Binding Identities and Attributes Using Digitally Signed Certificates

Joon S. Park, NRL/ITT Ravi Sandhu, George Mason Univ.

Introduction

- In this paper, we
 - Analyze the basic structure of digital certificates and classify the nature of the information.
 - Identify 3 different binders.
 - Describe each binder and compare with others.

Joon S. Park INFS 767 2

Digital Certificate

- What is it?
 - Signed by a CA to confirm that the information in it is valid and belong to the subject.
- Purpose?
 - To provide the integrity of the information (e.g., identities or attributes) in the certificates.

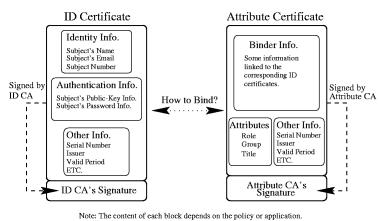
Joon S. Park INFS 767

Related Work

- X.509 Certificates
- Attribute Certificates
- SPKI (Simple Public Key Infrastructure)
- PGP (Pretty Good Privacy)
- Smart Certificates

Joon S. Park INFS 767

Basic Structure of Certificates



Joon S. Park **INFS 767**

5

Basic Structure of Certificates

- We classify the nature of information in certificates into blocks.
- The content of each block depends on applications and policies.
- ID certificates should contain authentication information.
- Attribute certificates should link to ID certificates.

Joon S. Park **INFS 767** 6

Binders

- What is a binder?
 - A mechanism to link attributes to proper identities
- Factors
 - Different CAs
 - Different lifetimes
 - Strength
- To satisfy the requirements, we identify
 - Monolithic Signature
 - Autonomic Signature
 - Chained Signature

Joon S. Park INFS 767

Monolithic Signature **ID** Certificate Identity Info. Attribute Certificate Subject's Name Subject's Email Subject Number Attributes Signed by Authentication Info. Signed by Role Group Subject's Public Key Info. Subject's Password Info. ID CA ID CA Other Info. Serial Number Issuer Valid Period ETC. ID CA's Signature Note: The content of each block depends on the policy or application. Joon S. Park **INFS 767**

Monolithic Signature

- The simplest binding mechanism.
- Identity and attributes are tightlycoupled.
- Problems
 - Multiple CAs, Different Lifetimes

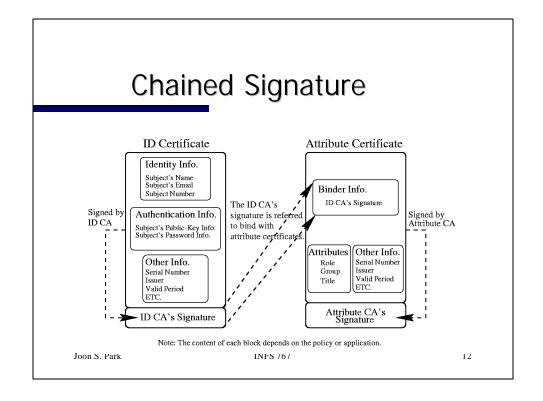
Joon S. Park INFS 767

Autonomic Signature ID Certificate Attribute Certificate Identity Info. Binder Info. Subject's Name Subject's Email Subject Number Subject's Name Subject's Email Subject Number ID Serial Number Subject's Public-Key Info. Subject's Password Info. Some information in Signed by Authentication Info the ID certificate is Signed by Attribute CA ID CA Subject's Public-Key Info. Subject's Password Info. referred to bind with attribute certificates Attributes Other Info. Serial Number Issuer Valid Period Other Info. Role Serial Number Group Title ETC Valid Period ETC. Attribute CA's Signature ID CA's Signature Note: The content of each block depends on the policy or application. Joon S. Park **INFS 767** 10

Autonomic Signature

- Supports multiple CAs and different lifetimes.
- Binding some information (e.g., subject's name) in ID certificates and attribute certificates.
- Identity and attributes are looselycoupled.

Joon S. Park INFS 767



Chained Signature

- Supports multiple CAs and different lifetimes.
- Binding ID CA's signatures in ID certificates and attribute certificates.

Joon S. Park INFS 767 13

A Comparison

	Monolithic	Autonomic	Chained
CAs	Single	Multiple	Multiple
Lifetimes	Same	Different	Different
Binding Strength	Tightly- Coupled	Loosely- Coupled	Medium
Reusability	Low	High	Medium
Certificate Discovery	Easy	Medium	Difficult

Joon S. Park INFS 767

Conclusions

- In this paper
 - We analyzed the basic structure of digital certificates and classified the nature of the information.
 - We identified 3 different binders.
 - We described each binder and compared with others.

Joon S. Park INFS 767 15