COMPUTERS & SECURITY 60 (2016) 15–36

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Revocation and update of trust in autonomous delay tolerant networks

C.I. Djamaludin *, E. Foo, S. Camtepe, P. Corke

School of Electrical Engineering and Computer Science, Queensland University of Technology, 2 George Street, Brisbane, Australia, 4000

ARTICLE INFO

Article history:
Received 24 August 2015
Received in revised form 23 December 2015
Accepted 28 March 2016
Available online 1 April 2016

Keywords:
Delay tolerant network
Autonomous
Key management
Key revocation
Trust
Reputation

ABSTRACT

A Delay Tolerant Network (DTN) is a dynamic, fragmented, and ephemeral network formed by a large number of highly mobile nodes. DTNs are ephemeral networks with highly mobile autonomous nodes. This requires distributed and self-organised approaches to trust management. Revocation and replacement of security credentials under adversarial influence by preserving the trust on the entity is still an open problem. Existing methods are mostly limited to detection and removal of malicious nodes. This paper makes use of the mobility property to provide a distributed, self-organising, and scalable revocation and replacement scheme. The proposed scheme effectively utilises the Leverage of Common Friends (LCF) trust system concepts to revoke compromised security credentials, replace them with new ones, whilst preserving the trust on them. The level of achieved entity confidence is thereby preserved. Security and performance of the proposed scheme is evaluated using an experimental data set in comparison with other schemes based around the LCF concept. Our extensive experimental results show that the proposed scheme distributes replacement credentials up to 35% faster and spreads spoofed credentials of strong collaborating adversaries up to 50% slower without causing any significant increase on the communication and storage overheads, when compared to other LCF based schemes.

1. Introduction

In comparison to conventional networks, delay-tolerant Mobile Ad-Hoc Networks (MANETs) (Lu et al., 2014) are highly disconnected, dynamic, and distributed networks that create opportunistic ephemeral connections between nodes that can span large geographic areas such as Vehicle AdHoc Networks (VANETs). There is no guarantee that a reliable source to destination path can be maintained for long periods of time. This means information transfer between mobile nodes is in the form of data bundles, as a store and forward scheme (Guo et al., 2010) relayed through multiple intermediary autonomous nodes or through multiple paths. Hence, DTN applications and protocols have to be designed as delay invariant. While key and trust management form the foundation for most security mechanisms such as entity authentication and confidentiality, any key and trust management solutions designed for conventional networks with infrastructure components are unsuitable for DTNs (Fall, 2003; Galati, 2010). Therefore, new decentralised approaches to trust and key management are required for secure DTNs operating under adversarial conditions.

The use of up-to-date keys in a DTN is integral to the security of the nodes and the network. Hence, during the key management life cycle (pre-deployment, initial bootstrapping, operation, and revocation Moore et al. (2007), nodes may

* *Corresponding author.* Tel.: +61 7 3138 9512
E-mail addresses: chris.djamaludin@student.qut.edu.au (C.I. Djamaludin), e.foo@qut.edu.au (E. Foo), seyit.camtepe@qut.edu.au (S. Camtepe), peter.corke@qut.edu.au (P. Corke).
http://dx.doi.org/10.1016/j.cose.2016.03.008
0167-4048/

be required to revoke and update their keys Raya et al. (2006). A node may perform key revocation under two circumstances. The first is considered to be a *planned* revocation. This may be for reasons such as a limited time validity on the key, enforcement of security policies, or increasing key security. As a result, a new key pair is required to provide the confidentiality and authentication requirement in the DTN. This is possible under the assumption that the node still retains sole control of the old private key. However, there are instances where the private key may have been compromised, with the node no longer retaining sole control and possession. This poses a major security vulnerability as the compromised private key allows any node to decrypt messages and impersonate another node. This is the second circumstance of key revocation, and is considered to be an *unplanned* key revocation event.

Key transition messages used in Pretty Good Privacy (PGP) (Ubuntu, 2015) provide a *planned* key revocation solution over conventional networks without centralised Public Key Infrastructure (PKI). The key transition message informs other users of the requirement that the old key is no longer being actively used, and that users should begin using the new key. Key identifiers such as fingerprints are included, and the message is signed by both the old and new private keys to signify control of both. The dual signature also acts as a transfer of trust between the old key to the new key, effectively transferring the web of trust. However, in an *unplanned* key revocation scenario, where a node is revoking the old key due to the potential compromise of the private key, a key transition message cannot be used. PGP requires users to generate a revocation certificate immediately after they generate their key pair whilst they still retain control of the private key (Zimmermann, 1995). However, the revocation certificate must also be secured against accidental or malicious disclosure by an adversary. There is also no trust transfer between the old key and new key when key revocation is required. Therefore, the question arises whether the trust associated with the old key can be transferred to the new key in an *unplanned* key revocation scenario for an autonomous DTN. Previous work in revocation for DTNs focus on node revocation, where a misbehaving node is removed from the network (Hoeper and Gong, 2009; Moore et al., 2007; Raya et al., 2008). Key revocation schemes that are presented are dependent on a centralised infrastructure such as Road Side Units (RSUs) in VANETs (Lin et al., 2008), along with Certicate Authorities (CAs) to handle the trust transference (Raya et al., 2006), and Certicate Revocation Lists (CRLs). Proposals that move away from a centralised scheme to a distributed scheme still rely on the CA as the most trusted party in the network, along with CRLs, which are difficult to scale (Kumar et al., 2014).

This paper presents a secure and fully distributed key revocation and update scheme for DTN nodes operating under adversarial conditions. The scheme assumes a DTN without a centralised PKI that ensures entity authentication. With the existence of malicious nodes performing Sybil/impersonation attacks, the scheme utilises the LCF trust system Djamaludin et al. (2013) concept of using social contacts to provide entity confidence and trust transference during an unplanned key revocation scenario. This is similar to the key transition message used in PGP, except for use where control of the private key is no longer with the key owner. The presented scheme is compared against a control scenario where old keys are revoked and the new replacement keys are distributed through normal key distribution methods of Djamaludin et al. (2013). Two variations of adversary nodes perform the Sybil or impersonation attacks: A single adversary where only one node is performing the Sybil attack and a multiplying adversary where more nodes become aware of the opportunity to perform the Sybil attack. The scheme is extensively simulated and evaluated over a long period of time and large geographic area using a random movement model. Several security evaluation metrics such as public key distribution of revoked keys, new public keys, and spoofed keys are measured. The certificate distribution metrics were also measured to determine the impact of certificates and their effect on public key distribution. The results show that the proposed scheme distributes replacement keys faster, whilst slowing the spread of spoofed keys of strong collaborating adversaries. These results are achieved without causing any significant increase on the communication and storage overheads.

Organisation of the paper is as follows. Related works on key revocation for DTNs is outlined in Section 2. Section 3 covers the system, threat and adversarial models as well as definitions of the common terminology and the security properties used throughout the paper. The new Distributed Signing (DS) key revocation and replacement scheme along with two other comparable LCF based key revocation schemes are outlined in Section 4. In Section 5, the experimental and simulation setup is explained in detail. Experiment results are discussed and compared with existing revocation schemes in Section 6. Finally, Section 7 concludes.

2. Related work

In this section, we cover the related prior works in two groups: Centralised schemes based on traditional PKI schemes utilising a CA, and decentralised schemes based on monitoring and reputation such as Identity Based Cryptography (IBC) and threshold cryptography based proposals. From these related works, we discuss the technical gaps presented, and the motivations.

2.1. *Centralised PKI schemes*

Many Wireless Sensor Network (WSN)/DTN/MANET/VANET key revocation schemes are based on traditional centralised PKI implementations (Misra et al., 2014; Raya et al., 2006, 2007, 2008). These key revocation schemes on the Internet rely heavily on CRLs (Solo et al., 2002). The CRL is a list that identifies a revoked certificate, which is signed by the CA and made available to nodes of a network from public distribution points (Gan et al., 2014).

Raya et al. (2006) proposed a CA based certificate revocation model for vehicular networks. They assume a VANET where a trusted third party manages the identities, credentials and cryptographic keys of the nodes. They also assume certificates are not valid for an unlimited duration, and the revocation should occur in a timely manner as to avoid exploitation by adversary nodes (Raya et al., 2006). The CA is responsible for revoking certificates and can do so through two methods. The