PolicyMaker

A way to manage trust

based on

"Decentralized trust management"

Proc. IEEE conference on Security and Cryptography

Matt Blaze, Joan Feigenbaum, Jack Lacy

What is Trust Management?

- Security policies.
- Security credentials.
- Trust relations.

Where is trust management used?

- File management in a multiuser environment.
- Establishing secure communication.
  – This problem has been attacked with PGP and X.509.
- Restricting what people can do.
  – Banks will let a single employee approve a loan of $10.000 but a loan of $10.000.000 might need the approval of more than one employee.

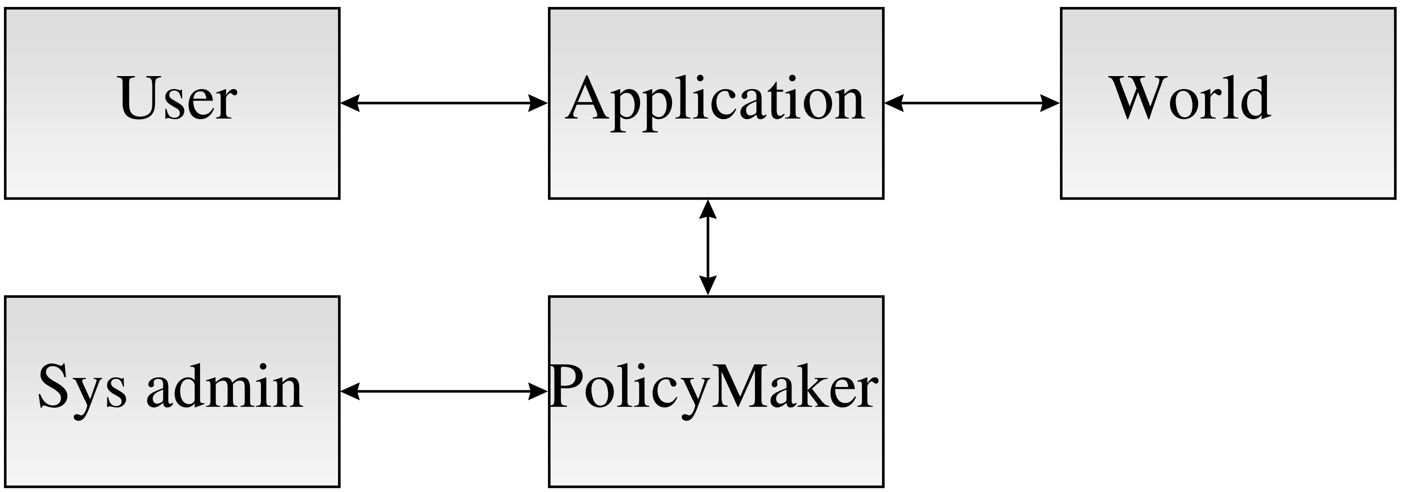
Other uses

- Workforce management.
  - Companies want employees only to be able to view Internet sites relevant to their work or only forward email.
- Copyright protection.
  - Want to allow people to view a document but not copy or print.
- Electronic voting.

Current steps to process a request

- Obtain certificates, verify signature on certificates on application request, determine public keys of original signer(s).
- Verify that certificates are unrevoked.
- Attempt to find a “trust path” from trusted certifier to certificate of public key in question.
- Extract names from certificates.
- Look up names in a database that maps names to the actions they are trusted to perform.
- Determine whether requested action is legal, based on the names extracted from the certificates and whether the certifications authorities are permitted to authorize such actions according to local policy.
- Proceed if everything seems valid.

PolicyMaker architecture



PolicyMaker language

- Trust information in assertions:
  - *Source* **ASSERTS** *AuthorityStruct* **WHERE** *Filter*
- Basic function to process queries:
  - key_1, ..., key_n **REQUESTS** *ActionString*
- Can use e.g. Safe-TCL, AWKWARD (safe AWK) or Java to write filters.

An Example, Email

POLICY ASSERTS

pgp: “0x0012203a4b51677d8090”

WHERE PREDICATE=regexp:(From: Alice) && (Organization: Bob Labs)

Allows the person holding the above key to claim being Alice in Bob labs.

pgp: “0x0012203a4b51677d8090”

REQUESTS “From: Alice, Organization: Bob labs”.

Defering policymaking

POLICY ASSERTS

Bobs_key

WHERE PREDICATE=

regexp(”Bob Labs”)

Can now trust certificates from Bob:

Bobs_key

ASSERTS

Alice_key

WHERE PREDICATE =
regexp(“From: Alice”)

Alice_key

REQUESTS “From Alice

Organization: Bob labs”

will succeed but these will fail:

Alice_key

REQUESTS “From Alice

Organization: Matt labs”

Alice_key

REQUESTS “From John

Organization: Bob labs”

Where is trust management used?

- Establishing secure communication.
  - This problem has been attacked with PGP and X.509.
- Restricting what people can do.
  - Banks will let a single employee approve a loan of $10.000 but a loan of $10.000.000 might need the approval of more than one employee.
- File management in a multiuser environment.

Other uses

- Workforce management.
  - Companies want employees only to be able to view Internet sites relevant to their work or only forward email.
- Copyright protection.
  - Want to allow people to view a document but not copy or print.
- Electronic voting.