Best Readings Topics on Communications and Information Systems Security

- ## Authentication

Xiaohui Liang, Xu Li, Qinghua Shen, Rongxing Lu, Xiaodong Lin, Xuemin Shen, and Weihua Zhuang, "Prediction to Enable Secure and Reliable Routing in Wireless Body Area Networks", Proceedings of IEEE INFOCOM'12, pp. 388-396, 2012.
In this paper, we propose a distributed Prediction-based Secure and Reliable routing framework (PSR) for emerging Wireless Body Area Networks (WBANs). It can be integrated with a specific routing protocol to improve the latter's reliability and prevent data injection attacks during data communication. Specially-tailored lightweight source and data authentication methods are employed by nodes to secure data communication. Further, each node adaptively enables or disables source authentication according to predicted neighbor set change and prediction accuracy so as to quickly filter false source authentication requests. We demonstrate that PSR significantly increases routing reliability and effectively resists data injection attacks through simulations.

- ## Botnets

A. Dainotti, A. King, K. Claffy, F. Papale, A. Pescapè, "Analysis of a "/0" Stealth Scan from a Botnet", Proceedings of ACM SIGCOMM/SIGMETRICS Internet Measurement Conference IMC'12, pp. 1-14, 2012.
We present the measurement and analysis of a horizontal scan of the entire IPv4 address space conducted by the Sality botnet in February 2011. This 12-day scan originated from approximately 3 million distinct IP addresses, and used a heavily coordinated and unusually covert scanning strategy to try to discover and compromise VoIP-related (SIP server) infrastructure. This work offers a detailed dissection of the botnet's scanning behavior, including general methods to correlate, visualize, and extrapolate botnet behavior across the global Internet.

-

Cooperative Security

Rongxing Lu, Xu Li, Xiaohui Liang, Xuemin Shen, and Xiaodong Lin, "GRS: The green, reliability, and security of emerging machine to machine communications", IEEE Communication Magazine, Vol. 49, No. 4, pp. 28-35, 2011.
Machine-to-machine communications is characterized by involving a large number of intelligent machines sharing information and making collaborative decisions without direct human intervention. The flourishing of M2M communications still hinges on fully understanding and managing the existing challenges: energy efficiency (green), reliability, and security (GRS). In this article, we first formalize M2M communications architecture to incorporate three domains - the M2M, network, and application domains - and accordingly define GRS requirements in a systematic manner. We then introduce a number of GRS enabling techniques by exploring activity scheduling, redundancy utilization, and cooperative security mechanisms.

-

Cyber Attacks

Jun Yan, Yihai Zhu, Haibo He, and Yan Sun, "Multi-Contingency Cascading Analysis of Smart Grid Based on Self-Organizing Map", IEEE Transactions on Information Forensics and Security, vol. 8, no. 4, pp. 646-656, 2003.
Cyber Attack Growing energy demands and environment concerns have significantly increased the interest of academia, industry and governments in development of a smart and secure electrical power grid. The goal of this paper is to advance methods of vulnerability analysis and to develop innovative responses to maintain the integrity of power grids under complex attacks (both cyber-attacks and physical failures). Specifically, in this study, we propose an integrated approach combining the spatial analysis based on self-organizing map (SOM) with electrical characteristics (load) to assess the vulnerability and cascading efforts of multiple component sets in the power grid. The results find in this paper could hopefully contribute to developing robust, secure, and reliable future grid systems.

Li, Xiaohui Liang, Rongxing Lu, Xuemin Shen, Xiaodong Lin, and Haojin Zhu, " Securing Smart Grid: Cyber Attacks, Countermeasures and Challenges", IEEE Communication Magazine, Vol. 50, No. 8, pp. 38-45, 2012.
Smart grid has emerged as the next-generation power grid via the convergence of power system engineering and information and communication technology. In this article, we describe smart grid goals and tactics, and present a three-layer smart grid network architecture. Following a brief discussion about major challenges in smart grid development, we elaborate on smart grid cyber security issues. We define a taxonomy of basic cyber-attacks, upon which sophisticated attack behaviors may be built. We then introduce fundamental security techniques. By discussing some interesting open problems, we finally expect to trigger more research efforts in this emerging area.

-

Eavesdropping

Lin, Rongxing Lu, Xuemin Shen, Yoshiaki Nemoto, and Nei Kato, "Sage: A Strong Privacy-preserving Scheme against Global Eavesdropping for Ehealth Systems", IEEE Journal on Selected Areas in Communications, Vol. 27, No. 4, pp. 365-378, 2009.
The eHealth system is envisioned as a promising approach to improving health care through information technology, where security and privacy are crucial for its success and large-scale deployment. This paper proposes a strong privacy-preserving scheme against global eavesdropping, named SAGE, for eHealth systems. The SAGE can achieve not only the content oriented privacy but also the contextual privacy against a strong global adversary. Extensive analysis demonstrates the effectiveness and practicability of the proposed scheme.

Hyoungsuk Jeon, Jinho Choi, Steven W. McLaughlin, and Jeongseok Ha, "Channel aware encryption and decision fusion for wireless sensor networks", IEEE Trans. Inform. Forensics Security, vol. 8, no. 4, pp. 619-625, 2013.
This paper studies a simple and efficient physical-layer security to prevent passive eavesdropping on transmitting data from sensors to an ally fusion center. The paper proposes a novel encryption scheme and decision fusion rules for a parallel access channel model by employing a low complexity and energy efficient modulation technique, noncoherent binary frequency shift keying. The proposed scheme takes advantage of a free natural resource, i.e., randomness of wireless channels, to encrypt the binary local decision of each sensor. The proposed scheme achieves perfect secrecy with a simple structure that is suited for sensors of limited complexity.

-

Intrusion Detection Systems

Abror Abduvaliyev, Al-Sakib Khan Pathan, Jianying Zhou, Rodrigo Roman, "On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks", IEEE Communications Surveys and Tutorials, Vol. 5, No. 3, pp.1223-1237, 2013.
This paper surveys recently proposed works on Intrusion Detection Systems (IDS) in WSNs, and presents a comprehensive classification of various IDS approaches according to their employed detection techniques. The three main categories explored in this paper are anomaly detection, misuse detection, and specification-based detection protocols. We give a description of existing security attacks in WSNs and the corresponding proposed IDS protocols to tackle those attacks. We analyze the works with respect to the network structure of WSNs.

K. M. M. Vieira, A. SCHULTER, C. B. Westphall; C. M. Westphall, "Intrusion Detection for Grid and Cloud Computing", IEEE IT Professional Magazine, Vol. 12, No. 4, pp. 38-43, 2010.
Providing security in a distributed system requires more than user authentication with passwords or digital certificates and confidentiality in data transmission. The Grid and Cloud Computing Intrusion Detection System integrates knowledge and behavior analysis to detect intrusions.

- ## Physical Security

H. Chen, Y. Chen, and D. Summerville, "A Survey on the Application of FPGAs for Network Infrastructure Security", IEEE Communications Surveys and Tutorial, Vol. 13, No. 4, pp. 541-561, 2011.
Given the rapid evolution of attack methods and toolkits, the performance gap between the execution speed of security software and the amount of data to be processed is ever widening. Possessing the ?exibility of software and high parallelism of hardware, recon?gurable hardware devices, such as Field Programmable Gate Arrays (FPGAs), have become increasingly popular to close the gap. This paper presents a survey of the state-of-art in FPGA-based implementations that have been used in the network infrastructure security area, categorizing currently existing diverse implementations. Combining brief descriptions with intensive case-studies, we hope this survey will inspire more active research.

- ## Privacy

Sherali Zeadally, Al-Sakib Khan Pathan, Cristina Alcaraz, and Mohamad Badra, "Towards Privacy Protection in Smart Grid", Wireless Personal Communications, Springer, pp. 1-25, 2012.
The smart grid is an electronically controlled electrical grid that connects power generation, transmission, distribution, and consumers using information communication technologies. In this paper, we present an analysis of recently proposed smart grid privacy solutions and identify their strengths and weaknesses in terms of their implementation complexity, efficiency, robustness, and simplicity.

Daojing He, Chun Chen, Jiajun Bu, Sammy Chan, Yan Zhang and Mohsen Guizani, " Secure Service Provision in Smart Grid Communications", IEEE Communications Magazine, vol. 50, no. 8, pp. 53-61, 2012.
The smart grid provides a platform for third-party service providers to remotely monitor and manage energy usage for consumers. At the same time, the involvement of service providers brings a new set of security threats to the smart grid. In this article, we first identify the cyber security challenges on service provision in the smart grid. Then we present two main security issues related to service provision and provide potential solutions. Finally, we suggest directions of future work on secure service provision by describing several open issues.

Daojing He, Chun Chen, and Jiajun Bu, Sammy Chan, Yan Zhang, "Security and Efficiency in Roaming Services for Wireless Networks: Challenges, Approaches, and Prospects ", IEEE Communications Magazine, vol. 51, no. 2, pp. 142-150, 2013.
Seamless roaming over wireless networks is highly desirable to mobile users, but ensuring the security and efficiency of this process is challenging. In this article, we first identify the challenges unique to roaming services as a set of mandatory and optional requirements. Next, we provide a brief state-of-the-art survey of existing work and point out their limitations in securing roaming

services. To complement the security provided by the existing work, we then propose some mechanisms that can meet the aforementioned security and efficiency requirements. Finally, we present challenges that need to be addressed in roaming authentication.

Xu Li, Rongxing Lu, Xiaohui Liang, Xuemin Shen, Jiming Chen, and Xiaodong Lin, "Smart Community: an Internet of Things Application", IEEE Communication Magazine, Vol. 49, No. 11, pp. 68-75, 2011.
In this article, we introduce an Internet of Things application, smart community, which refers to a paradigmatic class of cyber-physical systems with cooperating objects (i.e., networked smart homes). We then define the smart community architecture, and describe how to realize secure and robust networking among individual homes. We present two smart community applications, Neighborhood Watch and Pervasive Healthcare, with supporting techniques and associated challenges, and envision a few value-added smart community services.

Rongxing Lu, Xiaohui Liang, Xu Li, Xiaodong Lin, and Xuemin Shen, "EPPA: An Efficient and Privacy-Preserving Aggregation Scheme for Secure Smart Grid Communications", IEEE Transactions on Parallel and Distributed Systems, Vol. 23, No. 9, pp. 1621-1632, 2012.
In this paper, we propose an efficient and privacy-preserving aggregation scheme, named EPPA, for smart grid communications. EPPA uses a super-increasing sequence to structure multidimensional data and encrypt the structured data by the homomorphic Paillier cryptosystem technique. For data communications from user to smart grid operation center, data aggregation is performed directly on ciphertext at local gateways without decryption, and the aggregation result of the original data can be obtained at the operation center. Through extensive analysis, we demonstrate that EPPA resists various security threats and preserve user privacy, and has significantly less computation and communication overhead than existing approaches.

- ## Theoretical Aspects

Hyoungsuk Jeon, Daesung Hwang, Jinho Choi, Hyuckjae Lee, and Jeongseok Ha, "Secure type-based multiple access", IEEE Trans. Inform. Forensics Security, Vol. 6, No. 3, pp. 763-747, 2011.
This paper considers data confidentiality in a distributed detection scenario with a type-based multiple-access (TBMA) protocol where a large set of sensors sends local measurements to an ally fusion center (FC) over an insecure wireless medium called the main channel. The proposed TBMA protocol, called secure TBMA, activates sensors having strong and weak main channel gains and makes the sensors follow different reporting rules based on the magnitudes of their channel gains. The proposed scheme delivers unconditional/perfect secrecy without assuming any superiority of the ally FC over the enemy FC in terms of computational capability, secret key, and so on.

Benjamin Fabian, Seda Gürses, Maritta Heisel, Thomas Santen and Holger Schmidt, "A Comparison of Security Requirements Engineering Methods", Special Issue: Security Requirements Engineering, Springer, Vol. 15, No. 1, pp. 7-40, 2010.

This paper presents a conceptual framework for security engineering, with a strong focus on security requirements elicitation and analysis. This conceptual framework establishes a clear-cut vocabulary and makes explicit the interrelations between the different concepts and notions used in security engineering. Further, we apply our conceptual framework to compare and evaluate current security requirements engineering approaches, such as the Common Criteria, Secure Tropos, SREP, MSRA, as well as methods based on UML and problem frames. We review these methods and assess them according to different criteria, such as the general approach and scope of the method, its validation, and quality assurance capabilities. Finally, we discuss how these methods are related to the conceptual framework and to one another.

M. Bloch, J. Barros, M. R. D. Rodrigues. S. W. McLaughlin, "Wireless Information-Theoretic Security", IEEE Trans. Inf. Theory, Vol. 54, No. 6, pp. 2515-2534, 2008.
This paper considers the transmission of confidential data over wireless channels. Based on an information-theoretic formulation, the important role of fading is characterized in terms of average secure communication rates and outage probability. A practical secure communication protocol is developed, based on multilevel coding and optimized low-density parity-check (LDPC) codes, which allows to achieve communication rates close to the fundamental security limits in several relevant instances. Finally, a set of metrics for assessing average secure key generation rates is established, and it is shown that the protocol is effective even in the presence of imperfect channel state information.

- ## Trust

B. Bhargava, L. Lilien, A. Rosenthal, M. Winslett, " The pudding of trust [intelligent systems]", IEEE Intelligent Systems, Vol. 19, No. 5, pp. 74-77, 2004.
If you can spot one trend in intelligent systems, I think it would be the issue of trust. I've seen many paper titles and workshops that involve "trust" I've wondered what kind of trust people want their computers to manage. Intuitively, we all know that trust is important and precious, something we might work hard to earn from others and might not assign generously when things really matter. But what is trust in computing? The literature gives numerous answers. When trying to define trust in computing, we end up with a pudding of things rather than a solid definition.

- ## Wireless Sensor Networks

Al-Sakib Khan Pathan, Hyung-Woo Lee, and Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges", Proceedings of the International Conference on Advanced Communication Technology (IEEE ICACT'06), Volume II, pp. 1043-1048, 2006.
Wireless sensor network is an emerging technology that shows great promise for various futuristic applications both for mass public and military. The sensing technology combined with processing power and wireless communication makes it lucrative for being exploited in abundance in future. The inclusion of wireless communication technology also incurs various

types of security threats. The intent of this paper is to investigate the security related issues and challenges in wireless sensor networks. We identify the security threats, review proposed security mechanisms for these networks. We also discuss the holistic view of security for ensuring layered and robust security.

- ## Worms

Alberto Dainotti, Antonio Pescapè, Giorgio Ventre, "Worm Traffic Analysis and Characterization", Proceedings of IEEE International Conference on Communications (ICC'07), pp. 1435-1442, 2007.
In this paper we propose a general methodology, we discuss issues involved, and we present a software platform which can be used for worm traffic analysis. We show some interesting preliminary results from our traffic analysis of two of the most relevant worms that spread over the Internet: Witty and Slammer. Our results provide interesting evidences of (spatial and temporal) invariance and give some hints on worm traffic fingerprinting.

- ## Ad-hoc Networks

M. Lima, A.L. dos Santos, G. Pujolle, "A survey of survivability in mobile ad hoc networks", IEEE Communications Surveys & Tutorials, Vol. 11, No. 1, pp. 66-77, 2009.
Many efforts have been done towards secure MANETs, but the conventional lines of defense are still inefficient to put all attacks off. This article examines survivable approaches whose goal is to enable networks to fulfill correctly their critical functions even in the presence of attacks or intrusions. We introduce the most relevant survivable MANET initiatives where either preventive or reactive defenses are combined with tolerant ones. We classify the defense lines taking into account intrusion tolerance mechanisms and also identify properties and requirements of survivability. The initiatives are categorized in three groups: routing discovery, data transmission and key management. For each one, they are correlated in terms of requirements and properties. The survey shows that security solutions do not yet explore relevant survivability properties and have only focused on one network layer or one type of attack.

- ## Routing

M. Nogueira; H. Silva; A. Santos; G. Pujolle, "A Security Management Architecture for Supporting Routing Services on WANETs", IEEE Transactions on Network and Service Management, Vol. 9, No. 2, pp. 156-168, 2012.
Due to the raising dependence of people on critical applications and wireless networks, high level of reliability, security and availability is claimed to assure secure and reliable service operation. Wireless ad hoc networks (WANETs) experience serious security issues even when solutions employ preventive or reactive security mechanisms. In order to support both network operations

and security requirements of critical applications, we present SAMNAR, a Survivable Ad hoc and Mesh Network ARchitecture. Its goal lies in managing adaptively preventive, reactive and tolerant security mechanisms to provide essential services even under attacks, intrusions or failures. We use SAMNAR to design a path selection scheme for WANET routing. The evaluation of this path selection scheme considers scenarios using urban mesh network mobility with urban propagation models, and also random way point mobility with two-ray ground propagation models. Results show the survivability achieved on routing service under different conditions and attacks.

- ## Integrity

G. Dán, H. Sandberg, "Stealth Attacks and Protection Schemes for State Estimators in Power Systems", Proceedings of IEEE Smart Grid Communications'10, pp. 214-219, 2010.
We consider stealthy false-data attacks against power system state estimators. We define a security metric to quantify the difficulty of performing an attack, and describe an efficient algorithm to compute it. We describe a sufficient condition for mitigating false-data attacks, and provide two algorithms for incremental deployment of data integrity protection-enabled devices such as to maximize their utility in terms of increased system security. We illustrate the effectiveness of our algorithms on two IEEE benchmark power networks under two attack and protection cost models.

- ## Internet of Things (IoT)

D. Miorandi, S. Sicari, F. De Pellegrini, I. Chlamtac, "Internet of things: Vision, applications and research challenges", Elsevier, Ad Hoc Networks, Vol, 10, No. 7, pp. 1497-1516, 2012.
The term "Internet-of-Things" is used as an umbrella keyword for covering various aspects related to the extension of the Internet and the Web into the physical realm, by means of the widespread deployment of spatially distributed devices with embedded identification, sensing and/or actuation capabilities. Internet-of-Things envisions a future in which digital and physical entities can be linked, by means of appropriate information and communication technologies, to enable a whole new class of applications and services. In this article, we present a survey of technologies, applications and research challenges for Internet-of-Things.

- ## Anonymity

S. Sicari, L. A. Grieco, G. Boggia, A. Coen-Porisini, "DyDAP: A dynamic data aggregation scheme for privacy aware wireless sensor networks", Elsevier, Journal of Systems and Software, Vol. 85, No. 1, pp. 152-166, 2012.
End-to-end data aggregation is a very relevant issue in wireless sensor networks (WSN) that can prevent network congestion to occur. Moreover, privacy management requires that anonymity and data integrity are preserved in such networks. Unfortunately, no integrated solutions have

been proposed so far, able to tackle both issues in a unified and general environment. To bridge this gap, in this paper we present an approach for dynamic secure end-to-end data aggregation with privacy function, named DyDAP. It has been designed starting from a UML model that encompasses the most important building blocks of a privacy-aware WSN, including aggregation policies.

- ## Voice over IP (VoIP)

M. Benini, S. Sicari, "Assessing the risk of intercepting VoIP calls", Elsevier, Computer Networks, Vol. 52, No. 12, pp. 2432-2446, 2008.
Voice over-IP (VoIP) solutions and services for corporate telephony are usually marketed as 'cost-free' and 'secure': this paper shows that both statements are false in general. Though being no doubt about the economical benefits resulting from the adoption of VoIP products instead of the standard telephony, hidden costs related to VoIP services security arise whenever a company intends to assure the privacy of its phone conversations. This conclusion is extensively justified in the literature and this article aims at reasserting it by analysing the risk that a VoIP phone call may be intercepted when travelling across the Internet.

- ## WiMAX (IEEE 802.16)

C. Kolias, G. Kambourakis, S. Gritzalis, "Attacks and Countermeasures on 802.16: Analysis and Assessment", IEEE Communications Surveys and Tutorials, Vol.15, No.1, pp. 487-514, 2013.
The IEEE 802.16 technology, commonly referred to as WiMAX, gains momentum as an option for broadband wireless communication access. So far, several research works focus on the security of the 802.16 family of standards. In this context, the contribution of this paper is twofold. First, it provides a comprehensive taxonomy of attacks and countermeasures on 802.16. Each attack is classified based on several factors, e.g. its type, likelihood of occurrence, impact upon the system etc. and its potential is reviewed with reference to the standard. Possible countermeasures and remedies proposed for each category of attacks are also discussed to assess their effectiveness. Second, a full-scale assessment study of indicative attacks that belong to broader attack classes is conducted in an effort to better comprehend their impact on the 802.16 realm. As far as we are aware of, this is the first time an exhaustive and detailed survey of this kind is attempted.

- ## RFID

P. Rizomiliotis, E. Rekleitis, S. Gritzalis, "Security Analysis of the Song-Mitchell Authentication Protocol for Low-Cost RFID tags", IEEE Communications Letters, Vol. 13, No. 4, pp. 274-276, 2009.

In this paper, we describe an attack against one of the most efficient authentication protocols for low-cost RFID tags recently proposed by Song and Mitchell. A weak attacker, i.e. an attacker that has no access to the internal data of a tag, is able to impersonate a legitimate reader/server, and to desynchronize a tag. The attack is very efficient and has minimal computational complexity. Finally, we propose a simple solution to fix the flaw.

- ## Cryptographic Procedures

T. Rams, P. Pacyna, "A Survey of Group Key Distribution Schemes With Self-Healing Property", IEEE Communications Surveys & Tutorials, Vol. 15, No. 2, pp. 820-842, 2013.
Secure key distribution schemes for group communications allow to establish a secure multicast communication between a group manager and group members through an unreliable broadcast channel. The article classifies, analyzes and compares the most significant key distribution schemes, by looking at the selective key distribution algorithms, at the predistributed secret data management, and at the self-healing mechanisms. It reviews polynomial-based algorithms, exponential arithmetic based algorithms, hash-based techniques, and others. Attention is paid to the self-healing property, which permits group members to recover missing session keys from the recent key distribution broadcast message, without any additional interaction with the group manager.

- ## Cloud

S. A. de Chaves, C. B. Westphall, F. R. Lamin, "SLA Perspective in Security Management for Cloud Computing", Proceedings of IEEE ICNS'10, pp. 212-217, 2010.
One of the network and services management problems is security, either in systems or in administrative matters, which involves not just what needs to be protected, but also what security service levels will be delivered. This paper explores Service Level Agreements for Security or just Sec-SLAs. Is tried to provide an overview on the subject, the difficulties faced during the security metrics definition process and the Sec-SLA monitoring, as well as an analysis on the Sec-SLA role in new paradigms like cloud computing.

- ## Security Management

C. B. Westphall, C. M. Westphall, F. L. Koch, "Management and Security for Grid, Cloud and Cognitive Networks", Journal of Information Systems of the FSMA, Vol. 2, No. 8, pp. 8-21, 2011.
This paper presents a number of research initiativesrelated to innovative and cut-edge technologies for Cloud Computing. These are chiefly in the fields of (i) environment security, (ii) quality assurance, (iii) service composition, and (iv) system management. We present technologies for intrusion detection; a SLA perspective in security management; customer

security concerns; a Cloud- based solution for eHealth; experimental assessment of routing for grid and cloud; simulator improvements to validate the green cloud computing approach, and a framework to radio layer operation in cognitive networks.

- ## Smartphone

Damopoulos D., Kambourakis G., Gritzalis S, "iSAM: An iPhone Stealth Airborne Malware ", Springer, IFIP Advances in Information and Communication Technology, Vol. 354, pp. 17-28, 2011.
Modern and powerful mobile devices comprise an attractive target for any potential intruder or malicious code. The usual goal of an attack is to acquire users' sensitive data or compromise the device so as to use it as a stepping stone (or bot) to unleash a number of attacks to other targets. In this paper, we focus on the popular iPhone device. We create a new stealth and airborne malware namely iSAM able to wirelessly infect and self-propagate to iPhone devices. iSAM incorporates six different malware mechanisms, and is able to connect back to the iSAM bot master server to update its programming logic or to obey commands and unleash a synchronized attack. Our analysis unveils the internal mechanics of iSAM and discusses the way all iSAM components contribute towards achieving its goals. Although iSAM has been specifically designed for iPhone it can be easily modified to attack any iOS-based device.
