My Papers

Manos Panaousis

March 25, 2018

2017

Abstract of [1]: Cybersecurity has become a key factor that determines the success or failure of companies that rely on information systems. Therefore, investment in cybersecurity is an important financial and operational decision. Typical information technology investments aim to create value, whereas cybersecurity investments aim to minimize loss incurred by cyber attacks. Admittedly, cybersecurity investment has become an increasingly complex one since information systems are typically subject to frequent attacks, whose arrival and impact fluctuate stochastically. Further, cybersecurity measures and improvements, such as patches, become available at random points in time making investment decisions even more challenging.We propose and develop an analytical real options framework that incorporates major components relevant to cybersecurity practice, and analyze how optimal cybersecurity investment decisions perform for a private firm. The novelty of this paper is that it provides analytical solutions that lend themselves to intuitive interpretations regarding the effect of timing and cybersecurity risk on investment behavior using real options theory. Such aspects are frequently not implemented within economic models that support policy initiatives. However, if these are not properly understood, security controls will not be properly set resulting in a dynamic inefficiency reflected in cycles of over or under investment, and, in turn, increased cybersecurity risk following corrective policy actions. Results indicate that greater uncertainty over the cost of cybersecurity attacks raises the value of an embedded option to invest in cybersecurity. This increases the incentive to suspend operations temporarily in order to install a cybersecurity patch that will make the firm more resilient to cybersecurity breaches. Similarly, greater likelihood associated with the availability of a cybersecurity patch increases the value of the option to invest in cybersecurity. However, absence of an embedded investment option increases the incentive to delay the permanent abandonment of the company's operation due to the irreversible nature of the decision.

Abstract of [2]: The occurrence of congestion has an extremely deleterious impact on the performance of Wireless Sensor Networks (WSNs). This article presents a novel protocol, named COALA (COngestion ALleviation and Avoidance), which aims to act both proactively, in order to avoid the creation of congestion in WSNs, and reactively, so as to mitigate the diffusion of upcoming congestion through alternative path routing. Its operation is based on the utilization of an accumulative cost function, which considers both static and dynamic metrics in order to send data through the paths that are less probable

to be congested. COALA is validated through simulation tests, which exhibit its ability to achieve remarkable reduction of loss ratios, transmission delays and energy dissipation. Moreover, the appropriate adjustment of the weighting of the accumulative cost function enables the algorithm to adapt to the performance criteria of individual case scenarios.

Abstract of [3]: This paper proposes a conceptual model to support decision makers during security analysis of Internet of Things (IoT) systems. The world is entering an era of ubiquitous computing with IoT being the main driver. Taking into account the scale of IoT, the number of security issues that are arising are unprecedented. Both academia and industry require methodologies that will enable reasoning about security in IoT system in a concise and holistic manner. The proposed conceptual model addresses a number of challenges in modeling IoT to support security analysis. The model is based on an architecture-oriented approach that incorporates socio-technical concepts into the security analysis of an IoT system. To demonstrate the usage of the proposed conceptual model, we perform a security analysis on a small scale smart home example.

Abstract of [4]: As security is a growing concern for modern information systems, Security Requirements Engineering has been developed as a very active area of research. A large body of work deals with elicitation, modelling, analysis, and reasoning about security requirements. However, there is little evidence of efforts to align security requirements with security mechanisms. This paper extends the Secure Tropos methodology to enable a clear alignment, between security requirements and security mechanisms, and a reasoning technique to optimise the selection of security mechanisms based on these security requirements and a set of other factors. The extending Secure Tropos supports modelling and analysis of security mechanisms; defines mathematically relevant modelling concepts to support a formal analysis; and defines and solves an optimisation problem to derive optimal sets of security mechanisms. We demonstrate the applicability of our work with the aid of a case study from the health care domain.

Abstract of [5]: Device-to-Device (D2D) communication is expected to be a key feature supported by 5G networks, especially due to the proliferation of Mobile Edge Computing (MEC), which has a prominent role in reducing network stress by shifting computational tasks from the Internet to the mobile edge. Apart from being part of MEC, D2D can extend cellular coverage allowing users to communicate directly when telecommunication infrastructure is highly congested or absent. This significant departure from the typical cellular paradigm imposes the need for decentralised network routing protocols. Moreover, enhanced capabilities of mobile devices and D2D networking will likely result in proliferation of new malware types and epidemics. Although the literature is rich in terms of D2D routing protocols that enhance quality-of-service and energy consumption, they provide only basic security support, e.g., in the form of encryption. Routing decisions can, however, contribute to collaborative detection of mobile malware by leveraging different kinds of anti-malware software installed on mobile devices. Benefiting from the cooperative nature of D2D communications, devices can rely on each others' contributions to detect

malware. The impact of our work is geared towards having more malware-free D2D networks. To achieve this, we designed and implemented a novel routing protocol for D2D communications that optimises routing decisions for explicitly improving malware detection. The protocol identifies optimal network paths, in terms of malware mitigation and energy spent for malware detection, based on a game theoretic model. Diverse capabilities of network devices running different types of anti-malware software and their potential for inspecting messages relayed towards an intended destination device are leveraged using game theoretic tools. An optimality analysis of both Nash and Stackelberg security games is undertaken, including both zero and non-zero sum variants, and the Defender's equilibrium strategies. By undertaking network simulations, theoretical results obtained are illustrated through randomly generated network scenarios showing how our protocol outperforms conventional routing protocols, in terms of expected payoff, which consists of: security damage inflicted by malware and malware detection cost.

Abstract of [6]: Near Field Communication (NFC) has enabled mobile phones to emulate contactless smart cards. Similar to contactless smart cards, they are also susceptible to relay attacks. To counter these, a number of methods have been proposed that rely primarily on ambient sensors as a proximity detection mechanism (also known as an anti-relay mechanism). In this paper, we empirically evaluate a comprehensive set of ambient sensors for their effectiveness as a proximity detection mechanism for NFC contactless-based applications like banking, transport and high-security access controls. We selected 17 sensors available via the Google Android platform. Each sensor, where feasible, was used to record the measurements of 1,000 contactless transactions at four different physical locations. A total of 252 users, a random sample from the university student population, were involved during the field trials. After careful analysis, we conclude that no single evaluated mobile ambient sensor is suitable for proximity detection in NFC-based contactless applications in realistic deployment scenarios. Lastly, we identify a number of potential avenues that may improve their effectiveness.

Abstract of [7]: It is well acknowledged that one of the key enabling factors for the realization of future 5G networks will be the small cell (SC) technology. Furthermore, recent advances in the fields of network functions virtualization (NFV) and software-defined networking (SDN) open up the possibility of deploying advanced services at the network edge. In the context of mobile/cellular networks this is referred to as mobile edge computing (MEC). Within the scope of the EU-funded research project SESAME we perform a comprehensive security modelling of MEC-assisted quality-of-experience (QoE) enhancement of fast moving users in a virtualized SC wireless network, and demonstrate it through a representative scenario toward 5G. Our modelling and analysis is based on a formal security requirements engineering methodology called Secure Tropos which has been extended to support MEC-based SC networks. In the proposed model, critical resources which need protection, and potential security threats are identified. Furthermore, we identify appropriate security constraints and suitable security mechanisms for 5G networks. Thus, we reveal that existing security mechanisms need adaptation to face emerging security threats in 5G networks.

Abstract of [8]: In this paper, a software tool for security analysis of IoT systems is presented. The tool, named ASTo (Apparatus Software Tool) enables the visualization of IoT systems using a domain-specific modeling language. The modeling language provides constructs to express the hardware, software and social concepts of an IoT system along with security concepts. Security issues of IoT systems are identified based on the attributes of the constructs and their relationships. Security analysis is facilitated using the visualization mechanisms of the tool to recognize the secure posture of an IoT system.

Abstract of [9]: When undertaking cyber security risk assessments, we must assign numeric values to metrics to compute the final expected loss that represents the risk that an organization is exposed to due to cyber threats. Even if risk assessment is motivated from real-world observations and data, there is always a high chance of assigning inaccurate values due to different uncertainties involved (e.g., evolving threat landscape, human errors) and the natural difficulty of quantifying risk per se. Our previous work [1] has proposed a model and a software tool that empowers organizations to compute optimal cyber security strategies given their financial constraints, i.e., available cybersecurity budget. We have also introduced a general game-theoretic model [2] with uncertain payoffs (probability-distribution-valued payoffs) showing that such uncertainty can be incorporated in the game-theoretic model by allowing payoffs to be random. In this paper, we combine our aforesaid works and we conclude that although uncertainties in cyber security risk assessment lead, on average, to different cyber security strategies, they do not play significant role into the final expected loss of the organization when using our model and methodology to derive this strategies. We show that our tool is capable of providing effective decision support. To the best of our knowledge this is the first paper that investigates how uncertainties on various parameters affect cyber security investments.

2016

Abstract of [10]: When investing in cyber security resources, information security managers have to follow effective decision-making strategies. We refer to this as the cyber security investment challenge.In this paper, we consider three possible decision support methodologies for security managers to tackle this challenge. We consider methods based on game theory, combinatorial optimisation, and a hybrid of the two. Our modelling starts by building a framework where we can investigate the effectiveness of a cyber security control regarding the protection of different assets seen as targets in presence of commodity threats. As game theory captures the interaction between the endogenous organisation's and attackers' decisions, we consider a 2-person control game between the security manager who has to choose among different implementation levels of a cyber security control, and a commodity attacker who chooses among different targets to attack. The pure game theoretical methodology consists of a large game including all controls and all threats. In the hybrid methodology the game solutions of individual control-games along with their direct costs (e.g. financial) are combined with a Knapsack algorithm to derive an optimal investment strategy. The combinatorial optimisation technique consists of a

multi-objective multiple choice Knapsack based strategy. To compare these approaches we built a decision support tool and a case study regarding current government guidelines. The endeavour of this work is to highlight the weaknesses and strengths of different investment methodologies for cyber security, the benefit of their interaction, and the impact that indirect costs have on cyber security investment. Going a step further in validating our work, we have shown that our decision support tool provides the same advice with the one advocated by the UK government with regard to the requirements for basic technical protection from cyber attacks in SMEs.

Abstract of [11]: Internet of Things (IoT) can be seen as the main driver towards an era of ubiquitous computing. Taking into account the scale of IoT, the number of security issues that emerge are unprecedented, therefore the need for proposing new methodologies for elaborating about security in IoT systems is undoubtedly crucial and this is recognised by both academia and the industry alike. In this work we present Apparatus, a conceptual model for reasoning about security in IoT systems through the lens of Security Requirements Engineering. Apparatus is architecture-oriented and describes an IoT system as a cluster of nodes that share network connections. The information of the system is documented in a textual manner, using Javascript Notation Object (JSON) format, in order to elicit security requirements. To demonstrate its usage the security requirements of a temperature monitor system are identified and a first application of Apparatus is exhibited.

Abstract of [12]: Research on next-generation 5G wireless networks is currently attracting a lot of attention in both academia and industry. While 5G development and standardization activities are still at their early stage, it is widely acknowledged that 5G systems are going to extensively rely on dense small cell deployments, which would exploit infrastructure and network functions virtualization (NFV), and push the network intelligence towards network edges by embracing the concept of mobile edge computing (MEC). As security will be a fundamental enabling factor of small cell as a service (SCaaS) in 5G networks, we present the most prominent threats and vulnerabilities against a broad range of targets. As far as the related work is concerned, to the best of our knowledge, this paper is the first to investigate security challenges at the intersection of SCaaS, NFV, and MEC. It is also the first paper that proposes a set of criteria to facilitate a clear and effective taxonomy of security challenges of main elements of 5G networks. Our analysis can serve as a staring point towards the development of appropriate 5G security solutions. These will have crucial effect on legal and regulatory frameworks as well as on decisions of businesses, governments, and end-users.

Abstract of [13]:
[14] [15] [16] [17] [18] [19] [20] [21] [19] [22] [23] [24] [25] [26] [27] [28] [14] [29] [30] [31] [32] [33] [34] [35] [36] [37] [38] [39] [40] [41]
[**?**]

References

[1] Michail Chronopoulos, Emmanouil Panaousis, and Jens Grossklags. An options approach to cybersecurity investment. *IEEE Access*, 2017.

[2] Dionisis Kandris, George Tselikis, Eleftherios Anastasiadis, Emmanouil Panaousis, and Tasos Dagiuklas. Coala: A protocol for the avoidance and alleviation of congestion in wireless sensor networks. *Sensors*, 17(11), 2017.

[3] Orestis Mavropoulos, Haralambos Mouratidis, Andrew Fish, Panaousis, Emmanouil, and Christos Kalloniatis. A conceptual model to support security analysis in the internet of things. *Computer Science and Information Systems.*, 14(2):557–578, 2017.

[4] Michalis Pavlidis, Haralambos Mouratidis, Emmanouil Panaousis, and Nikolaos Argyropoulos. Selecting security mechanisms in secure tropos. In *International Conference on Trust and Privacy in Digital Business*, pages 99–114. Springer, Cham, 2017.

[5] Emmanouil Panaousis, Eirini Karapistoli, Hadeer Elsemary, Tansu Alpcan, MHR Khuzani, and Anastasios A Economides. Game theoretic path selection to support security in device-to-device communications. *Ad Hoc Networks*, 56:28–42, 2017.

[6] Carlton Shepherd, Iakovos Gurulian, Eibe Frank, Konstantinos Markantonakis, Raja Naeem Akram, Keith Mayes, and Emmanouil Panaousis. The applicability of ambient sensors as proximity evidence for nfc transactions. In *IEEE Security and Privacy Workshops (SPW)*. IEEE, 2017.

[7] Vassilios G. Vassilakis, Haralambos Mouratidis, Emmanouil Panaousis, Ioannis D. Moscholios, and Michael D. Logothetis. Security requirements modelling for virtualized 5g small cell networks. In *24th International Conference on Telecommunications*, 2017.

[8] Orestis Mavropoulos, Haralambos Mouratidis, Andrew Fish, and Emmanouil Panaousis. Asto: A tool for security analysis of iot systems. In *1st IEEE SERA Workshop on the Internet of People And Things*. IEEE, 2017.

[9] Andrew Fielder, Sandra Konig, Emmanouil Panaousis, Stefan Schauer, and Stefan Rass. Uncertainty in cyber security investments. *arXiv preprint arXiv:1712.05893*, 2017.

[10] Andrew Fielder, Emmanouil Panaousis, Pasquale Malacaria, Chris Hankin, and Fabrizio Smeraldi. Decision support approaches for cyber security investment. *Decision Support Systems*, 86:13–23, 2016.

[11] Orestis Mavropoulos, Haralambos Mouratidis, Andrew Fish, Emmanouil Panaousis, and Christos Kalloniatis. Apparatus: Reasoning about security requirements in the internet of things. In *International Conference on Advanced Information Systems Engineering*, pages 219–230. Springer International Publishing, 2016.

[12] Vassilios Vassilakis, Emmanouil Panaousis, and Haralambos Mouratidis. Security challenges of small cell as a service in virtualized mobile edge computing environments. In *IFIP International Conference on Information Security Theory and Practice*, pages 70–84. Springer International Publishing, 2016.

[13] Adeyinka Adedoyin, Stelios Kapetanakis, Miltos Petridis, and Emmanouil Panaousis. Evaluating case-based reasoning knowledge discovery in fraud detection. In *24th International Conference in Case-based Reasoning*, 2016.

[14] Emmanouil A Panaousis, Levon Nazaryan, and Christos Politis. Securing aodv against wormhole attacks in emergency manet multimedia communications. In *5th International Mobile Multimedia Communications Conference*. ACM, 2009.

[15] Emmanouil A Panaousis and Christos Politis. A game theoretic approach for securing aodv in emergency mobile ad hoc networks. In *IEEE 34th Conference on Local Computer Networks (LCN)*. IEEE, 2009.

[16] Emmanouil A Panaousis, Christos Politis, Konstantinos Birkos, Christos Papageorgiou, and Tasos Dagiuklas. Security model for emergency real-time communications in autonomous networks. *Information Systems Frontiers,*, 14(3):541–553, 2012.

[17] Emmanouil A Panaousis, Tipu A Ramrekha, Grant P Millar, and Christos Politis. Adaptive and secure routing protocol for emergency mobile ad hoc networks. *International Journal of Wireless & Mobile Computing,*, (arXiv:1005.1740), 2010.

[18] Emmanouil A Panaousis, George Drew, Grant P Millar, Tipu A Ramrekha, and Christos Politis. A testbed implementation for securing olsr in mobile ad hoc networks. *International Journal of Network Security & Its Applications (IJNSA),*, (arXiv:1010.4986), 2010.

[19] Emmanouil A Panaousis, Tipu Arvind Ramrekha, and Christos Politis. Secure routing for supporting ad-hoc extreme emergency infrastructures. In *19th Future Network and Mobile Summit*. IEEE, 2010.

[20] Grant P Millar, Emmanouil A Panaousis, and Christos Politis. Robust: Reliable overlay based utilisation of services and topology for emergency manets. In *19th Future Network and Mobile Summit*. IEEE, 2010.

[21] TA Ramrekha, Emmanouil Panaousis, and C Politis. Routing challenges and directions for smart objects in future internet of things. In *IETF Internet Architecture Board and Internet Area Workshop on Interconnecting Smart Objects with the Internet, Prague, Czech Republic*. IETF, 2011.

[22] Tipu Arvind Ramrekha, Emmanouil Panaousis, and Christos Politis. Standardisation advancements in the area of routing for mobile ad-hoc networks. *Journal of Supercomputing, Special issue: Advancements in Communication Networks for Pervasive & Ubiquitous Applications*, 64(2):409–434, 2013.

[23] Farrukh Ehtisham, Emmanouil Panaousis, and Christos Politis. Performance evaluation of secure video transmission over wimax. *International Journal of Computer Networks & Communications,*, 3(6):131–144, 2011.

[24] RIFA-POUS Helena, Emmanouil A Panaousis, and Christos Politis. Recipients' anonymity in multihop ad-hoc networks. *IEICE Transactions on Information Systems, Special issue: Trust, Security and Privacy in Computing and Communication Systems*, 95(1):181–184, 2012.

[25] Grant Paul Millar, Emmanouil A. Panaousis, and Christos Politis. Distributed hash tables for peer-to-peer mobile ad-hoc networks with security extensions. *Journal of Networks,*, 7(2):288–299, 2012.

[26] Alkiviadis Tsitsigkos, Fariborz Entezami, Tipu Ramrekha, Christos Politis, and Emmanouil Panaousis. A case study of internet of things based on wireless sensor networks and smartphones. In *28th Wireless World Research Forum meeting*, 2012.

[27] Emmanouil A Panaousis, Tipu A Ramrekha, Christos Politis, and Grant P Millar. Secure decentralised ubiquitous networking for emergency communications. In *5th International Conference on Telecommunications and Multimedia*. IEEE, 2012.

[28] Georgios Polymerou, Emmanouil A Panaousis, Eckhard Pfluegel, and Christos Politis. A novel lightweight multi-secret sharing technique for mobile ad-hoc networks. In *29th Wireless World Research Forum meeting*, 2012.

[29] Emmanouil A Panaousis, ATR Ramrekha, Konstantinos Birkos, Christos Papageorgiou, Vahid Talooki, George Matthew, Cong Thien Nguyen, Corrine Sieux, Christos Politis, Tasos Dagiuklas, et al. A framework supporting extreme emergency services. In *18th ICT Mobile and Wireless Communications Summit*, 2009.

[30] Emmanouil A Panaousis, Christos Politis, and George C Polyzos. Maximizing network throughput. *IEEE Vehicular Technology Magazine,*, 4(3):33–39, 2009.

[31] Emmanouil Panaousis and Christos Politis. Non-cooperative games between legitimate nodes and malicious coalitions in manets. In *20th Future Network and Mobile Summit*. IEEE, 2011.

[32] Eckhard Pfluegel, Emmanouil Panaousis, and Christos Politis. A probabilistic algorithm for secret matrix share size reduction. In *19th European Wireless Conference*. IEEE, 2013.

[33] Levon Nazaryan, Emmanouil A Panaousis, and Christos Politis. End-to-end security protection. *IEEE Vehicular Technology Magazine,*, 5(1):85–90, 2010.

[34] Emmanouil Kafetzakis, Nikolaos V Boulgouris, Emmanouil Panaousis, and Anastasios Kourtis. Secure communications for mobile verification platforms. In *10th International Symposium on Wireless Communication System (ISWCS '13), Ilmenau, Deutschland*. IEEE xplore, 2013.

[35] Emmanouil Panaousis, Tansu Alpcan, Hossein Fereidooni, and Mauro Conti. Secure message delivery games for device-to-device communications. In *5th Conference on Decision and Game Theory for Security (GameSec)*. Springer, 2014.

[36] Levon Nazaryan, Nabeel Khan, Emmanouil A Panaousis, and Christos Politis. Performance evaluation of ipsec over wimax. In *23rd Wireless World Research Forum meeting (WWRF 23)*, pages 20–22, 2009.

[37] TA Ramrekha, GP Millar, EA Panaousis, and C Politis. Framework for ubiquitous networking, 2011.

[38] Emmanouil Panaousis, Aron Laszka, Johannes Pohl, Andreas Noack, and Tansu Alpcan. Game-theoretic model of incentivizing privacy-aware users to consent to location tracking. In *IEEE 14th International Conference on Trust, Security and Privacy in Computing and Communications (IEEE Trustcom 2015)*. IEEE xplore, 2015.

[39] Andrew Fielder, Emmanouil Panaousis, Pasquale Malacaria, Chris Hankin, and Fabrizio Smeraldi. Game theory meets information security management. In *IFIP International Information Security Conference*, pages 15–29. Springer, Berlin, Heidelberg, 2014.

[40] Emmanouil Panaousis, Andrew Fielder, Pasquale Malacaria, Chris Hankin, and Fabrizio Smeraldi. Cybersecurity games and investments: A decision support approach. In *5th International Conference on Decision and Game Theory for Security*, pages 266–286. Springer International Publishing, 2014.

[41] George Rontidis, Emmanouil Panaousis, Aron Laszka, Tasos Dagiuklas, Pasquale Malacaria, and Tansu Alpcan. A game-theoretic approach for minimizing security risks in the internet-of-things. In *IEEE International Conference on Communication Workshop*, pages 2639–2644. IEEE, 2015.