Context-Aware Security

Gleneesha Johnson
gjohnson@cs.umd.edu

Context

- Common definition from Dey et al. [DA99]

  …any information that can be used to characterize the situation of an entity. An entity is a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and applications themselves

- Contextual Attribute - a measurable context primitive
  - Common examples are location and time

Context-Aware Systems

- A system is context-aware if it can discover and utilize context to adapt its behavior based on the current situation
- Context can be supplied from a variety of sources
  - sensors embedded in a computing device, external sensors in the environment, a context providing service, and system state

Context-Aware Systems

- Seminal Paper by Weiser “The Computer for the 21st Century” [W99]
  - Many computers seamlessly integrated into the physical environment
  - Objective – to support and enhance a user’s experience by making life and tasks easier
- Significant body of research explores ways that objective can be accomplished
  - Location-aware application
- Less work on enhancing security

Traditional Security

- Coarse and context insensitive
- Based on relatively stable, well-defined, consistent configurations, and static contexts. [HSBER05]
- Shifting computing paradigm
  - Anytime, anywhere, anyone access
  - Rapidly and frequently changing context

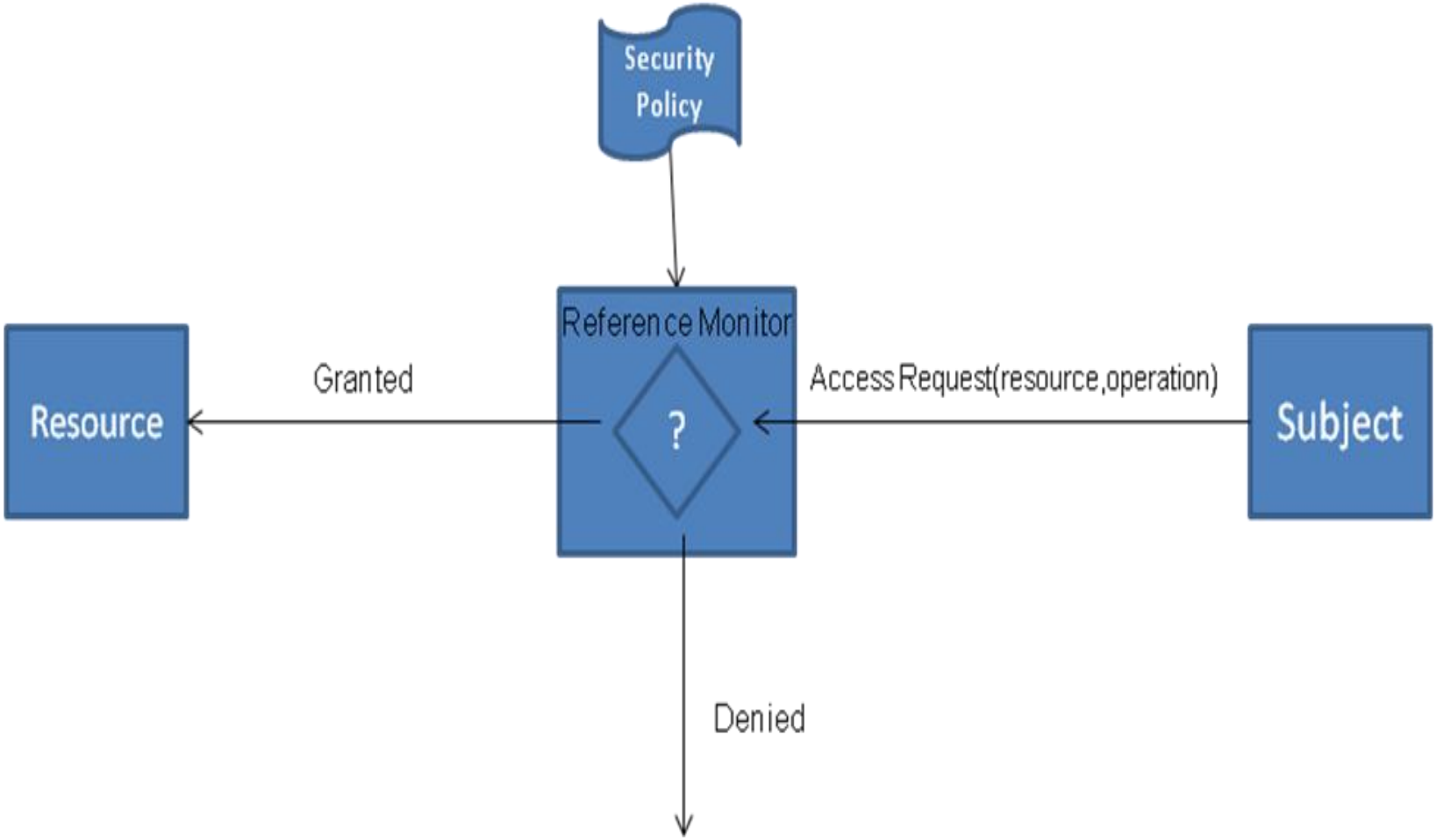
Context-Aware Security

- Security mechanisms dynamically adapting to the user's situation based on the provided context
- Context can be incorporated into various security services
  - Access control, encryption, authentication, etc.
- Context can incorporated into security in different ways
  - Supplement user attributes
  - Replace user attributes
- Majority of research focuses on access control

Access Control

- Objective is to prevent unauthorized access to protected resources
- Controls what subjects (active entities, such as users and processes) can access what resources (passive entities) and what operations they can perform (read, write)

Access Control Model



Context-Aware Access Control

- Incorporating context into access control allows decisions to be based on situation at time of resource request.
- Generalized RBAC (GRBAC)[CLSDAA00] – uses “environment roles” to capture security-relevant context of environment in which access request was made.
- Dynamic RBAC (DRBAC)[ZP04] – dynamically adjust user role and permissions based on context using state machines
- Many others

Context-Aware Security Issue

- Many of today's context-aware security systems are either vague about their notion of context, or use limited context
  - Abstracts away important aspects of the situation
  - Lead to poor security decisions based on an incomplete picture

Shrink-Wrapped Security

- A security paradigm in which a tight coupling is provided between a user's current situation and security
  - not possible when only limited context is utilized
- Requires a more comprehensive notion of context than what is currently used by context-aware security systems
  - Only consider *security-relevant context*

Security-Relevant Context

Security-relevant context consists of the set of contextual attributes that can be used to characterize the situation of an entity, whose value affects the choice of the most appropriate controls (measures) or the configuration of those controls to protect information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity and availability.

Security-Relevant Context

- The values of security-relevant contextual attributes affect the choice of the most appropriate controls because they impact the likelihood of certain threats to confidentiality, integrity, and availability being realized. Therefore, based on their values, the most appropriate controls and configuration of those controls can be employed to mitigate those threats.

Research Areas

- Secure context collection and management in a dynamic environment
  - Context authentication and integrity
  - Context privacy
- The formulation and enforcement of context-aware security policies
- Identifying relevant context

Identifying Relevant Context Exercise

References

- [DA99] Anind K. Dey and Gregory D. Abowd. Towards a Better Understanding of Context and Context-Awareness. Proceedings of the 1st International Workshop on Managing Interactions in Smart Environments. 1999.
- [W99] M. Weiser, "The Computer for the 21 st Century," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 3, pp. 3-11, 1999.
- [HSBER05] R. Hulsebosch, A.H. Salden, M.S. Bargh, PWG Ebben, and J Reitsma. Context Sensitive Access Control

- [CLSDAA00] Michael J. Covington, Wende Long, Srividhya Srinivasan, Anind Dey, Mustaque Ahamad, and Gregory Abowd. Securing context aware applications using environment roles
- [ZP04] Guangsen Zhang and Manish Parashar. Context-Aware Dynamic Access Control for Pervasive Applications.