Beyond Proof-of-compliance: Security Analysis in Trust Management

Author: Ninghui Li
   John C. Mitchell
   William H. Winsborough
Published: Proceedings of 2003 IEEE Symposium on Security and Privacy
Presenter: Dongyi Li
Trust Management

- A form of **distributed access control** that allows one principal to **delegate** some access decisions to other principals.
Simple Inclusion
Complete trust delegation

Alice.authenticatedCash ← CityBank.authenticatedCash

\{Cash authenticated by Alice\} \sqsubseteq \{Cash authenticated by CityBank\}
Simple Inclusion
Complete trust delegation

Texas.Driver ← China.Driver
Intersection Inclusion
Partial trust delegation

\[ \text{Walmart.qualifiedAlcoholCustomer} \leftarrow (\text{SSA.Adult}) \cap (\text{CityBank.Accountnumber}) \]
Linking Inclusion
Linking trust delegation

Alice.friend ← Alice.husband.friend.wife
Linking Inclusion

- TexasTransportation.ticketfree←UTsystem.University.student
In this paper, we cannot represent this kind of delegation by RT[0] language.
Threshold
Group trust delegation
Delegation

- Simple Inclusion
- Intersection Inclusion
- Linking Inclusion
- Threshold
Simple Member without any delegation

UTSA.student ← Bob
Simple Member without any delegation.

- Rachael.trustworthy ← Joey
- Rachael.trustworthy ← Monica
Trust Management

- Simple Member
- Delegation
  - Simple Inclusion
  - Intersection Inclusion
  - Linking Inclusion
  - Threshold
Delegation Advantages

Greatly enhances flexibility and scalability in distributed systems.
Glossary

- Policy, Policy Statement: Describes memberships and delegations, $P$;
- State, State of the TM: The union of all policies of all principals, $p$;
- $P \mapsto P'$: Principals are allowed to add or remove policies, so the state $p$ is changed to $p'$.
- $p \vdash Q$: Given a state $p$ and a Query $Q$, the relation means that $Q$ is true in $p$, or $Q$ is allowed in $p$. 
Glossary

- **Principal**: This paper uses A, B, C, D, E, F, X, Y and Z some time with subscript, to denote principals. I use real names such as Alice and Carrie in my presentation.

- **Role Name**: A word over some given standard alphabet, this paper use r, u and w, sometime with subscripts, to denote role names, I use some more comprehensive word.
Role: Takes the form of a principal followed by a role name, separated by a dot;
For example: Rachael.friends.
Rachael.friends means Rachael has the authority to designate the members of Rachael.friends.
Problem in Delegation

- Reduce the control that a principal has over the resources it owns.
Alice.guest ← Bob
Alice.guest ← Bob.date
Bob.date ← Charlie
However…

How could you bring her to my party!
Alice.guest ← Bob
Alice.guest ← Bob.date
Bob.date ← Charlie

So, Alice.guest ← Charlie
\( P \mapsto P' \)

\[
\{\text{Alice.guest } \leftarrow \text{Bob}\} \mapsto \\
\{\text{Alice.guest } \leftarrow \text{Bob}; \\
\text{Alice.guest } \leftarrow \text{Bob.date}; \\
\text{Bob.date } \leftarrow \text{Charlie}\}
\]
Problem origin

- Problem happens when we add or delete some policies, such as we add Alice.guest ← Bob. date;
  Bob. date ← Charlie

Things may be more and more out of control if Bob delegate more to others.
What should Alice do?

- Bob has to be invited.
- Charlie should not be invited.
Security Analysis

Existential
- Simple Safety, Existential Membership:
- Liveness, Existential Boundedness

Universal
- Simple Availability, Universal Membership
- Bounded Safety, Universal Boundedness
- Mutual Exclusion, Universal
- Containment, Universal
Existential Membership
Simple Safety

Does there exist a state in which a specific principal has access to a given resource?

Is \( \text{Alice.guest} \leftarrow \text{Charlie} \) possible?

\[ p \mapsto p' \mapsto p'' \mapsto p''' \mapsto p'''' \mapsto p''''' \mapsto p'''''' \ldots \]
Existential Boundedness
Liveness

Is it possible that a set of all principals that have access to a given resource bounded by a given set of principals.

Is \{Bob\} \sqsubseteq Alice.guest possible?

\[ p \mapsto p' \mapsto p'' \mapsto p''' \mapsto p'''' \mapsto p''''' \ldots \]
Universal Membership 
Simple Availability

In every state, does a specific principal have access to a given resource.

Is Alice.guest ← Bob necessary?

\[ p \mapsto p' \mapsto p'' \mapsto p''' \mapsto p'''' \mapsto p''''' \mapsto \ldots \]
Universal Boundedness
Bounded Safety

In every state, is the set of all principals that have access to a given resource bounded by a given set of principals.

Is \{Bob\} ⊆ Alice.guest necessary?

\[ p \mapsto p' \mapsto p'' \mapsto p''' \mapsto p'''' \mapsto p''''' \mapsto p'''''' \ldots \]
Universal Mutual Exclusion

In every state, are two given properties mutually exclusive.

\[ p \mapsto p' \mapsto p'' \mapsto p''' \mapsto p'''' \mapsto p''''' \mapsto p'''''' \mapsto p''''''' \mapsto \ldots \]
Universal Inclusion
Containment

In every state, does every principal that has one property also have another property.

Is Alice.guest \(\subseteq\) Bob.date necessary?

\[ p \mapsto p' \mapsto p'' \mapsto p''' \mapsto p'''' \mapsto p''''' \mapsto p'''''' \ldots \]
HRU Model

- Harrison-Ruzzo-Ullman Model

Access Matrix

‘The safety problem for protection systems under this model is to determine in a given situation whether a subject can acquire a particular right to an object.’

- Simple Safety is undecidable
‘...to our knowledge, no prior work investigates security analysis for trust management systems in the sense of verifying security properties that consider state changes in which restrictions are placed on allowed changes.’
Some of previous studies only considering queries in a fixed state’

‘Some consider universal analysis where no restriction is placed on how the state may grow’
Restrictions

- Growth-restricted: no policy defining these roles can be added
- Shrink-restricted: policy defining these roles cannot be removed.

\[ P \xrightarrow{R} P'' \xrightarrow{R} P'''' \xrightarrow{R} P''''' \xrightarrow{R} P'''''' \]
Trusted Principals

- We call those who make the agreement on some restrictions and would like to report their changes on policies as Trusted Principals.
- So what security questions can we answer even if we cannot monitor those who are un-trusted and can add or delete policies arbitrarily.
Lower Bound

Imagine ...
Lower Bound

- The only policies remaining are in the R-restricted set.
- Universal Membership, so we are able to know who will always be in the member list.
- Existential Boundedness, if the answer is ‘no’ in the case of Lower Bound, then the answer is ‘no’ forever.
Upper Bound

Suppose ...
Upper Bound

- Existential Membership
  Is it possible that the authorization leaked to some ‘bad guy’?

- Universal Boundedness
  Can we always constrain the authorization to a certain group?
Upper Bound

- G-unbounded:
  - Definite: g-unrestricted roles (un-trusted)
  - Possible: g-restricted roles (trusted)
How to compute upper Bound

We can consider one principal that does not occur in p to determine whether a role is g-unbounded.

To decide whether A.r is g-unbounded
Step 1: we add E to principal(p)
Step 2: check whether there exists a reachable state p’ such that A.r ←E
Security Analysis

Existential
- Simple Safety, Existential Membership:
- Liveness, Existential Boundedness

Universal
- Simple Availability, Universal Membership
- Bounded Safety, Universal Boundedness
- Mutual Exclusion, Universal
- Containment, Universal
Future Work

- Containment Analysis
- Making restrictions according to current policy state.