International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 6 161 - 163

Time Based Token Mechanism for Message Security in Critical Infrastructures

Merugu.Gopichand
Professor & Head, Department of IT,
VCE,Samshabad ,
Telagana,INDIA.
Email:gopi_merugu@yahoo.com

Abstract- Critical infrastructure is the term used for describing public infrastructure such as Energy, Water, and Telecommunications etc. These are usually widely distributed and networked. Such infrastructures may consist of various levels or zones and have their own security levels according their importance. Hence some of the zones may be weakly protected as may have lesser importance. These zones can thereby targeted and once compromised may be easily used to compromise other higher level zones as being in the same network, which is generally referred as Stepping Stone Attack. A Layered Security Mechanism can be implemented in such systems/infrastructure by using the principles of hash chain based methodology to prevent possible attacks. Though this eliminates stepping stone attack but does provide enough security if the communication channel is easily available for tampering. The attacker can physically tamper with the communication medium and obtain the required security level by listening to the key exchange. A time based token generation mechanism can mitigate this risk. Tokens would eventually be generated from the authentication key itself though being generated by a function involving time as one of its parameters. Thus even listening to communication medium by physical tampering wouldn't reveal the actual user authentication key.

*****

I. INTRODUCTION

Critical infrastructures play a vast role in human society, ranging from telecommunication to financial services such as banking. Organizations still using traditional security mechanisms for these infrastructures pose a great risk to the society as a whole.

The critical infrastructures and generally hierarchical and distributed and the traditional model of security provides higher security to the most important levels higher in the hierarchy whereas lower levels or the less important end with lesser security.

The attacker can make use of these less important areas of critical infrastructure to enter and launch a stepping stone attack.

A newer mechanism known as A Layered Encryption Mechanism for Networked Critical Mechanism [1] can prevent such attacks provided that the communication links are physically secured. As this mechanism uses the authentication key of system lower in hierarchy for encrypting messages, attacks such as man in the middle don't reveal security details of system with more security level or one which higher in the hierarchy. But in contrast if these communication links could be physically tampered then it ends up voiding its purpose.

A time based token generation mechanism can work together with a layered encryption mechanism to counter this risk. In this article, we focus on this mechanism in detail.

II. CRITICAL INFRASTRUCTURES

This section describes features of critical infrastructures. **Critical infrastructure** is a term used by governments to describe assets that are essential for the functioning of a society and economy.The common features of which can be seen in Fig:1.

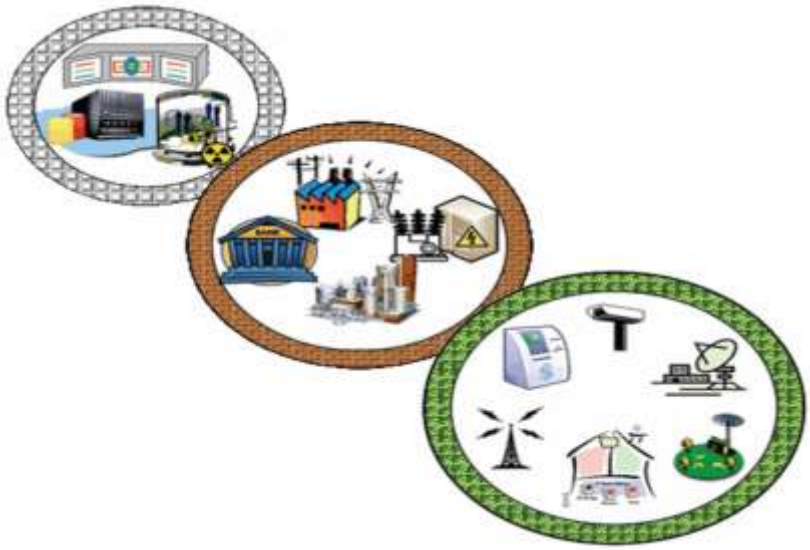

Fig: 1. Illustration of critical infrastructures.

A networked critical infrastructure has several levels of hierarchy. Each of the level has its own level of security with higher levels being much more secured compared to ones lower in hierarchy. These devices form weak points of critical infrastructure and targets for attackers. This is generally resolved by means of a Layered Encryption Mechanism.

III. LAYERED ENCRYPTION MECHANISM

This mechanism primarily consists of iterative hashing technique which generates keys meant for authentication of every level of hierarchy.

Hash Chain

Idea of Hash Chain is applying a hash function, say *H*, on a pre-selected value successively until the number of results has reached the required amount. This result-chain is said to be a hash chain.

$h_0 = r$
$h_n = H(h_{n-1}) = H(H(\ldots H(r)\ldots))$ *n* times

The following appealing properties enable it suitable for layered encryption mechanism.

• It is easy to find h_i if h_{i-1} is given
• It is computationally hard to find h_{i-1} if only h_i is given

This propertyis known the pre-image resistance which is a fundamental requirement on hash function.

Key Distribution

According to layered defense principle, critical infrastructure owners should divide their network zones into several security levels with different levels of perimeter defense.
We adopt a key pre distribution scheme, and introduce a key management device that can be a high-performance computer located in a top security zone. The distribution process can be organized into three steps. First, the key management device generates a series of unique *secret identities* for all devices. Then it generates a hash chain. Elements in this chain are assigned to devices as keys. Finally, we put all necessary information into devices' memory as follows:
• **Key**: Used for encrypted communications. It is selected from the generated hash chain, based on a device's security level. A higher security level corresponds with an earlier generated element in the hash chain. Devices with the same security level will get the same keys.
• **Key version**: During the lifetime of an infrastructure, the encryption key may be updated many times. The initial version value is zero, and is modified after each update.
• **Security level**: Indicates the security level of a device. This field also helps to negotiate key pairs between zones. It is collected from infrastructure owners.
• **Security level version**: Similar to key version, the security level of devices may change over time.
• **Secret identity**: Generated by the key management device and unique among all devices. It is used for update processes and does not appear in any communications, so it is impossible for a third party to get this information.

Pair-Key Negotiation

A negotiation of security keys is required for successful communication is shown in Fig: 2.The communication is among different levels of hierarchy and primarily based on security levels:
• If the neighbor's security level is higher than or equal to its own, it will use its key as the pair key to this neighbor.
• If the neighbor's security level is lower than its own, it will iteratively apply a hash function on the key according to the deviation value and get the result as its pair key to this neighbor.

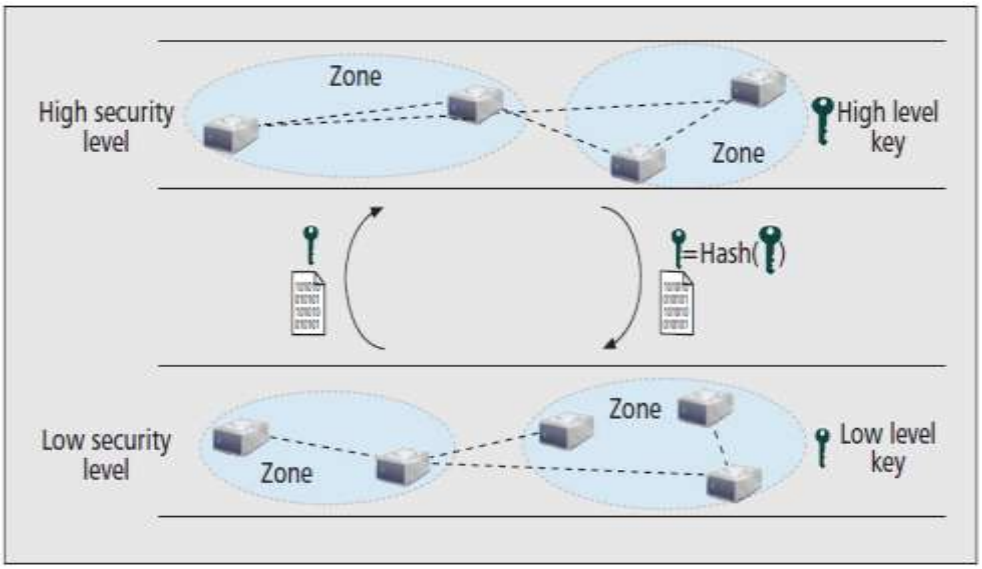

Fig: 2. Security *levels and key sharing.*

However, this isn't sufficient if at all the physical communication medium is easily available for tampering. If such risks exists the attacker could have access to the key associated lower most hierarchy by listening to key exchange once communication medium is hacked. The attacker would thereby have access to all information available in systems lower in hierarchy than the system whose key has been hacked. A Time Based Token Generation system is proposed to handle this issue.

IV. TIME BASED TOKEN MECHANISM FOR MESSAGE SECURITY

The idea is to have a function **g (x, t)** where,

x - Security key of devicehaving lower security level among communicating devices
t - Parameters of date and time of the critical infrastructure
g(x,t) - function which generates a string of alpha numeric characters by taking 'x' & 't' as its parameters

The g (x,t) should also have pre-image resistance property similar to iterative mechanism used in this context to prevent disclosure of original key 'x' in any case.

In any case of attack, the attacker would be left with a token which would change the very next minute of disclosure and would him clueless of the original authentication key.

This would serve as a solution especially in case of wireless networks in which all devices suffer from the same level of physical threat.

To avoid issues regarding date & time synchronization, a central time zone could consider for all zones pertaining to the critical infrastructure.

V.CONCLUSIONS

This paper addresses a key issue of message security in case of distributed critical infrastructure by means of including a time based token generation mechanism.

This mechanism provides required security in spite of having security issues in physical space.

However, insider threat is still beyond the reach of this paper. Only clever monitoring of working environment and scrutinization of working employees might reduce the risk involving the same.

References

[1] Huayang Cao, Peidong Zhu, and Xicheng Lu, "A Layered Encryption Mechanism for Networked Critical Infrastructures", Network IEEE, vol. 27, issue 1.
[2] L. Lamport, "Password Authentication with Insecure Communication," Commun. ACM, vol. 24, no. 11, 1981, pp. 770–72.
[3] Information Assurance Technical Framework (IATF) Release 3.0, National Security Agency, 2000; http://www.dtic.mil/dtic/tr/fulltext/u2/a393328.pdf.
[4] CryptlibEncryption Toolkit; http://www.cs.auckland.ac.nz/~pgut001/ cryptlib/.
[5] Challenging Issues and Limitations of Mobile Computing: Deepak G et al,Int.J.ComputerTechology&Applications,Vol 3 (1),177-181
[6] White Paper. *Mobile Cloud Computing Solution Brief*.AEPONA, 2010.
[7] Christensen JH. Using RESTful web-services and cloud computing to create next generation mobile applications, In *Proceedings of the 24th ACM SIGPLANconference companion on Object orientedprogramming systems languages and applications(OOPSLA)*, 2009; 627–634.
[8] Liu L, Moulic R, Shea D. Cloud service portal for mobile device management, In *Proceedings of IEEE7th International Conference on e-Business Engineering(ICEBE)*, 2011; 474.
[9] A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches Hoang T. Dinh, Chonho Lee, DusitNiyato, and Ping Wang