Abstract

Recently, identity-based cryptography (IBC) schemes are considered as a tool to secure ad hoc networks. In this work we focus on the role of the Trust Authority (TA) as a key escrow, a property that is inherent to all IBC schemes. We explore the special role of key escrow in ad hoc networks and show that this role significantly differs from key escrows in other networks. We introduce a series of adversary models for dishonest TAs in ad hoc networks, including a new model where a TA uses spy nodes that record communications in the network and report them to the TA. Our analytical results show that in many ad hoc network applications the TA can be prevented from being a key escrow.

1. Introduction

Implementing security in ad hoc networks is a very difficult task. One major challenge is the key management in the absence of an on-line Trusted Third Party (TTP), such as a Certification Authority (CA) in public key infrastructures (PKIs). Recently, researchers have drawn their attention to implementing identity-based crypto (IBC) schemes in ad hoc networks to address this problem, e.g. [4]. In IBC schemes unique humanreadable identities are used either directly as public keys [5] or to derive public keys [1]. Consequently, the public keys in IBC schemes are self-authenticating and thus do not require public key certificates. IBC schemes have a low overhead because parties do not need to exchange any key material prior securely communicating with each other. However, IBC schemes require a Trust Authority (TA) to bootstrap all nodes with their secret keys. Consequently, the TA is a key escrow in all IBC schemes. This might be a desirable feature in some cases such as governmental and military applications. However, we treat this property as a drawback of IBC schemes throughout this paper, because it might be a disadvantage in civil applications.

In this paper we analyze the special role of a TA as key escrow in the context of ad hoc networks, i.e. we take the special properties of ad hoc networks and their devices into account. Ad hoc networks are dynamic networks in which mobile nodes communicate over wireless links of limited transmission range. The communication range is usually increased by using multi-hop communication protocols. For our analysis we introduce three adversary models that cope with these special properties. We consider dishonest TAs that abuse their power as key escrow to launch attacks in the defined adversary models. We show that attacks are only feasible if certain restrictive assumptions hold.

The problem of key escrow in IBC schemes has been known since the introduction of those schemes and has been studied for static networks with an infrastructure and wired communication channels for several years. Preventing passive attacks by using a Diffie-Hellman-like (DH-like) key agreement is shown for honest-but-curious TAs in [2]. However, no countermeasures are known to prevent active attacks by dishonest TAs. Many methods have been proposed to limit the power of a TA. The most obvious method is to assign an expiry date to the system’s master secret key. However, this does not prevent dishonest TAs from launching attacks. Another method, proposed in [3], suggests encrypting all messages using additional private/public key pairs which are not known to the TA. However, this scheme is no longer an IBC scheme because public keys cannot be derived from identities, the main advantage of IBC schemes. Another approach of limiting the power of a TA is to distribute the master key to n TAs by implementing a (k, n) threshold scheme [1]. This method is considered for an
implementation in ad hoc networks in [4] and can be used as an additional countermeasure in our adversary models.

2. Adversary models for dishonest TAs

As the name implies, we usually trust a trusted third party. However, most users do not want that this TTP is able to listen to all their communications and they consider it as a drawback of a scheme if the TTP is a key escrow. In this section we introduce adversary models for dishonest TAs in IBC schemes in ad hoc networks that abuse their power as a key escrow to launch attacks on the users privacy. We give a more detailed discussion of the models and analysis of the attacks in the full paper including an analysis of passive attacks by honest-but-curious TAs. However, here we focus on active attacks by dishonest TAs that do not only eavesdrop on communications but also intercept, create, modify and re-direct messages. While eavesdropping is easy to do in a wireless network, preventing a broadcasted message from propagating through the network is relatively hard to achieve. In order to intercept messages the TA needs the ability to jam signals in a controlled manner without arousing suspicion of the neighboring (affected) nodes. However, we assume that the TA has all those capabilities in all our adversary models. A TA can use its described powers to masquerade as any party in the network. We would like to point out the power of such an active attack, because the TA has knowledge of all the key material of all users in the network. An example of such an active attack is a TA-in-the-middle-attack. Two parties $A$ and $B$ can be perfectly fooled by a dishonest TA and the attack cannot be detected. Note that the described attack also works in PKIs in which a CA issues false certificates. However, the attack in PKIs is detectable if a user notices that more than one valid certificates are issued for the same identity and public key.

Taking the limited transmission range of nodes into account we derive three adversary models for dishonest TAs. Here we focus on multi-hop communications between two parties $A$ and $B$, whereas the full paper also discusses the special one-hop case. The first two models can be derived intuitively for ad hoc networks. In Model I the TA is entirely out of communication range, i.e. outside the communication range of $A$, $B$ and all intermediate nodes $n$ on the routing path. In Model II the TA is either in direct communication range of $A$ or $B$ or any other node $n$ on the routing path. In Model III we introduce a new concept in which a TA uses spy nodes to increase its own communication range, e.g. to eavesdrop on communications outside its own range. These spy nodes record all communications in their communication range and send the recorded data back to the TA. They are also able to play back messages into the network that they received from the TA. Spy nodes use multi-hop routes to communicate with the TA where routing paths can consist of spy and regular network nodes. The spy nodes act and appear as regular network nodes and cannot be distinguished from such by the network nodes themselves. Spy nodes have the same power as regular nodes and do not possess the master key of the TA. They cannot intercept messages because this would require jamming or similar capabilities which is beyond their ability.

3. Analysis of attacks

In our analysis we only consider Model II and III because the TA or at least one of its spy nodes need to be in communication range in order to launch an attack.

3.1. Likelihood of successful attacks

In Model II a dishonest TA can launch an attack if the following condition holds.

**Condition 1:** The TA is in communication range of at least two nodes $n_i$ and $n_j$ on the routing path.

Note that the nodes $n_i$ and $n_j$ can include one or both of the endpoints $A$ and $B$. If Condition 1 holds, the TA can intercept all messages exchanged between $n_i$ and $n_j$. The TA then modifies the intercepted messages and plays them back into the routing path. The nodes $n_i$ and $n_j$ are both not aware of the attack, because the TA can simply masquerade as the respective neighboring node $n_i$ or $n_j$ or any other network node.

**Probability of successful attack:** In order for an attack to be successful, Condition 1 needs to hold for each protocol flow. However, due to the dynamics of ad hoc networks packets of different flows might not take the same route. Hence, the probability of a successful attack $P_{\text{suc}}$ depends on the number of protocol rounds $r$ and the probability $P_{N_f}(i)$ that the TA is in range of at least two nodes in each round $i$, i.e. $P_{\text{suc}} = \prod_{i=1}^{r} (P_{N_f}(i))$. To derive $P_{\text{suc}}$ we first need to calculate $P_{N_f}$. Let's say we have a total of $N$ nodes in the network, with $N_f$ nodes inside the TA's communication range and $N_O$ nodes outside. The probability of having at least two nodes in $N_f$ as part of the routing path cannot be easily derived, because $N_f$ and $N_O$ are not uniformly distributed in the network. However, we believe that the probability of having a node from $N_f$ on the path is much smaller than a node from $N_O$. This is true for most ad hoc network applications, e.g. in a battlefield where the TA remains.
in a safe place, whereas the nodes are placed far away in the enemy territory. Same is true in civil and other applications, just compare the situation to PKI schemes, where users are not necessarily roaming close to the CA that issued their certificates.

In Model III an active attack similar to the one described for Model II is feasible under the following two conditions.

Condition 2: At least one spy node \( s \) is a part of the routing path.

Condition 3: The spy node \( s \) and the TA are able to communicate on-line.

The active attack in this model can be seen as spy-in-the-middle-attack. The attack only works in the multi-hop case, because a spy \( s \) needs to be on the routing path, i.e. somewhere in the middle of \( A \) and \( B \), in order to relay the messages to the TA. The TA modifies the messages it receives from \( s \) (decrypting them first if necessary) and sends them back to the spy node which forwards the modified messages to the next node on the routing path.

Probability of successful attack: The communication between TA and its spy nodes needs to be very fast in order for this attack to work. Otherwise the delay would cause the communicating nodes to choose another routing path. Now we assume Condition 3 holds, i.e. in order to calculate the probability of a successful attack we need to determine the probability \( P_S \) that at least one spy node is part of the multi-hop communication path. We assume that spy nodes \( s \) and networks nodes \( n \) are uniformly distributed in the network. Let’s say we have \( N \) regular network nodes and \( S \) spy nodes in our network. The routing path length \( d \) excludes the nodes \( A \) and \( B \). The probability \( P_S \) of the event that we take \( d \) nodes out of the total set of all nodes, i.e. \( N + S \), in which at least one node is a spy node is given by \( P_S = 1 - \left( \frac{N}{N+S} \right)^d \). As in Model II the conditions for a successful attack must hold in each protocol flow and the overall probability can be computed similar to \( P_S \) in Model II. Hence, the probability \( P_{suc} \) depends on \( P_S \) in each round and thus on the path length \( d_i \) in each round \( i \). We can observe that by increasing the number of spy nodes \( S \) in the network the TA increases the probability of a successful attack, whereas decreasing the length \( d \) of the path decreases the chance. Note that the length \( d \) depends on many factors such as the network topology, the mobility pattern of the nodes and the implemented routing protocol. In the full paper we compute \( P_S \) and \( P_{suc} \) for a specific routing protocol and network settings.

3.2. Countermeasures

As a countermeasure for attacks in Model II in which a TA is able to modify messages but cannot stop the original messages from propagating, we suggest aborting the protocols if a node receives messages of different contents that belong to the same protocol flow.

We can observe for Models II and III that the shorter the routing path the less likely a successful attack. For this reason, we suggest that two nodes should establish a new shared key as soon as they are close to each other. Note that in Model III one-hop communication can totally eliminate the possibility of an active attack. Furthermore, we suggest using a different routing path for each packet. For example, the network nodes can use their mobility to enable the use of different routing paths for different protocol flows. In this way the overall probability of an successful attack can be significantly reduced. Note that if the TA or the spy nodes are outside the range in only one of the \( r \) rounds, the attack fails.

4. Conclusions

We conclude that the special properties of ad hoc networks combined with the presented countermeasures prevent a TA from being a key escrow in most ad hoc network applications. We plan to further investigate our third adversary model and explore more applications of this model.

References