Encryption Method in Cryptographic KeyManagement Wireless Ad Hoc Networks

A. Ramesh Babu
Associate Professor , Joginpally Baskar Institute of Engg & Technology, Hyderabad.

Abstract--As distributed computing systems grow in size, complexity and variety of application, the problem of protecting sensitive data from unauthorized disclosure and tampering becomes increasingly important. Cryptographic techniques can play an important role in protecting communication links and file data, since access to data can be limited to those who hold the proper key. In the case of file data, however, the routine use of encryption facilities often places the organizational requirements of information security in opposition to those of information management. Since strong encryption implies that only the holders of the cryptographic key have access to the cleartext data, an organization may be denied the use of its own critical business records if the key used to encrypt these records becomes unavailable (e.g., through the accidental death of the key holder). This paper describes a system, based on cryptographic "smartcards," for the temporary "escrow" of file encryption keys for critical files in a cryptographic file system. Unlike conventional escrow schemes, this system is bilaterally auditable, in that the holder of an escrowed key can verify that, in fact, he or she holds the key to a particular directory and the owner of the key can verify, when the escrow period is ended, that the escrow agent has neither used the key nor can use it in the future. We describe a new algorithm, based on the DES cipher, for the online encryption of file data in a secure and efficient manner that is suitable for use in a smartcard.

Introduction

Mobile ad hoc networks are complex wireless networks, which have little or no existing network infrastructure. These networks can be established in a spontaneous manner allowing organizations and network members to work together and communicate, without a fixed communication structure. The mobility, spontaneity and ad hoc nature of these networks makes them optimal solutions for disaster area communication and tactical military networks. Due to recent wireless technology advances, mobile devices are equipped with sufficient resources to realize implementation of these dynamic communication networks. However, for ad hoc networks to find a wide spread within both the military and commercial world, they must be secured against malicious attackers. Mobile ad hoc networks have distinct characteristics, which make them very difficult to secure. Such characteristics include: the lack of network infrastructure; no pre-existing relationships; unreliable multi-hop communication channels; resource limitation; and node mobility. Users cannot rely on an outside central authority, like a trusted third party (TTP) or certificate authority (CA), to perform security and network tasks. The responsibility of networking and security is distributed among the network participants. Users have no prior relationship with each other and do not share a common encryption key. Therefore, only after the network has been formed, the users establish trust and networking links. The establishment of networking links is identified as being vulnerable to security attacks. Trust establishment should allow protection for the network layer and ensure that honest links are created. The sporadic connectivity of the wireless links, inherent to mobile ad hoc networks, results in frequent link breakages. These characteristics introduce unique challenges to trust establishment. Both the routing and trust establishment protocols must be designed to handle the unreliable wireless communication channels: the dynamic topology changes and the distributive nature. The security solutions used for conventional wired networks cannot simply be applied to mobile ad hoc networks. More complex network management must be implemented to achieve trust establishment in mobile ad hoc networks. Mobile Ad-Hoc Networks: Applications Ad hoc network security research initially focused on secure routing protocols. All routing schemes however, neglect the crucial task of secure key management and assume preexistence and pre-sharing of secret and/or private/public key pairs]. This left key management considerations in the ad hoc network security field as an open research area. Security solutions which use cryptographic techniques rely on proper key management to establish trust. This chapter together with the next chapter focus upon key management which aids these cryptographic solutions.

Ad hoc network challenges

An ad hoc network is a dynamic type of network which is both similar and very different to its parent fixed communication network. In the following we introduce the properties of an ad hoc network as a way of defining its shortcomings and to highlight its security challenges.

a. Dynamic Network Architecture

Ad hoc networks have no fixed or existing network infrastructure. The network architecture is continuously changing as the network evolves. There is no pre-existing or fixed architecture which handles all network tasks such as: routing security and network management. Instead, the network infrastructure is spontaneously set up in a distributive manner. Each participating node shares the network's responsibilities. Distribution of network functionality avoids single point attacks and allows for the network to survive under harsh network circumstances. A fixed entity structure, such as a base station or central administration, is crucial for security mechanisms. A trusted third party member, which is expected in traditional networks, is similar to a fixed

entity as both define security services; manage and distribute secret keying information (which allows secure communication of data through encryption and decryption techniques). Therefore the absence of such a control entity introduces new opportunities for security attacks on the network.

b. Self Organized Nature

Wireless ad hoc nodes cannot rely on an off-line trusted third party member. The security functions of the trusted third party member are distributed among the participating nodes. Each node takes responsibility for establishing and maintaining its own security and is, therefore, the centre of its own world and authority. A wireless ad hoc network is therefore referred to as a self organized network.

c. No Prior relationships

In ad hoc networks, nodes can have no prior relationships with other nodes within the network. Prior acquaintance between nodes can be considered as pre-trust relationships between nodes. However, the ad hoc nature of these networks does not allow for these assumptions, as it cannot be assumed that secrets exist between the respective pair of nodes . If nodes can join and leave the network at random without prior trust relationships with nodes, access control becomes a difficult task for the security mechanism.

d. Multi-hop communication channel

Wired networks include fixed nodes and fixed wired communication lines. Wireless ad hoc networks have mobile wireless nodes (often in the form of hand held devices) and, as suggested, their communication medium is wireless. This allows for greater network availability and easy network deployment. Each node's transmission range is limited and network communication is realized through multi-hop paths. Co-operation and trust along these paths is a crucial aspect of the security mechanism and ensures successful communication. The shared wireless communication medium means that any user can participate in the network. This creates access control problems for security mechanisms as adversaries are able eavesdrop on communication or launch active attacks to alter message data.

e. Mobility

Nodes are expected to be mobile within an ad hoc network, creating a dynamic and unpredictable network environment. In certain situations the nodes' mobility is not totally unsystematic and assumptions can be made in the form of mobility patterns. An example of these patterns is evident in a vehicular ad hoc network where vehicles move along fixed paths, or roads, at speeds which have a high probability of being within the local speed limit. However, nodes demonstrate random mobility within these predictions. Connectivity between nodes is sporadic. This is due to the shared, error-prone wireless medium and frequent route failures which caused by the unpredictable mobility of nodes. Increased mobility can result in the multi-hop communication paths being broken and network services becoming unavailable. Security mechanisms must account for the weak connectivity and unavailability. Furthermore, due to mobility and sporadic connectivity, these mechanisms must also aim to be scalable with the changing network density.

Security objectives and services

Securing mobile ad hoc networks requires certain services to be met. A security service is a made available by a protocol which ensures sufficient security for the system or the data transferred. The security objectives for mobile ad hoc networks are similar to that of fixed wired networks. The security objects are described in six categories, adapted from discussions in:

- Authentication
- Access Control
- Data Confidentiality
- Data Integrity
- Non-repudiation
- Availability Services

Attacks

Threats or attacks upon the network come from entities. They are known as adversaries. Mobile ad hoc networks inherit all the threats of wired and wireless networks. With these networks' unique characteristics, new security threats are also introduced. Before the development of security protocols, it is essential to study the attacks associated with these unique networks.

a. Attack characteristics

Attacks will be launched against either the vulnerable characteristics of a mobile ad hoc network or against its security mechanisms. Attacks against the security mechanism in all types of networks, including mobile ad hoc networks, include authentication and secret key sabotage. Mobile ad hoc networks have distinctive characteristics, as identified in Section. Attackers are expected to target these points of vulnerability, for example the multi-hop nature of communication routes. The attacks are classified by their different characters. The attacks, accordingly, are classified as follows:

Passive and Active Attacks

Security attacks can be classified by the terms active and passive [Stalling, 2002]. Passive attacks attempt to steal information from the network without altering the system resources. Examples of passive attacks include, eavesdropping attacks and traffic analysis attacks. It is difficult to detect passive attacks as they leave no traceable affect upon the system resources or network functionality. Although the results or the need for securing against these attacks may not be monitored or visibly present, it is still a priority to protect networks from these seemingly harmless attacks, particularly in a military context. Concerning this point, Bruce mentioned: "*If security is too successful, or perfect then the security expenditures are seen as wasteful because success is too invisible*". However, Schneier assures one that, despite the lack of visible results, the need to secure information still exists. Active attacks attempt to modify system resources or network functionality. Examples of these attacks are message modification, message replay, impersonation and denial of service attacks.

Insider and Outsider Attacks

Malicious nodes are not authorized participants in the network, which launch outsider attacks. Impersonation, packet insertion, and denial of service are some

examples of outsider attacks. In contrast to outsider attackers, inside attackers are more difficult to defend against. Inside attacks are launched from nodes which are authorized participants in them network. Insider attacks are common in pure mobile ad hoc network, where any user can freely join or exit. Security mechanism become vulnerable when participates are malicious and the confidentiality of keying information can be compromised. Thus, an advantage of the non-repudiation and authentication techniques, malicious insider nodes can be identified and excluded.

Layer Attacks

There are threats at each layer of the mobile ad hoc network communication protocol. The physical layer is vulnerable to passive and active attacks. The attacks found at the physical layer are as follows: eavesdropping; denial of service; and physical hardware alterations. Encrypting the communication links and using tamper-resistant hardware helps to protect the physical layer. However, at the data link layer adversaries can flood the communication links with unnecessary data to deplete network resources. Security mechanisms that provide authentication and non-repudiation can prevent this, as they allow invalid packets transfers to be identified. At the application layer messages are exchanged in an end-to-end manner using wireless multi-hop routes established by the network layer. The wireless multi-hop routes are invisible to the application layer. Conventional security techniques used for wired networks can be used to prevent expected attacks upon the application layer. The application layer is dependent upon the network layer to provide secure routes between the two communicating parties. The network layer provides a critical service to the mobile ad hoc network, and the routing protocol. In the context of trust and security, the provision of secure routes is one of the most vital elements for trust establishment.

File Encryption Scheme

One of the lessons learned from the design of CFS is that the problem of encrypting files on-line in a file system is somewhat different from other kinds of encryption problems. No single standard encryption mode[7] has all the properties required for file system use; further compounding the problem are concerns $f(n)$, $g(n)$ are publically known functions that map an integer representation n into unique bit strings of the DES codebook size (64 bits). m is the length of the precomputed stored stream (presently 256K bytes). Observe that the stream ciphers defined by $DES1(K1, f(p \bmod m))$ and $DES1(K1, g(p \bmod m))$ can be precomputed for each $K1$ given $2m$ bytes of storage. The CFS daemon precomputes these streams when the cattach command is issued for a particular key. With the streams precomputed, each block encryption requires only one online DES operation (the codebook cipher based on $K2$). When decryption is performed on the card, the streams cannot be wholely precomputed in the card's small local memory. Instead, the card calculates $DES1(K1, f(p \bmod m))$ and $DES1(K1, g(p \bmod m))$ for each cipherblock sent to it. ($f(p \bmod m)$ and $g(p \bmod m)$ are sent to the card from the host computer as parameters with the cipher block.) Although this is computationally slower than the pre-computed cipher, requiring three DES encryptions per block instead of one, bandwidth to the card interface (aserial link) remains the primary limitation on encryption speed.

Performance Evaluation

In order to measure the efficiency of our proposed scheme, we compare our scheme with SMOCK. We focus on the evaluation of key storage space and time consumption of key establishment.

Key storage space

Key storage space measures the total number of keys (or key seeds) distributed in the network. In our proposed CBKM, every member node only needs to store a key seed. Each cluster head has an authentication key, a pair of public/private key, a certificate, a deviation angle t, and a key seeds table. Other shared session keys are established on demand. Assume there are N nodes and H clusters in our test scene. The total key storage space is:

$N_{total} = N_{mn} + N_{ch}$

$= (N-H)+5H+(N-H)$

$=2N+3H$

where NMN is the total number of keys stored in the member nodes, and NCH is the total number of keys stored in the cluster heads. In our proposed scheme, the total number of cluster heads is 10% of the network. In SMOCK, each node is distributed with $(a + b)$ keys. a is the total number of public keys in the network, and b is the number of private keys held by each node. The total number of distributed keys in a network with N nodes is $N(a + b)$. we plot the total storage requirements for different sizes of ad hoc networks. The x-axis is the total number of mobile nodes in the network, and N varies from 100 to 1000. The y-axis represents the total number of distributed keys (or key seeds) in the network. we can find that the proposed CBKM scheme saves much key storage space

Conclusions

Key escrow is not appropriate for all file encryption applications. Some data are simply too private; personal diaries, certain individual medical and financial records and other data for which there is no motivation for the data owner to allow third party access are poor candidates for escrow. Other data, such as dayto-day operational business records, have such high availability requirements to preclude any encryption at all. Escrow serves the "middle ground" for which security requirements suggest the need for cryptographic protection while availability requirements dictate the need for access. File encryption overcomes the major shortcomings of software-based and manual escrow systems. Unlike manual systems, the escrowed keys can be reliably pre-audited to ensure their validity without compromising sensitive data. And unlike either system, once the card is returned, the owner is assured of whether the escrow process was used and that no further decryptions can occur. Escrowed decryption is completely under the control of the card past possession of the card conveys no future privileges.

References

[1] Denning, D. E., "Encryption and Law Enforcement." *Georgetown University, Computer Science Dept.,* Feb. 21, 1994, available by anonymous ftp from cpsr.org.

[2] Diffie, W. and Hellman, M. E., "New Directions in Cryptography." *IEEE Trans. on Information Theory*, IT-11:644 654, November 1976.

[3] Lacy, J., Mitchell, D. and Schell, W., "CryptoLib: Cryptography in Software." *Proc. Fourth USENIX Security Workshop,* October 1993.

[4] Ioannidis, J. and Blaze, M., "Architecture and Implementation of Network-Layer Security Under Unix." *Proc. Fourth USENIX Security Workshop,* October 1993.

[5] National Bureau of Standards, "Data Encryption Standard." *FIPS Publication #46*, NTIS, April 1977.

[6] A. Baggio, "Wireless sensor networks in precision agriculture", in ACM Workshop on Real-World Wireless Sensor Networks (REALWSN 2005), Stockholm, Sweden, June 2005.

[7] A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler, J. Anderson, "Wireless Sensor Networks for Habitat Monitoring", in First ACM Workshop on Wireless Sensor Networks and Applications, Atlanta, GA, USA, September 2002.

[8] G. Fuchs, S. Truchat, F. Dressler, "Distributed Software Management in Sensor Networks using Profiling Techniques", in 1st IEEE/ACM International Conference on Communication System Software and Middleware (IEEE COMSWARE 2006): 1st International Workshop on Software for Sensor Networks (SensorWare 2006), New Dehli, India, January 2006.