ESTIMATION OF THE SECURITY LEVEL IN A MOBILE AND UBIQUITOUS ENVIRONMENT BASED ON THE SEMANTIC WEB

Reijo Savola
VTT Electronics, P. O. Box 1100, FIN-90571 Oulu, Finland

Keywords: Information security, security metrics, Semantic Web, mobile ad hoc networks

Abstract: The emerging Semantic Web enables semantic discovery and systematic maintenance of information that can be used as reference data when estimating the security level of a network, or a part of it. Using suitable security metrics and ontologies, nodes can estimate the level of security from both their own and the network's point of view. The most secure applications and communication peers can be selected based on estimation results. In this paper we discuss security level estimation in a mobile and ubiquitous environment based on the Semantic Web. An interdisciplinary security information framework can be built using the Semantic Web to offer metrics and security level information for product quality, the traffic and mobility situation, general statistical knowledge and research results having an effect on the security level.

1 INTRODUCTION

Semantic Web (Berners-Lee *et al*., 2001) is an extension of the current Web, in which information is given well-defined meaning, better enabling computers and people to work in cooperation. The Semantic Web provides an infrastructure that enables not just web pages, but databases, services, programs, sensors, personal devices, and household appliances to both consume and produce data on the web (Hendler *et al*., 2002). Semantic Web agents are autonomous goal-directed agents that can act in cooperation with other agents and establish their own trust and reputation databases. The agents can seek information according to their goals and flexibly negotiate their interaction models with other agents.

Another emerging paradigm, *mobile and ubiquitous computing*, aims at providing the technological means of offering user-friendly information and communication services, anywhere and anytime. The ubiquitous computing scenarios are expected to involve a great number of small, handheld, wireless computing devices that enable interaction between users, environment and computing elements. Mobile ad hoc networks (MANETs) (IETF, 2004) have great potential for broad use in making ubiquitous computing possible and successful, enabling self-organization and dynamic operation.

Ubiquitous computing can clearly benefit from the Semantic Web, which provides the infrastructure for the extensive usage of distributed knowledge. Devices that use the Semantic Web are able to combine information and functionality from local and remote sources, as well as to configure themselves in new environments.

The current security research effort for the Semantic Web concentrates on *trust* – particularly trust management and trust negotiation. *Trust negotiation* is the iterative disclosure of credentials and requests for credentials between two parties, with the goal of establishing sufficient trust that the parties can complete a transaction (Winslett *et al*., 2002). Digital credentials on the Semantic Web are attributes similar to those one uses in human society to deem trust. In addition to trust negotiation and management, the new possibilities offered by the Semantic Web can be used to raise the overall security of a network by estimating the security level and selecting applications and connections based on it. Many kinds of interdisciplinary information affect this level, e.g. product quality, human factors, trust management, cryptographic strength, and chosen algorithms. Statistical security level information can be stored in databases and systematically updated using trusted searches in the Semantic Web. The databases can be at individual nodes' disposal to

Savola R. (2005).
ESTIMATION OF THE SECURITY LEVEL IN A MOBILE AND UBIQUITOUS ENVIRONMENT BASED ON THE SEMANTIC WEB.
In *Proceedings of the Seventh International Conference on Enterprise Information Systems*, pages 256-262
DOI: 10.5220/0002551802560262

support their self-organized security level estimation.

The main contributions of this work are in the introduction of a mechanism that uses databases on the Semantic Web to carry out security level estimation, and in the identification of the type of component metrics that are needed for an example case of mobile ad hoc networks, the connectivity basis of ubiquitous computing. However, the same estimation mechanism can be used in general on the Semantic Web.

The rest of the paper is organized in the following way. Section 2 gives overviews of security metrics and the security concerns of mobile ad hoc networks. Section 3 introduces our proposal for estimation of the security level. Finally, Section 4 represents conclusions and directions for further research. The related work consists of security research work in MANETs and the information management solutions on the Semantic Web.

2 BACKGROUND

2.1 Security Metrics

There is often considerable controversy when the term "metrics" is used. The difference between *measurements* and *metrics* is the following. Measurements provide a one-time view of specific measurable parameters and are represented by numbers, weights or binary statements. On the other hand, metrics are produced by taking measurements over time and comparing two or more measurements with predefined baselines, thus providing a means for interpretation of the collected data (Jelen, 2000). Synonyms for metric are, e.g., measure, score, rating, rank, or assessment result (Henning, 2001). The wide majority of the available security metrics approaches have been developed for evaluating the maturity of security engineering *processes*. The most widely used of these maturity models is the Systems Security Engineering Capability Maturity Model SSE-CMM (ISO/IEC 21827, 2002). Another well-known model, Trusted Computer Security Evaluation Criteria TCSEC – "The Orange Book" – (U.S. Department of Defense, 1985), expresses the security engineering process using classes and divisions as evaluation levels. Although a high level of security engineering may tend to give a higher level of technical security, it cannot be guaranteed.

Although it is essential to measure the security engineering process, we here focus on *technical security metrics*. The object to be measured in technical metrics is the actual system, not the associated processes. Technical security metrics can be used to describe, and hence compare, technical objects – e.g. algorithms, specifications, architectures and alternative designs, products, and as-implemented systems at different stages of the system's lifecycle. In general, metrics are found most useful when they can be used *proactively* – predicting or trying to understand the future situation. (Jonsson, 2003) sorts the methods of security measurement into the following:

- **Risk analysis** is an estimation of the probability of specific threats and vulnerabilities and their consequences and costs;
- **Certification** is the classification of the system in classes based on the design characteristics and security mechanisms; and
- **Measures of the intrusion process** is a statistical measurement of a system based on the effort it takes to make an intrusion.

Technical security metrics can be used in the following ways:

- **Goal establishment**;
- **Prediction** before implementation or in an implemented system;
- **Comparison** of the security level of technical objects;
- **Monitoring or scanning** the security level of an object; and
- **Enabling analysis**: e.g., metrics enable analysis in fault injection testing.

2.2 Security Metrics for Mobile Ad Hoc Networks

As mobile ad hoc networks have the potential to offer the underlying connectivity for the mobile and ubiquitous environment, we here investigate their security concerns. The ultimate goal of the security solutions for MANETs is to provide services for the desired security needs, mainly *confidentiality*, *integrity*, *availability*, *authentication* and *non-repudiation*, at the desired security level. Table 1 presents the typically needed security services and attack types in MANETs.

In general, the research has noted that traditional security solutions, such as public key infrastructures or authentication mechanisms, also have potential for MANETs, but in many cases they are not sufficient by themselves. Overviews of the research efforts can be found in (Hubaux *et al*., 2001), (Yang *et al*., 2004) and (Zhou & Haas, 1999). The nature of the basic mechanisms of the ad hoc paradigm causes vulnerabilities, e.g.:

Table 1: Security needs and attack types for MANETs

DIMENSION	GOAL
Confidentiality	Critical information never disclosed to unauthorized entities
Integrity	A message being transferred is never corrupted
Availability	Prevention of / survivability from denial of service attacks
Authentication	Ensuring correct identity of a node
Non-repudiation	Origin of a message cannot deny having sent the message
ATTACK TYPE	EXPLANATION
Passive eavesdropping	Discovery of desired information by listening to routing data. Detection of this type of attack is challenging.
Denial of service	Produced either by unintentional failure or malicious action.
Impersonation	Nodes joining the network undetectably, or sending false routing information (black hole and wormhole attacks
Disclosure	Disclosure of critical information (data in nodes, routing data)

Lack of central administration,

- **Routing:** routing mechanisms are more vulnerable than in conventional networks because each node can act as a relay;
- **Co-operation:** if a node does not respect the co-operation rules – i.e. it is *selfish* – the performance of the network can be severely affected;
- **Variation in memory and computation resources:** many of the nodes are expected to be low-priced consumer electronics with cheap and slow computation capability and limited storage size, and
- **Energy constrained operation:** many of the nodes are expected to operate on battery power. Sleep or standby modes are used to conserve energy, during which they may not be reachable. Sleep deprivation torture is used by attackers.

Table 2 lists some component security metrics areas (Savola, 2004), a composition of which forms the basis for estimation of the overall security level in mobile ad hoc networks. The most critical component metrics emphasize *trusted information distribution* in a mobile ad hoc network. In this context, distribution means the location of the critical information in the network with regard to time. Trusted information includes key, routing, mobile entity identity and packet forwarding information. Technical challenges, such as the trusted information distribution, dominate the overall security level in the first stages of the technical evolution of MANETS. As technology matures, aspects such as product quality become more emphasized. To some extent, the component metrics structure of MANETs shown in Table 2 is the similar to that in other types of networks. Mobile ad hoc networks set very challenging security requirements because of their infrastructure-less structure.

It should be noted that the current insufficient knowledge of the nature of security hinders the research community from finding rigorous and objective solutions to the component metrics contributing to the overall security.

3 PROPOSED APPROACH

In this section we present the principle of a security level estimation mechanism that can be used in a ubiquitous and mobile computing environment that is based on the Semantic Web. Since mobile ad hoc networks have great potential as a technology for ubiquitous environments, we use them as an example. However, the same approach can be used in other connectivity platforms of the Semantic Web – only the required component security metrics vary depending on the platform technology.

In our approach, the estimation of security level is based on information gathered by agents in the Semantic Web and maintained in trusted databases. This information can be accessed by trusted measurement agents in the network's nodes.

The approach is self-organized with one exception: a hierarchy of trusted voting and countermeasure entities is required. If individual *trusted* nodes volunteer for these roles, the approach is self-organized. The objectives for the mechanism include:

- **Local monitoring** in each node,
- **Utilization of statistical knowledge** of the security level,
- **Measurements are independent** of the routing mechanism, and

Table 2: Some component metrics areas in MANETs

Component	Sub-component	Heuristic claim
Trust and key management	Initial trust	The better the assumed initial trustworthiness corresponds to actual trustworthiness, the more secure the system.
	Operational trust	The better the assumed operational trustworthiness corresponds to actual trustworthiness, the more secure the system.
Routing	Routing information	The better the distribution of routing information in the network corresponds to the best possible distribution, the more secure the system.
Mobility	Identity information	The better the distribution of mobile entity identity information corresponds to the best possible distribution, the more secure the system.
	Packet forwarding information	The better the distribution of packet forwarding information corresponds to the best possible distribution, the more secure the system.
Human factors	Usability	The more usable the system is, the more secure it is.
	Performance	The better the system performs, the more secure it is.
	Security awareness	The more security-aware users are, the more secure the system.
	Social engineering	The more resistant the system is to social engineering, the more secure it is.
	Freedom of use	The more freedom is offered, the more vulnerable the system is.
Cryptographic algorithms	Cryptographic strength	The better the cryptographic strength of the used cryptosystems, the more secure the network.
Wireless-ness	Listening	The harder it is for a listener to demodulate and decode the radio signal sent in the wireless environment, the higher the security level.
	Interference	The harder it is for an attacker to cause interference to the radio signals sent in a wireless network, the higher the security level in that network.
Scale	Scale of size	The bigger the network, the more vulnerable it is.
	Scale of use	The more popular the network, the more vulnerable it is.
Physical protection	HW tamper resistance	The more tamper-resistant HW is used in a node, the more secure the network.
	SW tamper resistance	The more tamper-resistant SW is used in a node, the more secure the network.
	Location of node	The more the physical environment is protected from attackers, the more secure the network.
Product quality	Functionality	The more functional the system is, the more secure it is.
	Reliability	The more reliable the system is, the more secure it is.
	Usability	The more usable the system is, the more secure it is.
	Efficiency	The more efficient the system is, the more secure it is.
	Maintainability	The more maintainable the system is, the more secure it is.
	Portability	The more portable the system is, the more secure it is.
Other factors	Privacy	
	Legislation	
	Commercial	
	Cultural	
	Force majeure scenarios	

– **Decision mechanism to revocate the trust** of suspicious nodes based on the observations of more than one node.

Clearly, there are two separate goals in the estimation process: estimation of the security level of a *node* and estimation of the security level of the *network* (or part of the network).

3.1 Information Gathering

The information needed for security level estimation can be stored in databases. The purpose of them is to offer correct and up-to-date component metrics and reference information contributing to the security level. The following kinds of metrics and security level reference information are useful for estimating the security level of MANETs (compare to Table 2):

- **Trust management**: digital credential information can be obtained using credential management techniques, see e.g. (Winslett *et al*., 2002);
- **Routing**: traffic information and information on recent attacks can be gathered in trusted *traffic control databases*; maintained by devoted Semantic Web agents;
- **Mobility**: up-to-date mobility information on nodes can also be maintained in trusted traffic control databases;
- **Human factors**: statistical databases of *human factors* can be used to depict research results of typical human behavior in different kinds of applications, and take cultural and group-dependent factors into account;
- **Cryptography**: databases with information on the cryptographic strength of different kinds of cryptosystems can be maintained by devoted agents;
- **Wireless-ness**: up-to-date research information on the security of wireless devices can be maintained in trusted *wireless security research* databases;
- **Scale**: a network can assign an agent to keep track of the size of the network, and the popularity of network types can be tracked in traffic control databases;
- **Physical protection:** manufacturers can be released physical protection certificates of their products as part of the *digital product quality certificates* that can be digital credential information;
- **Product quality**: the devices used in the network can be certified with the level of product quality information attached to the digital certificates. Certificates can be obtained from trusted *certification pages*.
- **Privacy**: A *trade-off database* can be used to estimate the effects of privacy requirements on the security level; and
- **Legislative, commercial, and *force majeure*** issues have their own databases.

3.2 Trust Establishment and Management

The most critical part of the security level estimation is the trust establishment and management between the database maintainers and their users. The agents that are gathering information into the databases also need to establish their own trusted connections. It is important to note that trust management is not static – access rights can be delegated and revocated dynamically.

Distributed trust models (Blaze *et al*., 1996) developed for the Semantic Web can be used in establishing the trust between different agents residing in different nodes in the network or in another network. Examples of trust management systems assuming *a priori* knowledge of authority include PolicyMaker (Blaze *et al*., 1996), KeyNote (Blaze *et al*., 1999), SPKI/SDSI (Simple Public Key Infrastucture / Simple Distributed Security Infrastructure) (Ellison *et al*., 1999), and Delegation Logic (Li *et al*., 2003). (Winslett *et al*., 2002) introduce TrustBuilder, which supports automated *trust negotiation* between strangers on the Web. (Kagal *et al*., 2003) propose a policy-based framework for pervasive computing environments that extends SPKI and role-based access control. In the latter approach trust distribution depends on, e.g., domain, delegation chain and policies.

In the MANET research community, network-level (rather than application-level) trust distribution mechanisms have also been proposed. (Zhou & Haas, 1999) introduce the idea of distributing a CA (Certification Authority) throughout the network, in a threshold fashion, at the time of network formation. In their *threshold cryptography*-based approach, the duties of CA (issuing, revoking, and storing of certificates) are distributed among the nodes. More recent proposals include (Čapkun *et al*., 2003) and (Luo *et al*., 2002). More state-of-the-art references can be found in (Hubaux *et al*., 2001).

Suitable *ontologies*, i.e. taxonomies with a set of inference rules, see (Chandrasekaran *et al*., 1999) for more information, for information gathering of different classes of metrics and reference levels are needed. Using these ontologies in connection with trust establishment and management, automatic updating of the trusted security level databases is possible.

3.3 Key Elements in the Estimation Process

In our estimation approach the key elements of the architecture are a Measurement Agent (MA) attached to each node of a MANET, and a Voting Agent (VA). A Countermeasure Agent (CMA) is also used for the Intrusion Detection functionality. The estimation is carried out in a mobile ad hoc network by co-operation between MAs and VAs. Each MA in the network maintains a *private metrics repository* with the following information for each metric:

- **Metric objects:** a collection of measurable objects to be measured, e.g. a property in routing information messages;

- **Metric methods:** methods associated with the metrics; and
- **Metric measuring rod:** a database associated with the metrics that consists of *reference information* classified according to the *level of security*. The measuring rod database can include security level data that is either generally known or gathered from statistical data. The classification in the reference information may be based on quantitative or qualitative (using thresholds) reasoning.

The component metrics areas discussed earlier can form the basic high-level structure for the private metrics repository of a MANET node.
In addition to the metrics repository, an MA maintains a *private reputation repository* of the network elements of a MANET or the elements that are visible to that particular node. The repository contains critical reputation information as an input to the estimation process.

A Voting Agent (VA) contains the same functionality as MA. In addition, it has an organizer role in case several MAs are going to make decisions concerning the security level and trustworthiness of a node; certain trusted nodes can have VAs in an ad hoc network. A Countermeasure Agent (CMA) acts on the results obtained from the voting process. Certain trusted nodes can have CMAs.

3.4 Estimation and Voting

The basic *node-level estimation* process is carried out continuously by the node's MA. The MA uses the data stored in its metrics and reputation repository to estimate the current level of security from its own node point of view. Moreover, the VA updates the MAs with information messages containing critical information on the changes in nodes and communication in the network vicinity. The critical information is updated in the reputation repositories of the MAs to support their *estimation of the security level in the network*.

An MA can access suitable databases, depending on the semantic guidelines it needs to estimate the security level. At node level, MAs support the decision processes of the nodes that use the security level information as an input. For example, the trustworthiness of a service may be assessed using the security level monitoring carried out in an MA.

There are a lot of situations where *democratic voting* can be used to support decisions to be made about the security level. For instance, if an MA detects a node with suspicious activity in the vicinity, voting can be used to justify the countermeasures to be carried out by a CMA. An MA can also inform a VA about its own security level estimates of an object. A voting process can be used to compare other MAs' observations of the same object.

3.5 Challenges

Mobile ad hoc networks are intrinsically resource-constrained, which makes our approach difficult to implement using the current technology. However, as the required level of security is often higher in cases where there are better memory and computation resources in use, the introduced approach is possible.

The selection of Voting Agents and Countermeasure Agents is also a problem in cases where complete self-organization of the network is a goal. Suitable trust establishment procedures are needed to select these trusted entities from a group of nodes. Trust distribution mechanisms between the database services and its users need to be addressed as well.

Suitable ontologies for information gathering from different classes of component security metrics are needed. This is a challenging task and requires a rigorous analysis of the metrics to be used. In addition, information gathering ontologies for the purposes of estimation algorithms in Measurement Agents are needed.

As a long-time goal, general-level statistical knowledge has to be collected on: security algorithms, network products, user behavior, applications, experiences from virus and worm attacks, etc. – about all critical issues contributing to the overall level of security.

4 CONCLUSIONS AND FUTURE WORK

The emerging Semantic Web offers powerful tools for carrying out self-organized estimation of the security level in mobile and ubiquitous networks and their nodes. Semantically relevant security level information can be gathered and maintained in databases. Information gathering agents can gather information on, e.g., the traffic situation in the network, digital credentials, statistical knowledge of critical components of security, and research results that affect the level of security. Measurement Agents located in the network nodes can use the databases to estimate the security level from their point of view. Moreover, network-level security is increased due to the democratic voting mechanism of

independent measurement entities, each independently aiming at a higher security level in the network.

If we are able to develop intelligent and feasible ontologies for the information gathering, we might even learn more about the nature of security. In today's information technology world there is a lot of knowledge that just has to be combined in a suitable way to assess the overall security level, i.e. "find the forest from the trees." The current limited knowledge of the nature of security is hindering us from finding rigorous solutions to the aspects of overall security.

Our future work will include further exploration of component metric areas for mobile ad hoc networks and development of ontologies for information gathering and estimation processes. Our initial framework of security metrics will certainly be updated during the course of the research – we do not know *a priori* the compositional hierarchy of causalities in such a concept as security. Our future work will also include building an experimentation ubiquitous environment for analyzing the measurement method presented in this paper. It will be also possible to investigate trust establishment in this environment. Moreover, techniques for reducing the memory and computation resource needs of the approach are to be investigated.

REFERENCES

Berners-Lee, T., Hendler, J., and Lassila, O., 2001. The Semantic Web. *In Scientific American*, 284(5): 34-43.

Blaze, M., Feigenbaum, J., Ioannidis, J., and Keromytis, A. D., 1999. *The KeyNote Trust Management System, V 2*. IETF RFC 2704, Available at: www.ietf.org

Blaze, M., Feigenbaum, J., and Lacey, J., 1996. Decentralized Trust Management. In *Proceedings of IEEE Symposium on Security and Privacy*, 164-173.

Čapkun, S., Buttyán, L. and Hubaux, J-P., 20 03. Self-Organized Public-Key Management for Mobile Ad Hoc Networks. In *IEEE Transactions on Mobile Computing*, Vol. 2, No. 1, 52-64.

Chandrasekaran, B., Josephson, J.R., and Benjamins, V. R., 1999. What Are Ontologies, and Why Do We Need Them? In *IEEE Intelligent Systems*, Jan/Feb., 20-26.

Ellison, C., Frantz, B., Lampson, B., Rivest, R., Thomas, B., and Ylönen, T., 1999. *SPKI Certificate Theory*. IETF RFC 2693, Sep. Available at: www.ietf.org

Hendler, J., Berners-Lee, T., and Miller, Er., 2002. Integrating Applications on the Semantic Web. In *Journal of the Institute of Electrical Engineers of Japan*, Vol 122(10), October, p. 676-680.

Henning, R. (ed.), 2001. Workshop on Information Security Scoring and Ranking. Information System Security Attribute Quantification or Ordering.

Hubaux, J.-P., Buttyán, L., and Capkun, S., 2001. The Quest for Security in Mobile Ad Hoc Networks. In *Proceedings of the 2nd ACM International Symposium of Mobile Ad Hoc Networking and Computing (MobiHoc)*, 146-155.

Internet Engineering Task Force (IETF), 2004. *MANET Working Group.* Available at: www.ietf.org

ISO/IEC 21827. 2002. *Information Technology – Systems Security Engineering – Capability Maturity Model (SSE-CMM).*

Jelen, G., 2000. SSE-CMM Security Metrics. In *NIST and CSSPAB Workshop*, Washington, D.C..

Jonsson, E., 2003. *Dependability and Security Modelling and Metrics*, Lecture Slides, Chalmers University of Technology, Sweden.

Kagal, L., Finin, T., and Joshi, A., 2003. A Policy Language for a Pervasive Computing Environment. In *Proceedings of the 4th Int. Workshop on Policies for Distributed Systems and Networks (POLICY'03)*.

Li, N., Grosof, B. N., and Feigenbaum, J., 2003. Delegation Logic: A Logic-based Approach to Distribution Authorization. *In ACM Transactions on Information and System Security*, Vol. 6., No. 1., Feb., 128-171.

Luo, H., Zerfos, P., Kong, J., and Zhang, L., 2002. Self-Securing Ad Hoc Wireless Networks. In *Proceedings of the 7th Int. Symposium on Computers and Communications (ISCC)*, 567-574.

Savola, R., 2004. Estimation of the Security Level in Wireless E-Commerce Environment based on Ad Hoc Networks. In *Proceedings of the 5th European Conference E-COMM-LINE*, Bucharest, Romania, Oct. 21-22.

U.S. Department of Defense, 1985. *Trusted Computer System Evaluation Criteria (TCSEC)* "Orange Book", U. S. Department of Defense Standard, DoD 5200.28-std.

Winslett, M., Yu, T., Seamons, K. E., Hess, A., Jacobson, J., Jarvis, R., Smith, B., and Yu, L., 2002. Negotiating Trust on the Web. In *IEEE Internet Computing*, Nov/Dec, 30-37.

Yang, H., Luo, H., Ye, F., Lu, S., and Zhang, L., 2004. Security in Mobile Ad Hoc Networks: Challenges and Solutions. In *IEEE Wireless Communications*, Vol. 11, No.1, Feb., 38-47.

Zhou, L., and Haas, Z. J., 1999. Securing Ad Hoc Networks. In *IEEE Network Magazine*, Vol. 13, No. 6, Nov/Dec, 24-30.