

CS590U Access Control: Theory and Practice

Lecture 6 (September 11th)
Trust Management: PolicyMaker
and KeyNote

Goals of the Trust Management Approach

- Flexible and scalable access control for large-scale, open, decentralized systems
 - resource sharing in decentralized systems
 - coalitions, multi-centric collaborative systems
 - grid computing
 - electronic commerce
 - health care systems
 - etc.

2

The Trust-Management (TM) Approach

- Multicentric access control using delegation
 - access control decisions are based on distributed policy statements issued by multiple principals
- Common characteristics of TM systems:
 - treat public keys as principals
 - use digitally signed credentials

3

The [BFL'96] Paper

- General principles
 - Unified mechanism
 - Locality of control
 - Separation of mechanism from policy
 - Associates access permissions directly with public keys

4

Previous work

- PGP
 - associates <name, email> with public keys
- X.509 / PEM
 - associates DN with public keys

5

The PolicyMaker Language

- Queries
 - $key_1, key_2, \dots, key_n$ REQUESTS *ActionString*
- Assertions
 - *Source* ASSERTS *AuthorityStruct* WHERE *Filter*
 - *Source*: either a public key or POLICY
 - *AuthorityStruct*: either a public key or a filter
 - *Filter*: programs in a "safe" language

6

Source

- *Source* : either a public key or POLICY
- Certificates
 - signed by the public key
- Policies
 - locally stored in trusted storage

7

AuthorityStruct

- Either a keyid or a filter program
- Filter programs
 - Predicates: accepts or rejects action strings
 - Annotators: append annotations to action strings as well as accepts/rejects

8

Examples

- POLICY
ASSERTS
 pgp:"0x01234567"
WHERE
 PREDICATE = regexp:
 "Organization: Bob Labs";

9

Examples

- pgp:"0x01234567"
ASSERTS
 pgp:"0x7654321"
WHERE
 PREDICATE=regexp:"From:
 Alice)";

10

Examples: Query

- This query succeeds
 - pgp: "0x7654321" REQUESTS "From:Alice
Organization: Bob Labs"
- The following two queries fail
 - pgp: "0x7654321" REQUESTS "From:John
Organization: Bob Labs"
 - pgp: "0x7654321" REQUESTS "From:Alice
Organization: Matt Labs"

11

Query Semantics

- Unclear
 - because AuthorityStruct is a program
- Issues with Annotators
 - hard to deal with

12

KeyNote

- Second generation of PolicyMaker
 - Fixing *AuthorityStruct*
 - Use an environment consisting of name/value pairs instead of *ActionString*
 - Use an expression language for filters
- Described in RFC 2704

13

Elements of a TM System

- A language for describing actions
- A mechanism for identifying principals
- A language for specifying application policies
- A language for specifying credentials
- A compliance checker

14

Elements in KeyNote

- Actions: a collection of name-value pairs.
- Principals: public keys.
- The compliance checker returns an application-configured policy compliance value

15

KeyNote Assertions

- `<Assertion> ::=`
 - `<VersionField>?`
 - `<AuthField>`
 - `<LicenseesField>?`
 - `<LocalConstantsField>?`
 - `<ConditionsField>?`
 - `<CommentField>?`
 - `<SignatureField>? ;`

16

The Authorizer Field

- `<AuthField> ::=`
 - `"Authorizer:" <AuthID>`
- `<AuthID> ::=`
 - `<PrincipalIdentifier> |`
 - `<DerefAttribute>`

17

The Licensees Field

- `<PrincExpr> ::= "(" <PrincExpr> ")"`
 - `| <PrincExpr> "&&" <PrincExpr>`
 - `| <PrincExpr> "||" <PrincExpr>`
 - `| <K>"-of(" <PrincList> ")"`
 - `| <PrincipalIdentifier>`
 - `| <DerefAttribute> ;`
- `<PrincList> ::= <PrincipalIdentifier>`
 - `| <DerefAttribute>`
 - `| <PrincList> "," <PrincList>`

18

Conditions in KeyNote

- `<ConditionsProgram> ::=`
 - | `<Clause> ";" <ConditionsProgram>`
- `<Clause> ::=` `<Test> "->" "{"`
`<ConditionsProgram> "}"`
 - | `<Test> "->" <Value>`
 - | `<Test>`
- `<Value> ::= <StrEx> ;`

19

See the RFC for Details of Syntax on Tests

20

Query Answering Inputs

- A KeyNote query has four parameters:
 - Requesting principals.
 - The action attribute set describing the action.
 - The set of compliance values of interest to the application, ordered from `_MIN_TRUST` to `_MAX_TRUST`
 - Assertions

21

Query Answering Inputs

- A KeyNote query has four parameters:
 - Requesting principals.
 - The action attribute set describing the action.
 - The set of compliance values of interest to the application, ordered from `_MIN_TRUST` to `_MAX_TRUST`
 - Assertions

22

Evaluation of a KeyNote Query

- Basic idea: determine to which degree each principal supports the query
 - requester fully supports the query
 - other principals support the query to the max as computed by assertions

23

Evaluation of a KeyNote Query

- The Assertion Compliance Value of an assertion is the minimum of the assertion's Conditions Compliance Value and its Licensee Compliance Value.

24

Evaluation of KeyNote Query

- The Conditions Compliance Value of an assertion is the maximum value among all successful clauses listed in the conditions section.
- If no clause's test succeeds or the Conditions field is empty, an assertion's Conditions Compliance Value is considered to be the `_MIN_TRUST` value.
- If an assertion's Conditions field is missing entirely, its Conditions Compliance Value is considered to be the `_MAX_TRUST` value.

25

Limitations of KeyNote

- Cannot write an assertion saying if someone has this attribute, then he has that permission
 - assertions used together must talk about the same kind of permissions
- Limitation of capability-style TM systems

26

A Simple Example

- A book store wants to give 15% discount to students of a nearby university
- How to do this in KeyNote?

27

A Simple Example

- KeyNote Solution 1
 - bookstore delegates discount permission to the university
 - the university explicit delegates the discount permission to the students
- Not scalable.

28

A Simple Example

- KeyNote Solution 2
 - the university creates a new pair of keys for students and issues a complete delegation from this key to the students' keys
 - bookstore delegates discount permission to the student key
- What about faculties, staffs, graduate students, third-year CS students?

29

A Simple Example

- Ideal solution: the bookstore expresses the policy in one assertion and students use student IDs to get discount
- Not possible in KeyNote

30