Mapping Systems Security Research at Chalmers

M. Almgren, Z. Fu, E. Jonsson, P. Kleberger, A. Larsson,
F. Moradi, T. Olovsson, M. Papatriantafilou, L. Pirzadeh, and P. Tsigas
Department of Computer Science and Engineering
Chalmers University of Technology
SE–412 96 Gothenburg, Sweden

Abstract—**The department of Computer Science and Engineering at Chalmers University has a long tradition of research in systems security, including security metrics, attack detection, and mitigation. We focus on security issues arising in four specific environments: (1) backbone links, (2) sensor networks, (3) the connected car, and (4) the smart grid. In this short summary we describe recent results as well as open research questions we are exploring.**

I. Introduction

At the department of Computer Science and Engineering at Chalmers University, there is a long tradition of research in systems security.[1] More than two decades ago, we started to look at *security metrics* and modeling and today the research include attack detection and alert correlation as well as mitigation of, for example, Denial of Service attacks. We also have on-going projects focusing on systems security issues in four *specific environments*: (1) backbone links, where both efficiency of the algorithms as well as user privacy is of concern, (2) sensor networks with each node being limited in its capabilities, (3) the connected car, and (4) the smart grid. These areas will be further described below.

II. Security Metrics and Modeling

It has been claimed that going from qualitative to quantitative aspects is the way of progress for a scientific discipline [1]. The ultimate conclusion of this should be that science is not *real* science until it can be assessed in a quantitative way, i.e. measured. In particular, for security-related areas we will not be able to evaluate scientific progress properly until we can find metrics for it, including giving proper definitions and a clear-cut terminology.

In this way, our research in security metrics establishes a foundation for other research efforts within the department. The research effort started over two decades ago [2–4] and one notable result is a classification of intrusions with respect to technique as well as to result [5], derived from the traditional decomposition of security into three main aspects (“CIA”).

There exists a large number of suggestions for how to measure security, with different goals and objectives. In many cases the goal is to find a *single overall* metric of security. However, given that security is a complex and multi-faceted property, we believe that there are fundamental problems in finding such an overall metric. Thus, we are currently developing a framework for security metrics that is based on a number of system attributes taken from the security and the dependability disciplines [6]. Having metrics related to different types of attributes facilitates making quantitative assessment of the concept of combined security and dependability and improves our understanding of the underlying system properties.

III. Attack Detection and Protection Mechanisms

A. Intrusion Detection and Logging

It is difficult to build secure systems and, sometimes, legacy or operational constraints do not even allow the systems to be run in a secure fashion. The goal of an intrusion detection system (IDS) is to detect active misuse and attempts, either by legitimate users (“insiders”) or by external parties. Since the seminal paper by Denning [7], intrusion detection systems have seen a tremendous development in the type of data collected, the analysis, as well as the user interface [8]. However, these systems are still hampered by fundamental problems, such as the base-rate fallacy [9].

In our projects, we have looked at a range of issues relevant to intrusion detection systems. For example, it is critical to *log* the right type of data [10, 11], as well as being able to extract *attack manifestations* [12] in an efficient manner. An IDS needs data both to measure how well it is performing and to automatically learn to discriminate between attacks and normal behavior. For that reason we have presented a synthesized dataset for fraud detection systems [13] as well as investigated methods to reduce the amount of training data needed through the use of *active learning* [14]. We have also investigated complementary methods to collect data for an IDS [15] and proposed a multi-sensor model to improve the attack detection when using different types of sensors [16].

Currently, we are adapting some of the techniques described above to the *special environments* described below.

B. Mitigating Denial of Service Attacks

An important aspect of security for emergency preparedness is the availability of systems. We study methods to protect the network and applications against denial of service (DoS) attacks, i.e. attacks that overwhelm the system so that the normal requests cannot be answered. Attacks can be addressed in application-level and network-level.

Along the former type and by considering adversaries that can eavesdrop and launch directed DoS attacks to the

[1] Other types of security research at the department, such as *language-based security*, are not included in this summary.

applications' open ports, solutions based on pseudo-random port-hopping have been suggested [17]. In [18] we proposed a general method that can also be used for a group of processes, and not just a client-server pair, as was the case in the earlier work. In addition, our proposed solution tolerates time differences (in particular clock-drifts) between the nodes, which was earlier not known how to achieve.

DDoS attacks, i.e. distributed DoS attacks, are challenging not only for the targets of the attacks, but also for the network, as large volume of illegitimate traffic share the same network resources as legitimate traffic and can furthermore cause congestion phenomena and performance degradation. To mitigate that, the unwanted traffic needs to be controlled as close to the source(s) as possible. By building on earlier work and improving on distribution of control aspects, we proposed a proactive cluster-based method, which we call CluB , to mitigate DDoS attacks [19]. The method balances the effectiveness-overhead tradeoff by addressing the issue of granularity of control in the network. CluB can collaborate with different routing policies in the network, including contemporary datagram options. We have also studied ways to improve methods that use tokens to distinguish legitimate traffic. Our algorithm [20] reduces the effect of a particular form of attack (denial-of-capability, which applies to token-based methods for mitigation) [21]. With this algorithm, the legitimate hosts can get service with guaranteed probability.

As the above methods are complementary, we plan to continue on both approaches and to also study methods for integrating them. In particular, we are working on methods to adapt the port-hopping solutions [18], which are application-centered, to overlay networks, which are specialized networks defined and maintained by distributed applications (e.g. on-line social networks), with access control [19, 20]. Taking the Internet perspective, such overlays can be defined among participating routers, which may cooperate to achieve secure routing and to mitigate DDoS attacks.

IV. Focus on Specific Environments

A. Large-Scale Internet Backbone Traffic Analysis

Access to real-life large-scale datasets is in many cases crucial for understanding the true characteristics of network traffic, application behavior, and malicious behavior. However, the collection and the subsequent analysis of these datasets pose some special requirements. For example, *user privacy* is very important, and thus the data needs to be desensitized before being analyzed, a process that may influence the type of analysis method that can be used. The scale of the data also affects the collection of data and the analysis.

We have collected several large-scale datasets in a number of passive measurement projects on an Internet backbone link belonging to a national university network. The datasets have been used in different studies as part of the following projects.[2]

As part of the *MonNet project*, Internet backbone traffic was investigated to find malicious traffic in order to see how and to what extent protocols are abused. Initial studies investigated protocol features of packet headers [23] and packet header anomalies in order to discuss potential security problems, such as incorrect use of IP fragmentation [24].

The objective of the *Malbone project* is to measure and understand larger communication patterns among hosts over a longer time period. This may include normal as well as malicious behavior. Analysis in [25] spans from simple attribute aggregates (such as top IP and port numbers) to advanced temporal analysis of communication patterns between normal and malicious hosts.

The final project, the *AntiSpam project*, is focused on the problem of spam or unsolicited email. Email is probably one of the most popular application on the Internet, but spam is an increasing problem and has been estimated to cost businesses significant amounts of money. Current antispam tools are limited in that they only hide the spam from users' mailboxes. Therefore, we want to move the defense against spam as close to the spammers as possible in order to reduce problems such as the amount of unwanted traffic and waste of mail server resources. We are currently investigating spam detection through a social network based analysis (first proposed in [26]). Using e-mail addresses as nodes and letting edges symbolize any e-mail exchange, we have generated "email networks" using anonymized collected email traffic [27]. By focusing on structural and temporal properties of such networks, we have found several properties that are statistically different for spam and legitimate traffic. Deployment of these distinguishing characteristics for detection of spammers at the network level without a need to consult email contents is the subject of our ongoing research.

B. Sensor Networks

There are many promising application areas for wireless sensor networks. The possibilities span areas as civil security, health care, agriculture, research, environmental, commercial and military applications [28]. Security is critical for many applications of sensor networks, both due to sensitivity of data and the need to remain functional in presence of attacks. Wireless sensor networks come with additional security challenges, in large due to hardware limitations and the wireless communication medium [29, 30]. Malicious insider nodes are a serious threat due to the physical access of the nodes [31].

There are many services, several building upon each other, that are needed for wireless sensor network applications. Our aim is to provide such high level networking protocols for sensor networks and/or ad-hoc networks that are both secure and self-stabilizing. Self-stabilization lets nodes recover from arbitrary faults once conditions are back to normal. We take into account the serious threat of compromised nodes inside the network.

Accurate clock synchronization is imperative for many applications in sensor networks, such as mobile object tracking, detection of duplicates, and TDMA radio scheduling. In [32],

[2] More information about the data collection process and the collected datasets can be found in [22].

we presented the first secure and self-stabilizing algorithm for clock synchronization in sensor networks. Clustering organizes a network into groups that, e.g., can be used for forming backbones, for routing, for aggregating data, and for building hierarchies that allow for scaling. In [33], we presented the first self-stabilizing (k, r)-clustering algorithm for ad-hoc networks providing k cluster heads within r communication hops. Multiple paths are used to improve security, availability and fault tolerance. In [34] we provided the first security module providing symmetric key cryptography for the Contiki wireless sensor network operating system. We have also looked at the areas of routing and public key cryptography.

Going forward, we aim to secure additional fundamental network services. Routing is needed in any sensor network application that does not merely store sensor readings locally. Thus, to set up a secure sensor network, secure routing is one such needed service. Combining different protocols together into a secure and fault tolerant package for increased efficiency and ease of use would be fruitful. Additionally, it could cut down costs if different services could share mechanisms with each other and thus reduce the total amount of needed calculations and/or messages.

C. Securing the Connected Car

An upcoming trend in the automotive industry is to equip the vehicle with a wireless network gateway, enabling the vehicle to connect to an external network (i.e. Internet). The benefits from introducing such a connection are many, not only will there be new applications introduced for the driver and passengers, but there will also be a new possibility of performing remote diagnostics and issuing remote firmware updates over the air (FOTA) to the vehicle.

Introducing the connected car, communication with the Electronic Control Units (ECUs) in the in-vehicle network will be possible through a wireless network gateway. This communication will no longer require physical access to the vehicle and may be performed at any time. The wireless gateway may also be used for taking part in the emerging Vehicle-to-Vehicle (V2V) communication networks, where vehicles can exchange information with each other to, for example, increase traffic safety. Since the vehicle is a safety-critical system, and to ensure that the new external network traffic introduced in the in-vehicle network will not be a threat to the safety nor the security of the vehicle, necessary security mechanisms need to be in place. It has recently been shown that such mechanisms are still lacking for the vehicle setting [35].

Our research is focused towards securing the in-vehicle network and the communication with the connected car, so that services to future vehicles can be provided in a secure and safe manner. One of the main research focus is to provide a secure infrastructure for remote diagnostics and software updates over a wireless link. In [36] we presented a set of guidelines for such a wireless infrastructure.

A defense-in-depth approach to address the security needs has also been proposed, where we look at methods for prevention, detection, deflection and forensics [37]. Furthermore, the Controller Area Network (CAN) and FlexRay-protocols used in the in-vehicle network has been evaluated with respect to a set of security properties [38, 39].

Some general challenges for applying security mechanisms to the connected car are the limited resources available in processing power and memory, cost sensitivity and the lifetime of the solution as the vehicle can be used for many years.

A complete security architecture for the connected car is still missing, and we intend to continue contributing in defining one.

D. Security Issues in the Smart Grid

The Smart Grid is being promoted on both sides of the Atlantic as the way to solve problems in energy production, distribution, and consumption in the future. The definition of what the smart grid exactly will entail varies depending on perspective, but its main idea is to allow two-way communication of both power and data between devices, thus allowing for a more adaptive and effective way to utilize energy. However, a documented consequence is that new vulnerabilities are appearing[3] and some "features" have large security implications [40]. Given that electricity is required for many other critical services in society, any security vulnerability within this software-intensive critical system will attract attention from hostile groups or organized crime.

We have investigated open security issues in a wide range of critical systems [41] and are currently looking especially at the issues within the smart grid [42]. Among the security challenges of the smart grid is the sheer scale of the deployment and that any vulnerability may have a very large impact on society as a whole. Among our recent work, we have considered the *optimal power flow* (OPF) problem as a minimum cost flow and applied a cost-scaling push-relabel algorithm in order to solve the OPF in a distributed agent environment [43]. We are also investigating issues related to the advanced metering infrastructure (AMI).

V. Conclusion

In this short summary, we have described the research related to systems security at the department of Computer Science and Engineering at Chalmers University. We have focused on current projects but also included a discussion of research topics we are actively exploring.

Acknowledgment

This work was supported by the Swedish Civil Contingencies Agency (MSB), the .SE - The Internet Infrastructure Foundation, and the SIGYN II project (2009-01722) cofunded by VINNOVA, the Swedish Governmental Agency for Innovation Systems. The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 257007.

[3] http://edition.cnn.com/2009/TECH/03/20/smartgrid.vulnerability/index.html

References

[1] M. Bunge, *Scientific Research. Strategy and Philosophy.* Berlin: Springer-Verlag, 1967.

[2] E. Jonsson, M. Andersson, and S. Asmussen, “An attempt to quantitative modeling of behavioural security,” in *Proc. 11th International Information Security Conference (IFIP/SEC’95), Cape Town, South Africa*, 1995.

[3] E. Jonsson, L. Strömberg, and S. Lindskog, “On the functional relation between security and dependability impairments,” in *ACM New Security Paradigms Workshop, (NSPW 1999), Caledon Hills, Canada*, Sep. 1999.

[4] S. Brocklehurst, B. Littlewood, T. Olovsson, and E. Jonsson, “On measurement of operational security,” in *COMPASS ’94, Proceedings of the Ninth Annual Conference on Computer Assurance*. Gaithersburg: IEEE Computer Society, 1994, pp. 257–266, ISBN 0-7803-1855-2.

[5] U. Lindqvist and E. Jonsson, “How to systematically classify computer security intrusions,” in *Security and Privacy, 1997. Proceedings., 1997 IEEE Symposium on*, May 1997, pp. 154 –163.

[6] E. Jonsson, “Towards an integrated conceptual model of security and dependability,” in *Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on*, Apr. 2006, p. 8 pp.

[7] D. E. Denning, “An intrusion-detection model,” *IEEE Transactions on Software Engineering*, vol. SE-13, no. 2, pp. 222–232, Feb. 1987.

[8] M. Almgren and E. Jonsson, “Tuning an IDS – learning the user’s preferences,” in *11th Nordic Workshop on Secure IT Systems (NordSec 2006)*, V. Fåk, Ed. Linköping university, Sweden: Published by Linköping university, Sweden, Oct. 19–20, 2006, pp. 43–52.

[9] S. Axelsson, “The base-rate fallacy and its implications for the difficulty of intrusion detection,” in *Proceedings of the 6th ACM Conference on Computer and Communications Security*, Kent Ridge Digital Labs, Singapore, November 1999.

[10] S. Axelsson, U. Lindqvist, U. Gustafson, and E. Jonsson, “An approach to UNIX security logging,” in *Proceedings of the 21st National Information Systems Security Conference*. Arlington, Virginia: National Institute of Standards and Technology/National Computer Security Center, Oct. 5–8, 1998, pp. 62–75.

[11] E. Lundin Barse, “Logging for intrusion and fraud detection,” Ph.D. dissertation, Chalmers University of Technology, 2004.

[12] U. Larson, E. Lundin Barse, and E. Jonsson, “METAL - a tool for extracting attack manifestations,” in *Proceedings of Detection of Intrusions and Malware & Vulnerability Assessment workshop (DIMVA)*, Vienna, Austria, July 7-8 2005.

[13] E. Lunding Barse, H. Kvarnström, and E. Jonsson, “Synthesizing test data for fraud detection systems,” in *19th Annual Computer Security Applications Conference (ACSAC ’03)*. Published by the IEEE Computer Society, 2003.

[14] M. Almgren and E. Jonsson, “Using active learning in intrusion detection,” in *17th IEEE Computer Security Foundations Workshop (CSFW 2004)*. Asilomar, USA: IEEE Computer Society, Jun. 28–30, 2004, pp. 88–98.

[15] M. Almgren and U. Lindqvist, “Application-integrated data collection for security monitoring,” in *Recent Advances in Intrusion Detection (RAID 2001)*, ser. LNCS, W. Lee, L. Mé, and A. Wespi, Eds., vol. 2212. Davis, California: Springer-Verlag, Oct. 10–12, 2001, pp. 22–36.

[16] M. Almgren, U. Lindqvist, and E. Jonsson, “A multi-sensor model to improve automated attack detection,” in *Recent Advances in Intrusion Detection (RAID 2008)*, ser. LNCS, R. Lippmann, E. Kirda, and A. Trachtenberg, Eds., vol. 5230. Cambridge, MA, USA: Springer-Verlag, Sep. 15–17, 2008, pp. 291–310.

[17] G. Badishi, A. Herzberg, and K. Idit, “Keeping denial-of-service attackers in the dark,” *Dependable and Secure Computing, IEEE Transactions on*, vol. 4, no. 3, pp. 191–204, 2007.

[18] Z. Fu, M. Papatriantafilou, and P. Tsigas, “Mitigating distributed denial of service attacks in multiparty applications in the presence of clock drifts,” *Reliable Distributed Systems, 2008. SRDS’08. IEEE Symposium on*, pp. 63–72, 2008.

[19] Z. Fu, , M. Papatriantafilou, and P. Tsigas, “Club: A cluster based method for mitigating distributed denial of service attacks,” in *26th Annual ACM Symposium On Applied Computing*. ACM Press, 2011.

[20] Z. Fu, M. Papatriantafilou, P. Tsigas, and W. Wei, “Mitigating denial of capability attacks using sink tree based quota allocation,” *Proceedings of the 2010 ACM Symposium on Applied Computing*, pp. 713–718, 2010.

[21] K. Argyraki and D. Cheriton, “Network capabilities: The good, the bad and the ugly,” *ACM HotNets-IV*, 2005.

[22] F. Moradi, M. Almgren, W. John, T. Olovsson, and P. Tsigas, “On collection of large-scale multi-purpose datasets on internet backbone links,” in *Workshop on development of large scale security-related data collection and analysis initiatives (BADGERS 2011)*, 2011.

[23] W. John and S. Tafvelin, “Analysis of internet backbone traffic and header anomalies observed,” in *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*, ser. IMC ’07, 2007, pp. 111–116.

[24] W. John and T. Olovsson, “Detection of malicious traffic on backbone links via packet header analysis,” *Campus-Wide Information Systems*, vol. 25, no. 5, 2008.

[25] M. Almgren and W. John, “Tracking malicious hosts on a 10gbps backbone link,” in *15th Nordic Conference in Secure IT Systems (NordSec 2010)*, 2010.

[26] P. O. Boykin and V. P. Roychowdhury, “Leveraging social networks to fight spam,” *Computer*, vol. 38, no. 4, 2005.

[27] F. Moradi, T. Olovsson, and P. Tsigas, “Analyzing the social structure and dynamics of e-mail and spam in massive backbone internet traffic,” Chalmers University of Technology, no. 2010-03, Tech. Rep., 2010.

[28] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A survey on sensor networks,” *Communications Magazine, IEEE*, vol. 40, no. 8, pp. 102 – 114, Aug. 2002.

[29] E. Shi and A. Perrig, “Designing secure sensor networks,” *Wireless Communications, IEEE*, vol. 11, no. 6, pp. 38 – 43, dec. 2004.

[30] X. Chen, K. Makki, K. Yen, and N. Pissinou, “Sensor network security: a survey,” *Communications Surveys Tutorials, IEEE*, vol. 11, no. 2, pp. 52 –73, 2009.

[31] ——, “Node compromise modeling and its applications in sensor networks,” in *Computers and Communications, 2007. ISCC 2007. 12th IEEE Symposium on*, Jul. 2007, pp. 575 –582.

[32] J.-H. Hoepman, A. Larsson, E. M. Schiller, and P. Tsigas, “Secure and self-stabilizing clock synchronization in sensor networks,” in *Prooceedings of the 9th Scandinavian Workshop on Wireless Ad-hoc Networks (Adhoc 2009)*, 05 2009, pp. 78 – 82.

[33] A. Larsson and P. Tsigas, “Self-stabilizing (k,r)-clustering in wireless adhoc networks with multiple paths,” in *OPODIS’10, 14th International Conference On Principles Of Distributed Systems*, Tozeur, Tunisia, December 2010.

[34] L. Casado and P. Tsigas, “Contikisec: A secure network layer for wireless sensor networks under the contiki operating system,” in *Proceedings of the 14th Nordic Conference on Secure IT Systems: Identity and Privacy in the Internet Age*, ser. NordSec ’09. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 133–147.

[35] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, “Experimental Security Analysis of a Modern Automobile,” in *Proceedings of the 31st IEEE Symposium on Security and Privacy (SP)*, 2010, pp. 447–462.

[36] D. K. Nilsson, U. E. Larson, and E. Jonsson, “Creating a Secure Infrastructure for Wireless Diagnostics and Software Updates in Vehicles,” in *Proceedings of the 27th International Conference on Computer Safety, Reliability, and Security (SAFECOMP)*, ser. LNCS, vol. 5219. Newcastle upon Tyne, UK: Springer-Verlag, Sep. 2008, pp. 207–220.

[37] D. K. Nilsson and U. E. Larson, “A Defense-in-Depth Approach to Securing the Wireless Vehicle Infrastructure,” *Journal of Networks*, vol. 4, no. 7, pp. 552–564, Sep. 2009.

[38] ——, “Simulated Attacks on CAN Buses: Vehicle Virus,” in *Proceedings of the 5th IASTED Conference on Communication Systems and Networks (ASIACSN)*. Langkawi, Malaysia: IASTED, Apr. 2-4 2008.

[39] D. K. Nilsson, U. E. Larson, F. Picasso, and E. Jonsson, “A First Simulation of Attacks in the Automotive Network Communications Protocol FlexRay,” in *Proc. of the 1st International Workshop on Computational Intelligence in Security for Information Systems (CISIS)*. Springer, 2008.

[40] F. Cohen, “The smarter grid,” in *Proceedings of IEEE Symposium on Security and Privacy*, vol. 8, 2010, pp. 60–63.

[41] FORWARD Consortium, “Forward white book: Emerging ICT threats,” http://www.ict-forward.eu/media/publications/forward-whitebook.pdf, Jan. 2010.

[42] SysSec Consortium, “Syssec: Managing threats and vulnerabilities in the future internet,” http://www.syssec-project.eu, Mar. 2011.

[43] P. Nguyen, W. Kling, G. Georgiadis, M. Papatriantafilou, and L. Bertling, “Distributed routing algorithms to manage power flow in agent-based active distribution network,” in *Innovative Smart Grid Technologies Conference Europe (ISGT Europe), 2010 IEEE PES*, 2010.