My Papers

Manos Panaousis

March 2, 2018

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 sociotechnical 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.

[4] [5] [6] [7] [8] [9] [10] [11] [9] [12] [13] [14] [15] [16] [17] [18] [4] [19] [20] [21] [22] [23] [24] [25] [26] [27] [28] [29] [30] [31] [32] [33] [34] [35] [36] [37] [38] [39] [40] [41] [3] [42] [2]

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] 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.

[5] 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.

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

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

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

[21] 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.

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

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

[24] 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.

[25] 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.

[26] 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.

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

[28] 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.

[29] 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.

[30] 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.

[31] 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.

[32] 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.

[33] 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.

[34] 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.

[35] 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.

[36] 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.

[37] 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.

[38] 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.

[39] 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.

[40] 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.

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

[42] Emmanouil A Panaousis and Tipu A Ramrekha. Grant p. *Millar et Christos Politis Adaptive and Secure routing protocol for emergency mobile ad hoc networks, Aticle: International Journal of Wireless & Mobile Networks*, 2010.