On Some Security Issues in Pervasive Computing - Light Weight Cryptography

Rukma Rekha N, Asst. Professor
Dept. of CIS
University of Hyderabad
Hyderabad, India
rukmarekha@gmail.com

PrasadBabu M.S, Professor
Dept. of CSSE
Andhra University
Visakhapatnam, India
drmsprasadbabu@yahoo.co.in

***Abstract*—Pervasive Computing Environment is a world where technologies fadeout into the background. The technology is invisible to the user and he is least distracted by the technology. This paper tries to focus on the issues of pervasive computing and reveals the security issues in pervasive computing. We try to find out the role of light weight cryptography in pervasive computing and a comparison between traditional and light weight cryptographic approaches was made.**

Keywords-pervasive computing;light weight cryptography;security issues

I. INTRODUCTION

"Pervasive Computing Environment is a world where specialized elements of hardware and software are connected by wires, radio waves and infrared and it is so ubiquitous that no one else will notice their presence" This is the idea Mark Weiser [2] had in his paper while referring to the vision of pervasive computing. They are the technologies that disappear into the back ground and the user has no idea about it or the user is least distracted about the technology. It is because the things in the technology can think, control and can even take decisions by connecting to the other things that are there in the pervasive environment.

In order to create a pervasive environment, support from different areas such as web technology, embedded devices, wireless technology, nomadic computers[1] and portable devices are required. Web technology facilitates ubiquitous access to all the devices in a pervasive environment. Wireless technology ensures there is no loss of connectivity among nomadic devices, where the location of the devices changes from time to time. Portable devices and embedded devices helps the user not to restrict his work place to a specific room or building and also eases him to carry it from one place to other place in terms of weight, connectivity, usage etc. This way the infrastructure with which the user interacts is minimized to a great extent or it can even be made invisible to the user thereby lessening the user distraction to the possible extent. A pervasive system is made unobtrusive by embedded devices in an environment such as wearable computers, smart homes, speech and gesture recognition sensors, optical switching devices and embedded sensors.

The goal of the paper is to identify the role of light weight cryptography in pervasive computing. As part of it we will start the paper by identifying the issues in pervasive computing. Then we focus on the security challenges of pervasive computing there by identifying the role of cryptographic approaches in a pervasive environment. We try to identify the need of light weight cryptography and try to compare the security parameters of light weight cryptography with respect to traditional cryptographic techniques. Section 2 gives a brief idea of pervasive computing and its issues. Section 3 focuses on security issues of pervasive computing and the role of light weight cryptography in a pervasive environment. Section 4 tries to compare the different cryptographic algorithms both traditional and light weight. Section 5 concludes the paper and the future scope related to light weight cryptographic algorithms.

II. PERVASIVE COMPUTING

Satyanarayanan[3] identifies that the roots of pervasive computing are laid in the mid 1970's itself where distributed and mobile computing are taking their shape. The issues being identified in pervasive computing now are those that are already there in distributed and mobile computing areas. Also, new problems and issues were introduced by pervasive computing which doesn't have any relation to the earlier problems. In many of the cases, existing solutions will help us to resolve the issues whereas for few of them, we have to find an entirely new solution.

Distributed computing is a collection of more than two computers are connected to a network, where the connection can be either wired or wireless. The wireless LANS thus constructed using distributed system raised a no. of issues for the mobile clients resulting the era of mobile computing. Although the basic idea of mobile computing is not so different from distributed systems, some key constraints on mobile elements such as power consumption, size, weight, variation in the network quality resulted in a few specialized techniques for them [3].

Pervasive computing which is built on the basic ideas of distributed and mobile computing also do have few constraints due to which it is supposed to focus on few key issues like effective usage of pervasive environment, invisibility of the infrastructure to the user, scalability of the pervasive environment , smartness of the devices in order to have less user distraction. Mark Weiser's [2] ideal assumption about pervasive environment is invisibility of the infrastructure which may seem highly impractical and can be brought down to minimal user distraction. Peer to Peer technology assists the emerging technology by sharing data among peer devices without the necessity of relying on a centralized server. It helps the companies to be in constant touch with their clients, thereby resulting in business growth.

Technologies such as nano technology initiates use of Net-ready chips, RFID tags that can be embedded in human bodies, objects that can help us to track their location and positions. Such devices are very much helpful for old patients, infants to track their location and position in case of emergencies and also as part of monitoring. Also small objects in big malls can be identified even if they got struck amidst piles of large entities. This ensures us that pervasive computing can help us a lot in health care domain. Constant communication with wireless gadgets can ensure constant feedback loop which is a new way of reaching customers.

Pervasive Environment can be implemented on a variety of devices such as PDAs, laptops, mobile phones, digital cameras and printers. Mobile users get transparent access to resources outside their current environment. Software's such as voice recognition system, hand writing recognition system, face recognition system do help the pervasive system to reach its goal of minimal user distraction. These systems help us to give voice commands to a computer to get a work done such as opening a file, transferring some data on the web. Also hand written recognition system helps us to avoid forgeries despite the existence of digital signatures and signcryption schemes. Confidential data being displayed in a room can be hidden by detecting an unrecognised face with the help of a face recognition system.

Pervasive devices exist in no. of sizes each suited to a particular task such as tabs, pads and boards. Pervasive environment uses hundreds of computers in a room and these hundreds of computers will become to be invisible to common awareness. People will simply use them unconsciously to accomplish everyday tasks. A Pervasive space requires economical and low-power devices with a convenient display, network connectivity among all the devices, and some software's to implement the pervasive applications.

The Key Characteristics that are expected from a Pervasive Computing environment are Mobility, Invisibility, Smartness and Security. Mobility need to be achieved with minimal user intervention by the help of mobile devices which are portable such as mobile devices, laptops etc. Invisibility refers to the user consciousness of a system which can be minimized by embedding smart sensors in human bodies, different accessories that they wear such as clothes, glasses, pens, jewellery. Also wireless connectivity among the different locations, an user accesses such as his office, home, car etc. ensures that these devices are always connected and user has no idea of transfer of the data from one location to the other when he moves around. This results in minimal user distraction. Smartness of a pervasive computing system depends on how it reacts to a situation on different circumstances. This can be achieved by context awareness and environment sensing through which system can sense the surroundings around it either by face, voice, temperature or other parameters depending on the context and takes the right decision.

A pervasive computing system that has minimal user distraction has to be *context-aware.* It must be aware of user's physical location, daily routine, psychological balance personal history, behavioural patterns, and so on. The desired information can be obtained from his personal profile information

The goal of a pervasive computing framework is to support services offered by different devices in a heterogeneous environment. It is most likely that most of the devices have little or no knowledge of other entities and the services they offer. This introduces important security issues especially when a new device makes available a new service for the first time. Security is essential in a pervasive environment to establish mutual trust between infrastructure and device with minimal intrusion".

III. ISSUES WITH PERVASIVE COMPUTING

Pervasive computing enables nothing fundamentally new. As stated earlier it makes use of existing technologies such as distributed and mobile systems and makes the things faster and easier to do by minimizing the user distraction. The aim of distributed computing is to make the networks disappear and reappear as disks or memory. This challenges the existing design of operating and windows systems where an additional hardware or software can be uploaded only by shutting down the system. Let us see, some of the issues of pervasive computing.

In a scenario of pervasive environment, where devices plug in and plug out depending on the location, context and time, necessity to install new software may occur at any point of time. This may not be feasible because we'll never be able to shutdown every device of a pervasive environment at once. Future design of operating systems may be done in such a way that an additional hardware can be uploaded into a system just by performing a plug- in operation[6] such that we don't have to shut down the system at least once.

The network connectivity of a device within pervasive environment is another issue under consideration in a pervasive environment. Although providing wireless network in a closed room is possible by infrared or electromagnetic technologies, their performance in an open area like a corridor or a lawn, or an open stadium is again restricted. Currently we require three different types of connections to access a mobile device namely tiny range wireless, long range wireless, and very high speed wired. It's high time that a single connection that can perform the above three functions is to be discovered.

Transparency[3] is another major issue in a pervasive environment . Self-tuning can be of great help in this effort. A mobile user's need and tolerance for proactivity are likely to be closely related depending upon his expertise on a task and his familiarity with the environment. A system has to observe user behaviour and context to strike the right balance. For proactivity to be effective, a pervasive computing system should track user intent and keep his profile updated from time to time.

Surrogate services[4] are another issue where the devices of a pervasive environment are being compromised in the size, weight as a result in their computing capability so as to make them portable. The basic idea here is that rather than increasing the size of a device for its computational capability, whenever needed we surrogate the services to the nearest capable system. Identifying the surrogate device and mutual trust between the surrogate device and the mobile device are the key issues in this part. When the mobile device leaves the network, its surrogate bindings are broken, and any data staged or cached on its behalf are discarded.

The capability of a mobile device in a pervasive environment in terms of bandwidth, charging time, latency is another issue. The question that arises here is that do we need a bulky device that performs all operations or a light weight one which supports limited no. of operations. For a given device, the minimum expectation is that, even under worst-case environmental conditions the application must run satisfactorily. One has to count on bandwidth, latency and batteries capability to ensure these.

Another issue is the resource management[3] of the pervasive devices especially in terms of power consumption. Relentless pressure to make such computers lighter and more compact, results in severe restrictions on battery capacity. The device should be environment aware, so that it can optimize its resources in idle conditions.

Lastly, Security is a major issue in Pervasive computing environment. Security is already a burning problem in distributed systems and mobile computing, and is now greatly complicated by pervasive computing. Connecting with a no. of unknown devices and interacting with them is a daily job for every pervasive device. But, how much do you trust the other device? Exploiting this information is critical but if not strictly controlled, it can be put to a variety of unsavoury uses ranging from targeted spam to blackmail. This may also cause

potential loss of knowledgeable users from using a pervasive computing system. We will discuss much about this in the next section.

IV. SECURITY ISSUES IN PERVASIVE COMPUTING

In a pervasive space where a number of devices come and go into the network, the issue of trusting a particular device is always there. Traditional way of ensuring a particular user is by user authentication through which access control can be restricted for the sake of security. In a pervasive space where there is no central control and the users are also not predetermined. Mobile users expect to access locally hosted resources and services anytime and anywhere, leading to serious security risks and access control problems [4].Jim Moorris suggested a method which acts like a lock to a house which may not entirely prevent the burglars from entering the home. Similarly, a system can be built which may not entirely resist an attack but ensures that the attacker surely leaves with a digital print which is an equivalent of a finger print in the real world [2].

Mobile devices are portable and hand held and have restricted processing capabilities, memory capacities, bandwidth support, power consumption, software support because of their size and weight. Also the processing environment is so heterogeneous that predicting any behaviour of any device may seem unfeasible. In such a scenario, security information in different domains is subject to inconsistent interpretations in such an open, distributed environment.

Security in a pervasive system should ensure exact and accurate implementation of the basic features namely confidentiality, integrity, authentication, non-repudiation and access control. In addition to the above, different parameters that are to be met by a security mechanism offered in a pervasive environment are discussed here.

- Robustness and dependability on the security mechanism is of great importance as it is of great difficulty to achieve that in such a world of wide varieties of computing technologies.
- Limited user distraction restricts user authentication every time when the device interacts with a new device and performs some operation such as data access. Building such trust mechanisms within the design of the framework can be an alternative. Also, data integrity should be maintained in a data transfer.
- Security mechanism should resist any attacks done by an attacker. Attacks may range from simple denial of service to malfunctioning of the system.

Considering the security issues of a pervasive system, there are two paths in which we can resolve them, One deals with the network security and system security issues. [4], [7] already have different protocols that can be implemented in the architecture of the system so as to avoid such security risks and much more such protocols are on the way. The second path is implementation of some cryptographic techniques in the pervasive environment such that only authenticated users have the access to the real information. Mark Weiser [2] also suggested that cryptographic techniques can be used to transfer secure messages from one ubiquitous computer to another and to safeguard private information stored in networked systems. Michel Collins [5] on the other hand suggested that security of a system should be analysed at the design of frameworks itself and some encryption techniques can be applied while data is being exchanged between devices. This can be of great help for the future coming applications, but for the legacy systems applying an encryption mechanism within the system seems to be more practical.

Also, after having sufficient number of such techniques, we can always allow, a foreign user, to access certain services without creating a new identity for him or insecurely opening up the system in any way. Such a scenario is explained in [4]. But that can be achieved only when we have such a trust in the security mechanism of our pervasive environment. The level of trust can be increased by introducing several cryptographic techniques in the implementation of a pervasive environment. Overall, cryptographic techniques make a great path for secured pervasive devices.

V. LIGHT WEIGHT CRYPTOGRAPHY

Traditional cryptography existence was there even before the aura of pervasive computing. There have been a number of cryptographic algorithms both symmetric and asymmetric , block and stream ciphers along with one time pads and feedback shift registers. Standard algorithms like DES, AES and RSA and stood resistant towards linear, differential and algebraic attacks despite of a few reduced round attacks. It will be of great help towards security point of view if we could use such algorithms in a pervasive environment. But, as discussed in Section 3, we are well aware that pervasive devices have restricted capabilities in terms of memory storage, computational capabilities, power consumption and all. Restricted computational capability and

memory storage limits implementation of traditional cryptographic algorithms in pervasive environment. This may result even in compromise of the security of a pervasive environment.

Light Weight Cryptography is designed for constrained devices. These devices have constraints in terms of speed, processing, memory space, power consumption, area, energy, size etc. Example of constrained devices includes mobile phones, RFID tags, smart cards etc. Alex [9] refers light weight cryptography as that it is as light as feathers and in terms of security it is as strong as dragon scales.

Lightweight cryptography got its focus when deployed in pervasive computer systems, where traditional cryptographic algorithms were not a viable option. The challenge is to design secure applications without any heavy-key cryptography. Mobile applications are even ensuring that authentication is no longer enough, dealing with privacy is also a matter to be considered.

Thomas in [8] says there is always a trade off between security, cost and performance in light weight cryptography. Light weight cryptography has to compromise a no. of parameters compared to traditional cryptography. For example, key length is reduced from 256 bits to 56 bits, no. of rounds that run in an encryption process are reduced from 48 to 16 and the mode of architecture shifts from parallel to serialized. Memory requirement is reduced from giga bytes to kilo bytes. Processing speed comes down from GHz to KHZ. All this is because of the restrictions that we have for pervasive devices and pervasive environment.

Lightweight cryptographic algorithms should have a short internal state because of their restricted area, and perform serialization operations as parallel processing could consume more power. Also, they should have a short processing time such that their energy consumption is saved and should support short output to reduce communication cost amongst the devices. Also, we have a few ultra light weight cryptographic algorithms where the underlying logic is the simple implementation of logic gates. The lightness of an algorithm also depends on the number of logic gates used, usually referred as gate equivalents. Irrespective of the underlying logic in an algorithm, we need to ensure that they satisfy both confusion and diffusion properties.

Axel Poschman[8] also suggests that this is not intended for all adversaries and it is not a substitution for traditional cryptographic techniques. Most light weight cryptographic implementations target towards application specific integrated circuits (ASICs). Field programmable gate arrays (FPGAs) are other option but they consume more power than ASICs. Power consumption is a primary concern for light weight cryptographic applications. With the development of low-cost, low-power FPGAs for battery powered devices, they are becoming an interesting target for light weight cryptography.

VI. COMPARITIVE STUDY OF LIGHT WEIGHT CRYPTOGRAPHIC ALGORITHMS

Light weight cryptographic algorithms are designed in two ways. One is, an algorithm developed from scratch keeping in mind that it should be applied in resource constrained environment. In such algorithms we make sure that the no. of gate equivalents are as less as possible along with the computational cost. PRESENT is one such popular light weight cryptographic algorithm. It is supposed to have the least no. of gate equivalents amongst the available light weight algorithms [8]. Second way of designing a light weight algorithm is to consider the available traditional cryptographic algorithm such as DES,AES,RSA and try to optimize the functionalities such as block size, no. of rounds etc. The advantage of such algorithms is that we have already confidence in the existing algorithm but optimization of certain parameters in the algorithm may either add complexity or may compromise on security. DESL, DESXL are few such algorithms where the no. of S-boxes are reduced from 8 to 1 and there was also reduction in the chip area of the optimized algorithm.

When it comes to application of the light weight cryptographic algorithms in real time industry, they can be categorized in two ways again namely hardware –oriented and software-oriented ciphers[8]. Hardware oriented ciphers are more applicable in areas where our concern is about the chip size and no. of clock cycles required for its execution. Such types of algorithms are more useful in nomadic devices such as smart cards. Software oriented ciphers are of great help when our concern is more about the memory requirements and power consumption. Other generic category is symmetric versus asymmetric ciphers[8]. Although its quite popular that asymmetric cryptographic algorithms offer more security than the earlier ones, its better to use symmetric ciphers in scenarios where authentication and integrity are of prime importance than non-repudiation and confidentiality. This can save us from the additional computational cost and power consumption that occur by using asymmetric algorithm.Finally its the designers decision to choose among asymmetric, symmetric and software oriented and hardware oriented ciphers based upon his requirements along with the constraints carried by them. Its quite obvious that all the applications don't have the same constraints based on their location, size etc.

Either it is an algorithm developed from scratch, are an optimized version of traditional algorithm, the designer while designing a LWC algorithm must maintain a balance among three major design goals, security, cost and performance.

Light weight applications on ECC

Elliptic curve cryptography is another interesting area when it comes to less memory requirements and computational costs. ECC applied algorithms are of great use in environments where the level of security is medium and span of the security provision is less for example for a single session. Compared to hardware oriented ciphers, software oriented ciphers may offer better performance on application of ECC. It's because making changes in the hardware every time may not be feasible every time. Also, hyper elliptic curve cryptography is of great help in such resource constrained environments as they offer much lesser memory requirements compared to ECC. But still there are less applications of HECC in resource constrained environments due to lack of standardizations compared to ECC. But still, experiments are being done using HECC in low level security application areas. Here the user can be assured of its security till the genus level of the curve is 3 , beyond which it loses its group property while performing arithmetic operations. This may cause a security breach in the application.

VII. CONCLUSION AND FUTURE WORK

Pervasive computing environment makes the user least distracted unlike the current technology where a user is supposed to fix to the computer to respond to all the commands. Pervasive devices have the capability to think, control and take decisions for a given task. Despite all these advantages pervasive computing environment have to deal with a no. of issues out of which security issues are of prime concern. Light weight cryptography plays an important role in pervasive computing to deal with the security issues. A study of various categories of light weight cryptographic algorithms is considered based on their requirements and constraints. Application of ECC to such algorithms can result in better performance with less computational cost. Security can further be enhanced by using hyper elliptic curves in place of elliptic curves but is limited to curves of genus 3.

REFERENCES

[1] Pervasive(ubiquitous)computingtoday, http://stylusinc.com/Common/whitepapers/WhitePapers/Pervasive%20Computing%20Today.pdf

[2] Mark Weiser, The Computer for the 21st Century, Scientific American, September 1991

[3] M.Satyanarayanan, PervasiveComputing:Vision and Challenges, IEEE Personal Communications ,2001.

[4] LalanaKagal,TimFinin, and AnupamJoshi,Trust-Based Security in Pervasive Computing Environments, Computer Communications, Elseiver, December 2001

[5] Michael Collins,Simon Dobson, Paddy Nixon, Security Issues with Pervasive Computing Frameworks, in workshop on privacy,Trust and Identity issues for Ambient Intelligence at Pervasive 2006 , pp 1-7, (2006)

[6] Munirul, Haque and Sheikh Iqbal Ahamed, Security in Pervasive Computing: Current Status and Open Issues, International Journal of Network Security, Vol.3, No.3, PP.203–214, Nov.2006

[7] Zeeshan Bilal, Ashraf Masood, Firdous Kausar, Security Analysis of Ultra-lightweight Cryptographic Protocol for Low-cost RFIDTags:Gossamer Protocol, in Proceedings of International Conference on Network-Based Information Systems, August 2009

[8] Thomas Eisenbarth, Sandeep Kumar, Christof Paar and Axel Poschmann, Leif Uhsadel, A Survey of Lightweight-Cryptography Implementations, IEEE Design & Test of Computers, November- December 2007

[9] Jianhua Ma, Qiang fu Zhao, Vipin Chaudhary, Jingde Cheng, Laurence T. Yang, Runhe Huang, and Qun Jin, Ubisafe computing Vision and challenges, L.T.Yang et al.(Eds.): ATC 2006, LNCS4158, pp.386– 397, Springer-Verlag Berlin Heidelberg 2006

AUTHORS PROFILE

Ms.N.RukmaRekha obtained her B.Tech, M.Tech degrees from Andhra University in 2003 and 2005 respectively. Currently, she is pursuing her Ph.d as part-time from the same university. She has around 6 years of teaching experience. She has the experience of guiding around 16 Post graduate students for their M.Tech/M.C.A Project Thesis. Ms. Rukma Rekha is now Assistant professor from Dept.of Computer and Information Sciences in University of Hyderabad.

Prof. Maddali Surendra Prasad Babu obtained his B. Sc, M.Sc and M. Phil and Ph.D. degrees from Andhra University in 1976, 1978, 1981and 1986 respectively. During his 27 years of experience in teaching and research, he attended about 28 National and International Conferences/ Seminars in India and contributed about 33 papers either in journals or in National and International conferences/ seminars. Prof. M.S. Prasad Babu has guided 98 student dissertations of B.E., B. Tech. M.Tech. & Ph.Ds. Prof Babu is now Professor in the Department of Computer Science & Systems Engineering of Andra University College of Engineering, Andhra University, Visakhapatnam. Prof. M.Surendra Prasad Babu received the ISCA Young Scientist Award at the

73rd Indian Science Congress in 1986 from the hands of late Prime Minister Shri Rajiv Gandhi. Prof. Babu conducted the proceedings of the Section of Information and Communication & Sciences and Technology including computer Science of the 94th Indian Science Congress as a president of that section in January 2007. Prof. Babu was also the sectional committee member of the Indian Science Congress in the sections of Mathematics and ICT in 1988 and 2005 respectively. He is also sectional secretary for the section of Information and Communication & Sciences and Technology of Indian Science Congress.