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, 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:


REFERENCES


Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

ECC 2022, June 15–16, 2022, Barcelona, Spain
© 2022 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-9603-5/22/06.
https://doi.org/10.1145/3528580.3535333