

Approximating SAML Using Similarity Based Imprecision

G. Navarro¹ and S. N. Foley²

¹Dept. of Information and Communications Engineering
Universitat Autònoma de Barcelona, Spain.

²Department of Computer Science
University College, Cork, Ireland.

INTELLCOMM 2005, Montreal.

Outline

- 1 Outline
- 2 Introduction
 - Applications of Imprecise Security
- 3 Similarity-based Imprecision
 - SBIS Characteristics
 - Similarity function
 - Similarity threshold
 - SBIS in a SAML scenario
- 4 Conclusions

Introduction

absolute security vs. imprecise security

Introduction

absolute security vs. imprecise security

- **Absolute security** systems may fail in some situations:
 - Users share or disclose passwords to facilitate system access (Adams and Sasse, Comm. ACM 1999).
 - A strategy used by employees to pressure management in labour disputes is to **work to rule** (Odlyzko, FC2003).

Introduction

absolute security vs. imprecise security

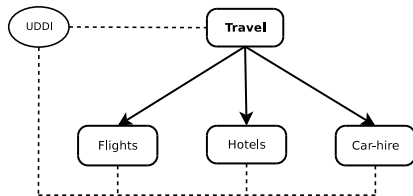
- **Absolute security** systems may fail in some situations:
 - Users share or disclose passwords to facilitate system access (Adams and Sasse, Comm. ACM 1999).
 - A strategy used by employees to pressure management in labour disputes is to **work to rule** (Odlyzko, FC2003).
- **Imprecise security**: allow a degree of imprecision to provide more flexibility and usability.
 - normally reducing the security of the system.

Some applications of imprecise security

- Some applications of imprecise security:
 - Overcome complexity in large organisations.
 - Emergency situations.
 - Ineroperbility of heterogeneous systems.

Some applications of imprecise security

- Some applications of imprecise security:
 - Overcome complexity in large organisations.
 - Emergency situations.
 - Ineroperbility of heterogeneous systems.
- Sample scenario: Web Services aggregation:



Similarity based imprecision

provide imprecision based on **similarity of authorisation**

→ *Supporting imprecise delegation in KeyNote using similarity measures.*, Foley 2002 (ISPW'02).

Similarity based imprecision

provide imprecision based on **similarity of authorisation**

→ *Supporting imprecise delegation in KeyNote using similarity measures.*, Foley 2002 (ISPW'02).

SBIS - Similarity-based Imprecise Security.

Similarity based imprecision

provide imprecision based on **similarity of authorisation**

→ *Supporting imprecise delegation in KeyNote using similarity measures.*, Foley 2002 (ISPW'02).

SBIS - Similarity-based Imprecise Security.

- SBIS system characteristics:
 - Accountability.
 - Auditability.
 - Constrained entry points.
 - Deterrents.
 - Least intrusive.

Similarity

- **Similarity function:** (i.e. P is the set of permissions)

$$_ \sim _ : (P \times P) \rightarrow [0, 1]$$

- $x \sim x = 1 \forall x \in P$
- $x \sim y = y \sim x \forall x, y \in P$

Similarity

- **Similarity function:** (i.e. P is the set of permissions)

$$_ \sim _ : (P \times P) \rightarrow [0, 1]$$

- $x \sim x = 1 \forall x \in P$
- $x \sim y = y \sim x \forall x, y \in P$
- May be used on any kind of security information (permissions, subjects, objects, authorisations, ...)

Similarity

- **Similarity function:** (i.e. P is the set of permissions)

$$_ \sim _ : (P \times P) \rightarrow [0, 1]$$

- $x \sim x = 1 \forall x \in P$
- $x \sim y = y \sim x \forall x, y \in P$
- May be used on any kind of security information (permissions, subjects, objects, authorisations, ...)
- Other types of functions: boolean, lattice, ...

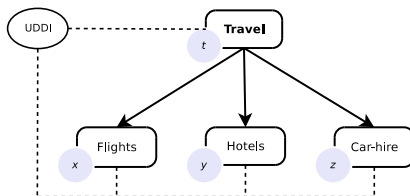
Similarity

- **Similarity function:** (i.e. P is the set of permissions)

$$_ \sim _ : (P \times P) \rightarrow [0, 1]$$

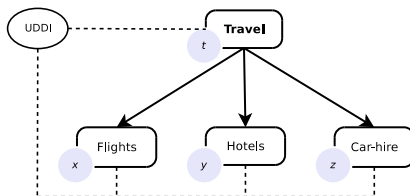
- $x \sim x = 1 \forall x \in P$
- $x \sim y = y \sim x \forall x, y \in P$
- May be used on any kind of security information (permissions, subjects, objects, authorisations, ...)
- Other types of functions: boolean, lattice, ...
- Widely used in CBR (Case-Based Reasoning).

Similarity example



- Absolute security enforcement:
 - A user needs a C_t credential to access *Travel*.
 - A user needs a C_a credential to access *Flights*.
 - ...

Similarity example



- Absolute security enforcement:
 - A user needs a C_t credential to access *Travel*.
 - A user needs a C_a credential to access *Flights*.
 - ...
- Better approach:
 - Allow a user access outsourced services with credential C_t .
 - C_t may be accepted instead of C_a to access *Flights*.
 - Security still being enforced at some degree: credential C_b cannot be used to access *Flights*.

Similarity matrix example

- **Similarity matrix** between credentials:

	C_t	C_a	C_b	C_c
C_t	1	0.6	0.6	0.6
C_a	0.6	1	0.2	0.3
C_b	0.6	0.2	1	0.2
C_c	0.6	0.3	0.2	1

Similarity matrix example

- **Similarity matrix** between credentials:

	C_t	C_a	C_b	C_c
C_t	1	0.6	0.6	0.6
C_a	0.6	1	0.2	0.3
C_b	0.6	0.2	1	0.2
C_c	0.6	0.3	0.2	1

- Similarity between credentials:

- $C_t \sim C_a = 0.5,$
- $C_a \sim C_b = 0.2,$
- $C_a \sim C_c = 0.3,$
- ...

Similarity threshold

Similarity threshold δ : similarity value accepted by the system.

Similarity threshold

Similarity threshold δ : similarity value accepted by the system.

- Given U (user credentials), C (system credentials), $U \in C$. If credentials $c \in C$ are needed to access service X , but $c \notin U$, the system may check:

$$\exists u \in U \mid c \sim u \geq \delta$$

Similarity threshold

Similarity threshold δ : similarity value accepted by the system.

- Given U (user credentials), C (system credentials), $U \in C$. If credentials $c \in C$ are needed to access service X , but $c \notin U$, the system may check:

$$\exists u \in U \mid c \sim u \geq \delta$$

- Security dial**: dynamic threshold, may change at execution time.

Similarity threshold example

Following the above example:

- moderate security level: $\delta = 0.5$
 - A user with credential C_t can also access *Flights*:
 - $C_t \sim C_a = 0.6 (\geq \delta)$.

Similarity threshold example

Following the above example:

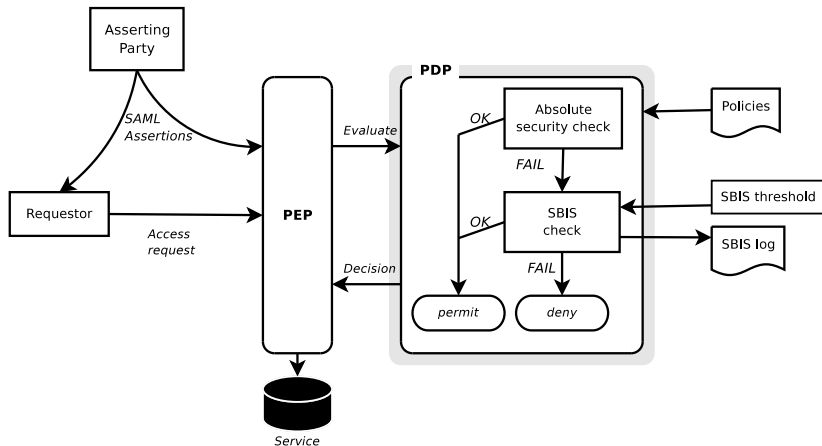
- moderate security level: $\delta = 0.5$
 - A user with credential C_t can also access *Flights*:
 - $C_t \sim C_a = 0.6 (\geq \delta)$.
- high security level: $\delta = 0.9$
 - The same user can only access *Travel*:
 - $C_t \sim C_a = 0.6 (\not\geq \delta)$.

Similarity threshold example

Following the above example:

- moderate security level: $\delta = 0.5$
 - A user with credential C_t can also access *Flights*:
 - $C_t \sim C_a = 0.6 (\geq \delta)$.
- high security level: $\delta = 0.9$
 - The same user can only access *Travel*:
 - $C_t \sim C_a = 0.6 (\not\geq \delta)$.
- low security level: $\delta = 0.1$
 - All users can do almost everything.

SBIS in SAML frameworks



Similarity-based assertion

- SAML assertions include a SBIS information element, which provides:
 - threshold,
 - function,
 - source,
 - history.

Similarity-based assertion

- SAML assertions include a SBIS information element, which provides:
 - threshold,
 - function,
 - source,
 - history.
- As an extension of the standard SAML XML Schema.

Similarity-based assertion

- SAML assertions include a SBIS information element, which provides:
 - threshold,
 - function,
 - source,
 - history.
- As an extension of the standard SAML XML Schema.
- Function is expressed in CBML (Case Based Markup Language).

Similarity-based assertion

- SAML assertions include a SBIS information element, which provides:
 - threshold,
 - function,
 - source,
 - history.
- As an extension of the standard SAML XML Schema.
- Function is expressed in CBML (Case Based Markup Language).
- This information can be used to avoid the cascading problem.

Conclusions

- The introduction of imprecision in security systems allows for more flexible and usable systems.

Conclusions

- The introduction of imprecision in security systems allows for more flexible and usable systems.
- This imprecision can be based on the similarity of authorisation.

Conclusions

- The introduction of imprecision in security systems allows for more flexible and usable systems.
- This imprecision can be based on the similarity of authorisation.
- We have provided an extension of SAML to support similarity-based imprecision.

Conclusions

- The introduction of imprecision in security systems allows for more flexible and usable systems.
- This imprecision can be based on the similarity of authorisation.
- We have provided an extension of SAML to support similarity-based imprecision.
- Important: SBIS is not for high security or critical systems, but systems where usability and flexibility is a key point.

Conclusions

- The introduction of imprecision in security systems allows for more flexible and usable systems.
- This imprecision can be based on the similarity of authorisation.
- We have provided an extension of SAML to support similarity-based imprecision.
- Important: SBIS is not for high security or critical systems, but systems where usability and flexibility is a key point.
- SBIS can provide enough flexibility to a system while ensuring some degree of security.

Thanks

Thanks. Questions?