[1] R. Berthier and W. Sanders. Specification-based intrusion detection for advanced metering infrastructures. In *17th Pacific Rim International Symposium on Dependable Computing (PRDC)*, pages 184-193, Dec. 2011. [bib | DOI]

It is critical to develop an effective way to monitor advanced metering infrastructures (AMI). To ensure the security and reliability of a modernized power grid, the current deployment of millions of smart meters requires the development of innovative situational awareness solutions to prevent compromised devices from impacting the stability of the grid and the reliability of the energy distribution infrastructure. To address this issue, we introduce a specification-based intrusion detection sensor that can be deployed in the field to identify security threats in real time. This sensor monitors the traffic among meters and access points at the network, transport, and application layers to ensure that devices are running in a secure state and their operations respect a specified security policy. It does this by implementing a set of constraints on transmissions made using the C12.22 standard protocol that ensure that all violations of the specified security policy will be detected. The soundness of these constraints was verified using a formal framework, and a prototype implementation of the sensor was evaluated with realistic AMI network traffic.

Keywords: Authentication;Intrusion detection;Monitoring;Protocols;Reliability;Timing;automatic meter reading;computer network security;formal specification;power distribution reliability;power meters;power system measurement;power system security;sensors;smart power grids;transport protocols;AMI network traffic;C12.22 standard protocol;access points;advanced metering infrastructure;energy distribution infrastructure reliability;innovative situational awareness solutions;modernized power grid security;security policy;security threat identify;sensor;smart meters;specification based intrusion detection;traffic monitoring;AMI;formal method;intrusion detection;specification-based security;

[2] B. Kordy, S. Mauw, S. Radomirović, and P. Schweitzer. Foundations of attack-defense trees. In *Formal Aspects of Security and Trust*, volume 6561 of *Lecture Notes in Computer Science*, pages 80-95. 2011. [bib | DOI]

We introduce and give formal definitions of attackâ€“defense trees. We argue that these trees are a simple, yet powerful tool to analyze complex security and privacy problems. Our formalization is generic in the sense that it supports different semantical approaches. We present several semantics for attackâ€“defense trees along with usage scenarios, and we show how to evaluate attributes.

[3] B. Kordy, M. Pouly, and P. Schweitzer. Computational aspects of attack-defense trees. In *Security and Intelligent Information Systems*, volume 7053 of *Lecture Notes in Computer Science*, pages 103-116. 2012. [bib | DOI]

Attackâ€“defense trees extend attack trees with defense nodes. This richer formalism allows for a more precise modeling of a system's vulnerabilities, by representing interactions between possible attacks and corresponding defensive measures. In this paper we compare the computational complexity of both formalisms. We identify semantics for which extending attack trees with defense nodes does not increase the computational complexity. This implies that, for these semantics, every query that can be solved efficiently on attack trees can also be solved efficiently on attackâ€“defense trees. Furthermore, every algorithm for attack trees can directly be used to process attackâ€“defense trees.

[4] D. Mougouei, M. Moghtadaei, and S. Moradmand. A goal-based modeling approach to develop security requirements of fault tolerant security-critical systems. In *International Conference on Computer and Communication Engineering (ICCCE)*, pages 200-205, July 2012. [bib | DOI]

Large amount of (security) faults existing in software systems could be complex and hard to identify during the fault analysis. So, it is not always possible to fully mitigate the internal or external security faults (vulnerabilities or threats) within the system. On the other hand, existence of faults in the system may eventually lead to a security failure. To avoid security failure of the target system we need to make it flexible and tolerant in the presence of security faults. This paper introduces a goal-based modeling approach to develop security requirements of security-critical systems (SCSs) by explicitly factoring the faults into the requirement engineering process. Our approach establishes a

model for security requirements (SRM) with respect to the formally described model of security faults (SFM). We care for fault tolerance in SRM by taking into consideration partial satisfaction of security goals. The proposed approach factors this partiality into the goals by applying proper mitigation techniques during the refinement process. This eventually contributes to a fault tolerant model for security requirements of the target system.

Keywords: Analytical models;Computational modeling;Fault diagnosis;Fault tolerance;Fault tolerant systems;Security;Unified modeling language;fault tolerance;security of data;software engineering;fault analysis;fault tolerant model;fault tolerant security critical systems;goal based modeling approach;refinement process;security failure;security faults;security requirements;software systems;intrusion tolerance;security fault;threat;vulnerability;

[5] X. Ou, S. Govindavajhala, and A. W. Appel. MulVAL: a logic-based network security analyzer. In *Proceedings of the 14th USENIX Security Symposium*, 2005. [bib | http]

To determine the security impact software vulnerabilities have on a particular network, one must consider interactions among multiple network elements. For a vulnerability analysis tool to be useful in practice, two features are crucial. First, the model used in the analysis must be able to automatically integrate formal vulnerability specifications from the bug-reporting community. Second, the analysis must be able to scale to networks with thousands of machines.

We show how to achieve these two goals by presenting MulVAL, an end-to-end framework and reasoning system that conducts multihost, multistage vulnerability analysis on a network. MulVAL adopts Datalog as the modeling language for the elements in the analysis (bug specification, configuration description, reasoning rules, operating-system permission and privilege model, etc.). We easily leverage existing vulnerability-database and scanning tools by expressing their output in Datalog and feeding it to our MulVAL reasoning engine. Once the information is collected, the analysis can be performed in seconds for networks with thousands of machines.

We implemented our framework on the Red Hat Linux platform. Our framework can reason about 84% of the Red Hat bugs reported in OVAL, a formal vulnerability definition language. We tested our tool on a real network with hundreds of users. The tool detected a policy violation caused by software vulnerabilities and the system administrators took remediation measures.

[6] W. Pieters, T. Dimkov, and D. Pavlovic. Security policy alignment: A formal approach. *IEEE Systems Journal*, PP(99):1, 2012. [bib | DOI]

Security policy alignment concerns the matching of security policies specified at different levels in socio-technical systems, and delegated to different agents, technical and human. For example, the policy that sales data should not leave an organization is refined into policies on door locks, firewalls and employee behavior, and this refinement should be correct with respect to the original policy. Although alignment of security policies in socio-technical systems has been discussed in the literature, especially in relation to business goals, there has been no formal treatment of this topic so far in terms of consistency and completeness of policies. Wherever formal approaches are used in policy alignment, these are applied to well-defined technical access control scenarios instead. Therefore, we aim at formalizing security policy alignment for complex socio-technical systems in this paper, and our formalization is based on predicates over sequences of actions. We discuss how this formalization provides the foundations for existing and future methods for finding security weaknesses induced by misalignment of policies in socio-technical systems.

Keywords: Attack trees;security logics;security policies;security policy alignment;security policy refinement;socio-technical systems;system models;

[7] W. Pieters, S. H. van der Ven, and C. W. Probst. A move in the security measurement stalemate: elo-style ratings to quantify vulnerability. In *Workshop on New Security Paradigms (NSPW)*, pages 1-14, 2012. [bib | DOI]

One of the big problems of risk assessment in information security is the quantification of risk-related properties, such as vulnerability. Vulnerability expresses the likelihood that a threat agent acting against an asset will cause impact, for example, the likelihood that an attacker will be able to crack a password or break into a system. This likelihood depends on the capabilities of the threat agent and

the strength of the controls in place. In this paper, we provide a framework for estimating these three variables based on the Elo rating used for chess players. This framework re-interprets security from the field of Item Response Theory. By observing the success of threat agents against assets, one can rate the strength of threats and controls, and predict the vulnerability of systems to particular threats. The application of Item Response Theory to the field of risk is new, but analogous to its application to children solving math problems. It provides an innovative and sound way to quantify vulnerability in models of (information) security.

Keywords: control strength, elo, item response theory, rating systems, risk assessment, security metrics, threat capability, vulnerability

[8] R. R. Rajkumar, I. Lee, L. Sha, and J. Stankovic. Cyber-physical systems: the next computing revolution. In *Proceedings of the 47th Design Automation Conference (DAC)*, pages 731-736, 2010. [bib | DOI]

Cyber-physical systems (CPS) are physical and engineered systems whose operations are monitored, coordinated, controlled and integrated by a computing and communication core. Just as the internet transformed how humans interact with one another, cyber-physical systems will transform how we interact with the physical world around us. Many grand challenges await in the economically vital domains of transportation, health-care, manufacturing, agriculture, energy, defense, aerospace and buildings. The design, construction and verification of cyber-physical systems pose a multitude of technical challenges that must be addressed by a cross-disciplinary community of researchers and educators.

Keywords: computer science, cyber-physical systems, engineering, grand challenges, new frontiers

[9] C. Rieger, Q. Zhu, and T. Basar. Agent-based cyber control strategy design for resilient control systems: Concepts, architecture and methodologies. In *5th International Symposium on Resilient Control Systems (ISRCS)*, pages 40-47, Aug. 2012. [bib | DOI]

The implementation of automated regulatory control has been around since the middle of the last century through analog means. It has allowed engineers to operate the plant more consistently by focusing on overall operations and settings instead of individual monitoring of local instruments (inside and outside of a control room). A similar approach is proposed for cyber security, where current border-protection designs have been inherited from information technology developments that lack consideration of the high-reliability, high consequence nature of industrial control systems. Instead of an independent development, however, an integrated approach is taken to develop a holistic understanding of performance. This performance takes shape inside a multi-agent design, which provides a notional context to model highly decentralized and complex industrial process control systems, the nervous system of critical infrastructure. The resulting strategy will provide a framework for researching solutions to security and unrecognized interdependency concerns with industrial control systems.

Keywords: Computer security;Control systems;Control theory;Process control;Sensors;Software;computer network security;control system CAD;decentralised control;multi-agent systems;process control;reliability;Cyber security;agent-based Cyber control strategy design;automated regulatory control;border-protection designs;complex industrial process control systems;critical infrastructure;decentralized industrial process control systems;high-reliability industrial control systems;information technology developments;multiagent design;resilient control systems;complex networked control systems;cyber awareness;cyber physical systems;cyber security;data fusion;hierarchical architecture;human systems;resilient control;

[10] L. Sha and J. Meseguer. Design of complex cyber physical systems with formalized architectural patterns. In *Software-Intensive Systems and New Computing Paradigms*, volume 5380 of *Lecture Notes in Computer Science*, pages 92-100. 2008. [bib | DOI]

The design of cyber physical systems (CPS) presents many challenges because of their complexity, strong safety requirements, distribution, and real-time nature. We propose a novel paradigm, based on the idea of using simplicity to control complexity, to achieve highly reliable CPS designs. The goal is to embody design rules of this complexity-control nature in highly reusable, very robust, and formally

verified architectural patterns. We discuss some preliminary work and experiments illustrating how this can be done for CPS systems.

[11] A. Teixeira, D. Pérez, H. Sandberg, and K. H. Johansson. Attack models and scenarios for networked control systems. In *Proceedings of the 1st International Conference on High Confidence Networked Systems (HiCoNS)*, pages 55-64, 2012. [bib | DOI]

Cyber-secure networked control is modeled, analyzed, and experimentally illustrated in this paper. An attack space defined by the adversary's system knowledge, disclosure, and disruption resources is introduced. Adversaries constrained by these resources are modeled for a networked control system architecture. It is shown that attack scenarios corresponding to replay, zero dynamics, and bias injection attacks can be analyzed using this framework. An experimental setup based on a quadruple-tank process controlled over a wireless network is used to illustrate the attack scenarios, their consequences, and potential counter-measures.

Keywords: attack space, cyber-physical systems, secure control systems, security

[12] S. J. Templeton and K. Levitt. A requires/provides model for computer attacks. In *Proceedings of the Workshop on New Security Paradigms (NSPW)*, pages 31-38, 2000. [bib | DOI]

[13] Q. Zhu and T. Basar. A dynamic game-theoretic approach to resilient control system design for cascading failures. In *1st International Conference on High Confidence Networked Systems (HiCoNS)*, pages 41-46, 2012. [bib | DOI]

The migration of many current critical infrastructures, such as power grids and transportations systems, into open public networks has posed many challenges in control systems. Modern control systems face uncertainties not only from the physical world but also from the cyber space. In this paper, we propose a hybrid game-theoretic approach to investigate the coupling between cyber security policy and robust control design. We study in detail the case of cascading failures in industrial control systems and provide a set of coupled optimality criteria in the linear-quadratic case. This approach can be further extended to more general cases of parallel cascading failures.

Keywords: cyber-physical systems, differential games, game theory, markov games, nash equilibrium

---