Policy Augmented S/MIME

Trevor Freeman
Trustworthy Computing
Microsoft Corp
Email Data Leakage Example

• US Air Force sent email to EADS with information about the Boeing bid for the Air Tanker

• US Air Force had to “level the playing field” by sending the EADS bid data to Boeing
Todays Problems

**ESS**
- Label at same level as data
  - Cannot discover label without access to data
  - Cryptographic access granted before access check
  - No guarantee client performs the check
- Access policy must be distributed to all recipients
  - Sender had not information about state of recipients client
- ESS only supports a single label per message

**S/MIME**
- S/MIME only supports a single credential type
- Encryption certificate discovery
- No MTA content scanning
Plasma Scenarios

• Business to Business
  – Collaboration
  – Supply chain
  – Ad-hoc

• Business to Consumer, Government to Consumer
  – Doctor-patient
  – Bank-customer
  – Agency-citizen

• MTA based AV content scanning
Plasma Requirements

• Multiple policies per message
  – Cannot assume logical combination of policies
• Policies for different authorities
• Policies can define multiple scopes
  – Access control, integrity, authentication, retention, etc.
• Support varying levels of identify assurance
• Be authentication technology independent
• Support recipients on varying service types
  – On-premise
  – Private or public cloud services
• Support MTA access to protected messages
Simple vs. Complex Polices

**Simple**
- Equivalent to S/MIME today
- Authenticated recipient of the message
- Define level of assurance of authentication
  - NIST SP800-63
- Examples
  - Doctor-patient, Bank-Customer
- Single policy per message

**Complex**
- Arbitrary complex access control policy
- Same as access to on-line content
- Policy defines attributes required for access
- Examples
  - Regulatory, organization
- Multiple polices per message
Plasma Access Control Model

- Email Policy Server is a PDP
- Email MUA is a PEP
- Senders MUA makes request to get list of policies
  - List is a set of policy references
- Senders MUA makes request to send message
- Recipient MUA makes request to decrypt message
Plasma Mail Flow

- Sender MUA encrypts message and sends key and policies to PDP
- PDP gives sender MUA message blob
- Senders MUA sends message with blob
- MTA scans message contents
- Recipient MUA discovers senders PDP from message blob
- Recipient MUA presents message blob and requests decryption key from senders PDP
- PDP asks recipients MUA for claims
- Recipient MUA supplies claims
- PDP releases message key to recipients MUA once compliance is verified
Plasma Goals

• Define protocol for interaction with email policy server
  – Protocol can be used by MUA or MTA
• Define how to include policy data to CMS enveloped data
• Abstract authentication and key exchange from S/MIME to remove dependency on X.509
• Define mechanism for publication of MTA keys for pre-authorization