Next Generation of Hybrid Threats

Next Generation of Hybrid Threats

Fulvio Valenza
fulvio.valenza@polito.it
Politecnico di Torino, Dip. Automatica e Informatica
Torino, Italy

ABSTRACT

Novel technologies and paradigms such as Cloud and Edge Computing, the Internet of Things (IoT), Network virtualization such as Software Defined Network (SDN), and Network Function Virtualization (NFV) are anymore present in our everyday life. They have been used in many use-cases and environments, like industrial control systems, modern buildings, homes, transportation, and critical infrastructures. Moreover, nowadays, novel devices and environments become more and more interconnected, fast, intelligent, and dynamic. The increasing use of these "smart" devices and environments brings a novel technological revolution that generates new opportunities and functionalities for consumers across all sectors, from agriculture to manufacturing, healthcare to transport, and industry to home[3, 5].

However, these novel advantages and benefits introduce new risks and challenges. Indeed, these novel and complex systems leveraging intelligent devices are vulnerable to attacks that exploit their physical, human, and cyber vulnerabilities by combining them in any order. People are exposed to new risks from the outside world as more threats can undermine cybersecurity[1, 2].

Generally, we can define “hybrid systems” as interconnected human, physical and cyber components and elements and “hybrid attacks” as multistep attacks that exploit the combination of human, physical, or cyber vulnerabilities in a hybrid system. Indeed, the physical security of a system, its cybersecurity, and human security are traditionally managed separately and by different people/teams within an organization. In hybrid systems, the cyber, physical, and human aspects can be leveraged in combination as part of the same attack. They typically also complement each other and must be protected together to mitigate and respond to the new hybrid threats. For example, human or digital surveillance can monitor a physical space. This novel and larger exposition surface, caused by hybrid threats, has impacted individuals’ privacy and wellness. Configuring enough and suitable protection and detecting the errors and vulnerabilities that new hybrid threats may exploit in these hybrid systems is more challenging than traditional systems and environments.

These challenges are also accentuated by many aspects and characteristics that include low computational power, inadequate software quality, and, more importantly, such environments combine human, physical and digital (cyber) aspects to the system design and implementation. These considerations are supported by the most recent Data Breach Investigations Report by Verizon[1], which show as cyber and physical attacks evolve as fast as the deployment of intelligent systems and are outpacing efforts to stop them.

Unfortunately, in the most recent state of the art, there is no notation and no framework to be able to represent threats that propagate across the physical, human, and digital aspects of a system or how to use them in combination. For example, how human vulnerabilities (e.g., phishing or bribery) can lead to threats to the cyber or physical aspects of the system or how cyber vulnerabilities can lead to threats to the physical environment. It is not sufficient for such a framework to combine the different aspects/components of the system. It must also represent the relationships between them, their inter-dependencies, and the compositional nature of systems[4, 6].

CCS CONCEPTS

• **Security and privacy → Formal security models**.

KEYWORDS

Threat Modelling, Security Analysis, Smart systems

ACM Reference Format:

Fulvio Valenza. 2022. Next Generation of Hybrid Threats. In *Proccedings of the European Interdisciplinary Cybersecurity Conference (EICC 2022), June 15–16, 2022, Barcelona, Spain.* ACM, New York, NY, USA, 1 page. https://doi.org/10.1145/3528580.3535333

REFERENCES

[1] D. Bringhenti, F. Valenza, and C. Basile. 2022. Toward Cybersecurity Personalization in Smart Homes. *IEEE Security & Privacy* 20, 01 (jan 2022), 45–53. https://doi.org/10.1109/MSEC.2021.3117471

[2] Manuel Cheminod, Luca Durante, Lucia Seno, Fulvio Valenza, Adriano Valenzano, and Claudio Zunino. 2017. Leveraging SDN to improve security in industrial networks. In *2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS).* 1–7. https://doi.org/10.1109/WFCS.2017.7991960

[3] S. K. Khaitan and J. D. McCalley. 2015. Design Techniques and Applications of Cyberphysical Systems: A Survey. *IEEE Systems Journal* 9, 2 (2015), 350–365. https://doi.org/10.1109/JSYST.2014.2322503

[4] Harjinder Singh Lallie, Kurt Debattista, and Jay Bal. 2020. A review of attack graph and attack tree visual syntax in cyber security. *Computer Science Review* 35 (2020), 100219.

[5] Jianxin Wang, Ming K. Lim, Chao Wang, and Ming-Lang Tseng. 2021. The evolution of the Internet of Things (IoT) over the past 20 years. *Computers & Industrial Engineering* 155 (2021), 107174. https://doi.org/10.1016/j.cie.2021.107174

[6] Wenjun Xiong and Robert Lagerström. 2019. Threat modeling – A systematic literature review. *Computers & Security* 84 (2019), 53–69.

EICC 2022, June 15–16, 2022, Barcelona, Spain

ACM ISBN 978-1-4503-9603-5/22/06.
https://doi.org/10.1145/3528580.3535333

[1] Verizon 2021 Data Breach Investigations Report. Available: https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf, Visited: April 2022.