Available online at www.sciencedirect.com

ScienceDirect

Procedia CIRP 52 (2016) 84 – 89

www.elsevier.com/locate/procedia

Changeable, Agile, Reconfigurable & Virtual Production

Efficiency and security of process transparency in production networks—a view of expectations, obstacles and potentials

Elisabeth Ilie-Zudor[a], Zsolt Kemény[a,*], Davy Preuveneers[b]

[a] *Fraunhofer Project Center PMI, Institute for Computer Science and Control, Hungarian Academy of Sciences, Kende u. 13–17, H-1111 Budapest, Hungary*
[b] *iMinds–DistriNet–KU Leuven, Celestijnenlaan 200A, B-3001 Heverlee, Belgium*

[*] Corresponding author. Tel.: +36-1-279-6180; fax: +36-1-466-7503. *E-mail address:* zsolt.kemeny@sztaki.mta.hu

Abstract

Much of the resilience and flexibility of production networks lies in the transparency of processes that allows timely perception of actual process states and adequate decisions or intervention at the proper point of the production system. Such degree of observability and permeability do, however, bear risks of malevolent tapping or interference with the information stream which, in the case of production systems, can put both business and physical processes at risk, requiring careful exploration of security threats in horizontal and vertical integration, and individual end-to-end connections likewise. Also, different levels of networked production present specific needs—high throughput and low time lag on the shop-floor level, or tolerances for confidence, gambling and bounded-rational views in cross-company relations—that may conflict with security policies. The paper presents a systematic summary of such apparently contradicting preferences, and possible approaches of reconciliation currently perceived to be relevant on various abstraction levels of production networks.

Peer-review under responsibility of the scientific committee of the Changeable, Agile, Reconfigurable & Virtual Production Conference 2016
Keywords: Production networks; process transparency; security; performance

1. Introduction

The past 1–2 decades have been marked by changes in industrial production that can be attributed to the mutually amplified tendencies of (1) changing consumer demands and environmental impact regulations requiring more effort and faster adaptation, and (2) the ability of the industry—at least, in a technical perspective—to address these evolving challenges. On one hand, industrial production is, nowadays, required to be more responsive to the diversity of demands (i. e., various degrees of customization and additional services tailored to the individual customer) and their quick changes (requiring tighter development and lead times and more adaptivity). On the other hand, efficient use of resources is gaining importance in view of competitive pressure and more stringent environmental regulations.

Dynamically changing production networks—as opposed to fixed supply chains, often centered around a single "major player" determining long-term roles—proved to be a feasible way of tackling the aforementioned challenges. Here, participants of varying size, expertise and production capacities engage in collaboration, often on a project-by-project basis, to meet the perceived demands—not excluding the possibility of simultaneously acting as competitors in connection with another production order. The emergence of such product development and production structures is, to a decisive degree, owing to greatly improved process transparency in design, production and logistics, with observations or sharing transactions often crossing both corporate and technological borders. This trend is individible from the development of theoretical foundations and applicable technologies putting the observability to use, often mentioned among characteristics of a "fourth industrial revolution" [1–4]. The most significant of these are advances in handling "big data" and extracting useful high-level information from large amounts of low-level and unstructured data, modeling of processes and corresponding measures of prediction and control, planning of mostly discrete and structured aspects of production (e. g., scheduling and assignment problems), negotiation and contract mechanisms with formal guarantees, and support for various forms of human involvement (most significantly, decision support and human-comprehensible (re)presentation of underlying knowledge).

Such degree of process transparency and precise intervention requires much more data to be collected, communicated and stored than it was typical in earlier industrial practice, and both the amount and the potential propagation of production-related information present new challenges. Aside from inter-

Peer-review under responsibility of the scientific committee of the Changeable, Agile, Reconfigurable & Virtual Production Conference 2016
doi:10.1016/j.procir.2016.07.018

operability problems arising from the heterogeneous nature of production networks, security and performance limits are the two focal areas of concern. The paper gives a state-of-practice review on problems and solutions applicable to production networks. The remainder of this paper is structured as follows. In section 2, we discuss common threats, countermeasures, and limitations of state-of-practice security solutions. Section 3 reviews contemporary solutions and trade-offs. We conclude in section 4 summarizing our main insights and identifying interesting topics for further research. The areas of problems, limitations and solutions reviewed in the paper are also summarized in Figure 1.

2. Focal problems in production networks

As recent attacks on SCADA systems by dangerous malware like Stuxnet, Duqu, Flame, and Gauss [5,6] have shown, cybersecurity is a growing concern for production networks, as many of the manufacturing systems in operation today were never designed with networked production and large-scale machine-to-machine connectivity in mind. This section reviews common threats, countermeasures, and limitations of state-of-practice solutions to secure production networks.

2.1. Common threats in networked production systems

Security threats and countermeasures in networked production systems cover two areas of concern [7], i. e., (1) *system security* to protect the organization's networks, software systems and physical production facilities from disruption and denial-of-service attacks, and (2) *information security* which deals with defending information from unauthorized access, use, disclosure, tampering or destruction. With process transparency in networked production as an emerging trend, the latter becomes far more important and challenging.

Intercepting and injecting of information. An important security threat deals with unauthorized access to information, either through (1) circumventing authentication by spoofing one's identity using a legitimate user's authentication credentials, or (2) sidestepping access control with an *elevation of privilege* attack where an unauthorized user (legitimate employee or attacker) penetrates all system defenses to gain access to or alter confidential information. Such attacks can take place on data *at rest* in a database (e. g., with an SQL injection attack [8]) or on data *in transit* between two network production facilities with an adversary executing a Man-In-The-Middle (MITM) attack (e. g., an SSL strip attack [9]).

With Cyber-Physical Systems gaining importance in networked production, the attack surface grows with ample opportunities for an intruder not only to collect information from a particular device or sensor, but also as a way to break into a single node and move laterally across the trusted production network [10] in order to tap into even more sensitive information on customers, suppliers and commercial strategies [11]. Disruption of physical processes by taking control of actuators or manipulating sensor data is also becoming an area of concern in CPS [12–14].

Aggregation and inference attacks. Production transparency is a key feature of Industry 4.0 [15]. Production assets will create data that can be tracked, collected, and analyzed in real-time across the organizational boundaries of the company. Hence, there is the inherent risk of losing control over information shared with partners in the value chain, and how they might use and share that data [7] with competitors.

Beyond information security threats in such business-to-business scenarios, there are also privacy concerns for the customer. With just-in-time individualized production and manufacturing, it is likely that the undesirable information disclosure threats due to inference attacks in social networks [16] will emerge in production networks as well. We expect that key obligations of the upcoming EU General Data Protection Regulation (GDPR) and technical compliance with such regulatory frameworks [17] will have a significant impact on networked production.

Human decisions and social engineering. User behavior has often been identified as playing a major role in security failures, and that is why humans are usually considered the weakest link in the security chain [18]. According to research from security software firm Trend Micro [19], more than 90% of cyberattacks begin with a *spear phishing* email, a form of phishing that uses information about the target to make the attack more specific and personal. Recent work by Krombholz [20] provides a taxonomy of well-known social engineering attacks.

While human behavior is often the weakest point in withholding confidential information, it can also become a barrier to disclosing information that is beneficial to be shared—both on the level of individual sharing decisions, and in setting up sharing policies. This can be the result of a limited horizon of knowledge regarding information handling processes in the production network [21], effecting that transparency is maintained in a limited range of participants only [22], or gambling behavior is practised that deteriorates the overall efficiency of cooperation [23,24].

2.2. Limits of countermeasures

Network intrusion detection systems and firewalls are frequently used to detect a variety of malicious access patterns and threats. Such countermeasures usually operate at the edge of the organization's network, and are sufficient to mitigate simple security attacks. With networked production, the trust boundaries of the organization's network continuously change, demanding for more dynamic solutions where access control is pushed towards all elements in the production network. Nayak *et al.* [25] proposed Reasonance, a system for securing enterprise networks where the elements in the network enforce dynamic access control policies based on both flow-level information and real-time alerts managed by OpenFlow [26] enabled switches. Much more challenging are *advanced persistent threats* (APT) [27] where the objective of the intruder is to achieve ongoing access without being detected. Such attacks make use of sophisticated evasion techniques, malware and other backdoors. They are usually not conducted to disrupt the service and therefore more difficult to detect. Mitigating such threats require sophisticated anomaly detection algorithms to identify unexpected information flows.

Application-level weaknesses have been the cause of many data breaches. For data *at rest*, encrypted databases [28] have been proposed to handle SQL queries over encrypted data.

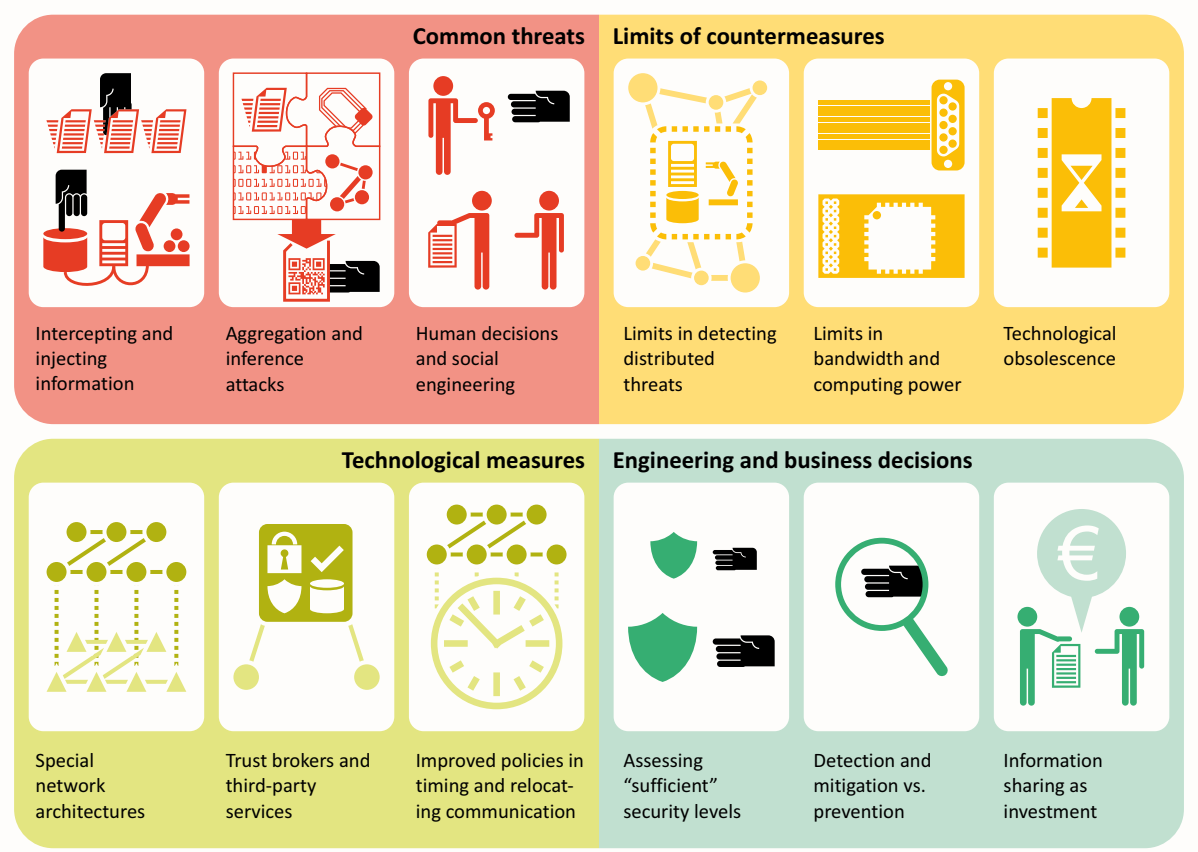

Fig. 1. Summary of areas of problems, limitations and possible solutions referred to in the paper

However, recent work has shown that inference attacks are also possible on encrypted database systems [29]. For data *in transit*, traffic analysis is a type of inference attack that intercepts and analyzes messages to deduce information from patterns in communication between production facilities, and encryption usually helps to protect against such security threats. However, work by Dryer *et al.* [30] has shown that traffic analysis is possible even on encrypted messages, hereby demonstrating that state-of-practice countermeasures may fail.

Limits in bandwidth and computing power. In contemporary production and manufacturing environments, industrial wireless networks of sensors, controllers and actuators are being rolled out to realize intelligent monitoring, manufacturing and control [31], albeit often without security measures in place to protect against eavesdropping.

The primary reason for this security gap was the mainstream belief that even lightweight cryptographic building blocks [32] imposed a performance overhead that jeopardized their successful application on resource constrained devices, such as passive RFID tags. When applied, their implementation was sometimes found inadequate in that the security protocols could be easily broken [33]. However, the last couple of years, work is ongoing on low-resource solutions [34] that make public-key cryptography practical on passive RFID tags by means of highly optimized hardware implementations.

Technological obsolescence. Last but not least, the increasing pace of technological obsolescence [35] has an impact on networked production. While new field devices might be technically superior, it does not mean that current solutions are functionally obsolete, even if they cannot be refurbished or upgraded with new software to support the latest features. From a managerial and system integration point of view, this means security decisions become a cost-benefit trade-off.

3. Solutions and trade-offs

The scientific state-of-the-art has proposed several solutions [25,36–39] that can be applied in the domain of production networks. In this section, we will review such solutions and discuss trade-offs that decision makers are faced with on how to maintain and secure their production infrastructure in a cost-effective manner.

3.1. Technological measures

Technological measures that are put in place in a networked production environment should be the outcome of a rigorous threat and risk assessment, for which existing process modeling frameworks such as STRIDE [40] and LINDDUN [41] can assist with eliciting security and privacy threats.

Special network architectures. Authentication and authorization are typical features of an access control layer in an information security architecture. Solutions like Resonance [25] implement dynamic network security policies in the network, at devices and switches, leaving little responsibility to either the hosts or higher layers of the network. This enables operators to specify how the network should control traffic when network conditions change, such as in the case of a security breach. Other in-network security systems and architectures are NetSecu and LiveSec. NetSecu [38] is a collaborative network security platform where security functions like firewalls, intrusion detection systems and anti-virus solutions can be dynamically enabled, disabled and upgraded for each NetSecu node at the edge of an access network. LiveSec [37] is a scalable and flexible security management architecture for large-scale networks. Interactive policy enforcement checks various end-to-end flows for compliance against a global policy table that identifies which security service elements should be traversed. Dynamic visualization of many real-time network events is another key feature of this network architecture.

Trust brokers and third-party services. Due to similar performance and scalability reasons, there is an emerging trend of moving networked production and other business processes at least partially to the cloud [31] to benefit from scalable data processing capabilities to improve the production and manufacturing process. Such third-party cloud-oriented architectures offer value-added services to industrial cyber-physical systems, by storing, integrating, aggregating and correlating data through data mining, machine learning and statistical analysis. However, adequate security policies must be enforced such that the trust boundaries across the organizations in the networked production process are not broken—in some cases, surveillance of these is also a part of third-party services, as in the auditing-based approach by Bhargava *et al.* [7].

Improved policies in timing and relocating communication. In production networks, much of the information can take several alternative paths, and a considerable part of data is not required to be forwarded immediately (as is the case, e. g., with low-level production data to be aggregated on a day-by-day or shift-by-shift basis for periodic forecasting or planning). Alternatives either exist already, or can be taken in consideration at a reasonably low overhead in design, development and operational costs—these mean additional reserves in improving both performance and security. Quantitative measures can be specified to express the need for transmitting a given piece of information by a given deadline, and communication timing can be evaluated for fulfilling such criteria and constraints in view of resources available in the network and in the individual devices in question. Much research and development has recently taken place for wireless sensor networks (WSN) where both network and device resources are subject to limitations [42,43]. Similar measures can be expressed for security aspects as well [44,45]. Examples in IoT middleware (see the frameworks in [44,46]) attest that such approaches are suitable for data exchange in dynamically changing, often self-organized, environments with timing and causality constraints that are also shared by production environments.

3.2. Engineering and business decisions

Cross-company relations in production networks impose specific needs that may conflict with security policies as well as operational and economic aspects within the border of a single company, such that finding the right balance between efficiency and security of process transparency in production networks involves important engineering and business decisions.

Assessing "sufficient" security levels. Even with growing customization, quantities remain an important aspect of industrial production, keeping economic feasibility in the focus for a wide spectrum of decisions in building up, maintaining and operating production assets. Attacks motivated by gaining competitive advantage underly similar considerations—in other words, a profit-motivated intruder is likely to attack if the balance of advantages vs. efforts seems to make this worthwhile. Game theory [47–49] is often applied to estimate the likeliness of attacks. All hierarchical levels of production networks have their own typical patterns of data abstraction, frequency, and obsolescence, setting different "break-even" points for a potential attack. Having to maintain security with finite resources at hand requires, therefore, a differentiated view at various layers of production and business [50,51].

Detection and mitigation vs. prevention. As mentioned before, industrial production, especially closer to the shop-floor level, is likely to include "legacy" components, possibly without feasible upgrade or retrofit of security-critical subsystems. Moderate computational resources of embedded devices are also limiting the attainable level of security [10]. Since de-facto vulnerability cannot be fully eliminated, the production system must be prepared to *detect* and *mitigate* unavoidable attacks instead. Such problems are, inherently, more pronounced in wireless sensor networks, hence, much progress in this field is stemming from detection mechanisms and robust protocols applied in WSN [52–54]. The development of cyber-physical production systems (CPPS) led to the emergence of comparable countermeasures for the conditions of industrial production, a part of the methods exploiting the distributed nature of CPPS (e. g., *swarm intelligence* [55]) where components can observe and attest each other's function and communication using locally available computational resources. Security in CPPS can be critical due to possible access to actuators or interference with control loops [12]—these threats are also addressed at the physical and control engineering level [13,14].

Information sharing as investment. Improved process transparency is, to a given degree, binding for production networks to function properly—still, sharing of information across corporate boundaries is often hampered by the perceived risks and costs of communicating more business information. In many cases, the assessment of risks vs. benefits is still biased by lack of experience or insight into the nature of information sharing in networked production. Formal methods of analysis of both the sharing processes and related human perception can help establish a more sober and realistic view (see Wu *et al.* for supply chains [56], and Prajogo *et al.* for parallels in long-term collaboration [57]), leading to regarding information sharing as a form of investment weighed up against an expected return.

The distributed attacks of recent years have also shed light on the importance of sharing information on detected threats.

While this, too, requires careful assessment of what and how is being shared, recent research has suggested benefits [58,59].

4. Conclusion

The paper presented a systematic summary of apparently contradicting preferences for process transparency versus security threat mitigation in production networks, and discussed common security threats, countermeasures and their limitations. While information sharing across corporate and technological borders does present security challenges, this is not the only point of possible attcks. In many cases, weaknesses persist even within corporate borders due to the spreading of networked production architectures in lower hierarchical levels that continue to deploy weakly protected legacy components. Also, human decisions and user behavior based on limited knowledge horizon can be both a potential point of security breach, as well as an obstacle to (adequately planned) sharing of production and business information.

The paper considered concrete network architectures, policies and technical measures, as well as trade-offs in a cost vs. benefit perspective as possible approaches of improvement and reconciliation of conflicting preferences. The overview of current practices and trends was found to convey the following key messages: (1) It is reasonable to expect that in production networks and participating companies, policies and infrastructure continue to be shaped by both technical and economical "common sense", as well as prevailing beliefs, inherently keeping some weak points. Therefore, detection and mitigation of unavoidable attacks, as well as development of robust solutions at various hierarchical levels continues to be important. (2) Much research is being conducted in modeling information sharing and attack phenomena. These investigations are likely to gain importance as they contribute to the proper understanding of the underlying problems—both in the context of the given level of production processes, as well as in an integrated perspective of larger entities—and enable the development of analysis and decision support tools. (3) With information sharing and transactions often crossing both corporate and technological borders, a holistic approach is needed towards dynamically managing the end-to-end security chain while offering the necessary flexibility to adapt business and production processes to continuously evolving trust boundaries between and across organizations.

Acknowledgement

Work presented in the paper has been supported by EU Horizon 2020 grants No. 691829 "EXCELL—Actions for Excellence in Smart Cyber-Physical Systems Applications Through Exploitation of Big Data in the Context of Production Control and Logistics", and by the Research Fund KU Leuven.

References

[1] Lee, J., Bagheri, B., Kao, H.A.. A cyber-physical systems architecture for industry 4.0-based manufacturing systems. Manufacturing Letters 2015;3:18–23.

[2] Monostori, L.. Cyber-physical production systems: Roots, expectations and R&D challenges. Procedia CIRP 2014;17:9–13. Variety Management in ManufacturingProceedings of the 47th CIRP Conf. on Manufacturing Systems.

[3] Bauernhansl, T.. Industrie 4.0 in Produktion, Automatisierung und Logistik: Anwendung, Technologien, Migration; chap. Die Vierte Industrielle Revolution – Der Weg in ein wertschaffendes Produktionsparadigma. Wiesbaden: Springer Fachmedien Wiesbaden. ISBN 978-3-658-04682-8; 2014, p. 5–35.

[4] Bildstein, A., Seidelmann, J.. Industrie 4.0 in Produktion, Automatisierung und Logistik: Anwendung, Technologien, Migration; chap. Industrie 4.0-Readiness: Migration zur Industrie 4.0-Fertigung. Wiesbaden: Springer Fachmedien Wiesbaden. ISBN 978-3-658-04682-8; 2014, p. 581–597.

[5] Langner, R.. Stuxnet: Dissecting a cyberwarfare weapon. IEEE Security and Privacy 2011;9(3):49–51. doi:10.1109/MSP.2011.67.

[6] Bencsáth, B., Pék, G., Buttyán, L., Félegyházi, M.. The cousins of Stuxnet: Duqu, Flame, and Gauss. Future Internet 2012;4(4):971. doi:10.3390/fi4040971.

[7] Bhargava, B., Ranchal, R., Ben Othmane, L.. Secure information sharing in digital supply chains. In: Advance Computing Conference (IACC), 2013 IEEE 3rd International. IEEE; 2013, p. 1636–1640.

[8] Clarke, J.. SQL Injection Attacks and Defense. 1st ed.; Syngress Publishing; 2009. ISBN 1597494240, 9781597494243.

[9] Nikiforakis, N., Younan, Y., Joosen, W.. Hproxy: Client-side detection of SSL stripping attacks. In: Kreibich, C., Jahnke, M., editors. Detection of Intrusions and Malware, and Vulnerability Assessment, 7th International Conference, DIMVA 2010, Bonn, Germany, July 8-9, 2010. Proceedings; vol. 6201 of *Lecture Notes in Computer Science*. Springer. ISBN 978-3-642-14214-7; 2010, p. 200–218. doi:10.1007/978-3-642-14215-4_12.

[10] Klick, J., Lau, S., Marzin, D., Malchow, J.O., Roth, V.. Internet-facing PLCs as a network backdoor. In: Communications and Network Security (CNS), 2015 IEEE Conference on. IEEE; 2015, p. 524–532.

[11] Wang, S., Wan, J., Li, D., Zhang, C.. Implementing smart factory of Industrie 4.0: an outlook. International Journal of Distributed Sensor Networks 2016;2016.

[12] Krotofil, M., Cardenas, A., Larsen, J., Gollmann, D.. Vulnerabilities of cyber-physical systems to stale data—determining the optimal time to launch attacks. International Journal of Critical Infrastructure Protection 2014;7(4):213–232.

[13] Ji, X., Wang, B., Liu, D., Dong, Z., Chen, G., Zhu, Z., et al. Will electrical cyber-physical interdependent networks undergo first-order transition under random attacks? Physica A: Statistical Mechanics and its Applications 2016;doi:http://dx.doi.org/10.1016/j.physa.2016.05.017.

[14] Backhaus, S., Bent, R., Bono, J., Lee, R., Tracey, B., Wolpert, D., et al. Cyber-physical security: A game theory model of humans interacting over control systems. Smart Grid, IEEE Transactions on 2013;4(4):2320–2327.

[15] Möller, D.P.. Digital manufacturing/industry 4.0. In: Guide to Computing Fundamentals in Cyber-Physical Systems. Springer; 2016, p. 307–375.

[16] Heatherly, R., Kantarcioglu, M., Thuraisingham, B.M.. Preventing private information inference attacks on social networks. IEEE Trans on Knowl and Data Eng 2013;25(8):1849–1862. doi:10.1109/TKDE.2012.120.

[17] Preuveneers, D., Joosen, W., Ilie-Zudor, E.. Data Protection Compliance Regulations and Implications for Smart Factories of the Future. In: 2016 International Conference on Intelligent Environments, IE 2016, London, United Kingdom, September 14-16. 2016 (to appear),.

[18] Sasse, M.A., Brostoff, S., Weirich, D.. Transforming the 'Weakest Link' - a Human/Computer Interaction Approach to Usable and Effective Security. BT Technology Journal 2001;19(3):122–131. doi:10.1023/A:1011902718709.

[19] TrendLabs APT Research Team, . Spear-Phishing Email: Most Favored APT Attack Bait. Tech. Rep.; 2012. URL: `http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf`.

[20] Krombholz, K., Hobel, H., Huber, M., Weippl, E.. Advanced social engineering attacks. J Inf Secur Appl 2015;22(C):113–122. doi:10.1016/j.jisa.2014.09.005.

[21] Aviram, A., Tor, A.. Overcoming impediments to information sharing. Ala L Rev 2003;55:231.

[22] Chengalur-Smith, I., Duchessi, P.. An empirical investigation of extensible information sharing in supply chains: Going beyond dyadic. Information Resources Management Journal (IRMJ) 2014;27(4):1–22.

[23] Kimmerle, J., Cress, U.. The impact of cognitive anchors on information-sharing behavior. Cyberpsychology, Behavior, and Social Networking 2013;16(1):45–49.

[24] Wang, Z., Ye, F., Tan, K.H.. Effects of managerial ties and trust on supply chain information sharing and supplier opportunism. International Journal of Production Research 2014;52(23):7046–7061.

[25] Nayak, A.K., Reimers, A., Feamster, N., Clark, R.. Resonance: dynamic access control for enterprise networks. In: Proceedings of the 1st ACM workshop on Research on enterprise networking. ACM; 2009, p. 11–18.

[26] McKeown, N., Anderson, T., Balakrishnan, H., Parulkar, G., Peterson, L., Rexford, J., et al. OpenFlow: enabling innovation in campus networks. ACM SIGCOMM Computer Communication Review 2008;38(2):69–74.

[27] Cole, E.. Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization. 1st ed.; Syngress Publishing; 2013. ISBN 9781597499491, 9781597499552.

[28] Hacigümüş, H., Iyer, B., Li, C., Mehrotra, S.. Executing sql over encrypted data in the database-service-provider model. In: Proceedings of the 2002 ACM SIGMOD International Conference on Management of Data. SIGMOD '02; New York, NY, USA: ACM. ISBN 1-58113-497-5; 2002, p. 216–227. doi:10.1145/564691.564717.

[29] Naveed, M., Kamara, S., Wright, C.V.. Inference attacks on property-preserving encrypted databases. In: Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security. CCS '15; New York, NY, USA: ACM. ISBN 978-1-4503-3832-5; 2015, p. 644–655. doi:10.1145/2810103.2813651.

[30] Dyer, K.P., Coull, S.E., Ristenpart, T., Shrimpton, T.. Peek-a-boo, i still see you: Why efficient traffic analysis countermeasures fail. In: Proceedings of the 2012 IEEE Symposium on Security and Privacy. SP '12; Washington, DC, USA: IEEE Computer Society. ISBN 978-0-7695-4681-0; 2012, p. 332–346. doi:10.1109/SP.2012.28.

[31] Yue, X., Cai, H., Yan, H., Zou, C., Zhou, K.. Cloud-assisted industrial cyber-physical systems: An insight. Microprocessors and Microsystems 2015;39(8):1262–1270.

[32] Eisenbarth, T., Kumar, S., Paar, C., Poschmann, A., Uhsadel, L.. A survey of lightweight-cryptography implementations. IEEE Des Test 2007;24(6):522–533. doi:10.1109/MDT.2007.178.

[33] Nohl, K., Evans, D., Starbug, S., Plötz, H.. Reverse-engineering a Cryptographic RFID Tag. In: Proceedings of the 17th Conference on Security Symposium. SS'08; Berkeley, CA, USA: USENIX Association; 2008, p. 185–193.

[34] Arbit, A., Livne, Y., Oren, Y., Wool, A.. Implementing public-key cryptography on passive rfid tags is practical. International Journal of Information Security 2015;14(1):85–99. doi:10.1007/s10207-014-0236-y.

[35] Barañano, I., Romero-Àvila, D.. Long-term growth and persistence with obsolescence. Economic Modelling 2015;51(C):328–339.

[36] Coates, G.M., Hopkinson, K.M., Graham, S.R., Kurkowski, S.H.. A trust system architecture for SCADA network security. Power Delivery, IEEE Transactions on 2010;25(1):158–169.

[37] Wang, K., Qi, Y., Yang, B., Xue, Y., Li, J.. LiveSec: Towards effective security management in large-scale production networks. In: Distributed Computing Systems Workshops (ICDCSW), 2012 32nd International Conference on. IEEE; 2012, p. 451–460.

[38] Chen, X., Mu, B., Chen, Z.. Netsecu: A collaborative network security platform for in-network security. In: Communications and Mobile Computing (CMC), 2011 Third International Conference on. IEEE; 2011, p. 59–64.

[39] Dacier, M., Kargl, F., König, H., Valdes, A.. Network attack detection and defense: Securing industrial control systems for critical infrastructures (dagstuhl seminar 14292). Dagstuhl Reports 2014;4(7).

[40] Hernan, S., Lambert, S., Ostwald, T., Shostack, A.. Uncover security design flaws using the STRIDE approach. MSDN Magazine 2006;URL: `http://msdn.microsoft.com/en-us/magazine/cc163519.aspx`.

[41] Wuyts, K., Scandariato, R., Joosen, W.. Empirical evaluation of a privacy-focused threat modeling methodology. Journal of Systems and Software 2014;96:122–138. doi:http://dx.doi.org/10.1016/j.jss.2014.05.075.

[42] Khader, O., Willig, A., Wolisz, A.. An autonomous framework for supporting energy efficiency and communication reliability in wsns. In: Wireless and Mobile Networking Conference (WMNC), 2013 6th Joint IFIP. IEEE; 2013, p. 1–8.

[43] Sallai, J., Horváth, P., Koutsoukos, X.. Self-organizing wsn protocol for real-time communication requirements. In: Distributed Computing in Sensor Systems (DCOSS), 2013 IEEE International Conference on. IEEE; 2013, p. 409–414.

[44] Fremantle, P., Scott, P.. A security survey of middleware for the Internet of Things. PeerJ PrePrints 2015;3:e1521.

[45] Wang, J., Xu, J., Liu, Y., Deng, W.. AST: Activity–security–trust driven modeling of time varying networks. Scientific reports 2016;6. doi:doi:10.1038/srep21352.

[46] Conzon, D., Bolognesi, T., Brizzi, P., Lotito, A., Tomasi, R., Spirito, M.A.. The VIRTUS middleware: An XMPP based architecture for secure IoT communications. In: 2012 21st International Conference on Computer Communications and Networks (ICCCN). 2012, p. 1–6. doi:10.1109/ICCCN.2012.6289309.

[47] Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., Smeraldi, F.. Game theory meets information security management. In: ICT Systems Security and Privacy Protection. Springer; 2014, p. 15–29.

[48] Spyridopoulos, T., Karanikas, G., Tryfonas, T., Oikonomou, G.. A game theoretic defence framework against dos/ddos cyber attacks. Computers & Security 2013;38:39–50.

[49] Furuncu, E., Sogukpinar, I.. Scalable risk assessment method for cloud computing using game theory (ccram). Computer Standards & Interfaces 2015;38:44–50.

[50] Eisenga, A., Rodriguez, W., Jones, T.. Methods on determining the investment in IT security. In: Nemati, H.R., editor. Advances in Information Security, Privacy, and Ethics: Analyzing Security, Trust, and Crime in the Digital World. IGI Global. ISBN 9781466648579; 2013, p. 22–34. doi:10.4018/978-1-4666-4856-2.ch002.

[51] Bartol, N.. Cyber supply chain security practices DNA—filling in the puzzle using a diverse set of disciplines. Technovation 2014;34(7):354–361. doi:http://dx.doi.org/10.1016/j.technovation.2014.01.005; special Issue on Security in the Cyber Supply Chain.

[52] Shafiei, H., Khonsari, A., Derakhshi, H., Mousavi, P.. Detection and mitigation of sinkhole attacks in wireless sensor networks. Journal of Computer and System Sciences 2014;80(3):644–653. doi:http://dx.doi.org/10.1016/j.jcss.2013.06.016; special Issue on Wireless Network Intrusion.

[53] Sahu, S.S., Pandey, M.. Intelligent Computing, Communication and Devices: Proceedings of ICCD 2014, Volume 2; chap. A Probabilistic Packet Filtering-Based Approach for Distributed Denial of Service Attack in Wireless Sensor Network. New Delhi: Springer India. ISBN 978-81-322-2009-1; 2015, p. 65–70.

[54] Patel, M.M., Aggarwal, A.. Security attacks in wireless sensor networks: A survey. In: Intelligent Systems and Signal Processing (ISSP), 2013 International Conference on. IEEE; 2013, p. 329–333.

[55] Park, H., Seo, D., Lee, H., Perrig, A.. Smatt: Smart meter attestation using multiple target selection and copy-proof memory. In: Computer Science and its Applications. Springer; 2012, p. 875–887.

[56] Wu, L., Chuang, C.H., Hsu, C.H.. Information sharing and collaborative behaviors in enabling supply chain performance: A social exchange perspective. International Journal of Production Economics 2014;148:122–132.

[57] Prajogo, D., Olhager, J.. Supply chain integration and performance: The effects of long-term relationships, information technology and sharing, and logistics integration. International Journal of Production Economics 2012;135(1):514–522.

[58] Tosh, D.K., Molloy, M., Sengupta, S., Kamhoua, C.A., Kwiat, K.A.. Cyber-investment and cyber-information exchange decision modeling. In: High Performance Computing and Communications (HPCC), 2015 IEEE 7th International Symposium on Cyberspace Safety and Security (CSS), 2015 IEEE 12th International Conferen on Embedded Software and Systems (ICESS), 2015 IEEE 17th International Conference on. IEEE; 2015, p. 1219–1224.

[59] Tosh, D., Sengupta, S., Kamhoua, C., Kwiat, K., Martin, A.. An evolutionary game-theoretic framework for cyber-threat information sharing. In: Communications (ICC), 2015 IEEE International Conference on. IEEE; 2015, p. 7341–7346.