ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 4, October 2013

Security Attacks and Solutions On Ubiquitous Computing Networks

Ahmad Sharifi, Mohsen Khosravi, Dr. Asadullah Shah

Abstract*— Ubiquitous computing evolved tremendously and became an integral part of many fields and application domains. It not only causes maximized availability for users with wired or wireless networks but also supports any information technology equipment such as cell phones, PDAs, car navigation terminals and consumer information appliances as well as desktop computers and mobile PCs. This new computing paradigm also brings along modern and unique security challenges regarding vulnerabilities and appropriate solutions. Possible solutions for threats of ubiquitous environment to address these security issues are highlighted.

***Index Terms*— Ubiquitous, Network, Security, Mobile, Solution**

I. INTRODUCTION

In conventional computing environments, users actively prefer to interact with computers. Ubiquitous computing applications are feasible to be different, they will be embedded in the users physical environment and integrate smoothly with their everyday tasks. This new technology, involving elimination of time and position barriers are extremely inexpensive products that provide availability for users anytime and anywhere. The users are encircled with an easy and reliable information vicinity merging physical and computational basis into an integrated manner. Various human abilities in daily tasks, medicine, business, entertainment and education are enhanced to perform by this scenario using cellular phones, Personal Digital Assistants (PDAs) and other built in intelligent appliances related to different tools. Ubiquitous environment guarantees the accessibility of users to the Internet in multiple places with a variety of connection media and aware adoptability of service to the user status [1,9]. This facility is due to context implying computing context, user context, physical context, temporal context and context history. In other hands, this type of computing is broader than mobile computing considering that it interests not just mobility of computers but, more significant, mobility of the people. Context-aware computing instruments and implementations acknowledge to alterations in the environment in an intelligent manner to improve the computing environment for the user noticing the mobility of user and its context and requirement of context-aware behavior in mobile environment. The context includes:

- **Who (social):** Identification of people near the user
- **What (functional):** Tasks the user is running
- **Where (location):** The geographical position of user
- **When (temporal):** Temporal context defined
- **Why (motivating):** The reason of running task

The realization of ubiquitous computing desires obtaining seamless service provisioning for users and devices everywhere. Users in ubiquitous computing environment can access to variety of networks with high probability, reliability and availability whereas the security risk will increase as well. Some of ubiquitous applications are:

- **Smart tool box:** They are instruments with RFID tags; they have built-in antenna integrated with the box. Time usage and frequencies are used to inform suitable reconfiguration or status.
- **Smart supply chain:** With applying ubiquitous computing error level on companies can be reduced and tasks can be performed quickly.
- **Context-aware application:** They support to mobility, physiology of users. Data is gathered by sensors then it will be analyzed as well as a suitable decision will be made to satisfy the purpose.
- **Ubiquitous healthcare:** Management of chronic diseases via technology based ubiquitous patient monitoring services has been widely proposed as a viable option for economizing healthcare resources, and providing efficient, quality healthcare. They can monitor health status and perform appropriate designs.
- **Smart home:** Bringing ubiquitous computing applications to home environments is a great challenge. It enables occupants to remotely control or program an array of automated home electronic devices. They provide for owners comfort, security, energy efficiency (low operating costs) and convenience at all times, regardless of whether anyone is home.

II. SECURITY CHALLENGES AND NECESSITIES

A. Security

Security design must consider principles of time and location whereas ubiquitous computing is increased in multiple- environment openly [6]. Eavesdropping of communication media, Denial Of Service (DOS) and modification of information are patterns of attacks performed by a hacker due to obtaining control of user instruments. Moving across various networks smoothly without user-aware of what network is passing forms main objective to carry out reliable services without more insist on infrastructure. Protection from unauthorized user (security), prevention of access by an attacker through unauthorized techniques (integrity), providing accessibility for user entirely (availability) and avoiding an entity from refusing former actions (non-repudiation) are important factors in the security model. Noticing type of transferring data, possible distortion or misuse, weaknesses and features, the security issues in

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 4, October 2013

wireless network infrastructure for ubiquitous environments can be illustrated.

- Lack of authentication
- Recent flaws due to former attacks
- Unplanned growth to improve
- Lack of suitable security solution
- Weak control
- Elements interaction issues regarding upgrades
- Weak application

Although technical capability in the side of users maybe relies on distributed security mechanism, some circumstances require more security to address and ubiquitous computing enlist security in different approaches.

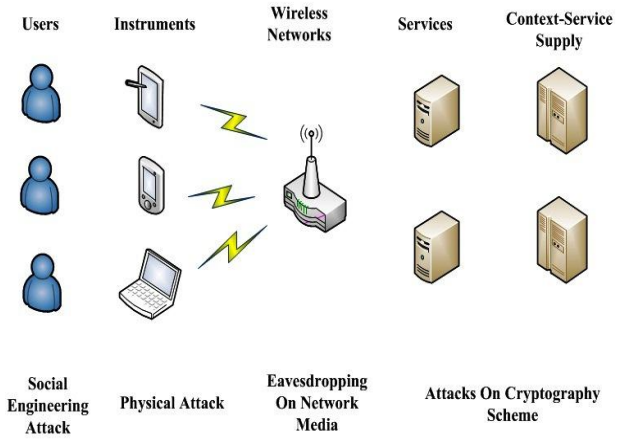


Fig 1- Ubiquitous environment and issues

Particular security requirements and solutions [1,3,4] can be determined as below:

- **Interoperability:** Every domain in ubiquitous environment is addressed by its proper security solution so it needs to be matching with existing local security solution.
- **Availability:** Whereas the environment is dynamic, incoming and outgoing entries affect networks entirely, so proper operation named Ubiquitous Device Management (UDM) act against alteration of environment to maintain availability.
- **Protection:** Credential in environment can be existed at different layers using IP Security (IPSec) and Secure Socket Layer (SSL). Different security protocols exist in different network infrastructure and unified protocols are required at the ubiquitous network level.
- **Delegation:** A running service regarding different networks and their mobile parts can change the network so it is necessary for users to authorize alterations and delegate their right to a management function running on their behalf.
- **Platform safety:** Ubiquitous networks are enhanced with capability to download application securely that allow proportional update or reconfigure. If there is no limitation on downloadable source for application so malicious applications may penetrate and reconfigure an instrument. For this reason, it is urgent to protect the platform from this kind of attacks.
- **Single sign on (SSO)**: Whereas, users often need to access multiple service providers getting involved with multiple authentications and various devices, services and networks, so it is required to implement a single sign-on solution which reforms the initiation for entries to authenticate once in all network domains to include reliable leaving and joining of ubiquitous networks without disturbances.
- **Content safety:** While significant capability of delivering multiple services by ubiquitous computing to users is noticed, assurance of being secure for providers in digital environment is guaranteed using a Digital Right Management (DRM) system to implement in ubiquitous instruments.

A. Challenges

The further aspects and the extended functionality that ubiquitous computing offers make it inclined to more vulnerabilities and disclosures concluding an extra responsibility to the security subsystem.

- **The extended computing boundary:** The new computing environment indicates the intangible conventional computing with related constraints of user locations. On this environment traditional methods concentrating solely on digital security are insufficient.
- **Privacy issues:** Because of physical outreach of ubiquitous computing, privacy of users is become as a perverse task. More intelligent spaces and computing capabilities that are openly extensive supplied by natural construction. These spaces can be captured and utilize context information. So the system forms a distributed observation system that can capture too much information about users and donates confidence of track prevention for users.
- **Trust security:** Trust is an association between two entities such that one entity credits other trusted entity and also is a representation of being reliable, secure and trustworthy in any interaction with the node. A trust security task will supply implements qualifying to utilize and doing performance of security related decisions autonomously.
- **Social issues:** Social cues can be extremely important for building models of security, privacy, and trust in a system. Knowing what other people think, talking with other people affected by the system (or responsible of it), and the general social pressures of belonging to a group can all affect people's perceptions of technology. Individual, group and behaviours are categorized as social issues. New ways of communicate, technologies, interaction and also human behaviour is considered.
- **User interaction issues:** Because of the nature of group interactions between users in the space, it is not easily possible to deny seeing or hearing of user information, thus consideration to overcome due to this issue must be taken into security plan by jointing physical and virtual aspects of access control with each other.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 4, October 2013

- **Information operation:** It is a serious concern in the network in the networks that is over new types of threats. It can be defined as actions taken that affect adversary information and information systems while defecting one's own information and information systems. In this way cyber terrorists and other techno-villains can exploit computer networks, inject misleading information, steal electronic assets or disrupt critical services monitor to prevent.
- **Security policies:** Implying a flexible and convenient approach to define and manage security policies in a dynamic context-aware form is dominant for ubiquitous computing. Policy Management tools provide administrators the capability to specify, implements, and imposes rules to exercise greater control over the behaviour of entities in their systems. The policy management software maintains an exhaustive database of corresponding device and resource interfaces. With the increase of heterogeneous device-specific and vendor-specific interfaces, these tools may need to be updated frequently to accommodate new hardware or software, and the system normally becomes difficult to manage. As a result, general purpose low-level management tools are limited in their functionality, and are forced to implement only generic or coarse-grained policies.

III. SECURITY ATTACK AND SOLUTIONS

A. Security attacks

Some famous security attacks on ubiquitous environments can be illustrated as below [7,10]:

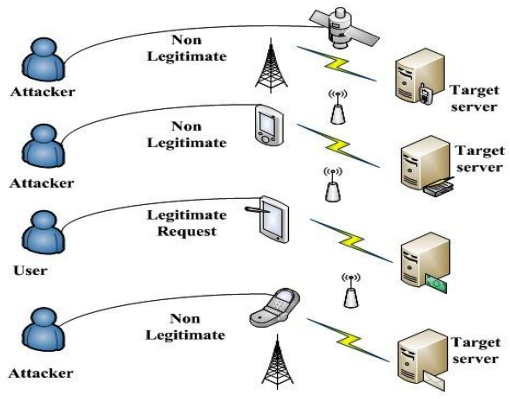


Fig 2- Attacks on different nodes

- **Man-in-the-middle attack:** Authentication of appliances in delivering services is very important. A user must authenticate the artefact mandatorily, while using a secret, i.e., password or PIN code. The Man-in-the-middle attack happens when artifacts or users forward challenges and responses to simulate the existence of other actors. When a client uses his credit card through terminal, even though proper security protocols are tangent, a masquerade attack is a probability. In other words, an attacker has the ability to modify the transaction without tampering with terminal and needless to steal the card. So this kind of attack cannot be verified to plug in the right terminal in any way due to not occurring in a virtual context. This kind of attack allows the impersonation of artifacts and users.
- **Access network attack:** Home gateway and outside service provider connect together through the access network. Obviously, if the attacker gathers the sensitive data form network packet at the household network connection point, critical information such as: financial data, user ID and other information can be exposed.
- **Illegal connection attack:** Whereas household appliances are connected to multiple networks through the home gateway which is normally controlled by web based management, the problem arises when the attacker can obtain this administration. Then it can attack against the rest of network easily. In addition may be an attacker pretends own as one internal legitimate user and control the home appliances. Leakage of information can lead to misuse of it that is not interested by users.
- **Capturing sensitive data:** Electronic sensors are commonly used in the ubiquitous systems and because of their poor computational opportunity in the monitoring procedure, while an attacker can use this reality with putting a receiver close to the sensor to achieve sensitive information from the implemented sensor directly. In these sensors, usually focus is about sensing tasks instead of cryptographic affairs.
- **Stealing Intermediary device:** An intermediary device gathers sensor data. If it goes in hand of an attacker, the device cannot be reused where it is counted as a breached source for network information to an attack purpose. In other words, this forms a potential vulnerability. In many cases, a device contains a maintenance interface.
- **Data manipulation:** Because of computational restrictions on sensors, they cannot authenticate the passing data directly. Record logs of traversing sensor data is kept on an intermediary device. Encryption and decryption techniques can be used to increase the authentication, although the how to use with poor intrinsic infrastructure on a computational manner is a challenge as well.
- **Impersonating and insiders:** A monitoring instrument can be deceived by an attacker pretending to be a technician. In this way, devices can be replaced with fake ones by the attacker. So an impersonating attacker is able to use free services form the network.
- **Denial Of Service (DOS):** This kind of attack occurs in high chances on the poor protected monitoring system while, batteries through intermediary devices could be drained or jamming appears on transmission links. This attack can cause to overload on the communication interfaces of the

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 4, October 2013

medical objectives and intensive computational process on centers processing plants. So identifying these situations in advance is important to take the appropriate steps.

B. Security solution

Security has a significant role for ubiquitous computing. In fact, it arises for many people as a primarily practical concern. In these kinds of environments and networks, some solutions to face with probable issues are proposed.[5]

IV. REAL TIME INTRUSION DETECTION

Available intrusion detection system (IDS), have varying weaknesses leading to tough deployment due to lack of considerations about heterogeneity, flexibility and resource limitation of ubiquitous networks. To figure out this problem a service-oriented and user-centric intrusion detection system (SUIDS) is suggested which record events and logs to imply protection mechanisms on different network appliances against intrusions. A user-centric approach is proposed to spontaneously compose a protection against malicious users. In SUDIS behaviour of users in long time by potential distributions are represented, which displays the expected result and relationship to any kind of actions for a user. In brief, the stages can be indicated as:

- Long term behaviors of users are accumulated.
- Possible distributions for services are developed.
- Normal and current behaviour of users are achieved.
- Statistical deviation between established behaviors and current ones are counted.
- If it is intrusion or not is recognized

V. ROLE BASED ACCESS CONTROL

Role based access control system (RBAC), is based on different roles on an individual occurring as part of an organization. In this method, each role is assigned to a set of permission to hold a place as a hierarchy among other entities. It includes two kinds of mappings, which are user role assignment (URA) and role permission assignment (RPA). These are updated separately. Users can be supplemented to the URA without changing RPA, providing new users a predefined role. And also RPA assigns users to acceptable behaviors that are restricted. The purpose of RBAC is that URA and PRA change less frequency than the permission of individual users. It has been adapted for use in ubiquitous computing environments. These steps are:

- The user role is achieved.
- The privileges related their role, are listed.
- Normal action of user is obtained.
- Privileges under role are controlled for allowance.
- In acceptable situation, a user is authenticated.

VI. TRUST BASED SECURITY SOLUTION

This proposal improves a security policy and assigning credentials to entities. Delegation of trust to third parties is focused in this mechanism. The solution has idea on extending of SPKI and RBAC for accessibility of smart devices connected together i.e., using Bluetooth. These steps are:

- Assigning credentials for a given entity is performed.
- Security policies are defined.
- Trusted entities are listed, then giving assigns to entities are initiated.
- Trust over user from trusted entities is achieved.
- A trust on a new user based on the feedback taken from trusted entities is established.
- Trust based authentication or access control is performed.

VII. LOCAL PROOF OF SECRET

It is a procedure [2] which can verify that a secret is locally known in order to prohibit man-in-the middle attacks in ubiquitous computing. It indicates how a user A can authenticates a virtual entity B. The trusted third party can certify some properties involving verification of an attribute.

VIII. RFID BASED AUTHENTICATION PROTOCOL

A radio frequency Identification (RFID) [8] is a microchip that is able of transmitting a unique serial number and other additional data through RF (radio frequency) signals. Ubiquitous computing involves computers and technology that blend seamlessly into day to day living. The purpose of RFID is to identify objects remotely by embedding tags into the objects. RFID tags are useful tools in manufacturing, supply chain management, inventory control, etc. In ubiquitous computing environment, components or RFID systems can exist anywhere. In tag's ID state, dynamic value means the tag only communicates with a fixed back-end database and the tag holding static ID indicates it can communicate with any reader in ubiquitous computing environment. RFID system must be formed to be secure against attacks such as eavesdropping, traffic analysis, message interception and impersonation, i.e., spoofing and replay. Even though RFID technology is known to be well-suited to linking the physical and virtual world, but before it could become a truly ubiquitous technology, there is still many researches challenges to be faced. Such challenges include security, privacy, deployment challenges such as health and safety and aesthetics, as well as technical challenges such as system failures and input data errors.

IX. INFORMATION LEAKAGE

Whereas there are sensitive information especially in expensive products, and concerning of users due to their information security, this matter is critical to solve. In other hand, RFID systems only response with distinguished emitting signals to a query which is related to neighborhood domain. Leakage of information can be occurred without awareness of users. Information leakage by insiders is more problematic while the asset value of information is higher. In situations of information sharing and information accessibility the problem is more serious. Therefore, it is most

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 4, October 2013

important to develop security technology that applies more strict control to inside information leakage while enabling staff inside the company to access inside information at any time in any place supporting high work efficiency.

X. TRACEABILITY

An opponent can record the transmitted message from a response of a target tag and establish a link between them. By this link, the location information of user can be detected to an opponent. In the authentication situations stages include:

- Reading RFID-tag from a product
- Transform of RFID-tag to the database server
- Check for validity of RFID-tag
- Match RFID-tag with an entity indicates authentication.

XI. BIOMETRICS

It implicates good properties to provide seamless and automated mechanisms for determining and confirming identity while, being less prominent. Finger print recognition, or face recognition techniques are faster than entering secure passwords and no need to carry special devices like PDA. Accuracy and seamless of biometric authentication techniques are very dependent on hardware. The principal concern focuses around the biometric template and sample. In whichever biometric technique that is used, these elements represent unique personal information. Unfortunately, unlike other forms of authentication (such as secret knowledge or tokens, which can be simply changed if lost or stolen), it is not possible (or necessarily easy) to change or replace biometric characteristics – they are an inherent part of the person. Therefore, once lost or stolen, they remain compromised and can no longer be reliably used. Also, biometric authentication techniques still lack a good and secure method of storing biometric features in a way that prevents compromise of sensitive data and preserves anonymity while providing enough flexibility to accommodate partial matches and reduce a suitable confidence level.

XII. CONCLUSION

Security and privacy are one of the most important issues on ubiquitous computing. The nature of the ubiquitous environment allows communications and devices traverse openly, anytime and anywhere, so modern computing networks have become increasingly ubiquitous. When services are provided easily for all various networks and their users, obviously the major concern of users due their critical information become a dominant point. In this paper the security challenges and attacks over the applications developed on ubiquitous computing environment and some security schemes have presented.

REFERENCES

[1] Adelstein. F., Gupta. S.K.S., Richard G.G., Schwiebert. L., "Fundamentals of mobile and pervasive computing", TATA McGRAW-HILL (Fourth reprint 2008)

[2] BUSSARD. L., ROUDIER. Y., "Authentication in Ubiquitous Computing", Workshop on Security in Ubiquitous Computing UBICOMP 2002, Göteborg Sweden.

[3] Campbell. R., Al-Muhtadi. J., Naldurg .P, Sampemane. G., Mickunas.M.D.," Towards Security and Privacy for Pervasive Computing".

[4] Forne. J., Hinarejos. F., Marin .A., Almena rez. F., Lopez. J., Montenegro.J.A, Lacoste, M., Diaz.D., "Pervasive authentication and authorization infrastructures for mobile users", ELSEVIER, information security technical report 12. 162-171, (2007).

[5] Kulkarni. D., Tripathi.,"Context-Aware Role-based Access Control in Pervasive Computing Systems", Dept. of Computer Science, University of Minnesota Twin Cities, MN 55455, USA (dkulk,tripathi)@cs.umn.edu.

[6] Leung. A., Sheng. Y., Cruickshank.H., "The security challenges for mobile ubiquitous services", ELSEVIER, information security technical report 12. 162-171, (2007).

[7] Hayat. Z., Reeve. J., Boutle. C., "Ubiquitous security for ubiquitous computing", ELSEVIER, information security technical report 12. 172-178, (2007).

[8] O'Driscoll. C., Cormac. D.M, Deegan. M., Mtenzi. F., O'Shea. B, "RFID: an Ideal Technology for Ubiquitous", Dublin Institute of Technology ARROW@DIT School of Electronic and Communications Engineering. Conference papers (2008)

[9] Pierre. S., "Mobile computing and ubiquitous networking: concepts, technologies and challenges", ELSEVIER, Telematics and informatics 18 (2001) 109-131

[10] Shinozuka. K., "Ubiquitous Security - Towards Realization of a Safe and Secure Digital World ", Oki Technical Review April 2007/Issue 210 Vol.74 No.2

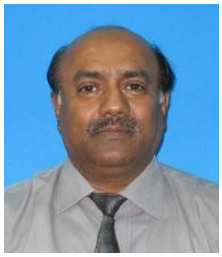
AUTHOR'S PROFILE

Ahmad Sharifi. He has received M.Tech in Computer Networks and Information Security from Jawaharlal Nehru Technological University (JNTU), Hyderabad, India. In addition, he has received his bachelor in Electronic engineering from industrial university of Shahroud, Iran. Ahmad has professional experiences on technical engineering on ISP and network designs for many years. In addition, he is involving with teaching in universities. He interests in Cryptography, WSN, ADHOC, MATLAB, OPNET and other related issues. His personal website is www.ahmadsharifi.com. Furthermore, he cooperates with RIPE NCC www.ripe.net via www.sharifisp.com that is Internet Service Provider.

Mohsen Khosravi. He is PhD student in the Information Technology department of Information and Communication Technology (KICT) of International Islamic University Malaysia (IIUM). He has received his

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 4, October 2013

master of Information Technology from Jawaharlal Nehru Technological University (JNTU), Hyderabad, India. His bachelor is software engineering from Azad university of Lahijan, Iran. His fields of interests are ADHOC, WSN and RFID that he works on it specially.



PROF. DR. ASADULAH SHAH.

He is Professor at Department of Information System, Kulliyyah of Information and Communication Technology, IIU Malaysia. Dr. Shah has a total of 28 years teaching and research experience. He has 105 research publications and 12 books published by International press. Dr. Shah has done his undergraduate degree in Electronics, Master's degree in Computer Technology from the University of Sindh, and PhD in Multimedia Communication, from the University of Surrey, England, UK. His areas of interest are multimedia compression techniques, research methodologies, speech packetization and statistical multiplexing. He has been teaching courses in the fields of electronics, computers, telecommunications and management sciences.