[1] L. Briesemeister, G. Denker, D. Elenius, I. Mason, S. Varadarajan, D. Bhatt, B. Hall, G. Madl, and W. Steiner. Quantitative fault propagation analysis for networked cyber-physical systems. In *2nd Analytic Virtual Integration of Cyber-Physical Systems Workshop (AVICPS)*, Nov. 2011. [bib | .pdf]

This paper presents an approach to analyzing a model of networked cyber-physical systems for fault propagation. We present an implementation of a probabilistic logic model, which allows for reasoning via symbolic evaluation as well as numeric evaluation to perform a quantitative fault analysis. Our models are built from a few building blocks, which can be instantiated as standard or high integrity; communication paths can be made redundant, and finally, whole subsystem blocks can be replicated. We assume an underlying networking infrastructure of TTEthernet, which allows traffic of time-triggered, rate-constrained, or best-effort modes with different safety features. We apply our approach to a case study of a brake-by-wire system that contains communication flows with different traffic modes according to their criticality.

[2] L. Briesemeister, S. Cheung, U. Lindqvist, and A. Valdes. Detection, correlation, and visualization of attacks against critical infrastructure systems. In *8th International Conference on Privacy, Security and Trust (PST)*, Aug. 2010. [bib | .pdf]

Digital control systems are essential to the safe and efficient operation of a variety of industrial processes in sectors such as electric power, oil and gas, water treatment, and manufacturing. Modern control systems are increasingly connected to other control systems as well as to corporate systems. They are also increasingly adopting networking technology and system and application software from conventional enterprise systems. These trends can make control systems vulnerable to cyber attack, which in the case of control systems may impact physical processes causing environmental harm or injury.

We present some results of the DATES (Detection and Analysis of Threats to the Energy Sector) project, wherein we adapted and developed several intrusion detection technologies for control systems. The suite of detection technologies was integrated and connected to a commercial security event correlation framework from ArcSight. We demonstrated the efficacy of our detection and correlation solution on two coupled testbed environments. We particularly focused on detection, correlation, and visualization of a network traversal attack, where an attacker penetrates successive network layers to compromise critical assets that directly control the underlying process. Such an attack is of particular concern in the layered architectures typical of control system implementations.

Keywords: critical infrastructure security; control system security; intrusion and anomaly detection; alert correlation; security information event management

[3] L. Briesemeister, S. Dawson, P. Lincoln, H. Saidi, J. Thornton, G. Durfee, P. Kwan, E. Stinson, A. J. Oliner, and J. C. Mitchell. Homogeneity as an advantage: It takes a community to protect an application. In *Workshop on Collaborative Methods for Security and Privacy (CollSec)*, Aug. 2010. [bib | .pdf]

We examine how to turn the scale of a large homogeneous software deployment from an operational and security disadvantage into an advantageous application community that can detect, diagnose, and recover from its own operational faults and malicious attacks. We propose a system called VERNIER that provides a virtualized execution environment in conjunction with collaborative diagnosis and response functions using a knowledge-sharing infrastructure. We report on the preliminary implementation of the system, its experimental evaluation, and lessons learned during development.

[4] L. Briesemeister and P. A. Porras. Formally specifying design goals of worm defense strategies. Proceedings of DETER Community Workshop on Cyber Security Experimentation and Test, June 2006. Extended Abstract. [bib | .pdf]

[5] L. Briesemeister and P. A. Porras. Automatically deducing propagation sequences that circumvent a collaborative worm defense. In *Proceedings of the 25th International Performance Computing and Communications Conference (Workshop on Malware)*, pages 587-592, April

2006. [bib | .pdf]

We present an approach to the question of evaluating worm defenses against future, yet unseen, and possibly defense-aware worm behavior. Our scheme employs model checking to produce worm propagation sequences that defeat a worm defense of interest. We demonstrate this approach using an exemplar collaborative worm defense, in which LANs share alerts about encountered infections. Through model checking experiments, we then generate propagation sequences that are able to infect the whole population in the modeled network. We discuss these experimental results and also identify open problems in applying formal methods more generally in the context of worm quarantine research.

[6] L. Briesemeister, P. A. Porras, and A. Tiwari. Model checking of worm quarantine and counter-quarantine under a group defense. Technical Report SRI-CSL-05-03, SRI International, Computer Science Laboratory, October 2005. [bib | http | .pdf]

We consider what it means to perform worm quarantine across a network with an emerging self-propagating worm outbreak. It is generally understood that an effective quarantine defense can under certain conditions reduce the infection growth rate, and ideally can prevent a worm from reaching its full saturation potential. This report attempts to more precisely define the desired properties of a quarantine algorithm, and suggest different forms of quarantine properties that vary in their ability to isolate infected nodes, ensure the existence of an uninfected population, and guarantee some persistent protection, no matter how the worm behaves. We employ the SAL formal modeling language and model checker to investigate these properties on a specific group-based quarantine algorithm. In addition to answering questions regarding algorithm correctness and validating some quarantine properties, the model checker disproves other quarantine properties. The proofs and counter-examples produced during this process help in algorithm design and may be useful in informing simulation experiments or building test cases. Using a game theoretic approach, counter-examples of a win scenario for the defense yield insight into smart worm behavior that defeats a known quarantine defense.

[7] M. Knapp, L. Briesemeister, S. Eker, P. Lincoln, A. Poggio, C. Talcott, and K. Laderoute. Pathway logic: Helping biologists understand and organize pathway information. In *IEEE Computational Systems and Bioinformatics Conference (CSB)*, Workshops and Poster Abstracts, pages 155-156. IEEE Computer Society, August 2005. [bib | .pdf]

[8] L. Briesemeister and P. Porras. Microscopic simulation of a group defense strategy. In *Proceedings of Workshop on Principles of Advanced and Distributed Simulation (PADS)*, pages 254-261, June 2005. [bib | DOI | .pdf]

We introduce a novel worm containment strategy that integrates two complementary worm quarantine techniques. The two techniques are linked, with one strategy employing the other as an indicator of worm infection. A group defense mechanism shares such indicators among neighboring networks, and when enough corroboration occurs, the network engages in traffic filtering to halt infection attempts.

We present an SSFnet-based microscopic simulation of the containment strategy against random scan worms, and explore various performance characteristics of the group defense mechanism. The simulation results help to characterize the conditions and degree to which the integrated quarantine strategy can both slow worm propagation and prevent the worm from reaching its full saturation potential.

[9] P. Porras, L. Briesemeister, K. Skinner, K. Levitt, J. Rowe, and Y.-C. A. Ting. A hybrid quarantine defense. In *Proceedings of the 2004 ACM Workshop on Rapid Malcode (WORM)*, pages 73-82, October 2004. [bib | DOI | .pdf]

We study the strengths, weaknesses, and potential synergies of two complementary worm quarantine defense strategies under various worm attack profiles. We observe their abilities to delay or suppress infection growth rates under two propagation techniques and three scan rates, and explore the potential synergies in combining these two complementary quarantine strategies. We compare the performance of the individual strategies against a hybrid combination strategy, and conclude that the hybrid strategy yields substantial performance improvements, beyond what either technique provides independently. This result offers potential new directions in hybrid quarantine defenses.

[10] L. Briesemeister, P. Lincoln, and P. Porras. Epidemic profiles and defense of scale-free networks. In *Proceedings of the 2003 ACM Workshop on Rapid Malcode (WORM)*, pages 67-75, October 2003. [bib | DOI | .pdf]

In this paper, we study the defensibility of large scale-free networks against malicious rapidly self-propagating code such as worms and viruses. We develop a framework to investigate the profiles of such code as it infects a large network. Based on these profiles and large-scale network percolation studies, we investigate features of networks that render them more or less defensible against worms. However, we wish to preserve mission-relevant features of the network, such as basic connectivity and resilience to normal nonmalicious outages. We aim to develop methods to help design networks that preserve critical functionality and enable more effective defenses.

[11] L. Briesemeister. Sensor data dissemination through ad hoc battlefield communications. In *Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS)*, Jan. 2003. [bib | .ps | .pdf]

We study the dissemination of sensor data (reports) from the sensor network to the mobile ground forces (soldiers) for sensor gateways deployed in a battlefield scenario. Our approach looks at both the addressing and distribution of sensor reports. First, we employ a subscription mechanism in which the sensor gateways address their reports to those soldiers who have currently subscribed to them. Second, we distinguish two schemes for propagating sensor reports. In a centralized approach, all sensor reports must go through one designated node (command post). In a distributed approach, the network routes sensor reports directly to the soldiers. In a generic soldier mobility model, soldiers move in small groups (squads) along a line to random destinations on the battlefield. Through simulations using this mobility model, we study the performance and overhead of the proposed methods for sensor data dissemination. We envision this research to be the first of a series of methods to manage information within mobile networks comprised of sensors and actuators in battlefield scenarios.

[12] L. Briesemeister and G. Hommel. Localized group membership service for ad hoc networks. In *Proceedings of International Workshop on Ad Hoc Networking (IWAHN)*, pages 94-100, Aug. 2002. [bib | .pdf]

We present a specification for a new, localized group membership service that maintains the membership status of adjacent nodes - called neighbors - in a mobile distributed system. The service builds on top of a neighborhood service which employs a simple heartbeat mechanism to discover and track neighbors in the mobile network. Both services assume unreliable communication as found in the wireless environment. No knowledge of the network topology is presumed.

We impose a deadline for installing views of the membership to force timely deciding protocols. We give a simple implementation of the neighborhood and the group membership service. If the deadline of view installations is at least the heartbeat rate, we can prove the correctness of our suggested implementation. An application in mobile ad hoc networking exemplifies potential areas of deployment for a localized group membership service.

[13] L. Briesemeister and G. Hommel. Integrating simple yet robust protocol layers for wireless ad hoc intervehicle communications. In *Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS)*, pages 186-192, Jan. 2002. [bib | .pdf]

We present an approach to simulating ad hoc network protocols integrated with their intended application. We implement the protocol layers and the application using the Specification and Description Language (SDL). Then, we simulate the ad hoc network directly from the SDL model. Using the interface of the SDL software tool, we incorporate the mobility model for hosts described in trace files.

We suggest applying mobile ad hoc networks to communicating vehicles in road traffic. As an example, we look at vehicles exchanging messages to detect traffic jams on highways. Simulations of this application in a realistic traffic scenario demonstrate the powerful effect and robustness of rather simple, distributed protocols communicating through a mobile ad hoc network.

[14] L. Briesemeister. *Group Membership and Communication in Highly Mobile Ad Hoc Networks*. PhD thesis, School of Electrical Engineering and Computer Science, Technical University of Berlin, Germany, Nov. 2001. [bib | http | .pdf]

This thesis proposes the use of a new routing paradigm to enable communication in highly mobile, ad hoc networks, which operate wirelessly in the absence of dedicated master stations or fixed infrastructure. Due to the mobility of the nodes, the network topology changes frequently and unpredictably.

We explore the new routing paradigm in the context of inter-vehicle communication. In such highly mobile ad hoc networks, the nodes commonly do not know the identity of their communication partners in advance. Rapid topology changes and scarce bandwidth prevent the nodes from exchanging updates regularly throughout the network. Therefore, we advocate a new routing paradigm that implicitly addresses message destinations based on the current situation of the network.

The originator of a message uses scoped and controlled flooding to reach the destinations. The receivers of the flooded message use their knowledge of the local environment to decide whether they match the intended destination of the message. Furthermore, we tailor the routing algorithm to overcome the problem of fragmentation in sparsely connected networks.

Our routing algorithm requires the mobile nodes to aggregate into a dynamic group. Being aware of the severe conditions inherent to ad hoc networks, we suggest a new, localized group membership service in which nodes track the membership only of adjacent nodes.

To evaluate our communication system, we simulate the mobile ad hoc network applied to a highway traffic jam scenario. We introduce several metrics to measure the performance of each implementation layer. The results of the simulations demonstrate the powerful effect of rather simple, distributed protocols communicating through a mobile ad hoc network and interacting in a realistic environment.

[15] L. Briesemeister. Localized group membership in highly mobile ad hoc networks. Poster at Second International Workshop on Networked Group Communication, Nov. 2000. (Be aware: poster in A0 format; set custom width/height of ghostview to 2500/3500 and zoom out). [bib | .pdf]

In inter-vehicle communication, vehicles in road traffic are equipped with a radio modem allowing them to contact other equipped vehicles in their vicinity. By acquiring and exchanging information, vehicles build knowledge about the local traffic situation which can improve comfort and safety in driving. As an example, vehicles inside a traffic jam learn about the current size and position of the congestion. Such information can yield up-to-date navigation guidance and also prevent fast vehicles from colliding with the stopped vehicles.

The vehicles form a mobile ad hoc network which consists of highly mobile hosts that communicate via wireless links. Due to mobility, the topology of the network changes continuously and wireless links break down and reestablish frequently. Moreover, the ad hoc network operates in the absence of a fixed infrastructure forcing the hosts to organize the exchange of information decentrally. In this poster, we describe the formal system model and a localized group membership service for such an ad hoc network.

[16] L. Briesemeister, L. Schäfers, and G. Hommel. Disseminating messages among highly mobile hosts based on inter-vehicle communication. In *IEEE Intelligent Vehicles Symposium*, pages 522-527, Oct. 2000. [bib | .pdf]

We present an approach to distributing messages among highly mobile hosts in ad hoc networks. We focus on using direct radio communication between moving vehicles on the road that requires no additional infrastructure. Thus, the vehicles need to organize access to the radio channel in a decentralized manner. We derive the medium access control from the standard IEEE 802.11. Also, the vehicles use omnidirectional antennas implying that a sender can transmit to multiple hosts simultaneously. As an example, we study a road accident that is reported to nearby vehicles. Simulations show us the quality of the proposed protocol by measuring how many vehicles inside a

zone-of-relevance are informed under various conditions.

[17] L. Briesemeister and G. Hommel. Overcoming fragmentation in mobile ad hoc networks. *Journal of Communications and Networks.*, 2(3):182-187, Sept. 2000. ISSN 1229-2370. [bib | .pdf]

We present an approach to multicast messages among highly mobile hosts in ad hoc networks. We suggest a new definition of a multicast that suits the special needs of inter-vehicle communication: Rather than explicit identification, a multicast group is defined implicitly by location, speed, driving direction and time. As an example, we study a road accident that is reported to nearby vehicles. We focus on sparse deployment of the system which is likely to occur soon after the system is introduced to the market. In this state, the resulting ad hoc network tends to be disconnected. We tailor the proposed algorithm to overcome this problem of network fragmentation. Simulations show us the quality of the proposed protocol by measuring how many vehicles inside a multicast area are informed in time under various conditions.

[18] L. Briesemeister and G. Hommel. Role-based multicast in highly mobile but sparsely connected ad hoc networks. In *Proceedings of the 1st ACM International Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc)*, pages 45-50. IEEE Press, Aug. 2000. [bib | .pdf]

We present an approach to multicasting messages among highly mobile hosts in ad hoc networks. We suggest a new definition of a role-based multicast that suits the special needs of inter-vehicle communication: Rather than by explicit identification, a multicast group is defined implicitly by location, speed, driving direction and time. As an example, we study a road accident that is reported to nearby vehicles. We focus on sparse deployment of the system which is likely to occur soon after the system is introduced to the market. In this state, the resulting ad hoc network tends to be disconnected. We tailor the proposed algorithm to overcome this problem of network fragmentation. Simulations show us the quality of the proposed protocol by measuring how many vehicles inside a multicast area are informed in time under various conditions.

[19] L. Briesemeister. Funkkommunikation zwischen Fahrzeugen zur Gefahrenwarnung im Strassenverkehr. Master's thesis, Technical University of Berlin, Department of Computer Science, Germany, Mar. 1998. [bib | http]

Diese Arbeit beschäftigt sich mit der Kommunikation geringer Reichweite zwischen mobilen Einheiten am Beispiel kommunizierender Fahrzeuge im Strassenverkehr. Dazu wird zunächst der Stand der Forschung auf diesem Gebiet dargestellt. Die Anforderungen an ein Kommunikationssytem für die Gefahrenwarnung im Strassenverkehr werden abgeleitet. Daraus wird ein Lösungsvorschlag mittels bekannter und modifizierter Algorithmen entwickelt. Der Lösungsvorschlag wird in bezug auf das verwendete Kanalzugriffsverfahren analysiert. Gütekriterien für die Anwendung zur Gefahrenwarnung werden motiviert und formalisiert. Der Weg zur Bewertung des System anhand dieser Gütekriterien wird aufgezeigt.

[20] L. Briesemeister, T. Scheffer, and F. Wysotzki. A concept formation based algorithmic model for skill acquisition. In *First European Workshop on Cognitive Modeling*, Nov. 1996. [bib | .ps]

We present an algorithmic model for acquisition of cognitive skills that is based on machine learning and problem solving algorithms. The principle is to use a problem solving approach for new problems that are not covered by the routine knowledge obtained from generalizing previous samples, and to use a machine learning algorithm to generalize these samples to an abstraction of the state space. We show the admissibility of our approach, discuss complexity results and present empirical results for Rubik's cube and a maze problem.

[21] L. Briesemeister and B. van Schewick. Grundlagen der Wahrscheinlichkeitsrechnung und Statistik. Seminar Methoden der Mustererkennung und Klassifikation at Department of Computer Science, Technical Unversity of Berlin, Nov. 1995. [bib | .pdf]

[22] L. Briesemeister, B. van Schewick, and T. Scheffer. Combination of problem solving and learning from experience (extended abstract). Technical Report 20/95, Department of Computer

Science, Technical University of Berlin, 1995. [bib | .pdf]

This file was generated by bibtex2html 1.96.