ISSN No. 0976-5697

Volume 4, No. 6, May 2013 (Special Issue)

International Journal of Advanced Research in Computer Science

REVIEW ARTICAL

Available Online at www.ijarcs.info

Infrastructure of Authentication and Authorization for Mobile Users Using Pervasive-PKI

Ms. Poonam. A. Manjare*, Prof. R. R Keole
First year M.E*, Asst. Professor, department of
Computer Science and Engg,
H.V.P.M's college of engg. & tech. Amravati, India.
manjarepoonam@gmail.com*, ranjitkeole@gmail.com

Abstract- In computer science distributed systems could be more secured with a distributed trust model based on PKI. PKI provides a framework to verify the identities of each entities of given domain. However, it becomes difficult to establish trust relationship across heterogeneous domains due to different actual trust mechanism and security policy as well as the intrinsic flaw of each trust model. Network and device heterogeneity, nomadic mobility, intermittent connectivity and, more generally, extremely dynamic operating conditions, are major challenges in the design of security infrastructures for pervasive computing. Yet, in a ubiquitous computing environment, limitations of traditional solutions for authentication and authorization can be overcome with a pervasive public key infrastructure (pervasive-PKI).

Keywords: Authentication, Authorization, Security Architecture, Trust, Ubiquitous Computing

I. INTRODUCTION

Advances in wireless technology and portable computing along with demands for higher user mobility have provided a major impetus towards ubiquitous computing. The promise of this new paradigm is the integration of microprocessors into everyday objects, able to communicate among themselves and with users by means of ad-hoc and wireless networking. Indeed, wireless networks provide mobile users with ubiquitous communication capabilities giving them access to information regardless of their location. In order to support business applications in ubiquitous networks, trust relationships between users need to be strengthened. Therefore, increasing confidence requires pervasive security services based on strong authentication and authorization mechanisms. In ubiquitous computing, the main security challenges arise from network heterogeneity as well as from a dynamic population of nomadic users with limited devices.

In this paper, we present a pervasive infrastructure for authentication and authorization services in heterogeneous networks, in the form of a pervasive public key infrastructure (pervasive-PKI). This infrastructure, developed as part of the UBISEC project, is able to provide authentication and access control services for users roaming between different heterogeneous networks. In this sense, the pervasive-PKI fully supports nomadic mobility, enabling secure services for users connecting through many different networking technologies (Wi-Fi, UMTS, Bluetooth, etc.), and in multiple network topologies, even when global connectivity is lost and some services are temporarily unreachable. We clearly differentiate between two modes of operation: in connected mode, on-line trusted servers are available and traditional techniques are applicable for validation of user credentials; however, in disconnected mode, the information necessary for this validation is not always available. To support the disconnected mode, we combine different solutions: an adapted privilege verifier for authorization, a new trust model for authentication, and a collaborative model to obtain unavailable information. Some of the functions traditionally performed by authentication and authorization infrastructures are integrated into user devices, providing support for credential validation in situations where central authorities are not available, like in peer-to-peer mobile ad-hoc networks (MANETs). Furthermore, the pervasive-PKI is also endowed with reconfiguration capabilities.

II. AUTHENTICATION AND AUTHORIZATION INFRASTRUCURES

Authentication solutions like Microsoft .NET Passport and Kerberos depend on user selected passwords. However, from a security point of view, it is more interesting to use further advanced technologies like digital certificates and PKIs, which combined with some complementary techniques and tools, can also be used as a starting-point to provide authorization.

A. Evidence-Based Computational Trust Management:

In a PKI, trust is fundamental to establish "certification paths" among entities, either CAs or end users. PKI configuration requires manual intervention, and applying hierarchies through cross-organizational boundaries on a large scale basis could be difficult. This scheme is not applicable to mobile users, because these often require peer-to-peer trust relations. In this kind of relationship, each user or domain can be a trust anchor. Although a peer-to-peer trust model is more flexible than traditional PKI, it suffers from scalability and uncertainty problems. For instance, PGP [1] is a well-known example of this type of system. For these reasons, evidence-based computational trust management models have been proposed such as PTM [3], Subjective Logic [4], SECURE [2], ENTRAPPED Platform [5], TMF [6], among others. These models consider risk and uncertainty issues, and bring dynamism and flexibility. However, open and peer-to-peer systems are vulnerable to Sybil attacks [7], and computational trust management models do not have well-referenced trust metrics for

CONFERENCE PAPER
"A National Level Conference on Recent Trends in Information Technology and Technical Symposium" On 09th March 2013
Organized by
Dept. of IT, Jawaharlal Darda Inst. Of Eng. & Tech., Yavatmal (MS), India

assessing and reasoning about attack-resistance [8]. Pervasive Trust Management (PTM) has been designed for mobile users, by providing them with autonomy to establish new peer-to-peer trust relations, even with unknown users. PTM models trust relations with continuous function ranging from 0 to 1, where these values represent the extreme cases of complete distrust and complete trust, respectively.

B. Component-Based Reconfigurable Architecture:

The dynamicity and heterogeneity of ubiquitous environments require security management to be flexible enough to be easily tailored to different operating conditions such as multiple authorization and authentication policies, variable user preferences, or scarce resources — when only key security services should be included into a featherweight security infrastructure. Component-based security architectures are currently emerging as a promising solution to reach such flexibility. Components are usually defined as entities encapsulating code and data which appear in software systems as units of execution, configuration, deployment, or administration. The component paradigm enables the security architect to master the complexity of implementation of a software infrastructure: since components can be composed to form higher-level units of code, one can observe and manipulate the infrastructure at the right level of abstraction and granularity, both during design and implementation phases. The resulting infrastructure is thus very modular.

III. OPERATION SCENARIO FOR PERVASIVE PKI

Let Peter and Alice be two mobile users that have temporal connectivity to centralized PKI services (for example, when they have a stable Internet connection). During this period of connectivity they work in connected mode, and they have full access to all PKI services offered by the infrastructure. Later, users move and lose global connectivity. However, they can still communicate among each other by forming a peer-to-peer MANET but they cannot accede to centralized PKI services. In this situation, which we call disconnected mode, users should be able to establish secure communications. In particular they should be able to perform authentication and access control decisions. The main objective of this research is focused on providing mechanisms that extend the PKI functionalities to mobile users when they work in the disconnected mode. To achieve this objective, we propose a new architecture for the pervasive-PKI, where functionality traditionally performed by a centralized infrastructure is moved to user devices, making certificate validation also possible in the disconnected mode.

Below, we state the main requirements for an infrastructure providing authentication and authorization services in ubiquitous scenarios, which lead to the design of the pervasive-PKI:

a. Operation over heterogeneous networks- Pervasive computing environments include many different network topologies and technologies (Wi-Fi, UMTS, Bluetooth, etc.). This heterogeneity implies multiple disconnected trust domains, where each domain applies its own policies and mechanisms for authentication and authorization.
b. Support for the authorization service- PKI-based mechanisms are suitable for authentication in heterogeneous trust domains, and also facilitate mobility over heterogeneous networks and temporal disconnection of services: users carry their credentials to authenticate themselves anywhere at any time.
c. Support for mobile users- A major challenge to implement mobility is the free roaming of users across different administrative domains. In the past, users have been demanding roaming in homogeneous GSM networks. However, in the near future, users will require context-aware computing involving an increasing number of heterogeneous networks and mobile devices.
d. Single sing-on (SSO) - Using an AAI, a user would register only once in his home domain. When he requests a resource in a visited network, he should always be authenticated and authorized by using his home domain credentials.
e. Support for temporal disconnections- When users move across different networks, global connectivity may be lost and some PKI services may be temporarily unreachable.
f. A dynamic trust model for disconnected modes- Several typical certificate validation processes, such as path processing and revocation status checking cannot be guaranteed when working in disconnected mode. Even more, unrelated users possibly certified by unknown CAs may want to interact. Therefore, we require a new trust model for situations where a certificate cannot be verified or new trust relations cannot be established by traditional PKI mechanisms.
g. Operation into limited devices- Mobile users typically used lightweight devices such as PDAs or mobile phones. Although these devices are easily portable they have much more limited capabilities than PCs or laptops. In particular these constrained devices have limited computational, communication and storage capabilities, and power consummation is also an important issue. We have to take these limitations into account, providing mechanisms that can be performed by very constrained devices.

IV. ARCHITECTURE

Authentication and authorization services for Internet users can be based on AAIs. In the connected mode, Public Key Infrastructures and Privilege Management Infrastructures (PMIs) can efficiently support both services, respectively. However, in the disconnected mode these infrastructures are not reachable and we require new solutions. This section proposes an architecture that extends the functionality of several PKI services to the disconnected mode. Fig 1 shows the proposed architecture for the pervasive-PKI. Mobile users obtain their credentials from a X.509 AAI and they store the certificates in their devices or smart cards. Further authentication and authorization will imply the validation of these credentials. In connected mode, part of the AAI can be used to help credential validation, whereas in disconnected mode the infrastructure is not reachable and several functionalities such as certificate path processing and revocation status checking are not available. Therefore, several cooperating software components installed in the user device have to be used to support credential validation.

CONFERENCE PAPER
"A National Level Conference on Recent Trends in Information Technology and Technical Symposium" On 09th March 2013
Organized by
Dept. of IT, Jawaharlal Darda Inst. Of Eng. & Tech., Yavatmal (MS), India

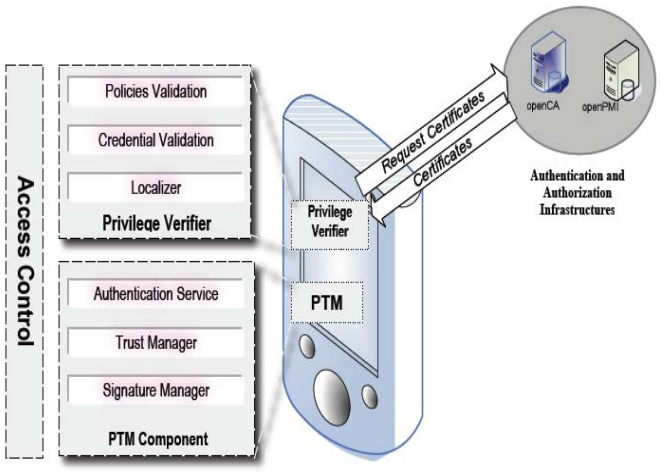

Figure 1. Proposed architecture for the pervasive-PKI

Mobile users can form self-organizing networks in isolation, in order to share services, or to participate in peer-to-peer applications. Thus, some devices have to behave as servers, making certain decisions about access control, establishment of new trust relationships, or validation of credentials, etc. In this section, we present the three software components that have to be included in user devices that allow implementing secure authentication and access control, even in disconnected mode: the PTM component, the Privilege Verifier (PV) and the Access Control Engine (ACE).

A. PTM Component:

PTM component manages trust information about users, validates public key certificates (PKCs), signs messages and verifies digital signatures. These functionalities are provided by three components:

a. The Authentication Service manages PKC validation, using the "trusted certificate list" holds in the user device. In the disconnected mode case, this component has been adapted by implementing our own algorithm for certification path validation. The algorithm uses recommendation information, trusted certificate list, and a revocation service if available [11].

b. The Trust Manager boots and manages trust information about users. Trust information includes trust values, and trustworthiness level according to a threshold. This information allows handling the trusted certificate list in a semi-automatic way. Likewise, this component maintains a black list of untrustworthy users.

c. Finally, the Signature Manager can act in two ways:
   a) For message signing, using the user's private key that can be placed in tamper-proof storage like a smart card.
   b) For signature verification, this uses the public keys bound to the certificates stored in the trusted certificate list.

B. Privilege Verifier (PV):

This component manages the validation of Attribute Certificates. The Privilege Verifier (PV) is divided into three components:

a. The Authentication Manager manages PKC validation. This component was adapted to disconnected mode to work in connection with the PTM component.

b. The Localizer component provides information to other components of the PV.

c. The Attribute Certificate Verifier (AC Verifier) component is in charge of validating the user AC and to get the privileges or role assigned to the user.

Therefore, this component supplies to the rest of modules with the information contained in the CA of the user. Attribute Certificate validation is performed as follows:

a) Firstly, the PV receives an AC supplied by the user or by another way to the pervasive-PKI system. The PKC linked to the AC can be supplied in the same way as the AC. If the PKC is not supplied, the AC Verifier can obtain it from the Localizer. If the Localizer stores the PKC into his local cache, send it to the AC Verifier, if not, requests the PKC to the PTM component.

b) The validation of PKCs is then delegated to the PTM component and is managed by the Authentication Manager. If the PKCs are valid, the authentication result is a Boolean value. Otherwise, the outcome is a trust level calculated by the PTM component.

c) The AC Verifier component uses the information supplied by the user and the PTM component to validate the user privileges based on policies and environment variables.

C. Access Control Engine (ACE):

This component is in charge of decision-making when controlling access to resources. It relies on the PTM to authenticate users requesting access, and on the PV to validate the credentials presented by the requester. Access is then granted or not depending on the current authorization policy. The ACE implementation mostly follows the XACML access control framework, clearly separating logic for policy enforcement and decision.

D. Reconfigurability:

A flexible authentication service should allow adapting the authentication method to the security context. This operation can range from fine-tuning some configuration parameters to changing the authentication algorithm. For instance, the strength of authentication may be tuned by selecting the threshold T for PTM trust values above which user entities are authenticated: T=1 for Boolean authentication if a CA is available on-line as in a traditional PKI; and T<1 for disconnected mode, where trust is managed in a P2P manner between entities. Independently from the network architecture, the PKI is expected to provide a list of security services which may need to be extended. Further, for each security service such as certificate validation, the interactions between the components can be described with several protocols [9].

V. CONCEPT IMPLEMENTATION

We considered the following scenario to demonstrate the functionalities of the pervasive-PKI in the UBISEC project. Let Peter, Alice and Bob be three users that previously do not know each other. Each user device (PDA) has the following software installed:

a. A Photo Album Service (PAS) application, which allows users to store, view and organize their digital pictures.
b. The pervasive-PKI providing access control to both shared and private pictures. Peter sometimes tries to break the security of all the devices that he can find. He doesn't have any picture in his album yet. Alice has some private pictures that she doesn't want to share. But, she has given permission to fans of the Pervasive club to access some of them. Bob has several pictures divided into two categories: private and free access. He is a fan of the Pervasive club. The users form ad-hoc networks in order to exchange pictures. The available pictures can be viewed or stored into the local photo album repository.

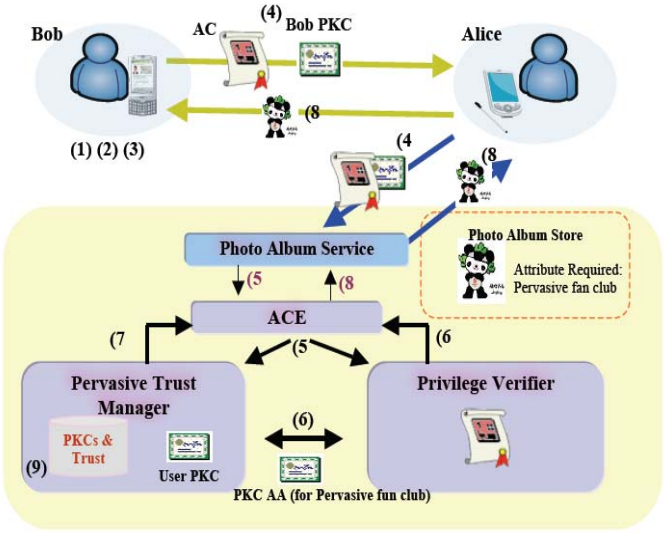

Figure 2. Test-bed scenario for the pervasive-PKI

VI. PERVACIVE-PKI

We tested two cases. In the first one, Bob act as client and Alice as server. Fig 2 shows the steps performed for a successful access to photo:

a. Bob starts the PAS application and joins the MANET.
b. Bob's PAS application starts a service discovery process to find other reachable PAS in the network.
c. Bob's PAS application shows all other available PAS. Alice's PDA offers pictures about the Beijing 2008 Olympic Games.
d. Bob asks for the picture of Beijing 2008 Olympics Jingjing Mascot, therefore, the identification and authorization process starts. Bob's credentials (PKC and AC) are sent to Alice to prove he has the rights to see the picture.
e. This request is delivered to Alice's pervasive-PKI software. Thus, the ACE component requests AC validation to the PV and PKC validation to the PTM.
f. The PV requests to the PTM the AA (for Pervasive fun club) PKC validation in order to validate the AC signature.
a) If the AA PKC is valid and trusted, the PV gets the attribute bound to Bob's AC.
b) The PV sends the response to the ACE component.
g. The PTM sends the response to the ACE concerning the user PKC validation.
h. The ACE sends the result to the PAS application to start sending Beijing 2008 Olympics Jingjing Mascot picture to Bob.
i. The PTM monitors Bob's behavior to update his trust level.

In the second case, Bob acts as server and Peter as client: Bob is also offering a few pictures, and Peter tries to get a new picture from Bob's PDA. Bob's PDA then performs the same steps to validate Peter credentials. However, Peter is an untrustworthy user. Moreover, he doesn't have enough privileges to obtain that picture since Peter is not a member of the Pervasive fun club. Then, the ACE component denies access to Peter and his trust level is updated. The PAS defines 28 different error codes arising from the validation process, i.e. output of the PV-PTM invocation. These error codes besides some other general patterns (like a DoS attack) are assigned weights by the PAS and continuously traced by the "Action Monitor" in the log files to recalculate the trust values.

VII. CONCLUSION

In particular, we have been focusing on the authentication and authorization in distributed environments, the security of shared resources, and the privacy of participants. In this paper, we presented a ubiquitous authentication and authorization infrastructure, which allows the validation of user credentials in heterogeneous networks where global connectivity can be lost and some services can become temporarily unreachable. Authentication and authorization are provided to users and applications through the combination of traditional PKI and new PMI services, notably thanks to a new trust model and the use of attribute certificates. Several software components are proposed for the users' devices, in order to extend several PKI functionalities to the disconnected mode. This modular infrastructure supports free roaming of users across different administrative domains and network technologies, and it is endowed with reconfiguration capabilities. We also described a proof-of-concept implementation of the pervasive-PKI developed in the UBISEC project. In the validation test bed we showed the functionality of the pervasive-PKI in the disconnected mode, computing the performance of our implementation.

VIII. REFERENCES

[1]. The International PGP Home Page. Available at http://www.pgpi.org/

[2]. IST SECURE project. http://www.dsg.cs.tcd.ie/dynamic/?category_id=206

[3]. F. Almenárez, A. Marín, D. Díaz and J. Sanchez. Developing a Model for Trust Management in Pervasive Devices. IEEE Workshop on Pervasive Computing and Communication Security, 2006.

[4]. A. Josang, "An Algebra for Assessing Trust in Certification Chains," Proc.Network and Distributed Systems Security Symposium (NDSS), 1999.

[5]. D. Ingram. An Evidence Based Architecture for Efficient, Attack-Resistant Computational Trust Dissemination in Peer-to-Peer Networks. Third International Conference on Trust Management (iTrust'05). 2005

[6]. M. Waseen, R. McClatchey, I. Willers. "Scalable Evidence Based Self-Managing Framework for Trust Management". Electronic Notes in Theoretical Computer Science (ENTCS). 179:59-73. 2007.

[7]. J. Doucer. The Sybil Attack. First International Workshop on Peer-to-Peer Systems. Vol. 2429. Pages: 251 - 260. LNCS. Springer-Verlag. 2002

[8]. A. Twigg, N. Dimmock. Attack-Resistance of Computational Trust Models. In Proceedings of the 12th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'03). 2003

[9]. E. Bruneton, T. Coupaye, M. Leclerc, V. Quéma, and J.-B. Stéfani. The Fractal Component Model and its Support in Java. Software - Practice and Experience (SP&E), special issue on Experiences with Auto-adaptive and Reconfigurable Systems, 36(11-12): 1257-1284, 2006.

[10]. J. Forné, J. L. Muñoz, F. Hinarejos, O. Esparza. "Certificate Status Validation in Mobile Ad-Hoc Networks". IEEE Wireless Communications, 16(1):55-62. 2009.