Chapter 82
Human Factors in Cybersecurity:
Issues and Challenges in Big Data

Xichen Zhang
University of New Brunswick, Canada

Ali A. Ghorbani
University of New Brunswick, Canada

ABSTRACT

Over recent years, the extensive development of information technology has dramatically advanced the way that people use the internet. The fast growth of the internet of things and mobile crowdsensing applications raise challenging security and privacy issues for the society. More often than before, malicious attackers exploit human vulnerability as the weakest link to launch cyberattacks and conduct fraudulent online activities. How to profile users' daily behavior becomes an essential component for identifying users' vulnerable/malicious level and predicting the potential cyber threats. In this chapter, the authors discuss human factors and their related issues in cyber security and privacy. Three categories of human behaviors—desktop behavior, mobile behavior, and online behavior—and their corresponding security and privacy issues are demonstrated in detail to estimate the vulnerabilities of internet users. Some future directions related to human-factor based security and privacy issues are proposed at the end of this chapter.

INTRODUCTION

In recent years, the growth of online Cloud services and the increasing number of remote users rise more complex security and privacy issues. Hence, human factors play crucial roles in the pervasiveness of cyber threats and attacks. As the fast and extensive development of cybersecurity technologies, novel and sophisticated approaches are used for fighting against digital cybercrimes. As a result, hackers need to seek new hacking methods to launch cyberattacks. With non-professional personnel being the weakest

DOI: 10.4018/978-1-7998-8954-0.ch082

link, most of the advanced attacks rely heavily on human factors. Human's interaction with the electric devices and their performance in normal security procedure can bring potential cyber threats and vulnerabilities in daily actions. Under this circumstance, how to profile human's daily behavior and evaluate users' malicious and vulnerable level should be paid more attention in both academia and industry.

With the help of daily user behavior analysis, cyber defenders and experts can flag and report abnormal online actions that are potentially suspicious and anomalous. However, accurate user profiling analysis is still challenging, due to the complex, diverse, and dynamic nature of human's online behaviors. Most of the previous studies only focus on technological perspective of defending cyberattacks. The limited availability of related research poses great difficulties for both researchers and industrial participators. So, the motivation of this Chapter can be summarized as follows. (1) The current research of cyberattack analysis is not adequate to capture human-based factors in cyber space. There is an immediate need for understanding human's daily online behaviors and labeling the malicious level or vulnerable level of an Internet user. (2) The recent studies of human-based factors in cyber security and privacy are diverse in terms of objectives, methodologies and domains. It is necessary to summarize different types of online behaviors in a consistent format. This can provide practical conveniences and guidance for researchers. (3) With the development of computing technologies, new methodologies and application scenarios (e.g., *mobile crowdsensing*, *adversarial machine learning*) can bring new trends of challenges and difficulties. It is a necessity to present new information threats under these domains and propose promising approaches for addressing such issues. All in all, by consolidating malicious and vulnerable human daily behaviors, and extracting intelligent insights from human daily factors, cyber defenders and experts can effectively detect cyber attackers, and reduce the impact of those information threats.

In this chapter we first introduce the role of human factors in cyberspace, and the importance of profiling user behaviors in cybersecurity. Then, from the following three aspects of human factors: *desktop behaviors, mobile behaviors, and online behaviors*, we propose the potential security and privacy issues in daily human practices, and then present important concepts, technologies and solutions of modeling users' normal behavior patterns and detecting abnormal, vulnerable and malicious actions. The contributions of this Chapter are: (1) We group the Internet users' behaviors into three categories: *desktop behavior*, *mobile behavior*, *and online behavior*, which is useful for researchers and participates to understand the nature of user's daily online actions; (2) For each type of user behavior, we present a comprehensive and up-to-date survey on the typical and important cyber issues and vulnerabilities. And readers can have a clear understanding of why human become the important factor in cyberspace, what are the common human-based vulnerabilities, how hackers target victims, and how to profile users' daily behaviors based on the available information. (3) At the end of this Chapter, we also propose some interesting and important research directions that can be worked in the future.

The rest of this Chapter is organized as follows. Section "Background" discusses the definition of insider attack and outsider attack, and then demonstrates the importance of user profiling techniques in the existing cyber defending approaches. Section "Security and Privacy Issues in Human's Desktop Behaviors" summarizes the common security and privacy issues for desktop users, and then propose some typical risk desktop behaviors and the corresponding mitigation methods. Section "Security and Privacy Issues in Human's Mobile Behaviors" presents common security vulnerabilities and threats of individual mobile users, and then discusses the essential security and privacy issues in a new emerging data sharing environment – mobile crowdsensing. In Section "Security and Privacy Issues In Human's Online Behaviors", three common and risk online behaviors (financial behavior, online social media, online Cloud) are discussed in detail. In Section "future research directions", some promising research