International Journal in Management and Social Science
Volume 09 Issue 11, November 2021 ISSN: 2321-1784 Impact Factor: 7.088
Journal Homepage: http://ijmr.net.in, Email: irjmss@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal

INSPECTING KEY MANAGEMENT FOR DIFFERENT SCHEMES IN CYBER SECURITY: NETWORKS&CHALLENGES

ARUN GUPTA
RESEARCH SCHOLAR, SUNRISE UNIVERSITY, ALWAR

DR. SUMIT BHATTACHARJEE
ASSOCIATE PROFESSOR, SUNRISE UNIVERSITY, ALWAR

ABSTRACT

Key technological advances in wireless communications, Micro Electro Mechanical Systems (MEMS), and digital circuitry have energized the research community to focus on the challenges of wireless sensor networks. In this paper, we propose a new pre-distribution key management scheme that meets the operational and security requirements of wireless sensor networks and provide authentication and key distribution in one set of protocols. Our scheme allows selective key revocation and node re-keying and posits improved network resiliency over existing key pre-distribution schemes. Cybersecurity is important for information dissemination, privacy and the human life. Managing cybersecurity related issues (such as banking hacks or phishing scams) during development, operation, and maintenance of cybersecurity models is a challenging task. Nearly no guidance is available on how to select, adapt, combine, and evolve cybersecurity models. This problem is due to the nature of cybersecurity models that are highly context-dependent. Therefore, cybersecurity models need tobe adaptableand in accordance with the respective project goals.

Keywords: -Cyber Security, Scheme, Network, Key,Wireless Sensor Networks

I. INTRODUCTION

wireless sensor networks have emerged as an innovative class of networked embedded systems due to the union of ever smaller, less costly embedded processors and wireless interfaces with micro-sensors based on micro-mechanical systems (MEMS) technology (Peters, Smith, Medeiros, and Rohrer, 2001). Wireless sensor networks are composed of small autonomous devices, or sensor nodes, that are networked together.

Each node is equipped with one or more sensors, storage and processing resources, and communication and instrumentation subsystems. The sensors observe phenomena; each sensor is specialized to monitor a specific environmental parameter such as thermal, optic, acoustic, seismic, or acceleration (Meguerdichian, Koushanfar, Potkonjak, and Srivastava, 2001). Sensor nodes typically perform their tasks unattended, often in remote locations. They may be deployed either inside, or nearby, target phenomenon to be studied.

Wireless sensor networks have emerged as an innovative class of networked embedded systems due to the union of ever smaller, less costly embedded processors and wireless interfaces with micro-sensors based

on micro-mechanical systems (MEMS) technology (Peters, Smith, Medeiros, and Rohrer, 2001). Wireless sensor networks are composed of small autonomous devices, or sensor nodes, that are networked together. Each node is equipped with one or more sensors, storage and processing resources, and communication and instrumentation subsystems. The sensors observe phenomena; each sensor is specialized to monitor a specific environmental parameter such as thermal, optic, acoustic, seismic, or acceleration (Meguerdichian, Koushanfar, Potkonjak, and Srivastava, 2001). Sensor nodes typically perform their tasks unattended, often in remote locations. They may be deployed either inside, or nearby, target phenomenon to be studied.

Typical sensor networks will support a variety of military, medical, environmental, and commercial applications. Remote sensors could reduce confusion within combat zones by collecting information about battlefield conditions. Sensor networks are currently being used for condition-based maintenance of complex equipment in factories. Natural environments (i.e., remote ecosystems, endangered species, disaster sites, forest fires.)

Typical sensor networks will support a variety of military, medical, environmental, and commercial applications. Remote sensors could reduce confusion within combat zones by collecting information about battlefield conditions. Sensor networks are currently being used for condition-based maintenance of complex equipment in factories. Natural environments (i.e., remote ecosystems, endangered species, disaster sites, forest fires.)

II. CYBER SECURITY NETWORK

In group communication, there is a need of distribution of common key to each member of the group securely and efficiently. To distribute the group key securely and efficiently, two group key management schemes have been proposed in this chapter.

In this chapter, various group key management schemes have been analysed with respect to their applications in field of cyber security. In group communication, the major challenges are higher rekeying cost, higher storage cost, higher computational load at central server, dynamicity of the group and perfect secrecy of the group.

Considering the limitations of the existing schemes, an ECC based group key management scheme with lowest storage cost is proposed, the computational load of central server is shared by the existing members of the network, communication cost is lower and cryptographic security is higher in comparison to existing cryptographic systems.

III. KEY MANAGEMENT

There are various proposed schemes for key management in the multicast groups from the simple minimal key storage scheme to the complex hybrid tree key distribution scheme, with their own advantages and disadvantages.

- **Minimal Key Storage Scheme**

The minimal key storage scheme is a very trivial scheme where each member Mi is allocated a unique KEK Ki where I is the member index. In this scheme each member of the multicast group has to stores two keys, itsKEK and the common SEK. When there is a change in membership in the group, GC has to encrypt the new SEKindividually with Ki's of the remaining N−1 members.Therefore, the communication overhead for updating themembers with the new key is O(N). To minimize the GCstorage, a pseudo-random function gr is used with a ran-dom seed ras an index to generate the key Kias Ki=gr(i). The GC has to store only two keys, the SEK andthe random seed r. Thus this method has constant key storage..

- **Logical Key Hierarchy**

An improved scheme for key management is the logical key hierarchy in which a logical tree of KEK's is constructed for a given group. In the tree, each leaf node is assigned a member, thus fixing the number of leaves to be the group size N. Every node of the tree is assigned a KEK. A member at a leaf node is assigned the set of keys that form the path from the root node. For example, member M1 is assigned the KEKs {K0, K11, K21, and K31}. Thus the member storage required is the height of the tree and the overhead is O(log N). Since a member shares the root key and all the intermediate KEKs with other users, all the keys possessed by the member except the one at the leaf node have to be updated when the member leaves the group. For example, when member M1 leaves the group, the keys K0, K11, K21 have to be updated.

The number of key update messages required is of the order of O(log N). But for this hierarchy, the GC has to store all the keys in the tree and hence the key storage overhead is of the order of O(N).

- **Hybrid Tree Distribution**

A better scheme for key management is the hybrid tree distribution. The minimal key storage scheme has constant key storage but communication overhead is O(N).

The logical tree structure has communication overhead as O(log N) but has storage overhead as O(N). The hybrid tree structure takes advantage of both the schemes.

In this scheme the entire members of the group are divided into clusters of size M with every cluster allocated to a single leaf node. Then there will be N/M clusters and also N/M leaves, we need to build a tree of depth logd (N/M), where d is the degree of the given tree. To illustrate the scheme let us consider, a group of 24 members.

These members are clubbed to form clusters of size M = 3. In this scheme the user storage is of the order of O(log(N/M)). The key update overhead is of the order of O(M + log(N/M)). So as long as M is not too large, the key update overhead is not severe. Thus the hybrid structure takes advantage of both the models and hence an efficient model for key management.

- **Secure Lock Using Chinese Remainder Theorem**

In this scheme, a secure lock is constructed using Chinese Remainder Theorem (CRT). The secure lock is used to lock the deciphering group session key. The single lock is transmitted with each encrypted message. Only users in the secure group can "unlock" the session key.

The principle behind the secure lock lies in the mathematics of the CRT. The CRT states that for N1, N2, . . ., Nn positive, relatively prime integers and R1, R2, . . ., Rn positive integers, a set of congruous equations $X \equiv R1 \bmod Ni$, $X \equiv R2 \bmod N2$, $X \equiv Rn \bmod Nn$ have a common solution X in the range of $[1, L - 1]$ where $L = N1 * N2 * N3 * \ldots Nn$ and n is the number of participants in the group.

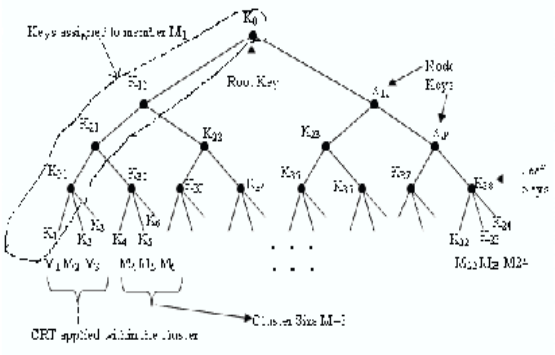

Fig 1. Proposed scheme for key management

IV. PROPOSED CYBERSECURITY CLASSIFICATION SCHEME

To the best of our knowledge, there are no specific guidelines of the best aspects of cybersecurity models. cybersecurity goes beyond the boundaries of traditional information security to include the person him/herself . The reference defined 100 requirements when considering end-to-end cybersecurity models. They discussed several questions to design a strong cybersecurity program that includes, among others; strategy, governance and control, standards and processes, laws and regulations, human resources and research and development. Recently, the reference identifies different angles on which to see cybersecurity; technical and conceptual issues , cyberspace as a domain of content, and even the cybersecurity context.

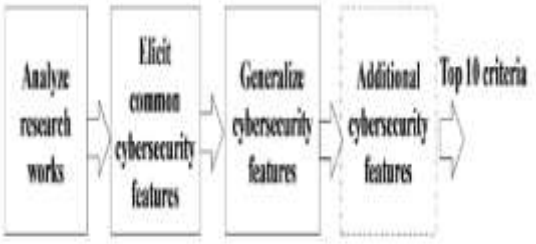

Fig 2. Proposed Classification Scheme

Figure 2shows the proposedclassification scheme. First, we studieda large set of cybersecurity models. Then, we elicit common cybersecurity features among studied works. Next, we generalize features such that more abstract features cover the low level features (e.g. confidentiality covers encryption techniques features, etc.). After that, we added other features that could be added to enhance our classification scheme in regard to cybersecurity models research gaps. Finally, our rules (constraints) converts features to a list of criterion. Therefore, wedevise the top 10 criterion basedon studied works and proposed by this work.

- **Basic security principles:** cybersecurity model should support the heart of information security; confidentiality, integrity, and availability.

- **Defense depth:** information security must protect information throughout the life span of the information, from the initial creation of the information on through to the final disposal of the information.

- **Defense strategy:** proactive models should take proactive decisions in regard to possible incidents such as legislation and proper guidelines and recovery plans. Preventive models trigger prevention actions one a threat is detected.

- **Compliance:** A compliance model follows a security standard or a best practice in a cybersecurity domain. Thus, allowing the cybersecurity model to make portable changes between securities related standards or cybersecurity models.

- **Information classification:** an important aspectof informationsecurity and the risk management is recognizing the value of information and defining appropriate procedures and protection requirements for the information.

- **Performance measurement:**the ability to measure performance of security initiatives effectively at various organizational levels. It also should audit whether the security policy and strategies are being effectively implemented.

- **Cybersecurity implementation level:** the level which security measures are being measured; the enterprise, national, or international level. The reference indicated that security should be placed in a holistic setting. The reference pointed out that cybersecurity requires a holistic approach. The references, showed that holistic approaches must be considered to cover various aspects of cybersecurity.

V. THE CHALLENGES OF COMPUTER SECURITY

Computer and network security is both fascinating and complex. Some of the reasons include:

- Security is not as simple as it might first appear to the novice. The requirements seem to be straightforward; indeed, most of the major requirements for security services can be given self-

explanatory, one-word labels: confidentiality, authentication, nonrepudiation, integrity. But the mechanisms used to meet those requirements can be quite complex, and understanding the m may involve rather subtle reasoning.

- In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features. In many cases, successful attacks are designed by looking at the problem in a completely different way, therefore exploiting an unexpected weakness in the mechanism.
- Having designed various security mechanisms, it is necessary to decide where to use them. This is true both in terms of physical placement (e.g., at what points in a network are certain security mechanisms needed) and in a logical sense [e.g., at what layer or layers of an architecture such as TCP/IP (Transmission Control Protocol/Internet Protocol) should mechanisms be placed].
- Security mechanisms typically involve more than a particular algorithm or protocol. They also require that participants be in possession of some secret information (e.g., an encryption key), which raises questions about the creation, distribution, and protection of that secret information.
- Computer and network security is essentially a battle of wits between a perpetrator who tries to find holes and the designer or administrator who tries to close them. The great advantage that the attacker has is that he or she need only find a single weakness, while the designer must find and eliminate all weaknesses to achieve perfect security.
- Security requires regular, even constant, monitoring, and this is difficult in today‟s short -term, overloaded environment.
- Security is still too often an afterthought to be incorporated into a system after the design is complete rather than being an integral part of the design process.
- Many users (and even security administrators) view strong security as an impediment to efficient and user-friendly operation of an information system or use of information.

VI. CONCLUSION

In group communication, there is a need of distribution of common key to each member of the group securely and efficiently. Various group key management schemes have been analysed and to optimize higher rekeying cost, higher storage cost, higher computational load at central server, secrecy of the group and dynamicity of group, two group key management schemes have been proposed. One of the proposed schemes is an ECC based group key management scheme in which the storage of each member is lowest, the computational load of central server is shared by the existing members of the network, communication cost is lower and cryptographic security is higher in comparison to existing cryptographic systems. The proposed scheme is compared with well-known existing group key management schemes and it has been found that computational overhead, storage cost, communication cost and rekeying cost are lower in the proposed scheme. The proposed scheme also achieves the forward secrecy and backward secrecy. The proposed scheme is dynamic in nature so, any set of members of the network can compute the group key efficiently. Another proposed scheme is based on the algebraic group theory. Security analysis of the second scheme has been done. It achieves the forward secrecy and backward secrecy of the data and it reduces the computational load of the server.

References:-

1. M. Carr, "Public–private partnerships in national cyber-security strategies," Int. Aff., vol. 92, no. 1, pp. 43–62, 2016.

2. Carnegie Mellon University, "Systems Security Engineering Capability Maturity (SSE-CMM®) Model Document Ver 3.0," 2010.

3. D. Henshel, M. G. Cains, B. Hoffman, and T. Kelley, "Trust as a Human Factor in Holistic Cyber Security Risk Assessment," Procedia Manuf., vol. 3, pp. 1117–1124, 2015.

4. L. Nnolim, "A framework and methodology for information security management," Lawrence Technological University, 2007.

5. Oracle®, "Information Security: A Conceptual Architecture Approach [White Paper]," 2011.

6. P. R. J. J. Trim and Y.-I. Lee, "A security framework for protecting business, government and society from cyber attacks," 2010 5th Int. Conf. Syst. Syst. Eng., pp. 1–6, Jun. 2010.

7. K. Fielden, "An Holistic View of Information Security : A Proposed Framework," Int. J., vol. 4, no. 1, pp. 427–434, 2011.

8. Atoum, A. A. Otoom, and A. Abu Ali, "A Holistic Cyber Security Implementation Framework," Int. J. Inf. Secur., vol. 22, no. 3, pp. 251–264, 2014.

9. H. Jo, S. Kim, and D. Won, "Advanced Information Security Management Evaluation System," KSII Trans. Internet Inf. Syst., vol. 5, no. 6, pp. 1192–1213, 2011.

10. M. Evans, L. A. Maglaras, Y. He, and H. Janicke, "Human Behaviour as an aspect of Cyber Security Assurance," CoRR, vol. abs/1601.0, 2016

11. A. Buecker, M. Borrett, C. Lorenz, and C. Powers, "Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security," IBM Redguides Bus. Leaders REDP-4528-01, vol. 4528, no. 1, 2010.