Chapter 2
Taxonomy of Cyber Threats to Application Security and Applicable Defenses

Winfred Yaokumah
https://orcid.org/0000-0001-7756-1832
University of Ghana, Ghana

Ferdinard Katsriku
University of Ghana, Ghana

Jamal-Deen Abdulai
University of Ghana, Ghana

Kwame Okwabi Asante-Offei
Ghana Institute of Management and Public Administration, Ghana

ABSTRACT

Application security measures are the controls within software systems that protect information assets from security attacks. Cyber attacks are largely carried out through software systems running on computing systems in cyberspace. To mitigate the risks of cyber attacks on software systems, identification of entities operating within cyberspace, threats to application security and vulnerabilities, and defense mechanisms are crucial. This chapter offers a taxonomy that identifies assets in cyberspace, classifies cyber threats into eight categories (buffer overflow, malicious software, input attacks, object reuse, mobile code, social engineering, back door, and logic bomb), provides security defenses, and maps security measures to control types and functionalities. Understanding application security threats and defenses will help IT security professionals in the choice of appropriate security countermeasures for setting up strong defense-in-depth mechanisms. Individuals can also apply these safeguards to protect themselves from cyber-attacks.

DOI: 10.4018/978-1-7998-3149-5.ch002

INTRODUCTION

Cyberspace represents the virtual environment that allows interaction of people, devices, software, networks, information, applications, critical information infrastructures, and services on the Internet using computing devices and telecommunication networks (ISO/IEC 27032, 2012). It is a complex environment of diverse entities and resources, comprising of stakeholders and their roles, cyberspace assets, threat agents and threats, vulnerabilities, and cybersecurity controls. Cyber threats are emerging risks posing a range of challenges to users of cyberspace (Marotta & McShane, 2018). Cybercriminals use cyberspace to launch attacks on information assets and critical information infrastructures. In 2018, it was estimated that cyberattacks cost the world economy some $45 billion (SecurityMagazine, 2019). The main medium by which cyber-attacks are carried out is via vulnerabilities in software applications and operating systems over communications networks. Thus, information technology (IT) security professionals are most concerned about threats to software systems, such as phishing and ransomware (Kerner, 2017). Though cyber-attacks may be detected, it often takes much time to recover from them (Kerner, 2017). According to a recent report, ransomware alone costs businesses more than $75 million per year (Oberly, 2019). It is suggested that cybersecurity threats will grow in importance, in particular, as the Internet-of-Things (IoT) becomes widespread (Rash, 2015).

With the aim of mitigating cyber-attacks, ISO/IEC 27032:2012 Guidelines for Cybersecurity provides guidance for reducing cyber risks. The standard describes cybersecurity practices and the roles of stakeholders in cyberspace, outlines guidelines for resolving common cybersecurity issues, and provide a framework for stakeholders to collaborate to resolve cybersecurity issues (ISO/IEC 27032, 2012). The standard identifies the following four major areas; a) information security, b) network security, c) Internet security, and d) critical information infrastructure protection (CIIP) (ISO/IEC 27032, 2012). According to Kerner (2017), though cybersecurity standards and practices have helped in the decline of network and client vulnerabilities, server vulnerabilities have increased by 34 percent. Apparently, organizations are losing the cyber-war due to overdependence on humans to protect computer systems (Needle, 2017). A recent studies and report note that human failure to comply with security policies (Yaokumah, Walker, Kumah, 2019), such as updating security patches, has led to the theft of 145.5 million credit cards and personal information (Anwar, 2019). Also, data breaches of 450 million records in 2018 and nearly 773 million passwords and email addresses were stolen in 2019 (Anwar, 2019).

Data breaches are carried out through software systems running on networks. Software systems security, often referred to as application security, is among the most important aspect of cyberspace security (McGraw, 2013). The International Information System Security Certification Consortium (ISC)[2] Common Body of Knowledge (CBK) defines the key areas of knowledge for application security as:

The controls that are included within systems and application software and the steps used in their development. Applications refer to agents, applets, software, databases, data warehouses, and knowledge-based systems. These applications may be used in distributed or centralized environments (Gregory, 2010, p.78).

Application security is one of the most important means of securing the cyberspace (McGraw, 2013). Threats to software systems can be malicious (such as distributed denial-of-service [DDoS] and injection attacks) or non-malicious (such as system crashes and Internet connection failures) (Refsdal et al., 2015). Malicious attacks are designed to steal information, deny access to, degrade, or destroy critical