Trust, Credentials, Delegation, and Access Control

Shiu-Kai Chin
Department of Electrical Engineering and Computer Science
Syracuse University
http://www.ecs.syr.edu/faculty/chin
Access Control Calculus

- Principal Expressions

\[ P ::= A \]
\[ P ::= P \land Q \]
\[ P ::= P \mid Q \]
\[ P ::= P \text{ for } Q \]

- Logical Formulas

\[ \varphi ::= p \]
\[ \varphi ::= \neg \varphi \]
\[ \varphi ::= \varphi_1 \land \varphi_2 \]
\[ \varphi ::= \varphi_1 \lor \varphi_2 \]
\[ \varphi ::= \varphi_1 \rightarrow \varphi_2 \]
\[ \varphi ::= \varphi_1 \leftrightarrow \varphi_2 \]
\[ \varphi ::= P \text{ says } \varphi \]
\[ \varphi ::= P \text{ speaks }_\text{for } Q \]
Descriptions in the Calculus

Integrity-checked messages \( K_{Alice} \) says \( \varphi \)

Key representing principal \( K_{Alice} \) speaks_for Alice

Key certificate \( K_{Bob} \) says \( (K_{Alice} \text{ speaks_for Alice}) \)

Relay/Quoting \( (Bob \mid Alice) \) says \( \varphi \)
\[ \iff \]
Bob says \( (Alice \text{ says } \varphi) \)

Delegation Bob for Alice

Roles Alice as Role \( \iff \) Alice | Role
Logical Rules for the Derivability Predicate \( \vdash \)

- If \( \phi \) is an instance of a propositional-logic tautology
  
  \[
  \frac{\vdash \phi}{\vdash \phi'} \quad \frac{\vdash \phi}{\vdash \phi} \quad \frac{\vdash \phi}{\vdash P \text{ says } \phi} \quad (\text{for all } P)
  \]

- \( (P \text{ says } (\phi \supset \phi')) \supset (P \text{ says } \phi) \supset (P \text{ says } \phi') \)

- If \( \phi \) a valid formula of the calculus of principals
  
  \[
  \frac{\vdash \phi}{\vdash (P \land Q) \text{ says } \phi \Leftrightarrow (P \text{ says } \phi) \land (Q \text{ says } \phi)}
  \frac{\vdash (P \lor Q) \text{ says } \phi \Leftrightarrow P \text{ says } Q \text{ says } \phi}{\vdash (P \text{ speaks_for } Q) \supset ((P \text{ says } \phi) \supset (Q \text{ says } \phi))} \quad (\text{for all } \phi)
  \]

\]
Authority and Trust

• If Bob believes that Alice is a controlling authority over some set of statement $s$ in $S$, then if Alice says $s$ then Bob believes $s$
  – Alice is to believed in matters represented by set $S$

• $A$ controls $\varphi \iff (P$ says $\varphi) \supset \varphi$
  – ($A$ controls $\varphi$) if and only if ($if (P$ says $\varphi$) then $\varphi$)
Example

• Bob receives an integrity checked statement from Alice saying “my phone number is 555-1212.”
  – Alice says “my phone number is 555-1212”
  – If Bob operates under the assumption Alice controls statements regarding her phone number then he will conclude Alice’s phone number is 555-1212

• Same principle applies to certificates regarding keys and attributes
  – Authority says (key speaks for principal)
  – If Authority controls (key speaks for principal) then key speaks for principal
  – If (key speaks for principal) and (keys says s) then (principal says s)
Delegation without Certificates

• Scenario: Dad sends his (under-aged) son to ask Mom for a beer
  – Son says Dad says give me a beer

• Quoting is essential, otherwise statement is
  – Son says give me a beer, which would be inappropriate to honor

• Mom’s access control list for beer (Mom as reference monitor) is
  – {Dad, Son | Dad}
Delegation with Certificates

• If Alice wishes to designate Bob as her delegate in certain matters, the following happens:
  – Alice signs a certificate stating that Bob is her delegate.
  – When Bob makes requests on Alice’s behalf from Carol, Bob presents the delegation certificate to Carol along with the request $Bob \mid Alice \text{ says } r$.
  – Carol will check her access control list to see if the request can be honored.
Logical Derivation

• The logic of delegation uses a delegation server $D$ (can be a process, person, or imaginary) whose purpose is to verify delegations

• For Alice to delegate to Bob, Alice tells the delegation server $D$ to “back” Bob – whenever Bob says Alice says $r$ then $D$ backs Bob
  – $D$ backs Bob $= \text{if Bob } | \text{Alice says } s \text{ then } D | \text{Alice says } s$

• If Bob serves Alice then Bob is Alice’s delegate
  – Bob serves Alice $= \text{Bob } | \text{Alice speaks for } D | \text{Alice}$
Definition of Delegation (for)

• \((Bob \ serves \ Alice) = (Bob \mid Alice = Bob \ for \ Alice)\)

• Consequence:
  – If Carol concludes \(Bob \ serves \ Alice\) then she can replace \(Bob \mid Alice\) by \(Bob \ for \ Alice\)
  – Requests of the form \(Bob \mid Alice \ says \ r\) can be interpreted by Carol as \(Bob \ for \ Alice \ says \ r\), i.e., the request Bob makes is for Alice
Other Common Examples

- Consider how a restaurant works
  - People acting as *waitstaff* (with identity tokens in the form of magnetic cards)
  - People acting as *managers* assigning people as *waitstaff* to tables
  - *People as waitstaff* placing food orders on behalf of customers, i.e., *people as waitstaff for customers*
- *People as waitstaff | customer says “fries and hamburger”* is interpreted as *People as waitstaff for customer says “fries and hamburger”*
- Certificates used in restaurants include order pad, bill printed out by cash register, credit card, credit card receipt, and cash.