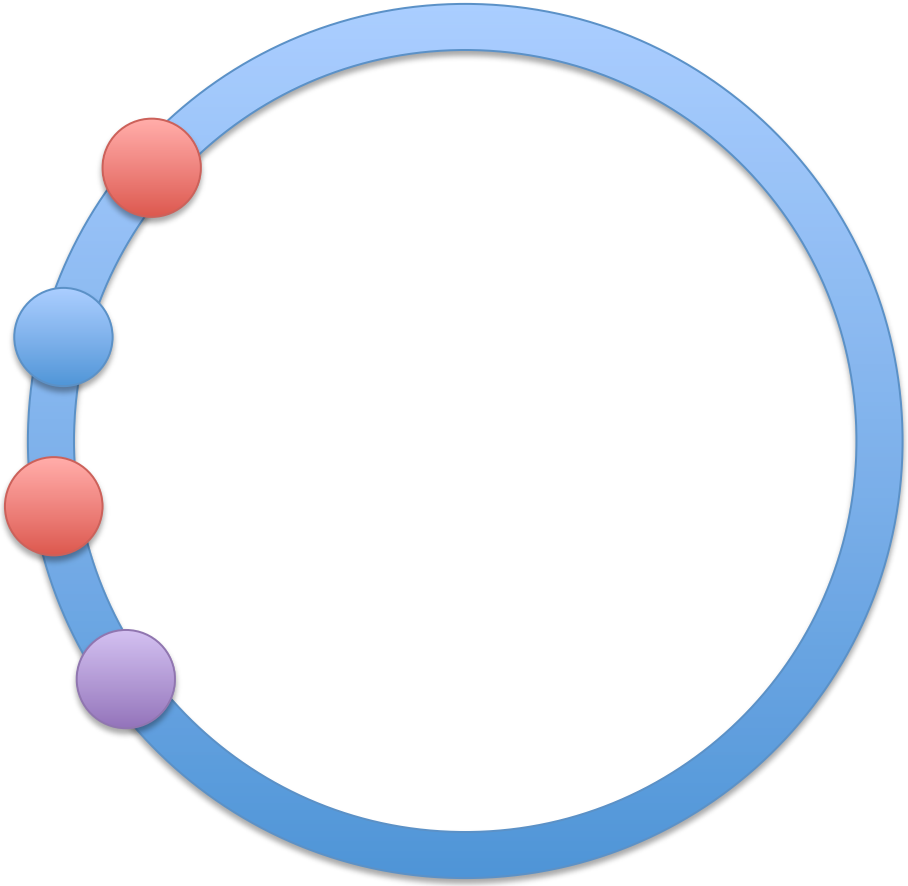
Labeled using a dense set to allow insertion of any number of intermediate trust levels

Labels of Trust Levels are NOT Values

- The value of a label is used only to create an ordering of trust levels.
- A label of 0.7 is **NOT** 0.1 more than a label of 0.6. It is simply has a higher position in the ordering.

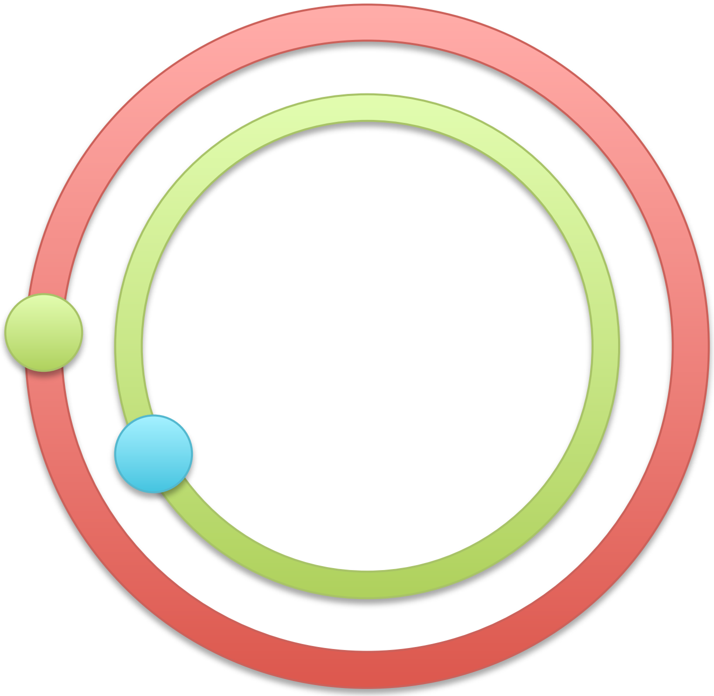


Orbit



A set of entities at the same trust level in context C

Orbits



Let $\mathbf{E} = \{E_1, \ldots, E_n\}$ be a set of entities.

Let $\mathbf{U} \in \mathbf{E} = \{U_1, \ldots, U_n\}$ be a set of users.

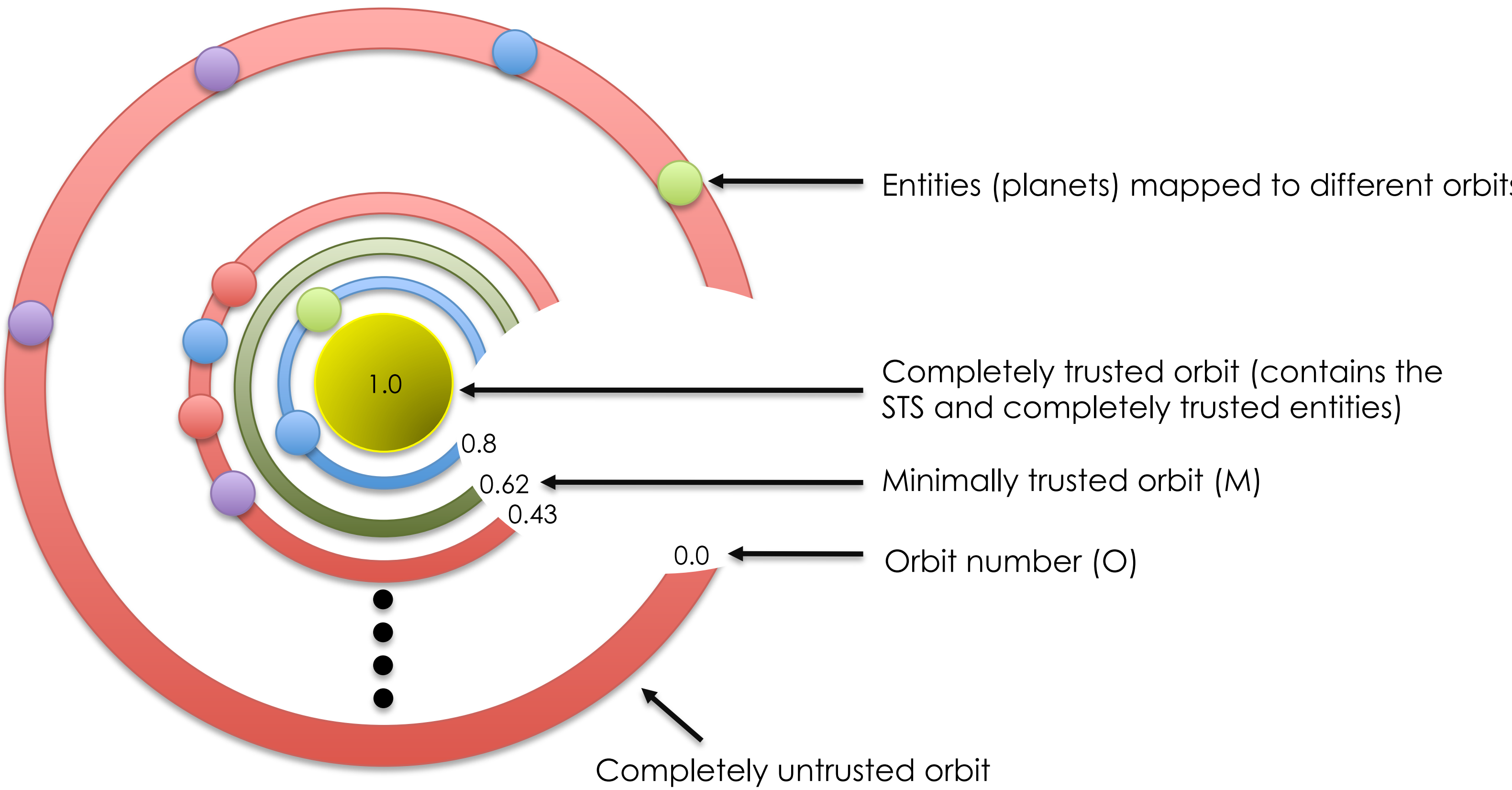
Let $\mathbf{C} = \{C_1, \ldots, C_n\}$ be a set of contexts.

Let $\mathbf{O} = \{O_1, \ldots, O_n\}$ be a set of orbits.

$$\forall E_i, E_j [E_i \in O_i, E_j \in O_j, O_i \neq O_j \rightarrow \mathrm{Trust}(U_i, E_i, C_i) \neq \mathrm{Trust}(U_i, E_j, C_i)]$$

Each orbit represents a different level of trust

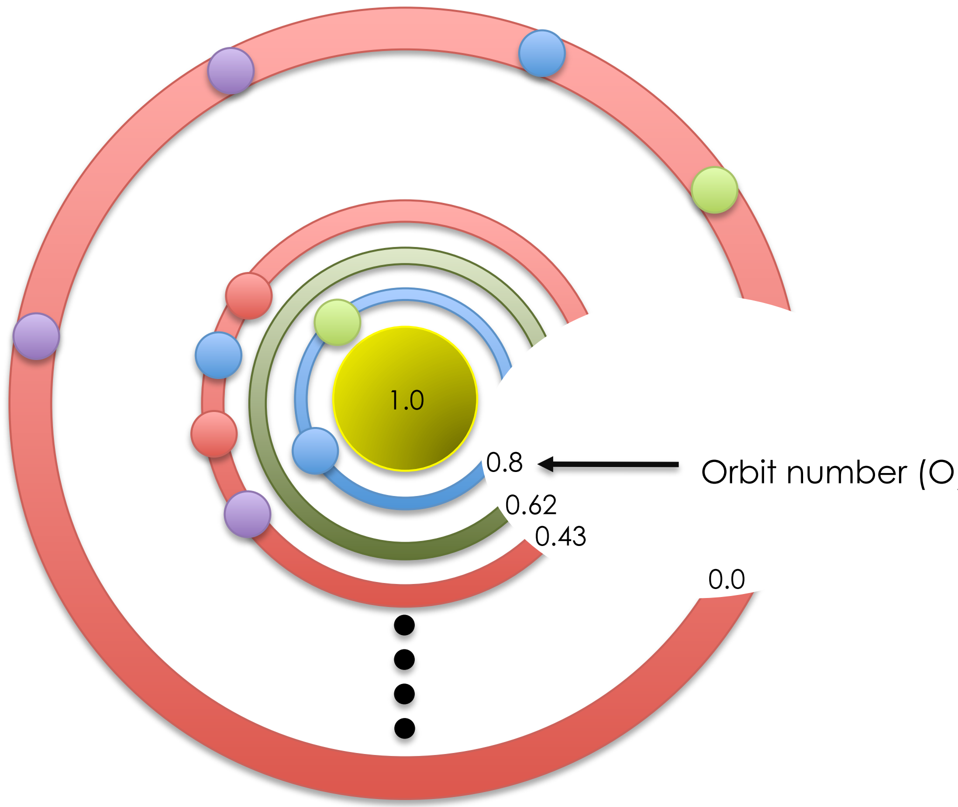
Solar Systems



An ordered set of disjoint orbits

Defined in a certain context by a given user

Solar Systems

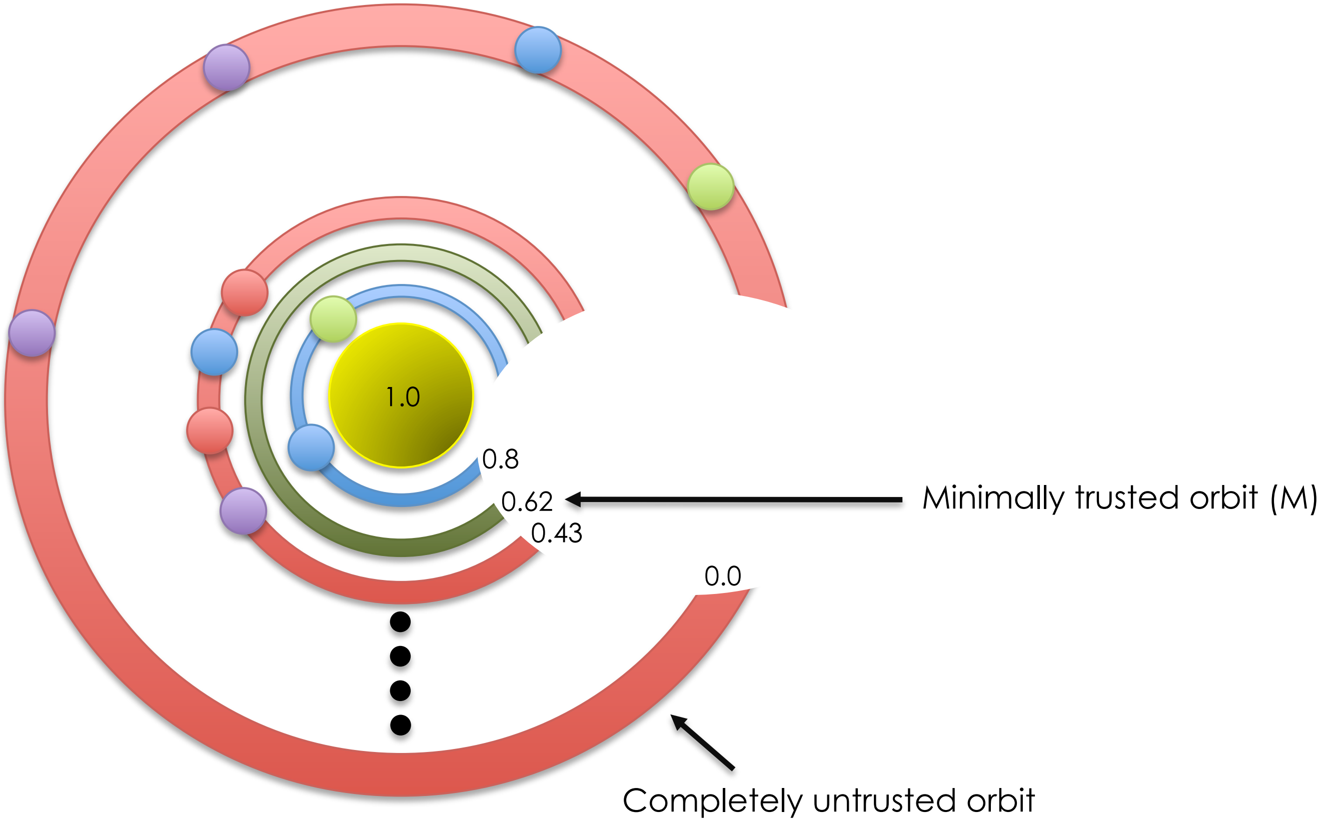


Given: O_i and O_j are orbits

$$(\forall i < j)[Trust(U_i, O_i, C_i) < Trust(U_i, O_j, C_i)]$$

Trust is ordered by orbit label

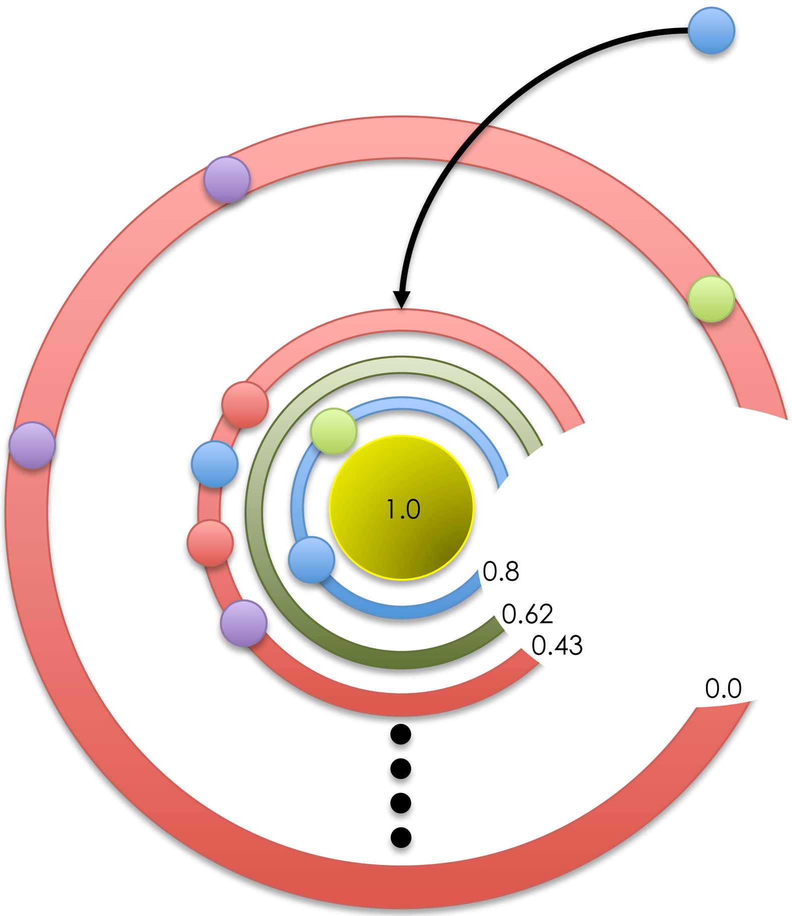
Minimally Trusted Orbit



An entity must be in an orbit ≥ the minimally trusted orbit in a given context to be trusted by the user

49

Policies



Given:

S_i is a solar system.

$\mathbf{O} = \{O_{0.0}, \ldots, O_{1.0}\}$ is a set of orbits, $O_n \in S_i$.

$\mathbf{C} = \{C_1, \ldots, C_n\}$ is a set of contexts.

$\mathbf{p} = \{p_1, \ldots, p_n\}$ is a set properties of entities.

$\mathbf{p}_l \subseteq \mathbf{p}$

$$f(C_j, p_l) = <S_i, O_n, C_j>$$

A policy generates <solar system, orbit> assignments based on specific properties and contexts

Policies

+

→ Orbit 0.7

→ Orbit 0.4

Example: Greater authentication evidence provides greater trust for some users

Relations

Given:
Alice is a brain surgeon
Context: brain surgery
Bob's policy on brain surgery

Bob places Alice in orbit **0.9** in his solar system in the brain surgery context

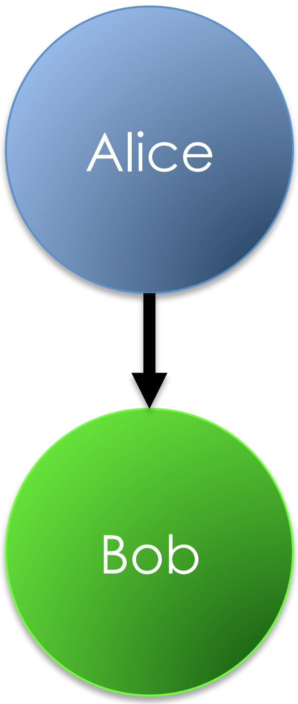
Given:
Alice is a brain surgeon
Context: auto repair
Bob's policy on auto repair

Bob places Alice in orbit **0.2** in his solar system in the auto repair context

$$\text{f(entity, policy)} = <\text{entity, orbit, solar system, context}>$$

Relations bind entities to orbits using policies

Direct Relations



Given:

E_R and E_S are two entities

S_R is the solar system of E_R

E_R has a direct relationship with E_S

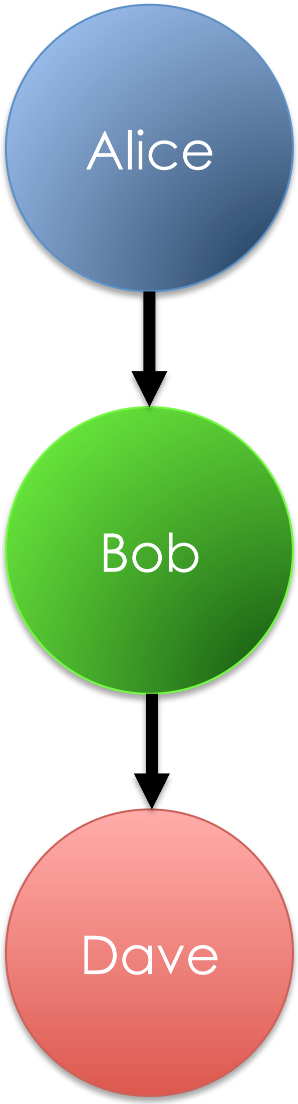
O_i is in an orbit of S_R

$$D_{RS} \rightarrow (E_S \in O_i) \wedge (O_i \in S_R)$$

Based on what one entity knows directly about another

Unidirectional

Indirect Relations



Given:

P_{RS} is a path from E_R to E_S

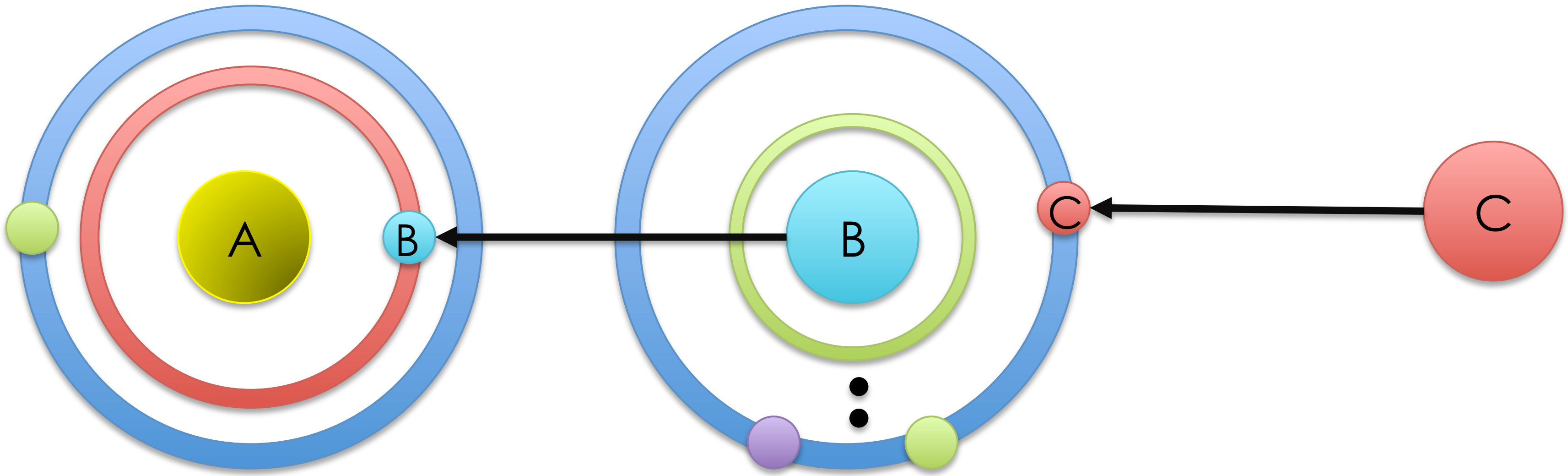
I_{RS} is an indirect relation from E_R to E_S

$$\forall D_{ij} \in P_{RS}[I_{RS} \rightarrow E_j \in O_i, O_i \in S_i]$$

Based on what one entity knows about another entity through intermediate parties in a given context

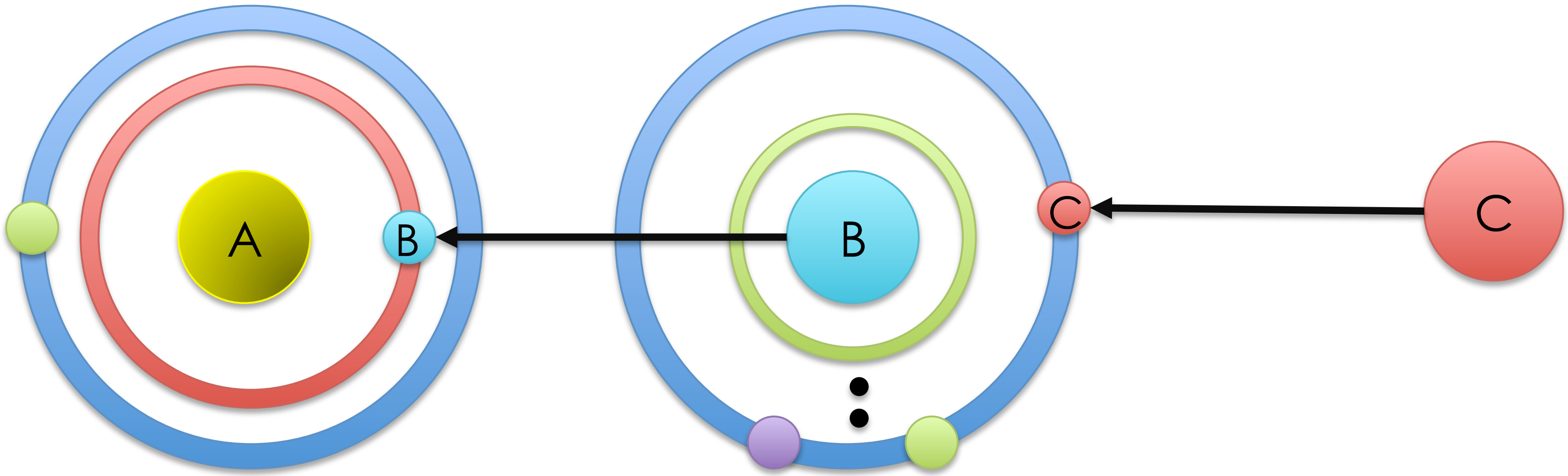
54

Paths



Represent trust relations

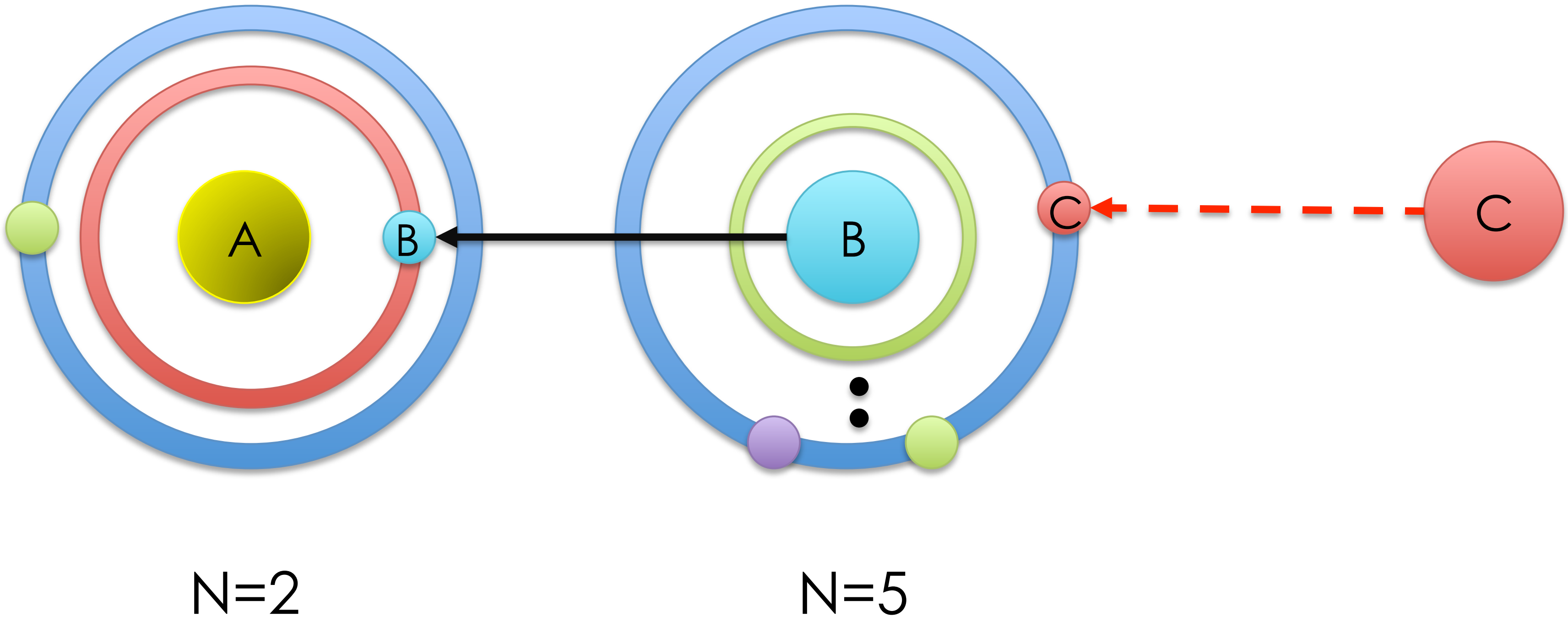
Paths



$$((S_1, O_1), \ldots, (S_{n-1}, O_n), (E_n, \emptyset))$$

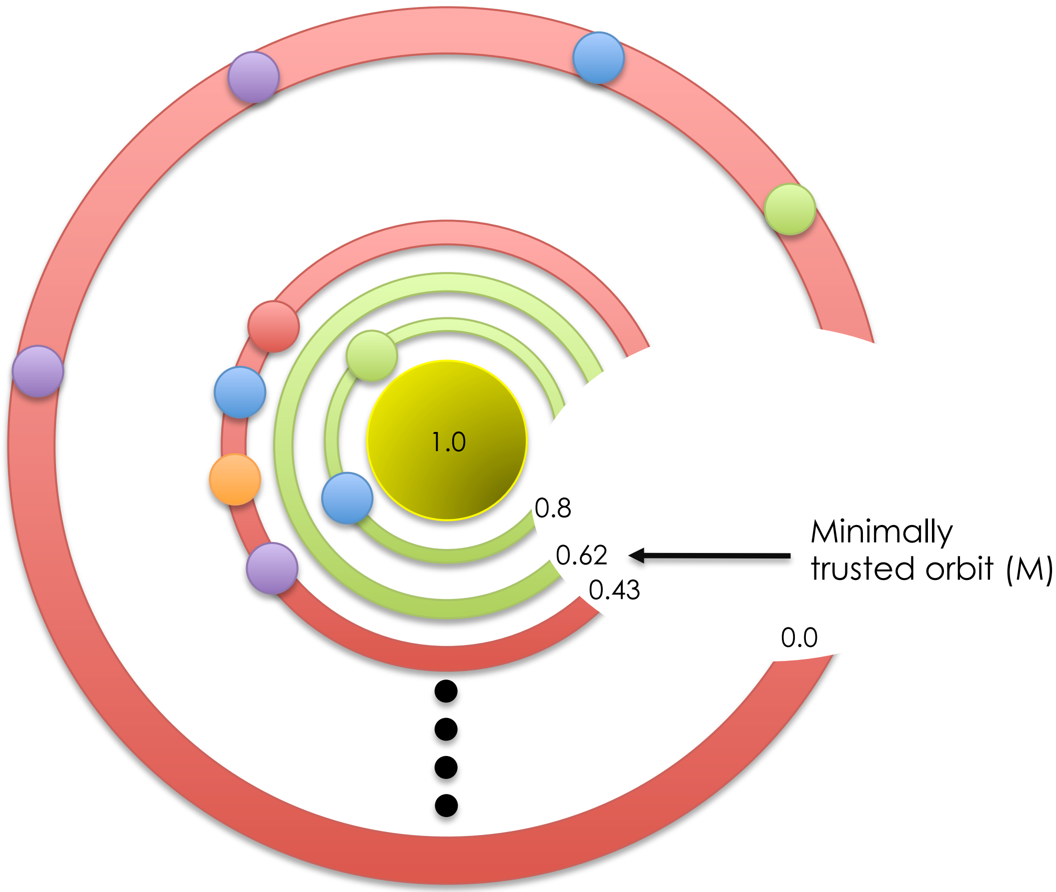
Represented with an ordered set of pairs

Maximum Path Node Count



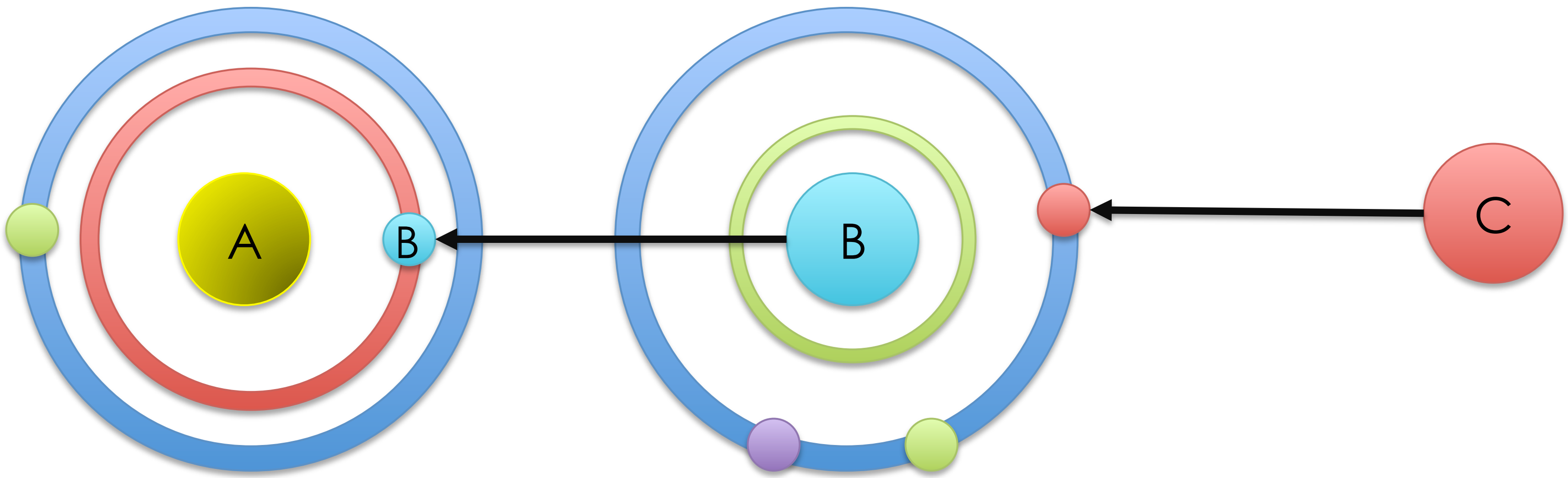
Each entity specifies the maximum node count (N) that it will accept in a given path

Sufficiently Trusted Direct Relations



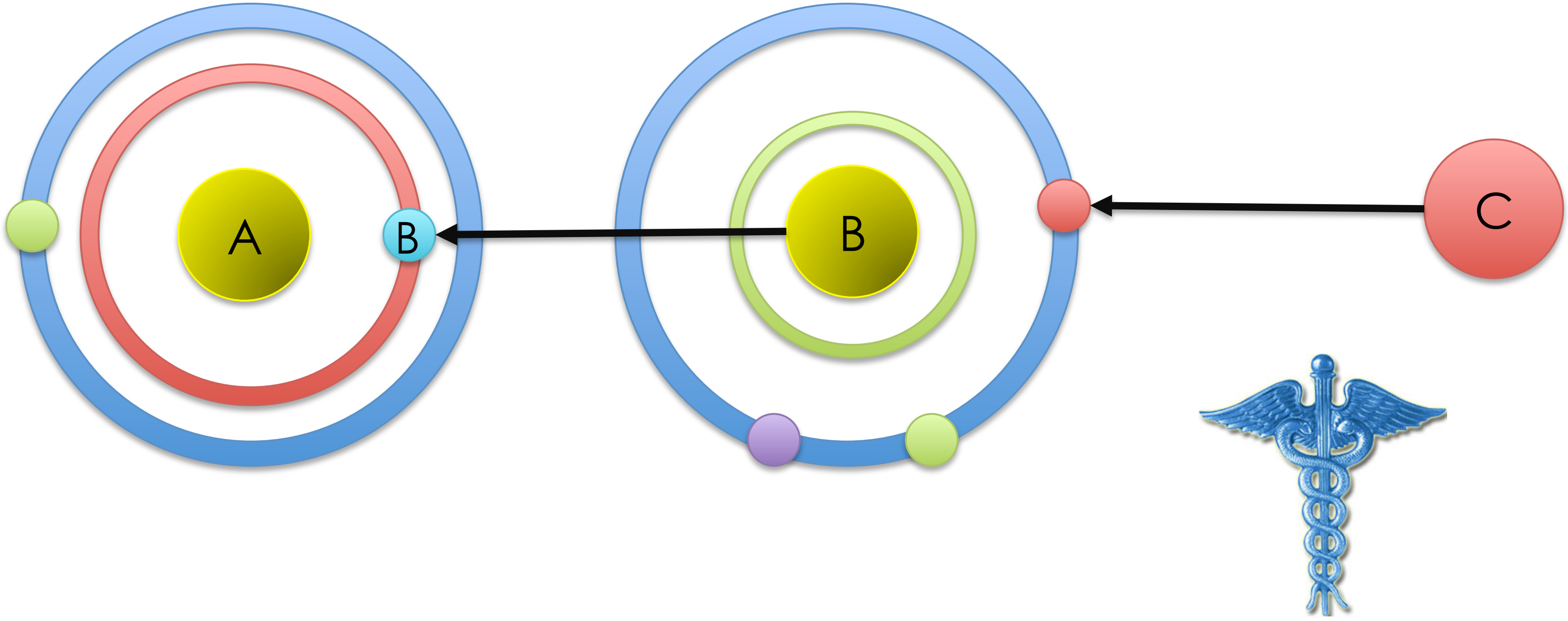
Occurs when an entity is in an orbit at least as trusted as the minimally trusted orbit in a given context

Sufficiently Trusted Indirect Relations



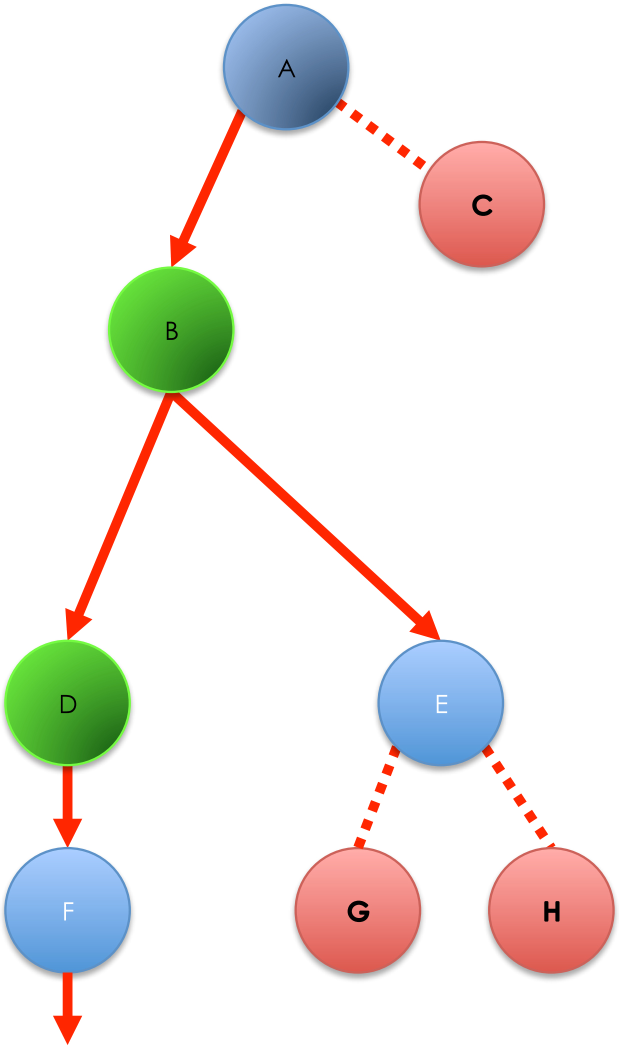
A path composed entirely of sufficiently trusted direct relations

Sufficiently Trusted Indirect Relations



A trusts B sufficiently in its current context. B trusts C sufficiently in its current context (ex: medicine)

Sufficiently Trusted Entities



$$T^{+}_{E_1 E_2} \rightarrow D^{+}_{E_1 E_2} \vee I^{+}_{E_1 E_2}$$

Entities a given user can reach through a path

Messages

Data sent from a sender to a receiver. Messages are trusted as much as the most trusted path to the sender.

62

Presentation Outline

Introduction

Defining Trust

Problems with Other Trust Models

How the Solar Trust Model Works (Overview)

Securely Mapping and Maintaining the Trust Network

Path Evaluation

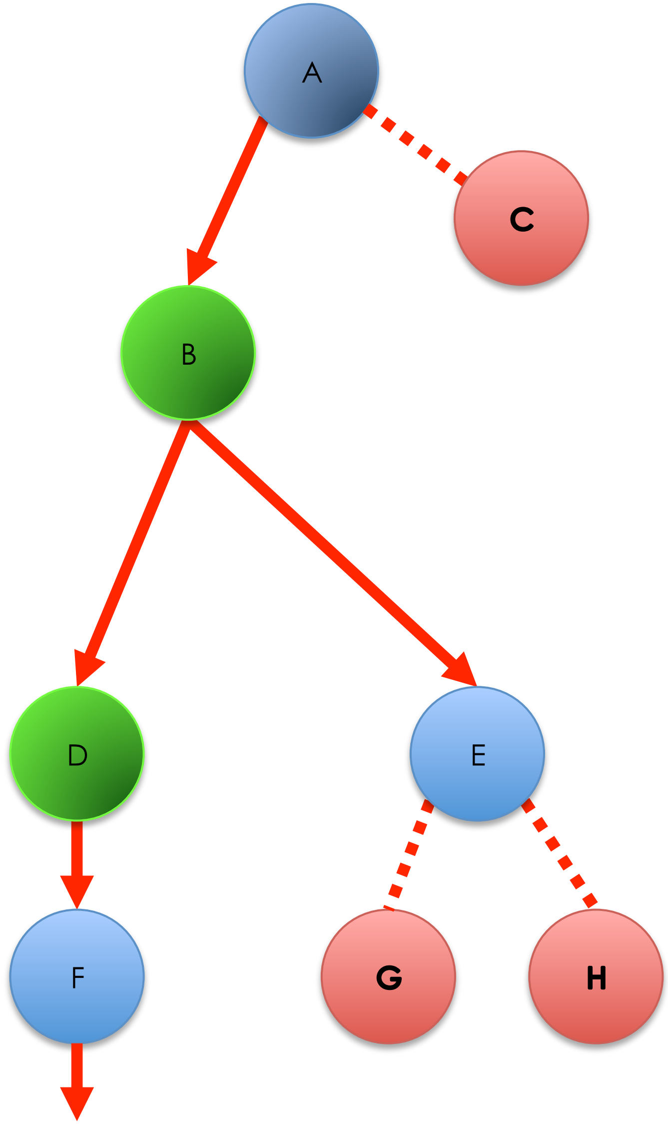
Computational Scalability

How the STM Addresses Problems with Other Trust Models

Future Work

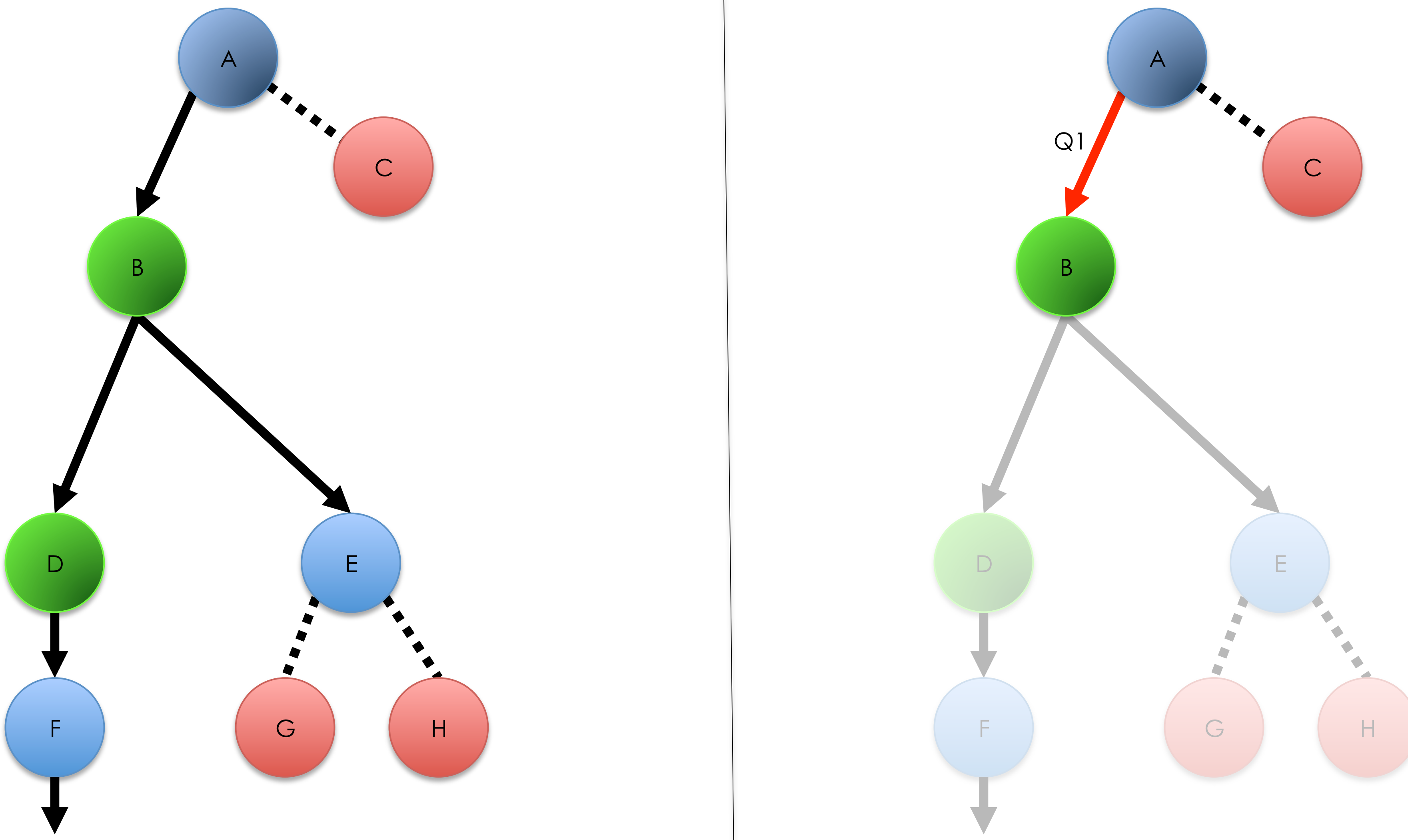
Contributions and Questions

The Path Discovery Problem



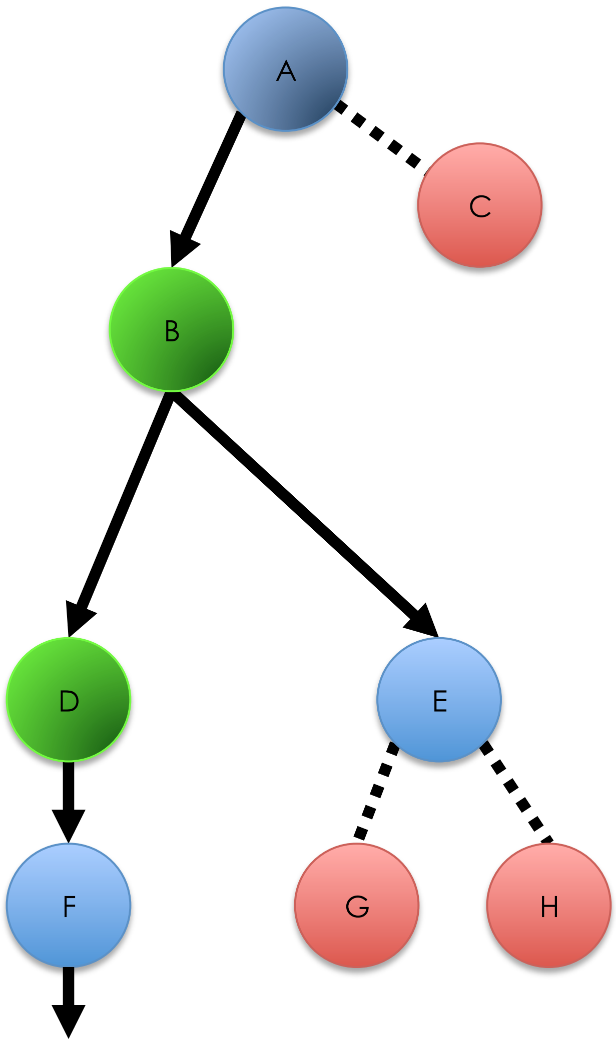
How can we securely find the DAG of all paths from a user to its sufficiently trusted entities?

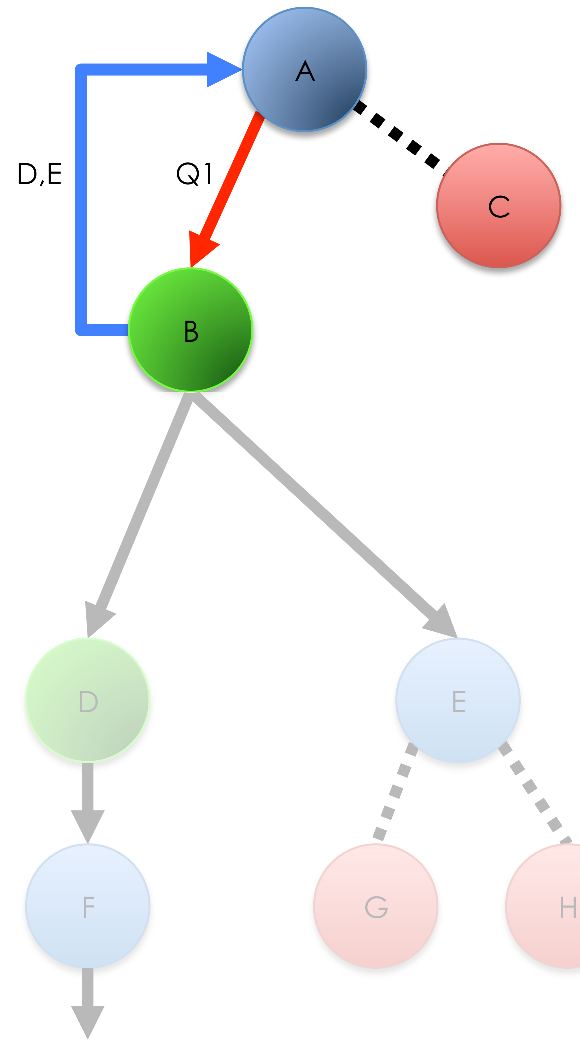
The Path Discovery Algorithm



A sends a path query message to its only sufficiently trusted direct relation, B

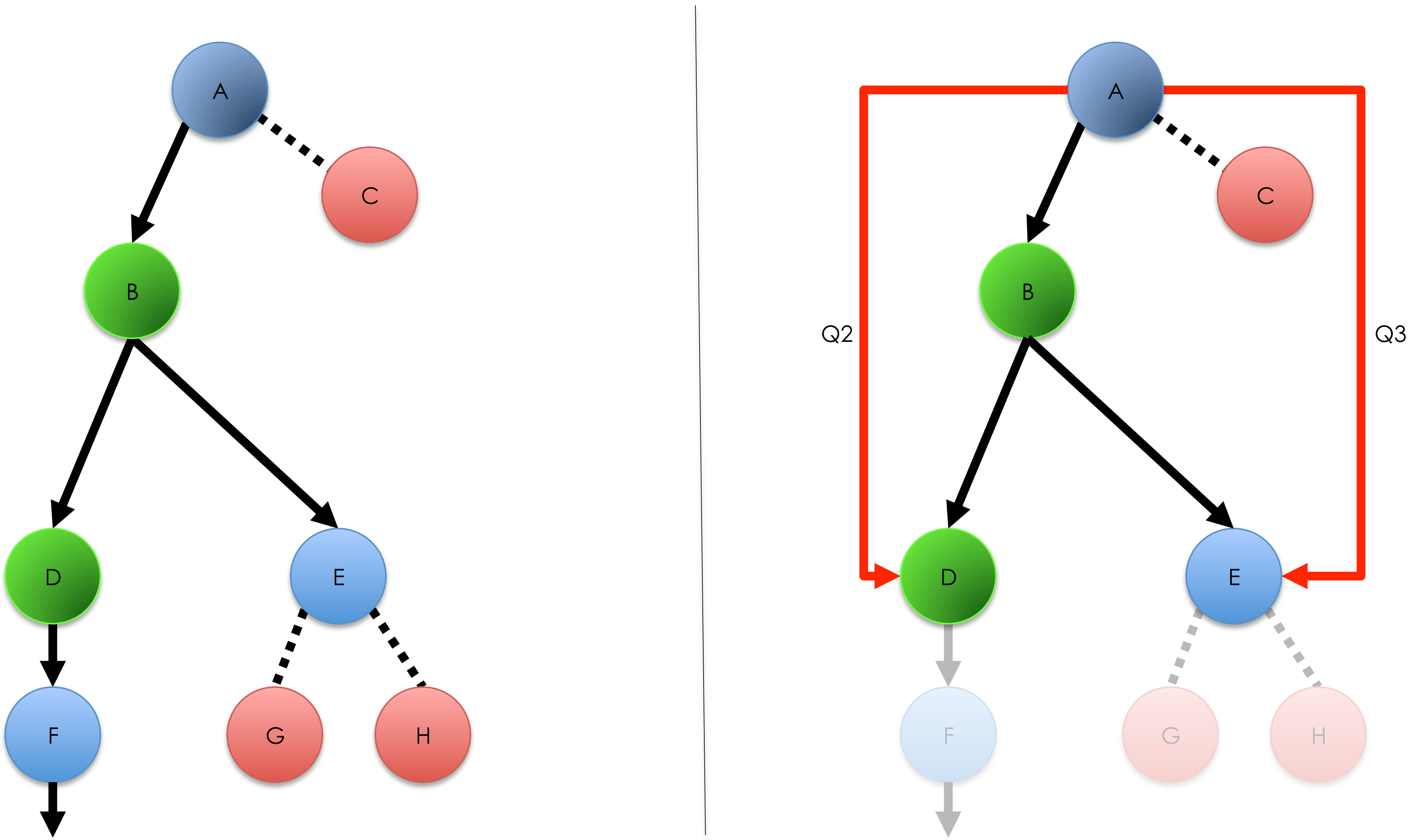
The Path Discovery Algorithm





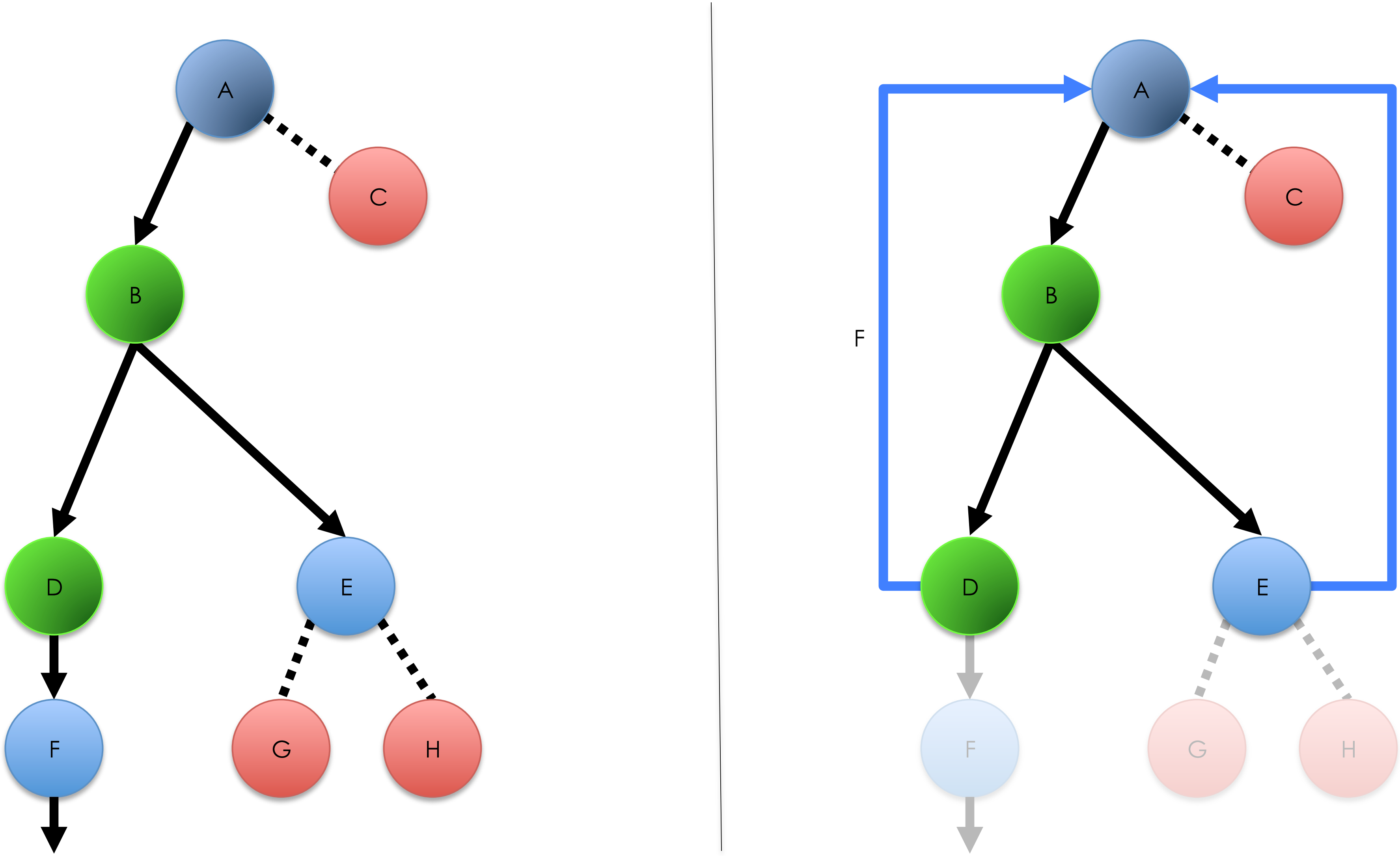
B replies with its sufficiently trusted direct relations

The Path Discovery Algorithm



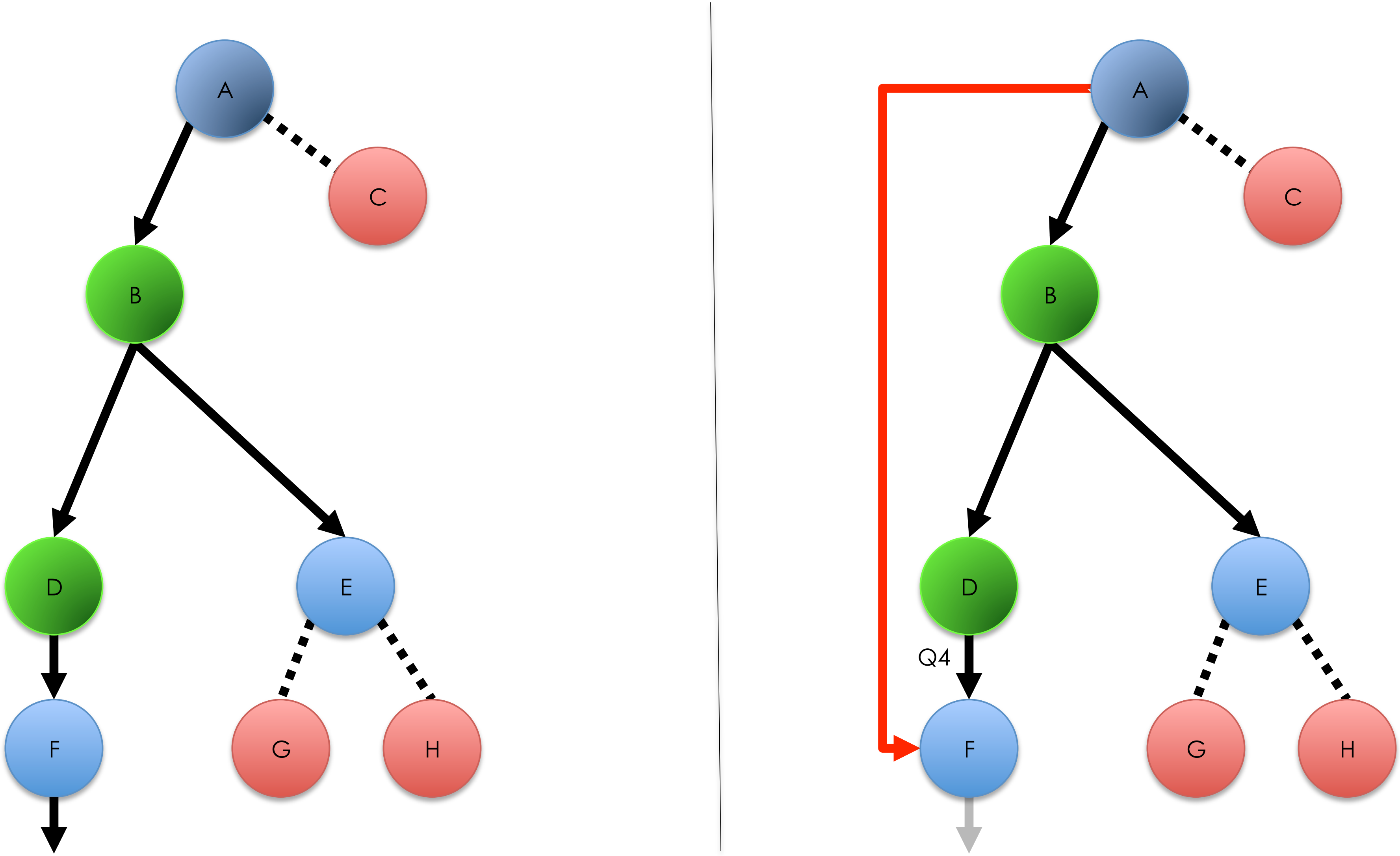
Repeat for D and E. E returns ∅ because it has no sufficiently trusted direct relations

The Path Discovery Algorithm



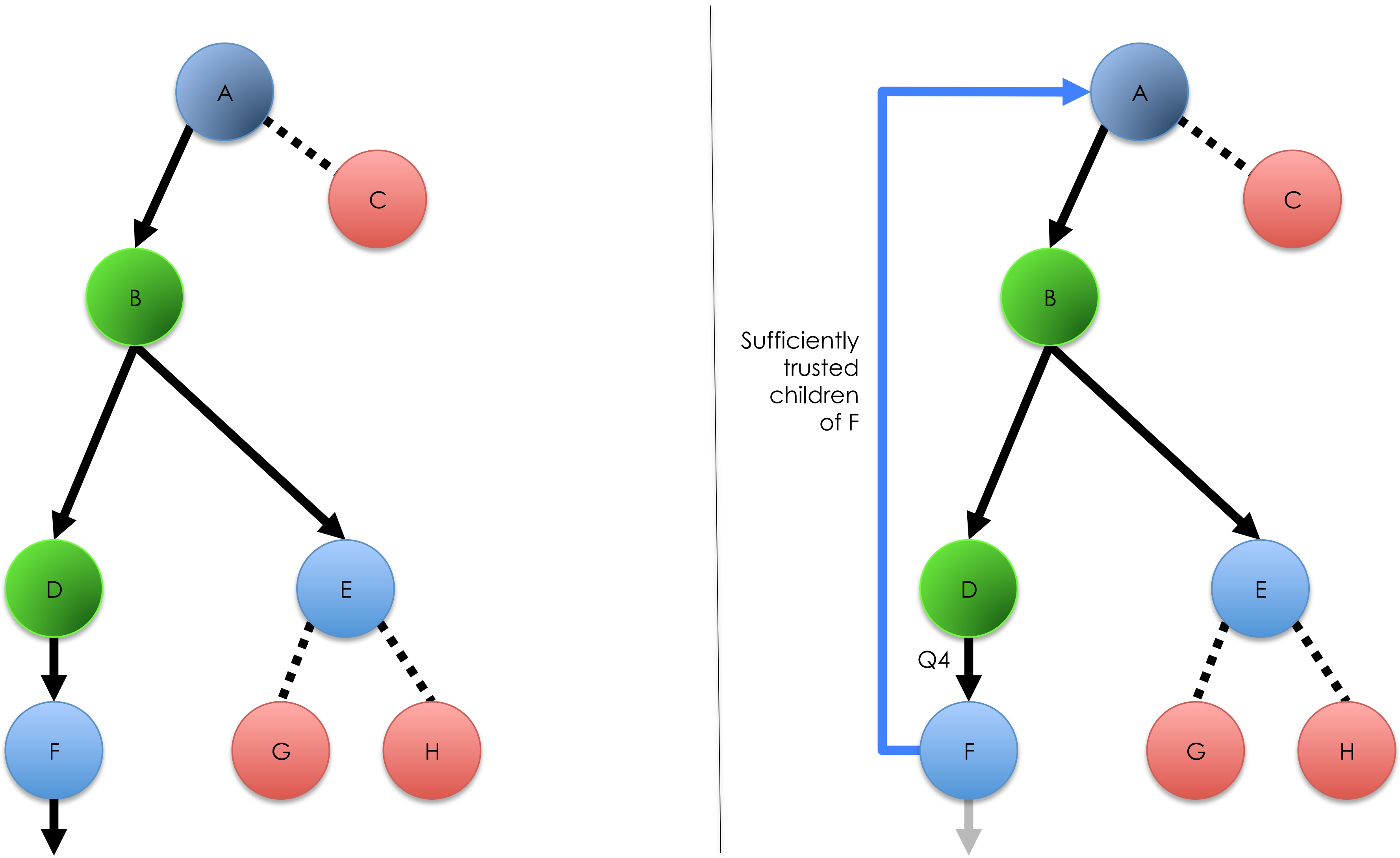
Repeat for D and E. E returns ∅ because it has no sufficiently trusted direct relations

The Path Discovery Algorithm



The procedure repeats until the path from A terminates

The Path Discovery Algorithm



The procedure repeats until the path from A terminates

Preventing Path Manipulation

Query and response messages are robust to manipulation!

Countermeasures include:

- Message and path signing
  (similar to, but predates, Blockchain)

- Nonces
  (prevents replay attacks)

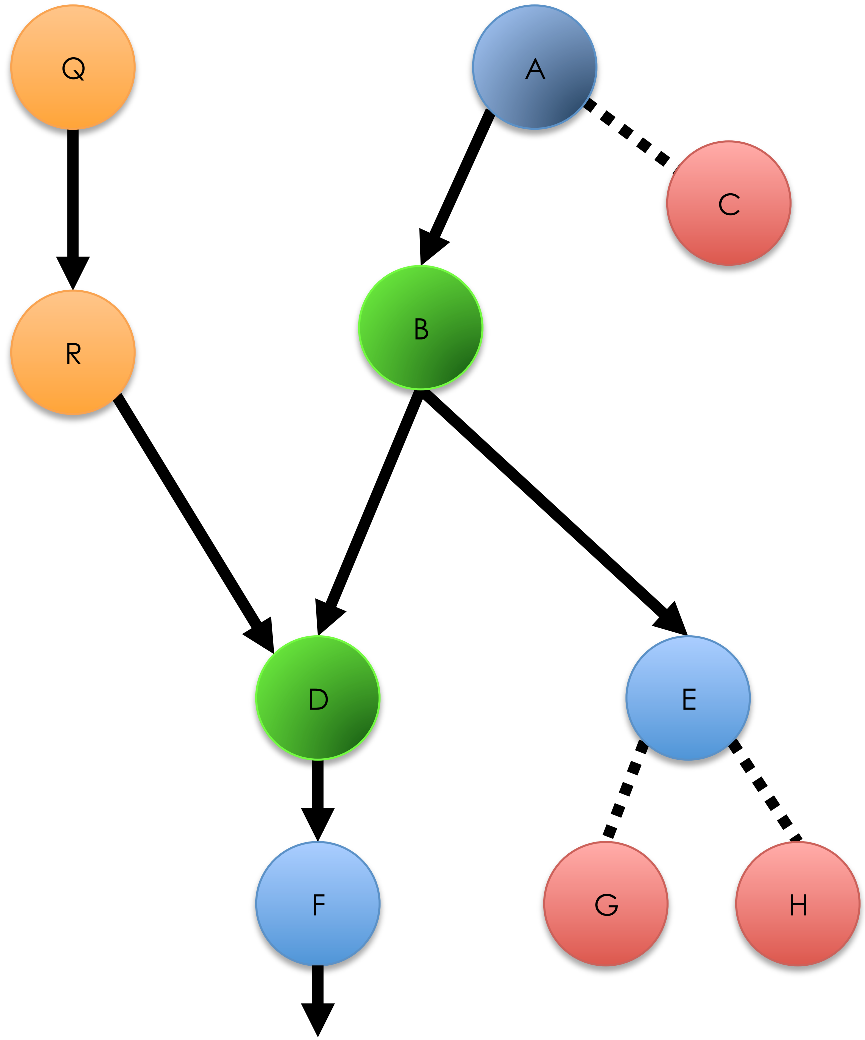
- Key trust evaluation
  A key is trusted as much as the path to the key

Path Updates

A path update algorithm updates all affected paths when a direct relation changes

Overlapping paths allow this to be done efficiently

Paths From Different Entities Overlap



Allows efficient path discovery and maintenance

Models real world relationships

Presentation Outline

Introduction

Defining Trust

Problems with Other Trust Models

How the Solar Trust Model Works (Overview)

Securely Mapping and Maintaining the Trust Network

Path Evaluation

Computational Scalability

How the STM Addresses Problems with Other Trust Models

Future Work

Contributions and Questions

Path Evaluation

- Paths are trusted no more than the orbit in which they originate

- Policies evaluate the properties of paths, further reducing their trustworthiness in some cases

Path Aging

- Paths monotonically decrease in trust over time unless refreshed
- This reflects the decreasing relevance of old observations over time in determining trust

Evaluating Context

Each solar system interacts with the others using their own interpreted contexts

Authentication

- An entity's identity can be authenticated by its observable properties, such as a public key

- That identity is trusted as much as the path to the identity

Certificate and Key Distribution and Revocation

- Certificates and keys can be sent as messages
- Trusted as much as the most trusted path to them
- If Entity E has no sufficiently trusted path to a certificate or key, it is revoked from E's perspective

Presentation Outline

Introduction

Defining Trust

Problems with Other Trust Models

How the Solar Trust Model Works (Overview)

Securely Mapping and Maintaining the Trust Network

Path Evaluation

Computational Scalability

How the STM Addresses Problems with Other Trust Models

Future Work

Contributions and Questions

Computational Scalability

- The number of relationships that anyone can have: O(nodes+edges)
  - Limited by the maximum path node count of every node along each path.
- Queries sent by each node: O(n)
- Replies to queries: O(n)
- Number of path updates sent when a relationship changes = number of paths that intersect the changed relationship: O(n)

Presentation Outline

Introduction

Defining Trust

Problems with Other Trust Models

How the Solar Trust Model Works (Overview)

Securely Mapping and Maintaining the Trust Network

Path Evaluation

Computational Scalability

How the STM Addresses Problems with Other Trust Models

Future Work

Contributions and Questions

How the Solar Trust Model Achieves Inter-organizational Scalability

- Trust is subjective
- No two individuals or organizations need to accept each other's trust scale, labels, levels, formulae, or a central authority

How the Solar Trust Model Achieves Context Sensitivity

- Trust relations take context into account
- Users choose the appropriate context for their needs
- Information is interpreted subjectively by users, based on their knowledge and experience

How the Solar Trust Model Provides Relative Trust

- Users may have any number of trust levels
- Trust levels are labeled with a dense set
- A new trust level can always be inserted between any two existing levels

How the Solar Trust Model Provides Non-Transitive Trust

- Trust information is interpreted by each node along a path of trust
- Each node decides how much it trusts information from other nodes

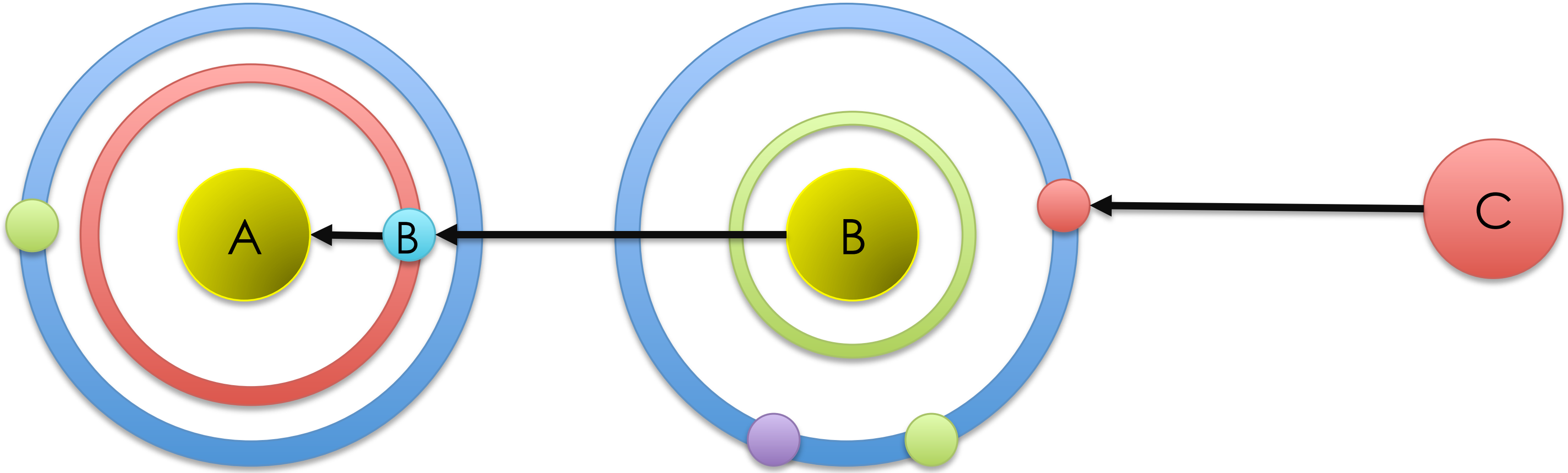
How the Solar Trust Model Provides Decentralized Trust

- There is no required central trust authority
- Each node computes trust based on its own policies, and information from other nodes

How the Solar Trust Model Achieves Interoperability

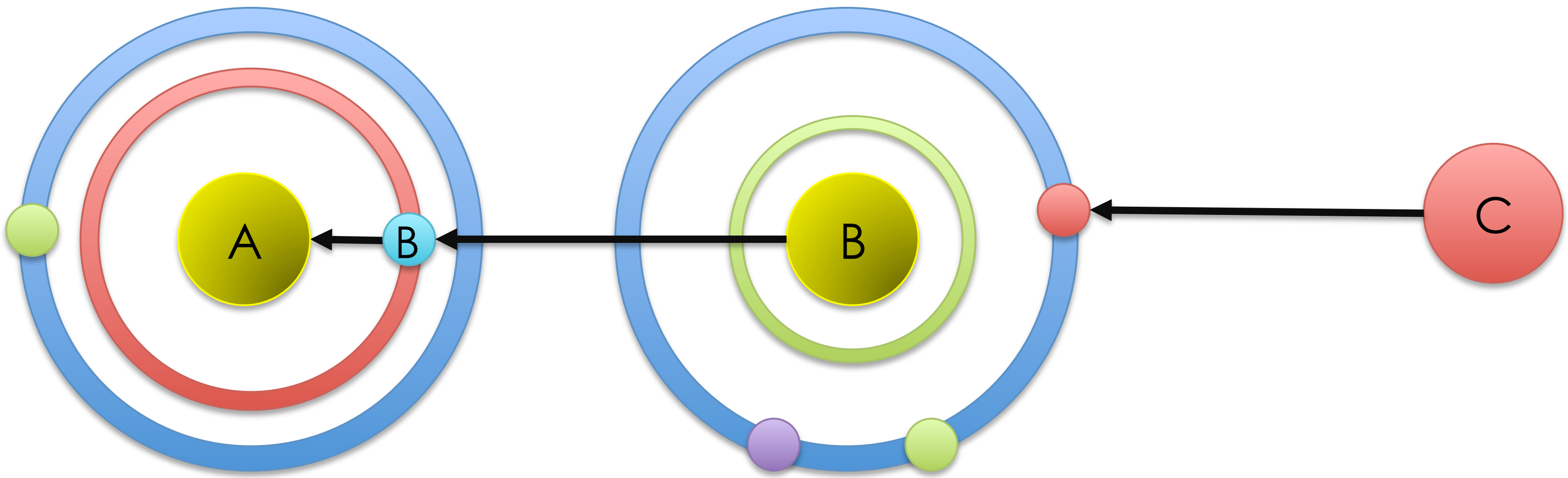
- No dependence on a central trust authority
- Trust is always determined from the perspective of each individual entity
- Advice of others can be followed to the extent it is trusted by each individual
- Decisions from other trust models can be used as inputs

Interoperability Example



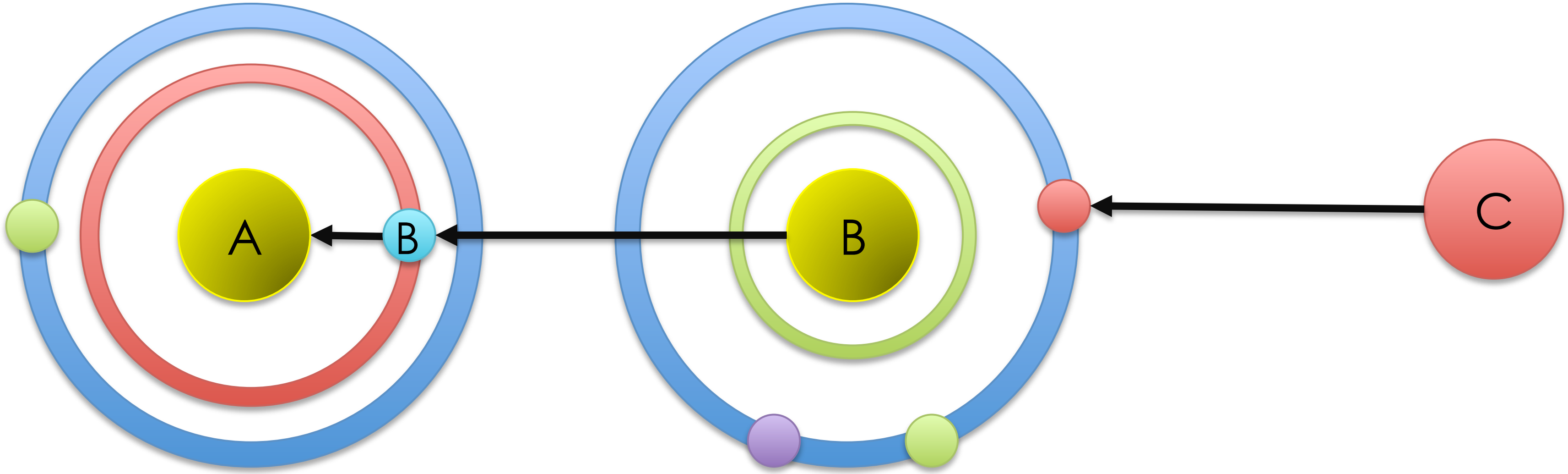
A orders its orbits using personal experience

Interoperability Example



B orders its orbits probabilistically, modeling expected behaviors based on past behaviors

Interoperability Example



C orders its orbits using outputs from another trust model

Presentation Outline

Introduction

Defining Trust

Problems with Other Trust Models

How the Solar Trust Model Works (Overview)

Securely Mapping and Maintaining the Trust Network

Path Evaluation

Computational Scalability

How the STM Addresses Problems with Other Trust Models

Future Work

Contributions and Questions

Future Trust Modeling Work

1. Exploration of statistical methods for use as policies

2. Use of reinforcement learning techniques to:

   A. Learn user preferences, in order to automatically assign entities to orbits.

   B. Learn optimal weights for identity properties in different contexts.

3. Development of multiple, independent STM implementations, leading to an RFC

Potential Applications of the STM to Aerospace Problems

1. How much can sensor data be trusted?
2. How much can you trust data from arbitrary sources?
3. Can a system of systems trust the behavior of its own components?
4. How should data from potentially untrustworthy sources be evaluated?
5. Data from two sources conflicts. Which should be trusted more?

Presentation Outline

Introduction

Defining Trust

Problems with Other Trust Models

How the Solar Trust Model Works (Overview)

Securely Mapping and Maintaining the Trust Network

Path Evaluation

Computational Scalability

How the STM Addresses Problems with Other Trust Models

Future Work

Contributions and Questions

Contributions

Developed the Solar Trust Model, which:

1. Efficiently represents user-specific trust relations using a dynamic trust network

2. Uses relative trust

3. Efficiently discovers and updates sufficiently trusted trust paths

4. Can be used for recommendations, authentication, key and certificate distribution and revocation

5. Does not require trust in a central trust authority

6. Has applications to current, real world problems

Questions