Lightweight Cyber Security in Pervasive Computing Environment

Shukun Tokas*
Vanita Kareer**

Abstract

Security is protection of information assets through use of technology, processes, and training. Cyber is a prefix used to describe an idea as part of the computer and information age. Combining the two terms, Cyber security implies protection of systems, networks, and data in cyber space. Pervasive devices have the capability to think, control and take decisions for a given task. Deployment of pervasive devices in unattended environment makes the network as well as device vulnerable to a variety of potential attacks. But at the same time pervasive computing devices as well as applications are extremely power and resource constrained. In such an environment traditional cyber security techniques are difficult to implement. So this research work explore on the core measures that need to be incorporated for lightweight cyber security.

Keywords: Pervasive Computing, Lightweight Cyber Security, Present

Introduction

The recent advances in wireless networks have encouraged significant increase in production and usage of sensors and significantly small mobile computing devices almost everywhere. These sensors and devices are capable of processing information locally and use a wireless connectivity to transmit captured data to a remote device or sensor. Example of such devices are mobile phone, Personal Digital Assistant, RFID tag, smart card etc. The next step is to link the physical world to digital networks so that a pervasive user can access contextual data virtually without imposing mobility restriction.

With change in environment, certainly the available network and network configurations changes as the mobile device or sensor moves in and out of wired or wireless networks. Now this movement of mobile devices among various networks makes the network vulnerable to a variety of potential attacks. As these mobile devices and sensors have inherent power and memory constraint, the conventional security solutions becomes either infeasible or ineffective. For such a mobile and distributed environment, a lightweight cyber security technique is required.

As stated earlier the need of lightweight cyber security emerges, as in the pervasive environment there are a number of mobile devices and sensors present at any given instant which have access to various wired/wireless networks posing cyber threats on the user data and device. Basically lightweight cyber security is needed or designed for constrained devices. These devices or sensor nodes are constrained in terms of speed, processing, memory space, power consumption etc. And for such resource constrained devices in unattended environments using traditional cryptographic algorithms is not a viable option, and the challenge would be to design an architecture for security without heavy-key cryptography and with short internal states.

This research work explores the key aspects and metrics which makes the cyber security system lightweight but at the same time strong enough to

Shukun Tokas*
IINTM, GGSIPU
Vanita Kareer**
IINTM, GGSIPU

prevent data from attack, damage, and unauthorized access.

This paper is organized as follows : section II discusses briefly cyber security and pervasive computing; section III describes the key aspects that needs to be incorporated to implement lightweight cyber security; and finally section IV gives a brief conclusion and plausible future scope.

Cyber Security and Pervasive Computing

Cyber Security

Cyber security is an interdisciplinary area that focuses on maintaining and reducing risks to the confidentiality, integrity, and availability of information and resources in computer and network systems[4].

One way to think of computer security is to reflect security as one of the main features[2]. Some of the techniques in this approach include:

- The principle of least privilege, where each part of the system has only the privileges that are needed for its function. That way even if an attacker gains access to that part, they have only limited access to the whole system[2].
- Automated theorem proving to prove the correctness of crucial software subsystems.
- Code reviews and unit testing are approaches to make modules more secure where formal correctness proofs are not possible[2].
- Defense in depth, where the design is such that more than one subsystem needs to be violated to compromise the integrity of the system and the information it holds[2].
- Default secure settings, and design to "fail secure" rather than "fail insecure" (see fail-safe for the equivalent in safety engineering). Ideally, a secure system should require a deliberate, conscious, knowledgeable and free decision on the part of legitimate authorities in order to make it insecure[2].
- Audit trails tracking system activity, so that when a security breach occurs, the mechanism and extent of the breach can be determined. Storing audit trails remotely, where they can only be appended to, can keep intruders from covering their tracks[2].
- Full disclosure to ensure that when bugs are found the "window of vulnerability" is kept as short as possible[2].

Pervasive Computing

The integration of cellular technology with the Web and wireless LANs in the late 1990s led to the emergence of mobile computing. Both the size and price of mobile hardware devices are falling continuously, providing the new opportunity of building a distributed system with mobile clients. Mobile computing is an important approach to information access and it prepares the way for pervasive computing - "anytime, anywhere". Pervasive computing is a superset of mobile computing [2]. The mobile computing goal of "anytime, anywhere" connectivity is extended to "all the time, everywhere" by integrating pervasiveness support technologies such as interoperability, scalability, smartness, and invisibility. In order to build a pervasive computing environment, four broad areas are essential: device, networking, middleware, and application. Traditional input or output devices, wireless mobile devices, and smart devices are the different device types which will be contained in an intelligent environment. The device could be an information source, or a processing centre, or even an agent responding to user actions. The way we consider devices is important. They are not only a repository of custom software managed by the user, but an interface of accessing an application or data space in addition [5]. The middleware is required to connect pervasive computing system devices with the end applications executing on different pervasive computing devices. It will provide transparent, autonomous, and continued services to solve problems due to the issues of mobility and heterogeneity. Pervasive

computing is more environment-centric than distributed and mobile computing, which means the application in a specific environment will determine the device, middleware and networking issues in that system.

Lightweight Cyber Security

As stated earlier conventional cryptographic solution is not a viable option for resource constrained devices and sensors in pervasive computing environment. Challenge is to design a infrastructure or applications or protocols light in implementation and at the same time strong in security, to make information and communication link safe from cyber attacks.

From the bird's eye perspective, security issues can be in one of the two broad dimensions – network security issues and system security issues. In this research work, we focus upon the system security issues, to secure information from plausible attacks.

Drawback with existing algorithms like Rivest Shamir Aduman, DES, Advanced Encryption Standard is the bigger block sizes and large number of rounds. One possible approach for lightweight cyber security could be writing protocols and algorithms from scratch. This approach certainly brings novelty but is difficult for stability reasons. Another possible approach for lightweight cyber security could be make use of exiting algorithms to develop algorithms and protocols for lightweight cyber security. And to develop such algorithms and protocols, following are the factors that plays important role in making them lightweight:

1. Perfom operations in serial sequence, as parallel operations consumes more power.
2. Restricted computational areas, as devices/ sensors are memory constrained.
3. Short processing time-slices, so as to save power consumption.
4. Should support shorter operations to reduce common cost among the devices.
5. Reduced key lengths and lesser number of rounds in encryption/decryption process, as it reduces processing time.

One such example is PRESENT, it is a promising block ciper with low implementation complexity, especially in hardware. consists of 31 rounds. The block length is 64 bits, and two key lengths of 80 and 128 bits are supported [3]. It is designed specifically for RFID tags or pervasive computing applications that are extremely power or cost constrained [3].

As there is always a tradeoff between security, cost, and performance, necessary parameters for lightweight cyber security algorithms must be chosen carefully so as to make the algorithms lightweight without compromising on the information security.

Conclusion and Future Work

The purpose is to transfer secure messages from one device/sensor in pervasive environment to a device/ sensor in another pervasive environment. There exists a number of cryptographic algorithms which could be used in pervasive environment, e.g PRESENT, but because of applicability issues arises need of a number of such algorithms. With an exhaustive understanding of cyber attacks, security parameters, resource constraints in pervasive computing environment, and existing cryptography algorithms – lightweight cyber security algorithms and protocols for communication could be formulated and tested for stable releases.

Hopefully, the aspect presented in this paper would stimulate future research and development efforts. Elliptic curve cryptography is an interesting area in cryptography which consumes less memory and works on less computational costs.

There is extreme need of small ciphers for devices for applications deployed in RFID tags or low cost smart cards. As the pervasive environment consists of a heterogeneous set of devices which supports different platforms, so the next step would be development of generalized lightweight cyber security solutions.

References

1. "cryptography and network security" by williamstallings.
2. http://en.wikipedia.org/wiki/Computer_security
3. "Understanding Cryptography" by Paar, Christof, Pelzl.
4. www.aaai.org.
5. Yau, S. S., Karim, F., Wang, Y., Wang, Y., Wang, B., and Gupta, S. 2002. Reconfigurable context – sensitive middleware for pervasive computing. IEEE Pervasive Computing 1(3).