Models, Protocols, and Architectures for Secure Pervasive Computing: Challenges and Research Directions

(Position Paper)

Roshan K. Thomas
McAfee Research, Network Associates, Inc.
rthomas@nai.com

Ravi Sandhu
George Mason University and NSD Security
sandhu@gmu.edu

Abstract

We explore the challenges and research directions in building models, protocols and architectures to support security in pervasive computing environments. We argue that to be successful, efforts to build these would have to recognize from the onset that pervasive computing settings are complex socio-technical system and would thus have to go beyond traditional system-centric approaches to analyzing and designing security.

1. Introduction

We explore the challenges and research directions in developing models, protocols and architectures to address security in pervasive (ubiquitous) settings. The motivation for this research comes from the realization that many of the assumptions and usage scenarios underlying classical/current security concepts, models, and solutions simply do not hold for pervasive computing. Mark Weiser, who originally coined the term "ubiquitous computing", had a vision where these computing devices essentially disappeared into the background [11, 12]. However, security poses fundamental challenges to realizing this vision.

We take the view that if security and privacy are to be successfully integrated into pervasive computing (percom), we have to recognize from the onset that percom settings are complex socio-technical systems. This represents a departure from the classical system-centric view of security that has accompanied the development of security models, protocols, and architectures over the last few decades.

2. Fundamental challenges to secure pervasive computing

The nature and vision of pervasive computing brings to the forefront some fundamental challenges in addressing security. We now discuss some of these.

The need to integrate the socio-technical perspective

The promise and potential of percom to be intertwined in our daily and routine activities require that we address the socio-technical issues of introducing security technology into the larger social setting. Thus issues related to the usability and confidence (trust) in security technologies, as well as how these technologies relate to the broader sociological, cognitive, economic and legal aspects of our lives, should be prime considerations. Unlike the traditional systems view of security, the design of security for percom must recognize the different personas and roles we possess (i.e. parent, employee, tax payer, citizen etc.) as part of our daily routines. Each of these personas requires that we take on a different security profile and apply a set of related security policies.

Breakdown of classical perimeter security and the need to support dynamic trust relationships

Classical security models rely extensively on perimeter defenses and stable trust relationships. Thus the use of firewalls to enforce perimeter security based on a tightly defined network boundary. Also, users of a system are assumed to be pre-registered and thus authentication and access control are centered on user identities. In a pervasive environment, the above assumptions simply do not hold. Pervasive computing extends traditional computing boundaries. Also, trust relationships are dynamic as the user community may be anonymous and constantly changing, making pre-registration unworkable, and user identity may not be known, available or relevant.

Balancing non-intrusiveness and security strength

Percom brings to the forefront the tension between usability and security. What is needed is a shift away from classical and intrusive security schemes such as those requiring explicit user input, such as to enter passwords, to a mode of operation where the required information can be sensed securely and automatically from the context and environment, and exchanged seamlessly with the communicating principals (devices)

Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops (PERCOMW'04)
0-7695-2106-1/04 $ 20.00 © 2004 IEEE

and users. The ability to provide a single-sign on feature to enable single-step authentication to multiple applications and stove-piped systems from multiple devices is thus a basic requirement. Some commercial products have started offering such features in environments such as medical information systems. However, the extension of this to a truly pervasive environment still remains a challenge.

Context awareness

The ability to sense and exploit contextual information to augment or replace traditional user attributes such as identity for the purpose of authentication and access control is critical to making security less intrusive in percom settings. Contextual information may be gathered from a user, one or more devices, the environment, the network or the application. A general research challenge here is the protocols and infrastructure required to sense, validate, and organize contextual information. Some research efforts have started looking into this [2].

Mobility, dynamism, and adaptability

Security for percom has to cater and adapt to the mobility and dynamism of pervasive environments. A user may be mobile and interact with multiple devices and access multiple applications. Applications and data may also migrate on behalf of roaming users. The user may also be frequently disconnected from networks. As we shall discuss later, these introduce many additional dimensions into the security models, protocols, and architectures necessary to support such scenarios.

Resource constrained operations

Pervasive computing environments are sensor rich and relying to a great extent on wireless communications. However, the computing platforms of sensors are resource constrained with respect to CPU power, energy, memory etc. and the wireless medium has limited bandwidth and throughput. These constraints severely limit the type of cryptographic operations, security protocols and security mechanisms that can be supported.

Balancing security and other service tradeoffs

Percom encompasses a wide variety of applications, usage scenarios, and data handling demands. To succeed, each application area would have to offer the right set of tradeoffs between a variety of service attributes that include security, privacy, usability, quality-of-service, and cost. Thus, a central challenge is to devise security models along with a set of supporting architectures, protocols and mechanisms that can offer tunable tradeoffs so as to meet the conflicting requirements and competing demands of various parties involved in percom transactions.

Having highlighted some broad challenges, we discuss issues specific to models, protocols and architectures.

3. Models

If we are to design coherent security protocols, architectures and mechanisms for percom, such designs have to be preceded by the development of abstract security models (see related discussion on the resurrecting duckling model in [8]). Abstract models allow us to analyze and understand a domain in terms of the fundamental entities and the relationships that tie these entities together, and without getting distracted by architecture and system-centric implementation details.

3.1. Models for authentication

Authentication services in percom settings should be able to handle scenarios that involve user mobility across networks, applications and devices, application migration across multiple execution platforms and devices, and disconnected network operations requiring localized trust establishment. This raises the following research challenges:

- How do we devise models that can offer a unified approach to model a continuum of trust starting with very specific, high strength, identity-based schemes that preserve accountability, to more general schemes that allow anonymity but yet provide adequate context-based entity recognition and trust establishment?
- What abstractions and metrics are required to classify the strength of the authentication (or level of trust) established in a percom environment?
- How do we use authentication strength to determine level of access that can be granted?
- What are the methodologies and models required to study and manage the tradeoffs between authentication strength, usability, cost, and other service parameters?

In general, developing models of authentication that go beyond simple, persistent identity and registration based schemes is an immediate research priority [6]. Some early efforts to derive confidence measures for authentication methods in percom are reported in [1].

3.2. Models for access and usage control

Beyond system-centric subject-object models

The right side of Figure 1 shows the classical system-centric view of access control traceable to the access matrix model, with the main abstractions being subjects, objects, and rights. The left hand side of the figure shows

our perspective on some of the additional fundamental abstractions and relationships that need to be considered when modeling access control in pervasive computing. In classic access control, a *user* is a unit of accountability, a *principal* is a unit of authentication and a *subject* is a unit of access enforcement. While many newer access control models have extended the basic access matrix model to accommodate the needs of new applications [3, 7, 9, 10], the socio-technical view on the left side of the figure has been largely ignored.

We believe that what distinguishes access control in percom is the highly dynamic, transient, and complex nature of the relationships on the left-hand side. In the percom setting, attributes of users transfer in part to principals and further to subjects, but principals and subjects also gain additional contextual attributes. Context represents an interface between the social and technical subsystems of the socio-technical system. The mobility of users and subjects requires us to model devices explicitly, as well as relationships of devices to these classical abstractions. This is again necessary as percom devices also form an interface between the social and technical subsystems of percom environments.

The entities and relationships on the left-hand-side of Figure 1 show the complexity of modeling access control in percom. For example, a user (U) may be represented by multiple principals in a percom environment, and each principal may have one or more contexts and each principle may map to one or more devices (a link terminating in a double-headed arrow represents a one-to-many relationship, while double-headed arrows on either end indicate many-to-many relationships). A context may apply to multiple principals and contexts may also be associated with each other, as shown by the C-C link. A principal may map to multiple subjects for the purpose of gaining access to multiple backend computer systems. These subjects will inherit the contexts associated with their principals and may run on different devices. Devices may also be related to each other by sharing common contexts while being used by one or more principals.

Exploiting contextual information

There is a clear need to formulate access control and usage models that exploit contextual information. Some preliminary work using well-known contextual information such as user location, time of access etc. have been studied by a number of research projects [5]. Contextual information also opens up possibilities for *proximity-based* and *encounter-based* access control. Proximity-based access control products have been used to provide physical security to buildings and more recently to cars, but these notions need to be studied in percom settings consisting of large populations of devices, heterogeneous networks and multiple backend systems. Proximity-based access control models also need to be integrated with single-sign on features to minimize intrusiveness and aid usability.

Encounter-based access control schemes grant entities authorizations to resources upon verifiable encounters of two or more entities. For example, this would be useful in a futuristic sensor-based air traffic control system, where an aircraft (A) has a guidance system that could be asked to sense an encounter with a second lead aircraft (B) and to follow B to the same runway for scheduled takeoff after B. Further, the lead aircraft, B, could provide continuous "reauthorization" by continually sensing to see if A is maintaining its encounter and not straying to the wrong runway. Collectively, this reduces the cognitive load on pilots which in turn reduces pilot errors.

3.3. Models for privacy

Privacy models for percom would have to encode well-known privacy principles, legal requirements for specific application areas, as well as general societal expectations. Several principles based on fair information practices that can be used to guide system design to ensure privacy are discussed in [4]. These include: notice, choice and consent, anonymity and pseudonymity, adequate security and access and recourse. This raises the following research challenges:

- How do we come up with modeling abstractions and policy languages to express privacy management policies that embody these principles?
- How can contextual information and content be filtered and abstracted to comply with one or more privacy policies?

In meeting the above challenges, privacy management must be integrated with context recognition and management.

3.4. Models for dissemination control

How will the dissemination of digital objects be controlled in a pervasive computing setting? The digital world makes it easy to copy and distribute multiple electronic copies. Access control models typically do not deal with copy protection and distribution. This topic has been investigated under the broad area of digital rights management (DRM). Thus a research challenge is to understand how emerging DRM models can be adapted and interfaced with percom environments to provide dissemination controls (DCON). Copies of digital objects may exist on multiple devices, potentially owned by one or more users, and exchanged, accessed and sold on multiple percom networks. The challenge here is to device models that maximize certain objectives (such as availability, privacy, revenue generation) while trading off others as required by specific application needs.

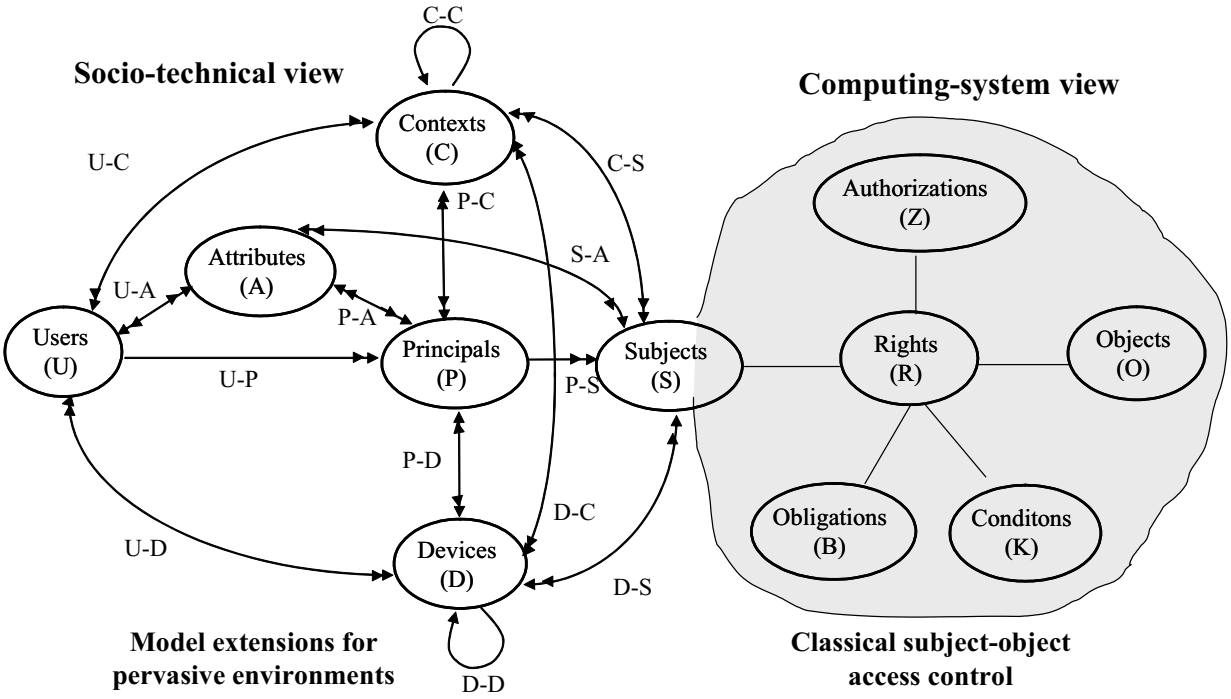

Figure 1. Domain extensions for modeling access control in pervasive computing

4. Protocols

We now describe some of the challenges in designing protocols to realize the models described earlier.

Multiple personas, addressing and security profiles

In a percom environment a user may have multiple personas, depending on the context, and require each of these personas to be associated with distinct security profiles and policies. This has implications on realizing the mapping between principals and contexts (P-C) as well as principals and devices (P-D) (see Figure 1). In turn, this affects protocol design. Thus a percom device may have to serve multiple principals and maintain multiple security profiles, on behalf of a single user. For example, as a terminal for location-based ecommerce, a device may be required to preserve anonymity of the user, but as a mediator for requests to the user's medical records, it may be required to negotiate privacy policies that call for sanitizing personal information as well as managing procedures for consent and notification. The same principal may also migrate from one device to another, or coexist on multiple devices.

The above also has implications on MAC and network layer protocol design for wireless percom devices. How should devices be addressed and found on percom networks in terms of the higher level personas they represent and services they participate in?

Mobility, portability and transparency of trust

The design of security protocols for percom should support a high degree of user mobility, transparency and portability across devices. The challenge is to design protocols such that successful completion of protocol handshakes and trust establishment is not based on a user having access to a designated device or workstation (see related discussion on Kerberos authentication in [1]).

Adaptability to disconnected operations

As percom networks involve wireless connectivity, security protocols for percom should be designed to accommodate intermittent connectivity and unreliable communications. As such, there should be minimal reliance on centralized, on-line services such as for trust establishment based on public key infrastructures (PKI). Where possible, protocols should be adaptive enough to exploit localized trust establishment and decision-making. Another challenge is to design protocols that allow rapid reconnection and reestablishment of security associations and application sessions to enable seamless user mobility.

Efficiency for resource constrained operations

This aspect is concerned with the challenges in designing protocols that are efficient and lightweight so as to be useful in percom settings where both device and network resources are limited. Packet headers inserted to

support security protocols have to be small and associated message exchanges have to be few, and requiring very little computational, storage and energy overhead to be incurred by the communicating parties. This is an active area of research by the sensor network community, but these schemes need to be adapted to cater to the characteristics of percom, namely user and application migration across contexts and devices.

Privacy preservation

One may view the research challenges in protocol design to support privacy at several levels of abstraction – device level addresses and routing information, user associated attributes (name, address etc.) and related contextual information such as location, time etc., as well as privacy of contents exchanged across percom networks. Protocols have to be flexible enough to support a variety of privacy principles and policies with the added requirement that the current contextual information determine the active set of policies to be applied. Thus a user may request location privacy from his device when participating in a certain activity and yet require that the device notify authorities of his exact location in an emergency (such as when a distress signal is sent).

Scalability

A general challenge in protocol design for percom is related to the issue of how to make protocols scale. Scalability issues arise in several dimensions including scalability to support massively large populations of devices and users, as well as scalability to support networks that span large distances. We need to examine how well-known protocols such as those for trust establishment (group keying, key distribution etc.) will scale to environments where user and device populations are highly mobile, and trust relationships are spontaneously formed, dynamic, and short-term.

5. Architectures

Architectures and protocols for secure pervasive computing go hand-in-hand in providing the facilities to enforce the security policies that are expressed by abstract models. At the device level, a grand challenge will be to efficiently design and integrate security services on top of standards such as IEEE 802.15.4. Depending on the application, hardware-based mechanisms for trusted boot-up and tamper detection may need to be provided. Also, the architecture of devices should enable rapid plug and play installation and execution of security services while ensuring portability and adaptability. The architecture must provide security mechanisms to prevent unauthorized usage resulting from theft of devices and yet be flexible enough to enable owners of devices to easily reinitialize the devices to transfer ownership or use.

Beyond the device level, several architectural challenges exist in providing security infrastructures for percom. These include the integration of security support into the communications within smart spaces (also referred to as active spaces) as well as the integration of security into context management services. Another challenge is the placement of trust management services so that context-based authentication and access control can be efficiently enforced without violating user privacy.

6. Summary and Conclusions

We have briefly explored some of the challenges facing the development of models, protocols and architectures to support secure pervasive computing. A socio-technical view of the complexity of the percom domain provides a logical starting point for such investigations.

References

[1] J. Al-Muhtadi et al A Flexible, Privacy-Preserving Authentication Framework for Ubiquitous Computing Environments, *Proc. Int. Workshop on Smart Appliances and Wearable Computing*, Vienna, Austria, July 2002.

[2] J. Al-Muhtadi et al, Cerberus: A Context-Aware Security Scheme for Smart Spaces, *Proc. 1st IEEE Conf. on Pervasive Computing and Comm. (PerCom),* 2003.

[3] S. Jajodia et al. Provisional Authorizations. *E-Commerce Security and Privacy*, Kluwer, 2001.

[4] M. Langheinrich. Privacy by Design -- Principles of Privacy-Aware Ubiquitous Systems*, Ubicomp 2001 Proceedings*, Lecture Notes in Computer Science, vol. 2201, pp. 273-291, Springer, 2002.

[5] N. Michalakis. PAC: Location Aware Access Control for Pervasive Computing Environments, MIT LCS, 200 Technology Square, Cambridge MA, 02139.

[6] B. Noble, Protecting Applications with Transient Authentication, *Proceedings of MobiSys* 2003, San Francisco, CA, May 5-8, 2003, pp. 57-70, ACM.

[7] J. Park and R. Sandhu, The UCON_{ABC} Usage Control Model. *ACM TISSEC*, Feb 2004.

[8] F. Stajano. *Security for Ubiquitous Computing*, John Wiley and Sons, Ltd., 2002.

[9] R. Thomas and R. Sandhu. Task-based Authorization Controls (TBAC): A Family of Models for Active and Enterprise-oriented Authorization Management, *Proc. of the IFIP 11.3 Workshop on Database Security,* 1997.

[10] R.K. Thomas. Team-based Access Control (TMAC): A Primitive for Applying Role-based Access Controls in Collaborative Environments," *Proc. 2nd ACM Workshop on Role-based Access Control,* 1997, ACM.

[11] M. Weiser. The Computer for the Twenty-First Century, *Scientific American,* Sept. 1991, pp. 94-104.

[12] M. Weiser. Hot Topics: Ubiquitous Computing, *IEEE Computer*, October 1993.