Lecture 5

Friday, 16 September 2022 15:30

role & reputation based trust mechanisms (TM)

trust negotiation
RT system
credential chain discovery

typical access control solution

subject shows ID / proving authorization

trust management alternative

subject has credentials / informs authorization

reputation-based TM (social interpretation) $\xrightarrow[\text{trust}]{\text{calculate}}$ trust relation / trust opinion / reliability (e.g. for performing a job / as trust a site) ; problem: mass attention to be sufficiently reliable with enough work

role-based TM (not important in fin. w)

trust is a fin.-measured word

RTM system (myth from judge)
trust is a measure (i.e. credibility)
trust changes in time
there is a correlation between
- trustworthiness of entity
- trust of entity
- reliability of entity

recommendation-based
many sources unknowingly available
e.g. YGP

role-based TM

eligibility for a resource may depend on belonging to a class (large-scale community, free-of-charge (e.g. on web))

issues:
- scalability
- how to find

role-based TM: trust is binary (trust value divided into trusted and untrusted)
- no risk
- delegation
- risk transitivity (RTT study-based)
- many sources unknowingly available
- scalability

problem: how to e.g. minimize accessibility?

e.g. maintain list of minimizers or delegate to a second 'accreditation bureau'

---

a credential is a statement

- issued and signed by issuer
- about a subject
- contains information about subject

requirements
- unforgeable
- verifiable
- signed

well defined semantics
- anyone may issue credentials
- the definition of e.g. states a very precise meaning
  - not assume the thing actual 'means' / guess in the definition meaning

confidentiality problem
- some credentials are confidential (e.g. medical record)

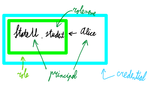
issues:
1. there are multiple security models; credentials need to be backed by a security infrastructure
   - prevent trust negotiation
   - (i.e. no trust without / after security check)
2. credentials are distributed; can be stored by subject and/or issuer
   - we need credential chain discovery

- credentials should be disclosed only according to a given access control policy
  e.g. during mutual record credentials requires strong authentication credential proof

---

RT: decentralized authority to define attributes
delegation of attribute authority

RT: has no pseudonyms, threshold or separation of duty



id = principal = Alice

four types of credentials

type 1: Epub.discount ← Alice

Epub states that "Alice belongs to Epub.discount"

set of all principals in the role Epub.discount

semantics: $Alice \in [\![Epub.discount]\!]$

issuer: Epub

subject: Alice

type 2: Epub.discount ← Hotel.staff

Epub states "if Hotel states that X is a member of Hotel.staff, then Epub's discount"

Epub delegates authority to Hotel

semantics: $[\![Hotel.staff]\!] \subseteq [\![Epub.discount]\!]$

issuer: Epub

subject: Hotel

type 3: Epub.discount ← Accreditation.university.student

Epub states

if Accreditation states that X is a accredited university student
X states that Y is a student
then Y states that Y gets a discount

"attribute-based delegation"

semantics: For every $X \in [\![Accreditation.university]\!]$, $[\![X.student]\!] \subseteq [\![Epub.discount]\!]$

type 4: IT Bureau.voyage ← IT Bureau.voyage ∩ IT Bureau.visa

IT Bureau states that "visa voyage may sign"

other subjects for that

semantics: $[\![IT\ Bureau.voyage]\!] \cap [\![IT\ Bureau.visa]\!] \subseteq [\![IT\ Bureau.voyage]\!]$

issuer: IT Bureau

subject: other subjects