Privacy Enabled Identity Management for C2 Systems

Gerald Beuchelt

gbeuchelt@mitre.org

gerald.beuchelt.ctr@hanscom.af.mil

MITRE

Public Release Approval 09-2192

Identity Management

- **Identity Management require technology *and* process**
  - **Digital identities are mapped to people and things**
  - **One person (or thing) may have more than one (digital) identity**
- **Technology: PKI or Active Directory are not Identity Management**
  - **PKI is – essentially – a authentication technology**
  - **Active Directory provides authentication and attribute services**
- **Processes need to be assessed and compliance continuously monitored**
  - **Trust frameworks like Identity Assurance Framework**

Public Release Approval 09-2192

Privacy

- Different types of privacy
  - Physical
  - Informational or Data Privacy
  - Organizational
  - Spiritual and intellectual

- Relevant in this discussion is data privacy

Public Release Approval 09-2192

Privacy Principle

Privacy Principle	Scope
Collection Limitation (CL)	Limit the creation, transmission, and collection of PII during the execution of mission threads.
Use Limitation (UL)	Use PII only for the purpose for which it was requested.
Access and Correction (ACC)	Enable access to PII and the ability to correct such data within the limits of policy.
Anonymity and Pseudonymity (P)	Use transient pseudonyms when possible and limit the exposure of identifiers.
Security and Safeguards (SECSAFE)	Provide a secure Information Assurance (IA) stance to protect the IdAM system.

Public Release Approval 09-2192

Privacy in Identity Management

- **Most modern commercial identity management technologies emphasize privacy aspects**
  - **Infocard (Windows CardSpace) built around Kim Cameron's "Laws of Identity" which emphasize privacy and user control**
  - **SAML and XACML have privacy profiles that allow user-meditated release of attribute information**
  - **Other "user-centric" identity management systems such as e.g. OpenID have been gaining popularity**
- **Identity management systems and technologies can be deployed privacy-aware – or not.**
  - **Centralized accounting/logging and correlation**
- **Other Privacy Enhancing Technologies**

Public Release Approval 09-2192

Using Privacy in Identity Management for Security

- Components of digital identities include
  - Unique identifiers (such as e.g. cryptographic keys)
  - Attributes
  - Relationships
- Privacy is secrecy about a digital identity's components
  - Limiting disclosure, use, and storage
- Secrecy about actor identity information protects the operational security

Public Release Approval 09-2192

Interpreting Collection Limitation

Collection Limitation
CL1: Any service provider will only request and collect the amount of information about a data subject or end-user that it needs.
CL2: Information about a data subject or end-user that gets sent unsolicited must be discarded.
CL3: A record of the relevant data should be created, as long as data retention and data-at-rest policies are applied.

Public Release Approval 09-2192

Interpreting Use Limitation

Use Limitation
UL1: End-user or data subject data received for authentication, authorization, or any other IdAM purpose must not be re-used for any other purpose. In particular, such data must only be used for authentication or authorization steps for which it was released.
UL2: Data retention policies should be established and implemented, so data is retained only as long as needed.

This is not in conflict with net-centric "Need to Share"

Identity attributes are part of security, not situational awareness

Public Release Approval 09-2192

Interpreting Access and Correction

Access and Correction
ACC1: Components, data subjects, or end-users should be enabled to access all information for which they are authoritative and be allowed to make corrections or amends, as long as these are permissible under the access control policy.
ACC2: The access control policies for Access and Correction should be adjustable over purpose and time.

Relevance to data authoritativeness:

Some attributes have highest fidelity when self-asserted

Public Release Approval 09-2192

Interpreting Pseudonymity

Pseudonymity
P1: Data in transit should only contain references to pseudonyms.
P2: Pseudonyms can be persistent or transient; transient pseudonyms are preferable where permissible by operational requirements.
P3: Pseudonyms for a given user should be valid only between two systems. For different pairs, different pseudonyms should be used.

Public Release Approval 09-2192

Identity Management Patterns

- Central Authentication
  - Mutually trusted authentication source like e.g. Kerberos
  - CL1, CL3, UL1, ACC2, P1
- Attribute Based Access Control (ABAC)
  - Realized in SOA Reference Architecture through SAML and XACML
  - CL1, CL2, UL1, ACC2, P1, P2
- Federated Authentication
  - Authentication is performed by federation partner
  - CL1, CL2, UL1, ACC2, P1, P2, P3
- Delegation
  - Authorization and identification is carried to secondary services
  - CL1, CL2, UL1, ACC2

Public Release Approval 09-2192

Relevance to C2 Systems

- **Limiting exposure of operator attributes addresses real security problems**
  - **Identities that are known to have high security clearances/many SCI compartments are higher value target**
  - **Correlating rank, clearance, or roles with names and addresses can result in direct personal risk**
- **Limit usefulness of compromised systems**
  - **De-centralized, but federated attribute and relationship storage**
- **Assist in decoupling of security and identity**
  - **Clear separation/layering of concern**
  - **Limit identity information to be dispersed**

Public Release Approval 09-2192

Other Privacy Concerns

- General privacy regulation
  - Business systems must comply with OMB Circular A-130 / DoDI 5400-11R
  - Operational C2 systems are exempt at this time
- Cross Domain Solution (CDS) benefits
  - Limiting attribute/identity flow between systems in different security domains
  - Simplifies information sharing while maintaining referential integrity to actor/subject

Public Release Approval 09-2192

Mapping to Technologies

- **Current Identity and Access Management technologies support privacy-enablement partially**
  - **Attribute Based Access Control (ABAC)**
  - **Identity Federation**
- **Gaps in various areas**
  - **Comprehensive log management/distributed auditing**
  - **Attribute-level authentication/authorization/verification**
- **Full implementation will require multi-system integration**

Public Release Approval 09-2192

Summary

- Privacy in identity management can improve operational security and limit attack surface
- Various privacy enhancing techniques may be applied to future distributed C2 systems
- Traditional privacy controls provide guidance on how to employ privacy principles
- Additional benefits (such as CDS “friendliness”) may be gained

Public Release Approval 09-2192