Security requirements for MANETS used in emergency and rescue operations

Inger Anne Tøndel, Martin Gilje Jaatun, Åsmund Ahlmann Nyre
SINTEF ICT
Trondheim, Norway
inger.a.tondel@sintef.no

Abstract

Existing work on security in mobile ad hoc networks has primarily focused on routing security in open ad hoc networks where anyone can participate, or closed networks protected by shared symmetric keys. Ad hoc networks for first responders in emergency situations have some unique characteristics that differ from general ad hoc networks, since it is desirable to restrict who can participate in the network without relying on a pre-deployed infrastructure. In this paper we present security requirements elicited for a first responder mobile ad hoc network in the OASIS project.

1. Introduction

Emergency and rescue operations are frequently identified as an application area of (mobile) ad hoc networks [1], [2], [3], and there are solutions (e.g. Pužar et al. [4]) for security of ad hoc networks that specifically address such uses.

As part of the OASIS project[1], we have worked on security solutions for supporting use of ad hoc networks in emergency and rescue operations. We surveyed available literature in order to reuse solutions suggested by others, but found that – though there were many novel/interesting solutions available – it was hard to determine which solutions were appropriate to our needs. We found that there were little published work on security needs or requirements for ad hoc networks in general, including ad hoc networks for emergency and rescue operations. Some relevant work was identified, as will be outlined in Section 2. The requirements identified also mostly covered routing and, in many cases, did not provide sufficient details to be testable. We therefore performed an independent security requirements elicitation process with the goal of identifying security requirements for ad hoc networks used for OASIS. As the process leading up to these requirements and the rationale for these requirements have been documented, we believe these requirements can be reused or used as inspiration in other work on security of ad hoc networks, and in ad hoc networks for emergency and rescue in particular.

2. Related work

Most of the work on security in ad hoc networks handles security requirements only superficially. The most relevant work that we are aware of is a study of known problems with existing routing protocols for ad hoc networks, as presented by Dahill et al. [5] and Sanzgiri et al. [6]. This study led to seven security requirements, covering spoofing of route signaling, fabrication and altering of routing messages, maliciously formation of routing loops, route redirection from shortest path, who should be part of route computation and discovery, and exposure of network topology. Ad hoc networks are divided into three categories, each requiring a different level of security. Emergency and response in disaster areas is considered part of the managed-hostile environments group, which should meet all the identified requirements.

A less detailed list of security requirements on routing protocols of ad hoc networks is provided by Zapata and Asokan [7]. They are concerned with routing updates, and states the importance of import authorisation[2], source authentication and integrity of routing information.

Data authentication is said to be covered by the combination of the above. Compromised nodes are not considered, as they believe this only to be relevant for military scenarios. Availability is also not covered as they find it unfeasible to prevent denial of service (DoS) attacks when using wireless technology.

Wrona [8] takes a different approach, and states that ad hoc networks in general have identical security requirements as other communication systems, but that ad hoc networks are extreme in the requirements on the sophistication and efficiency of the security mechanisms themselves, mainly because of the lack of infrastructure and the very dynamic and ephemeral character of relationships between network nodes. He does not however provide more details on the security requirements.

3. Method

In previous work [9] we have studied existing approaches to security requirements elicitation, and have identified the

[1] Open Advanced System for dISaster and emergency management, EU FP6 IST contract number 004677, http://www.oasis-fp6.org/

[2] only authorise route information if it concerns the node that is sending the information

most commonly recommended steps. Based on this we have proposed a four-step approach: 1) Identify security objectives, 2) Asset identification, 3) Threat analysis, and 4)Documentation of security requirements. Objectives is defined as “the high-level requirements or goals that are most important to customers, and the requirements that must be met to comply with relevant legislation, policies, and standards” [9]. Assets are important as “security requirements are primarily needed in order to protect our assets, and this will obviously be impossible to do properly unless we know what these assets are” [10]. During threat analysis we study likely attacks towards the most important assets.

As we did not have access to customers, objectives were identified based on previous work in OASIS and based on reading material on ad hoc networks for emergency and rescue operations. Assets were identified in a workshop using the approach described by Jaatun et al. [10]. This approach is based on brainstorming, something that may seem a bit too unstructured at first glance. Available publications on security requirements engineering however show that brainstorming techniques and similar is used in several approaches - with few problems experienced [11].

In the workshop assets are prioritised by considering the importance of the confidentiality, integrity and availability of each asset from the viewpoint of system users, owners and attackers. By including different viewpoints we are able to handle the fact that different actors view of an asset are not directly related [12],this way giving most focus to assets that are important for attackers as well as system owners and/or system users. In order to keep the method as lightweight as possible we use only four classes of priorities for our assets: high, medium, low and irrelevant. The total value of e.g. the confidentiality of an asset is then the sum of its value from the different viewpoints. This is of course a simplification, but still provides an easy and powerful way of finding which assets and which asset properties are important in the system.

Based on the result of asset identification, we studied the threats towards the assets that had been identified as most important. For the threat modelling we used attack trees as defined by Schneier [13], as his threat modelling method is well recognised and fits our approach well. Most attack trees were created in a workshop, the rest was created by one individual and checked by the other experts at a later point in time. At the end security requirements were created by going through the security objectives assets and threat models. The requirements were created by one individual and later checked by the others.

4. Objectives

The security objectives is listed in Table 1. As a basis for identifying these objectives we described what will be the typical usage of the OASIS ad hoc network and the main security issues as we see it.

The current predominant communication paradigm for first responders is voice communication over radio netwoks (e.g. TETRA). MANETS will enable distribution of rich content in uni-, multi- or broadcast mode. In addition to user nodes, we envisage a command post that is operated from a specialised vehicle and possess greater computing resources. In situations where external communication infrastructure is available, both the command post and first responders may connect to external resources (health networks, police networks, etc.).

Many of the challenges of securing MANETs in general [14] also apply to MANETs for first responders. We have identified two main types of attackers posing a threat to first responder MANETs: News media and terrorists[3]. News media is primarily interested in obtaining information on the tactical operation by launching passive attacks. Information is assumed to be most valuable in real-time, but remains interesting for critics in the evaluation process. Terrorists are interested in obstructing the network operations by launching active attacks to disrupt routing, forge communication, thwart legitimate access, etc. It is possible that a physical terrorist attack (e.g. explosion, fire, etc.) is extended by a follow-up attack on the first responder emergency operation network.

Organisations involved in emergency operations are typically hierarchically structured, where information flows upwards and decisions downwards. However, the operational hierarchy is affected by the type of personnel available at any given time, such that dynamics in responsibility and authority must be anticipated. As an example, police commanders are normally in charge of the overall operation, but if none with sufficient authority is present, a firefighter officer will assume this role. and functions in the operation. In addition, personnel from different organisations and regions must be allowed to participate and collaborate without compromising the security of the network. This makes key management for authentication and access control in particular, a troublesome task.

In a crisis situation, it is likely that some medical data will be exchanged. Confidentiality of medical data is required by law to protect the privacy of citizens. However, in the event of an emergency, preserving lives is considered more important than preserving privacy. If confidentiality requirements hamper operations, medical staff will plead just cause in order to ensure availability of data. For the same reason usability is also important, as security mechanisms significantly hampering the performance of first responders are not likely to be used.

The limited available resources of devices in MANETs are a prime concern when designing effective security mech-

[3] The terms news media and terrorists must be interpreted in a wide sense to incorporate anyone with similar interests and motivation. The list is by no means exhaustive, but serves as an example of threats that are predominant in first responder networks.

Nr.	Objective
O1	*Confidentiality:* For some information confidentiality may be required by law, e.g. for medical information. Mechanisms must thus be in place that is able to offer adequate protection of confidentiality.
O2	*Availability vs. confidentiality:* Availability is in many, if not most, cases more important than confidentiality, as the OASIS ad hoc network is intended used in crisis situations.
O3	*Integrity:* Integrity of information should be ensured as there are attackers that may want to attack integrity in order to hamper the operation.
O4	*Participation and collaboration:* Personnel from different organisations and regions must be allowed to participate and collaborate without compromising the security of the network.
O5	*Access control:* There is no intention of letting just anyone connect to the network and start interacting with it. This is a difference between a first responder network and the academic ideal ad hoc network.
O6	*User hierarchy:* Security solutions should support the hierarchical nature of emergency operations.
O7	*Dynamics of responsibility:* Security solutions should support dynamics in responsibility and authority.
O8	*Limited node resources:* Devices typically used for the OASIS ad hoc network will have limited computational power and battery available. The security solutions must take this into account.
O9	*Limited bandwidth:* The bandwidth available will typically be limited, and this must be taken into account when choosing and implementing security solutions.
O10	*Usability:* Security solutions must not render the system to difficult or troublesome to use.
O11	*Not dependent on central nodes:* The ad hoc network should function without any central nodes.

Table 1. Security objectives

anisms. This constraint also applies to the first responder case, but not to the same extent. Devices for first responders are not assumed to be COTS (Commercial Off-The-Shelf), but rather specifically designed to meet communication requirements and to withstand environmental stress.

5. Assets and threats

In the workshop a high number of assets were identified. Due to limited space we do not include the full result of asset identification and prioritation but instead describe the assets that were assigned the highest priority and the rationale for their importance.

By **nodes** we mean communication devices used by individual users, e.g. laptops, PDAs etc. The command vehicle can also be viewed as a specialy type of nodes. Nodes are likely to hold sensitive informaion and potentially also access credentials, and confidentiality is thus imiportant. Nodes are also important for being able to communicate, resulting in a need to protect both availability and integrity of nodes.

In an OASIS ad hoc network **sensitive information** can include information on the operation, details and location of field workers involved, identity and health information on injured, who is the sender of messages etc. **Access credentials**, including passwords and keys for encryption and signing, can be viewed as a special type of sensitive information. Confidentiality is of course important for all this information, but so is availability and integrity. Loss of integrity can result in wrong information being available, something that can damage the operation and in longer term result in information not being trusted. This is comparable to information not being available. For access credentials, attacks on availability and integrity can result in the network being unavailable for some users. Confidentiality of node, user and role **identities** is usually not of high importance, but integrity and availability can be important for access and use of the network.

Network access, availability of **bandwith** and ability to comunicate with managers, team mates and other teams is of course important to system users and owners. To achieve this the network is dependent on its **routing mechanism** and the **routing information**. Unavailabile or erroneous routing information should not be crucial, as this is addressed by common ad hoc routing protocols. It is however a problem if attackers can modify routing information in order to improve their own access to messages, or disrupt routing by e.g. dropping packets. Attackers that gain access to the network and its communication can also use this to perform other attacks. If the attacker's aim is to disrupt service, it is also easy to attack network throughput by jamming.

We also identified some less prioritised assets. As examples, access to external resources and the command vehicle was considered less important as they are not crucial for the funcioning of the network. We also considered the value of priority functions, but dropped this as we did not consider this to be likely used in our solutions.

For the most important assets identified we created attack trees to analyse the threat towards these assets. An overview of the attack trees created is shown in Table 2 and an example attack tree for the attack "Get access to bandwidth" is shown in Figure 1.

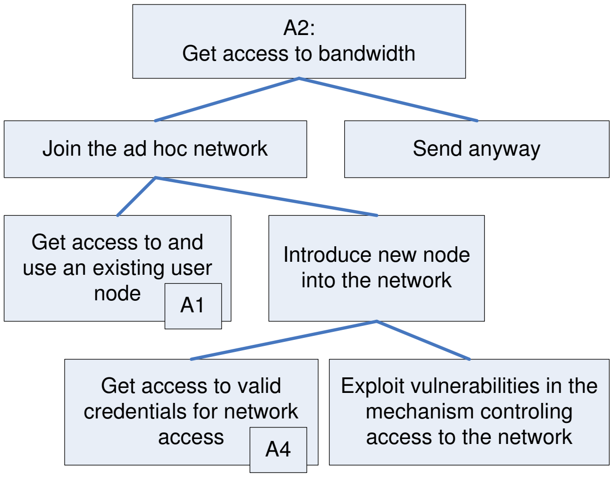
6. Documentation of security requirements

The requirements identified based on the objectives, assets and threats are listed in Table 3. We have aimed towards expressing "what is to happen in a given situation, as opposed to what is not ever to happen in any situation" [12] when phrasing the security requirements.

Attack tree		Main attacks identified
A1	Get access to and use an existing node	Access node, either physically or externally, and either get access to valid access credentials or bypass access control.
A2	Get access to bandwidth	Get access to an existing node. Introduce a new node by gettin valid access credentials for this node or by exploiting vulnerabilities in the access mechanism. Or send anyway.
A3	Get access to sensitive information	Get access to communication through eavesdroping or routing, and break any encryption. Get access to sensitive information on a node.
A4	Get access to access credentials	Get access to communication or nodes that contain access credentials and break any protection. Find credentials. Guess credentials. Perform social engineering attack.
A5	Stop users from getting access to ad hoc network	Infecting nodes, attack the access control mechanism. Perform DoS attack by e.g. jamming the network. Flip bits in communication related to access control.
A6	Attack integrity and/or availability of identities	Infect nodes and edit identities stored. Edit identities during transmission or routing. Edit own identity in order to increase own access rights or spoof as another user.
A7	Destroy integrity of information	Flip bits in communication. Destroy integrity of packets during routing. Destroy integrity of information stored on nodes.
A8	Hinder availability of information	Hinder routing by dropping packets or disrupting routing tables. A5. A7. A9.
A9	Destroy integrity or availability of credentials	Attack identities stored on nodes. Attack integrities during routing or transmission.

Table 2. Attack trees

Figure 1. Attack tree for access to bandwidth


A2:
Get access to bandwidth
Join the ad hoc network
Send anyway
Get access to and use an existing user node
A1
Introduce new node into the network
Get access to valid credentials for network access
A4
Exploit vulnerabilities in the mechanism controling access to the network

We have identified in total 30 requirements where eleven are directed towards nodes (R1-3, R6-7, R15, R17-19, R22, R24), twelwe are directed towards the network services (R8-11, R16, R20-21, R23, R25, R28-30) and seven concern both network and nodes (R4-5, R12-14, R26-27). The source of most requirements is an attack tree, as these show most detail as to what protectoin is needed. However, it was not all objectives that was naturally covered by studying threats, and thus the source of some requirements is an objective.

In addition to the requirements listed in Table 3 ther are some overall concerns that should be taken when choosing and developing mechanisms to fulfil the requirements. It is important to 1) Ensure usability of the nodes and network services (O10), 2) Limit the extra communication needed to ensure security (O9), 3) Select security solutions that do not require a lot of node resources (O8), and 4) Support and utilise the hierarchical nature of emergency operations (O6).

7. Discussion

We have devised in total 30 security requirements relevant for ad hoc networks as used in OASIS. The requirements differ from the requirements suggested by Dahill et al. [5] and Sanzgiri et al. [6] in that they cover more than just routing. In our requirements elicitation process we have also focused on objectives, assets and threats, while they mainly focused on problems with existing approaches. Our requirements are also more detailed than those presented by Zapata and Asokan [7] and Wrona [8]. The work on requirements have been used in the OASIS project as a basis for selecting a security solution for ad hoc networks used in OASIS, and in order to determine to what extent the final solution fulfilled the requirements.

Though we are convinced that the requirements can be used as inspiration, or maybe be reused, in related projects, we are aware of the need for further work on this area. The requirements have been created by three network security experts, and should be further validated by experts on emergency and rescue operations. This especially goes for the objectives used as a basis for creating the requirements. The requirements should also be tried out in other projects to find if they are reusable in the current form.

We are aware of several limitations of our asset identification methodology, e.g. the limitations of unstructured methods like brainstorming and the fact that the result will depend very much on the competence and main focus of the participators [10]. However, since our goal of asset identification is to identify the most important assets, and as brainstorming is commonly suggested for asset identification, we are confident that the method used is good enough

Nr	Requirement	Source
R1	*Node access:* Access to a physically available user node should require user authentication.	A1
R2	*Node lock:* Nodes should be locked after a predefined period of time of user inactivity, and should then require user authentication.	A1
R3	*External node access:* Functionality for external access to a user node should only be offered if clearly needed, and should then require user authentication.	A1
R4	*User input:* All user input, e.g. related to access control, should be validated in order to avoid input validation related vulnerabilities.	A1
R5	*Credential quality:* Access credentials should be difficult to guess and brute force, i.e. by putting restrictions of the length and characters used in passwords.	A1 A4
R6	*Stored credentials:* Access credentials should be protected from unauthorised access when stored, e.g. by access control and encryption mechanisms.	A1
R7	*Strength of node access mechanism:* The mechanism for access to user nodes should be able to withstand extensive security testing by security testing professionals.	A1
R8	*Network access:* Access to the OASIS ad hoc network should require authentication.	A2 A3
R9	*Strength network access mechanism:* The mechanism for access to the OASIS ad hoc network should be able to withstand extensive security testing by security testing professionals.	A2 A5
R10	*Link confidentiality:* The confidentiality of sensitive information must be protected while sent on the communication link.	A3
R11	*End-to-end confidentiality:* The confidentiality of sensitive information should be protected end-to-end during communication.	A3
R12	*Encryption algorithms:* All encryption mechanisms should be implemented with well recognised algorithms.	A3 A4
R13	*Encryption keys:* All keys used related to encryption should have a key length that is recognised to provide high protection.	A3 A4
R14	*Key management:* All key management mechanisms should be well known and recognised.	A3 A4
R15	*Command vehicle:* Access to the nodes of the command vehicle should be as protected as access to user nodes, with the addition of physical protection mechanisms.	A3
R16	*Communication of access credentials:* The confidentiality of access credentials must be protected end-to-end during communication.	A4
R17	*Node software:* Nodes should only have necessary software installed.	A5
R18	*Node security software:* Nodes should have installed common security mechanisms, like anti-virus software and firewalls.	A5
R19	*Patching/ updating:* Software on nodes should be regularly patched/updated.	A5
R20	*Transmission errors:* For all communication it should be possible to detect transmission errors.	A5-A9
R21	*Integrity of transmitted information:* Integrity of communication related to access control (or possibly all communication) should be protected while sent on the link in order to detect deliberate changes by attackers.	A5-A9
R22	*Administrator access on nodes:* Administrator access on user nodes should require separate access credentials than ordinary user access.	A6
R23	*Detection of misbehaving nodes:* The OASIS ad hoc network should include mechanisms for detecting misbehaving nodes.	A8
R24	*Integrity during storage:* The integrity of access credentials should be protected while stored on nodes.	A9
R25	*Integrity access credentials:* The integrity of access credentials should be protected en-to-end when sent over the OASIS ad hoc network.	A9
R26	*Identities vs. access rights:* Mechanisms must be in place that ensures node users cannot edit their identities and by that increase their access rights.	A6
R27	*Identities and spoofing:* Mechanisms should be in place that ensures users cannot edit their entities and by that spoof as another user.	A6
R28	*Support participation and collaboration:* The access control mechanism to the ad hoc network should support participation and collaboration from police, fire and medical professionals from the same or neighbouring districts.	O4
R29	*Decentralised access control:* Access control to ad hoc network should work without any centralised nodes.	O11
R30	*Support dynamics of responsibility:* If creating security mechanisms that control access based on responsibility, these should support changes in responsibility based on availability of resources.	O7

Table 3. Security requirements

to meet our needs at this stage. Still the assets identified should be validated by other experts. The same goes for the attack trees, in order to find if the important attacks have been covered.

We have created requirements with the aim of describing what should be done, not how, as recommended by Firesmith [15], among others. We are aware that in many cases security requirements contain more detail on the actual mechanism used. This will however make them less reusable, and also put more restrictions on the design and choise of mechanisms used. Still we recognise that some may find that the requirements provided are too high level, and that a requirements refinement activity may be needed for individual projects.

We have deliberately not assigned priority to any of the requirements, as this is likely to vary between projects. Note also that it is necessary to make tradeoffs between the requirements listed. As an example *R2 Node lock* should be addressed together with the overall concern of usability (O10).

8. Conclusion and further work

We have presented security requirements for ad hoc networks used in emergency and rescue operations. The requirements have been devised and used in the OASIS projects, but have been presented here as we believe they will be useful as input to other related projects. The requirements elicitation process have been described, as well as the main results of each step, in order to keep the rationale for the requirements. As future work, the usefulness of these requirements should be addressed for other projects and solutions, and they should be refined by other experts in order to improve their quality and assure their relevance.

Acknowledgments

This paper has presented results from the EU FP6 OASIS research project, with additional funding by the Norwegian Research Council. Thanks to Ingrid S. Svagård for making this research activity possible.

References

[1] L. Zhou and Z. Haas, "Securing ad hoc networks," *Network, IEEE*, vol. 13, no. 6, pp. 24–30, 1999.

[2] N. Milanovic, M. Malek, A. Davidson, and V. Milutinovic, "Routing and security in mobile ad hoc networks," *Computer*, vol. 37, no. 2, pp. 61–65, 2004.

[3] M. Asplund, S. Nadjm-Tehrani, and J. Sigholm, "Emerging information infrastructures: Cooperation in disasters," in *Proceedings of the 3rd International Workshop on Critical Information Infrastructures Security (CRITIS'08)*, October 2008.

[4] M. Pužar, T. Plagemann, and Y. Roudier, "Security and privacy issues in middleware for emergency and rescue applications," *Pervasive Computing Technologies for Healthcare, 2008. PervasiveHealth 2008. Second International Conference on*, pp. 89–92, 30 2008-Feb. 1 2008.

[5] B. Dahill, B. N. Levine, E. Royer, and C. Shields, "A secure routing protocol for ad hoc networks," Electrical Engineering and Computer Science, University of Michigan, Tech. Rep. UM-CS-2001-037, August 2001.

[6] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "A secure routing protocol for ad hoc networks," in *Proceedings of the 10th IEEE International Conference on Network Protocols.* IEEE Computer Society Washington, DC, USA, 2002, pp. 78–89.

[7] M. G. Zapata and N. Asokan, "Securing ad hoc routing protocols," in *Proceedings of the 3rd ACM workshop on Wireless security.* ACM Press New York, NY, USA, 2002, pp. 1–10.

[8] K. Wrona, "Distributed security: Ad hoc networks & beyond," in *Ad Hoc Network Security Pampas Workshop, RHUL, London*, September 2002, pp. 16–17.

[9] I. A. Tøndel, M. G. Jaatun, and P. H. Meland, "Security requirements for the rest of us: A survey," *IEEE SOFTWARE*, pp. 20–27, 2008.

[10] M. G. Jaatun and I. A. Tøndel, "Covering your assets in software engineering," in *Third International Conference on Availability, Reliability and Security, 2008 (ARES 08)*, 2008, pp. 1172–1179.

[11] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process," CMU/SEI, Tech. Rep. CMU/SEI-2007-TR-012, 2007. [Online]. Available: http://www.cert.org/archive/pdf/07tr012.pdf

[12] C. Haley, R. Laney, J. Moffett, and B. Nuseibeh, "Security requirements engineering: A framework for representation and analysis," *IEEE TRANSACTIONS ON SOFTWARE ENGINEERING*, vol. 34, no. 1, p. 133, 2008.

[13] B. Schneier, "Attack trees: Modeling security threats," *Dr. Dobb's Journal*, December 1999.

[14] B. Wu, J. Chen, J. Wu, and M. Cardei, "A survey of attacks and countermeasures in mobile ad hoc networks," in *Wireless Network Security*, ser. Signals and Communication Technology. Springer US, 2007, pp. 103–135.

[15] D. G. Firesmith, "Engineering security requirements," *Journal of Object Technology*, vol. 2, no. 1, pp. 53–68, 2003.