A Novel Framework for Security Enforcement in Networks for Disaster and Crisis Management

Vladimir Oleshchuk
Centre for Incident and Emergency Management (CIEM)
Department of ICT
University of Agder, N-4879 Grimstad, Norway
vladimir.oleshchuk@uia.no

ABSTRACT

The paper proposes a framework that provides security in networks deployed in disaster areas. Traditional networks are not well suitable to use in such setting due to many unusual constraints such as long delays, high packet drop rates, unavailability of central trusted entity etc. Under such constraints existing security protocols do not work. Proposed here approach provides solutions for some of these problems often listed as challenges in the literature. We consider delay-tolerant wireless networks as a most suitable for such setting, and propose a trust based approach that provides flexible and efficient solutions that can be used in disaster arears.

Keywords

Security, privacy, disruption-tolerant networks, subjective logic, attribute-based access control, web of trust

INTRODUCTION

Mobile devices (mobile phones, WI-FI capable devices) are playing an increasing important role in everyday life and becoming more and more ubiquitous. They provide personal connectivity all around the day and serving as primarily means for communication, information gathering and sharing. Large portion of such connectivity takes place via so called infrastructure-based wireless networks (Ma and Tsudik, 2010), where part of communication transits a fixed network infrastructure. However, in an area of disaster or crisis such a fixed network or at least part of it will not be available (for example, being physically destroyed etc.), resulting in disruption of connectivity of mobile devices.

Recent advances in technology propose several emerging network solutions that do not rely on any wired or fixed infrastructure, where nodes of the networks communicate either directly or via peers. In such networks, nodes are themselves responsible for network functionality like message forwarding, node authentication, (ad hoc) topology maintenance of etc. One of the most promising approaches for use in disaster and crisis situations are disruption-tolerant networks (DTNs) that are motivated to provide low-cost reliable connectivity to environments with no or little infrastructure. However, these constraints have significant implications on both security and privacy.

SECURITY AND PRIVACY IMPLICATIONS OF DISASTER CONTEXT

Typical feature of such emerging wireless networks is unavailability of permanently present central trusted authority. It has manifold implications on security requiring cooperation of devices (and their owners) to perform many essential networking tasks such as routing, maintaining network topology etc. Without central trusted authority devices have to collaborate to provide reasonable level of security related functionality such as establishment trust associations, detection and isolation malicious or compromised nodes, providing secure storage and routing, anonymity, etc.

Emerging of DTNs was motivated to bring low-cost best effort connectivity to challenging environments with limited or no fixed network infrastructure. This makes them perfectly suitable candidate to be deployed in disaster areas. However, more work on security and privacy protection in DTNs is still need to be done (Fall and Farrell, 2008) , for example, on the model for the authorization of traffic to tackle unwanted traffic. Another big challenge is to provide mechanisms for key management. Conventional mechanisms developed for centralized settings are not suitable in disaster and crisis situations where networks are often fragmented, with long message delays, high probability packet loss, involving highly mobile nodes and without centralized trusted authority. For example, long message delays and high probability packet loss make session key negotiation (like in SSL/TLS) impractical if not impossible.

Design of emergency and disaster management ICT systems is difficult. Design of secure and privacy-aware systems is even more difficult. There are three categories of security and privacy challenges that should be considered when such systems are designed (Manoj and Hubenko Baker, 2007): technological, sociological and organizational. All these categories of challenges are important and must be approached if we want to design systems that are both effective and usable. However, in this paper we will focus on technological challenges. Mainly, on technological challenges that arise due to a specific nature of emergency and disaster management setting. One of them, the primary one, is a need for rapid deployment of such systems to provide first-responders, disaster management workers and disaster victims with infrastructure for communication, information collection and sharing because of unavailability of communication infrastructure in the area of disaster (either destroyed or absent).

NETWORKS INFRASTRUCTURE FOR DISASTER AREAS

Mobile ad hoc networks (MANETs) have been proposed by many authors as an appropriate solution for disaster setting. However practical experience with such networks in disaster areas where they have to operate in situations where continues end-to-end connectivity may not be possible or difficult to achieve leads to recognition that Delay- and Disruption-tolerant network (DTN) architecture (Fall, 2003; Fall and Farrell, 2008) is more suitable. DTNs are designed to have very long round-trip delays, their end-to-end path might be unpredictable, messages may be lost, and they are often delivered out of order. All these properties make traditional security protocols unsuitable.

TRUST AND TRUSTWORTHINESS

The distributed nature of DSNs provides generally more robust and resilient solutions comparing with centralized approach where such centralized authority can be a single point of failure. However, traditional public-key infrastructure (PKI) is considered to be not well-suitable for DTNs, partly because of difficulty to access online servers. It has been proposed to use identity-based cryptography (IBC) to provide security in DTNs (Seth, Hengartner and Keshav, 2005). However, analysis provided in (Asokan, Kostiainen, Ginzboorg, Ott and Luo, 2007) leads to conclusion that IBC has no significant advantages over traditional cryptographic approaches with respect to integrity and authenticity but it can provide better confidentiality protection. One of the weak points of using IBC for DTNs is how trusted third party called PKG (public-key generator) can verify whether a new entity does have right to an identifier which will be used as a public key in the following communication in DTN. Generally, certificate revocation lists are considered unsuitable for DTNs (Seth, Hengartner and Keshav, 2005) due to delays and disconnected environments DTNs are designed for. The alternative revocation approach that can be used both in traditional PKI and IBC-like, can be based on shortlived certificates. However, it is not well suitable for DTNs either. The possible revocation approach that is suitable for DTNs can be based on evaluation of trustworthiness of certificates which would require continuous assessments of their trustworthiness.

Many distributed trust models (Jia, Lin, Tan, Li and Yang, 2012; Omar, Challa and Bonabdallah, 2009) proposed recent years utilize notions of reputation and trust assigned to nodes to support establishment of trust association between nodes as replacement for non available CAs. In such distributed models where no reliable PKI available, each node acts as its own CA. That is, it may issue and distribute its own certificates (Defrawy, Solis, and Tsudik, 2009). To work properly, such schemes need maintain knowledge of trustworthiness of nodes and certificates they issue. As was pointed out in (Jia, Lin, Tan, Li and Yang, 2012; Omar, Challa and Bonabdallah, 2009) , establishing an initial trust between nodes in the deployment phase is still an open problem. However, in the disaster scenario it is reasonable to assume that deployment will involve human participants and some of these participants may already have certificates issued by trusted CA prior disaster. Typical examples of such participants could be police officers, medical doctors and nurses, firemen, local administration officials, teachers, etc.

Generally, in DTNs deployed in disaster we assume existence of the areas three categories of nodes: nodes with digital certificates issued trusted CA prior disaster (possibly currently unreachable), nodes without such certificates but with capabilities to act as local CA for themselves and other nodes, and nodes without such capabilities. Having some nodes with certificates assigned by trusted CA provides a subset of nodes with initially assigned level of trustworthiness. Trustworthiness of a node without such certificate is unknown. However trustworthy nodes can combine their efforts and generate locally certificates for those nodes that do not have such capabilities. They can, in addition, use social information assuming that socially-related people are collocated and often share the same security context (Defrawy, Solis, and Tsudik, 2009; Costa, Mascolo, Musolesi and Picco, 2008).

SUBJECTIVE LOGIC

Subjective logic is a type of probabilistic logic that explicitly takes uncertainty and believes into account. It is suitable for modeling and analyzing situations arising in disaster setting which often involves uncertainty and incomplete knowledge. Subjective logic can be seen as an alternative to the Dempster-Shafer theory, with main difference from the former that subjective logic defines belief mass as a function of not only belief and uncertainty, but also of an a priori probability in the absence of any evidence. It is also argued (Jøsang, 2001) that subjective logic is suitable to formulate more expressive beliefs than Dempster-Shafer theory. For example, the consensus operator provided by subjective logic can be applied to dogmatic conflicting opinions, i.e. when the degree of conflict is very high. Such opinions can frequently arise in chaotic disaster situations. It overcomes shortcomings of Dempster's rule and other operators that have been proposed for combining possibly conflicting beliefs and can be seen as an essential for dealing with uncertainties in crisis management.

In this section we give brief overview of subjective logic necessary to explain the idea of using it in the proposed trust model.

First, we show how trustworthiness is expressed as a trust level. Following (Jøsang, 2001; Jøsang, 2002) we first define the term opinion, denoted ω, that expresses opinion about level of trustworthiness.

Let t, d and u be such that $t + d + u = 1$, $(t, d, u, a) \in [0,1]^3$. Then a triple $\omega = \{t, d, u, a\}$ is called an *opinion*, where components t, d, u and a represent levels of *trust*, *distrust*, *uncertainty* and *base rate* respectively, where a is the a priori probability in the absence of evidence. The levels of trustworthiness are expressed by opinions. Varying these parameters, we can express different levels of trust. Expressing trust using three values instead of just one trust level provides a more adequate trust model of real world with uncertainties. These parameters are not treated equally when different opinions are combined.

The subjective logic defines a set of logical operators for combining opinions including conjunction, recommendation, and consensus. For the purpose of this paper we will describe only consensus operator. For more details, related to subjective logic can be found in (Jøsang, 2001; Jøsang, 2002; Jøsang, 1999).

Consider two entities (subjects) A_1 and A_2 having two possibly different opinions $\omega_i = \{t_i, d_i, u_i, a_i\}$, $i = 1,2$ about trustworthiness of the same piece of evidence (for example, certificate). The consensus opinion of two possibly conflicting argument opinions is an opinion that reflects both argument opinions in a fair and equal way. The consensus operator $\oplus$ produces a consensus belief that combines the two separate beliefs into one $\omega = \omega_1 \oplus \omega_2$.

Let *A* and *B* be two entities (subjects) such that *A* is CA and *A* has issued certificate to *B*. Then *B* has issued certificate to *C*. Opinion about trustworthiness of certificate issued by *B* to *C* should be based on trustworthiness of *B* which also depends on trustworthiness of CA *A*. It can be interpreted that A recommends *B* as a trusted by issuing a certificate to *B*. Trustworthiness of *B* is based on showing a valid certificate signed by *A* and therefore depend on trustworthiness of *A*. In subjective logic, assume that $\omega_B^A = \{t_B^A, d_B^A, u_B^A, a_B^A\}$ denotes an opinion of *A* about trustworthiness of recommendations given by *B*. Assume that *B* issues certificate *s* to *C*. The opinion about trustworthiness of *s* is denoted as ω_s^C. When an entity wants to use *s*, it may to know ω_s^C. It is defined as combination of trustworthiness ω_s^B of *B* combined with trustworthiness ω_B^A of recommendations of *A*. For the purpose of deducing indirect opinion ω_s^C, the recommendation operator $\otimes$ is used (according to (Jøsang, 1999)) as follows:

$$\omega_s^C = \omega_s^{AB} = \omega_B^A \otimes \omega_s^B$$

The above two cases of illustrate how subjective logic is planned to be used in dealing uncertainty and incomplete knowledge that arise in disaster situations.

FRAMEWORK FOR PERMISSION MANAGEMENT

One of the primary challenges in disaster setting is a need for fast deployment. Another would be dynamic coalitions of semi-trusted parties that have to share information. The traditional approaches where participants are known in advance to the centralized security authorities are not usable due to time and resource constraints. New approach should support decentralized security management, authorization, authentication, key generation revocation, etc.

In this section we discuss an approach that is aimed to provide solution for the mentioned challenges. We assume that there are entities (subjects) like first-responder, victims etc. all of them can provide information describing real-time situation, but they also may need to receive information. Therefore, we assume that they have access to networked devices like smartphones, laptops, etc.

We assume that some owners of mobile devices may have one or more digital certificates, issued by trusted certification authorities (for instance, based on their occupation like police officer, medical doctor, etc.). Such certificates are both useful and necessary means for access control decisions (both authentication and authorization). At the same time, it always will be members of victim population who will not have such certificates. Since their trustworthiness is unknown, their ability to access services requiring authorization and authentication will be limited. Since in disaster setting most of CAs and identities management services are not available, we propose to combine social context and already certified parties to vouch on behalf of certificateless parties. The trustworthiness of such locally issued certificates (and their owners) will be calculated as combined opinion of trustworthiness of certificate issuers (based on subjective logic as described in the previous section).

Depending on certificate presented to service provider they can decide on trustworthiness of certificate owner and therefore on whether and what services and resources may be provided. Generally, such certificates should be seen as attribute certificates that certifies validity of various attributes that can be required to get specific permissions on accessed system.

Thus, we assume that each subject has some roles/attributes assigned that is expressed in the form of attribute certificate. Following dRBAC notation (Freudenthal, Pesin, Port, Keenan and Karamcheti, 2002), it can be written formally as:

[Subject -> Object] Issuer

meaning that Role/Attribute Object is assigned to Subject by Issuer. Such assignment must be approved as a certificate signed by Issuer. Object represents a role or an attribute that must be shown by subject to be able to do a specific security-sensitive activity (specified by Object). However, to provide flexibility, Issuer (which may be not available in disaster situation), want to permit subject to delegate object to other subjects when subject decide. Formally, it is expressed as:

[Subject -> Object'] Issuer

Now when Subject decides to delegate Object to Subject1, it can issue certificate in the form:

[Subject1 -> Object] Subject

Trustworthiness of this certificate can be calculated from trustworthiness of Subject and Issuer as explained in Subjective logic section above. Having opinion on trustworthiness this certificate can be used to deny security-sensitive action specified by Object if it is below the predefined threshold (usually defined by security policy).

Trustworthiness of the certificate for performing action Object could be increased if more then one subjects can approve delegation of action Object. Assume Subject1 and Subject2 have two certificates:

[Subject1 -> Object'] Issuer1

and

[Subject2 -> Object'] Issuer2

Then Subject1 and Subject2 together may delegate Object to Subject3 by issuing a new certificate:

[Subject3 -> Object] Subject1, Subject2

Trustworthiness of this certificate will be calculated by combining trustworthiness of Subject1 and Subject2 together with trustworthiness their corresponding issuers according to rules of subjective logic.

It is important to note that in disaster and crisis setting may not be feasible or even possible to find subject who may delegate some specific roles or attributes. Therefore, for the sake of flexibility and practicality, some trusted subjects (along or in a group) may be permitted to issue certificates for roles/attributes they do not have themselves. Then, it is up to certificate requester to decide whether to except them as trustworthy enough or reject.

The proposed approach provides flexible framework for role/attribute delegation without central CAs. Combining it with trust model that takes uncertainty into account (subjective logic), provide additional protection against malicious or compromised nodes.

CONCLUSION

In this paper we propose a framework for security enforcement in disaster and crisis situations. The framework is designed to be used with delay-tolerant wireless networks that are particularly suitable for use in crisis areas. However, such networks are known to be particular difficult to provide security since traditional solutions do not work. The framework proposed in this paper combines trust model based on subjective logic with distributed attribute based access control. More work is needed to provide solution that will be privacy-preserving, possibly based on anonymous certificates. Another challenging task is to design scheme for efficient revocation needed to deal with malicious and compromised nodes.

REFERENCES

1. Asokan, N., Kostiainen, K., Ginzboorg, P., Ott, J. and Luo, C. (2007) Applicability of identity-based cryptography for disruption-tolerant networking. In: *MobiOpp 07*, ACM, 52-56.
2. Costa, P., Mascolo, C., Musolesi, M. and Picco, G. (2008) Socially-ware routing for publish-subscribe in delay-tolerant mobile ad-hoc networks. *IEEE Journal on Selected Areas in Communications*, 26, 5, 748-760.
3. Defrawy, K.E., Solis, J. and Tsudik, G. (2009) Leveraging social contracts for message confidentiality in delay tolerant networks. In *Proceedings of 33rd IEEE International Computer Software and Applications Conference*, 271-279.
4. Fall, K. (2003) A delay-tolerant networks architecture for challenged internets. SIGCOMM'03, 27-33.
5. Fall, K. and Farrell, S. (2008) DTN: an architectural retrospective. *IEEE Journal on Selected areas in communications*, 26, 5, 828-836.
6. Freudenthal, E., Pesin, T., Port, L., Keenan, E. and Karamcheti, V. (2002) dRBAC: distributed role-based access control for dynamic coalition environments, In: *Proceedings 22nd International Conference on Distributed Computing Systems*, 411-420.

7. Jia, Z., Lin, X., Tan, S.H., Li, L. and Yang Y. (2012) Public-key distribution scheme for delay-tolerant networks based on two-channel cryptography. *J. of Networks and Computer Applications*, 35, 3, 905-913.
8. Jøsang, A. (2001) A Logic of Uncertain Probabilities. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 9, 3, 279-311.
9. Jøsang, A. (2002) The Consensus Operator for Combining Beliefs. *Artificial Intelligence Journal*, 142, 1-2, 157-170.
10. Jøsang A. (1999) An Algebra for Assessing Trust in Certification Chains. In *Proceedings of the Networks and Distributed Systems Security (NDSS'99).*
11. Ma, D. and Tsudik, G. (2010) Security and Privacy in Emerging wireless networks. *IEEE Wireless Communications*, 12-21.
12. Manoj, B. S. and Hubenko Baker, A. (2007) Communication challenges in emergency response. *Comm. of ACM*, 50, 3, 51-53.
13. Omar, M., Challa, Y. and Bonabdallah A. (2009) Reliable and fully distributed trust model for mobile ad hoc networks. *Computer &Security*, 29, 3-4, 199-214.
14. Seth, A., Hengartner, U., and Keshav, S. (2005) Practical security for disconnected nodes. In: *First Workshop on Secure Network Protocols (NPSec).*