Journal of Computer and System Sciences 80 (2014) 973–993

Contents lists available at ScienceDirect

Journal of Computer and System Sciences

www.elsevier.com/locate/jcss

A survey of emerging threats in cybersecurity

Julian Jang-Jaccard, Surya Nepal *

CSIRO ICT Centre, Australia

ARTICLE INFO

Article history:
Received 25 September 2012
Received in revised form 15 March 2013
Accepted 27 August 2013
Available online 10 February 2014

Keywords:
Cybersecurity
Malware
Emerging technology trends
Emerging cyber threats
Cyber attacks and countermeasures

ABSTRACT

The exponential growth of the Internet interconnections has led to a significant growth of cyber attack incidents often with disastrous and grievous consequences. Malware is the primary choice of weapon to carry out malicious intents in the cyberspace, either by exploitation into existing vulnerabilities or utilization of unique characteristics of emerging technologies. The development of more innovative and effective malware defense mechanisms has been regarded as an urgent requirement in the cybersecurity community. To assist in achieving this goal, we first present an overview of the most exploited vulnerabilities in existing hardware, software, and network layers. This is followed by critiques of existing state-of-the-art mitigation techniques as why they do or don't work. We then discuss new attack patterns in emerging technologies such as social media, cloud computing, smartphone technology, and critical infrastructure. Finally, we describe our speculative observations on future research directions.

1. Introduction

Our society, economy, and critical infrastructures have become largely dependent on computer networks and information technology solutions. Cyber attacks become more attractive and potentially more disastrous as our dependence on information technology increases. According to the Symantec cybercrime report published in April 2012 [17], cyber attacks cost US$114 billion each year. If the time lost by companies trying to recover from cyber attacks is counted, the total cost of cyber attacks would reach staggering US$385 billion [17]. Victims of cyber attacks are also significantly growing. Based on the survey conducted by Symantec which involved interviewing 20,000 people across 24 countries, 69% reported being the victim of a cyber attack in their lifetime. Symantec calculated that 14 adults become the victim of a cyber attack every second, or more than one million attacks every day [105].

Why cyber attacks flourish? It is because cyber attacks are cheaper, convenient and less risky than physical attacks [1]. Cyber criminals only require a few expenses beyond a computer and an Internet connection. They are unconstrained by geography and distance. They are difficult to identity and prosecute due to anonymous nature of the Internet. Given that attacks against information technology systems are very attractive, it is expected that the number and sophistication of cyber attacks will keep growing.

* Corresponding author.
E-mail addresses: julian.jang-jaccard@csiro.au (J. Jang-Jaccard), surya.nepal@csiro.au (S. Nepal).

http://dx.doi.org/10.1016/j.jcss.2014.02.005
0022-0000/

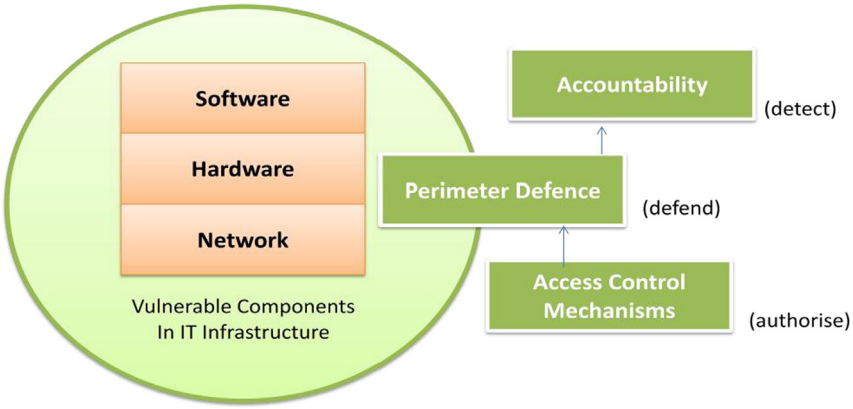

Fig. 1. Vulnerabilities and defense strategies in existing systems.

Cybersecurity concerns with the understanding of surrounding issues of diverse cyber attacks and devising defense strategies (i.e., countermeasures) that preserve confidentiality, integrity and availability of any digital and information technologies [18].

- **Confidentiality** is the term used to prevent the disclosure of information to unauthorized individuals or systems.
- **Integrity** is the term used to prevent any modification/deletion in an unauthorized manner.
- **Availability** is the term used to assure that the systems responsible for delivering, storing and processing information are accessible when needed and by those who need them.

Many cybersecurity experts believe that malware is the key choice of weapon to carry out malicious intends to breach cybersecurity efforts in the cyberspace [12]. Malware refers to a broad class of attacks that is loaded on a system, typically without the knowledge of the legitimate owner, to compromise the system to the benefit of an adversary. Some exemplary classes of malware include viruses, worms, Trojan horses, spyware, and bot executables [15]. Malware infects systems in a variety of ways for examples propagation from infected machines, tricking user to open tainted files, or alluring users to visit malware propagating websites. In more concrete examples of malware infection, malware may load itself onto a USB drive inserted into an infected device and then infect every other system into which that device is subsequently inserted. Malware may propagate from devices and equipments that contain embedded systems and computational logic. In short, malware can be inserted at any point in the system life cycle. Victims of malware can range anything from end user systems, servers, network devices (i.e., routers, switches, etc.) and process control systems such as Supervisory Control and Data Acquisition (SCADA). The proliferation and sophistication of fast growing number of malware is a major concern in the Internet today.

Traditionally, malware attacks happened at a single point of surface amongst hardware equipments, software pieces or at network level exploiting existing design and implementation vulnerabilities at each layer. Rather than protecting each asset, the perimeter defense strategy has been used predominantly to put a wall outside all internal resources to safeguard everything inside from any unwanted intrusion from outside. The majority of perimeter defense mechanism utilizes firewall and anti-virus software installed within intrusion prevention/detection systems. Any traffic coming from outside is intercepted and examined to ensure there is no malware penetrating into the inside resources. General acceptance of this perimeter defense model has occurred because it is far easier and seemingly less costly to secure one perimeter than it is to secure a large volume of applications or a large number of internal networks. To give more defined access to certain internal resources, the access control mechanisms have been used in conjunction with the perimeter defense mechanism. On top of perimeter defense and access control, accountability is added to identify or punish for any misbehaviors, as represented in Fig. 1. However, the combined efforts of perimeter defense strategy have been found to be increasingly ineffective as the advancement and sophistication of malware improves. Ever evolving malware always seems to find loopholes to bypass the perimeter defense altogether. We describe in details the most common exploitations in the three distinct layers of existing information system at hardware, software and network layers. We then discuss the pros and cons of the most representative defense mechanisms that have been used in these layers.

Malware evolves through time capitalizing on new approaches and exploiting the flaws in the emerging technologies to avoid detection. We describe a number of new patterns of malware attacks present in the emerging technologies. In choosing emerging technologies for illustration, we focus a few that have changed the way we live our daily life. These include social media, cloud computing, smartphone technology, and critical infrastructure. We discuss unique characteristics of each of these emerging technologies and how malware utilizes the unique characteristics to proliferate itself. For example, social media, such as social networking sites and blogs, are now an integral part of our life style as many people are journaling about their life events, sharing news, as well as making friends. Realizing its potential to connect millions people at one go, adversaries use social media accounts to befriend unsuspecting users to use as vehicles for sending spam to the victim's friends while the victim's machine is repurposed into a part of botnet. Cloud computing paradigm allows the