Diversity in Security Environments: The Why and the Wherefore

Anne V. D. M. Kayem (University of Cape Town, South Africa), Richard Ssembatya (University of Cape Town, South Africa) and Mark-John Burke (University of Cape Town, South Africa)

Source Title: Information Security in Diverse Computing Environment, © 2014.

DOI: 10.4018/978-1-4666-6158-5.ch001

Abstract

Information security is generally discussed in terms of preventing adversarial access to applications and to the data these applications handle. The authors note, however, that increasingly, creating information security solutions that are based on the difficulty of discovering the solution is no longer a truly viable approach. Some of the reasons for this include the increasing availability of faster processing power, high-performance computing systems, and big data availability. On the opposite end, issues such as frequent power outages in resource-constrained environments make applying standard security schemes challenging. In this chapter, the authors discuss examples that highlight the challenges of applying conventional security solutions to constrained resource environments. They postulate that effective security solutions for these environments require rather unconventional approaches to security-solution design. Such solutions would need to take into consideration environmental and behavioral factors in addition to drawing inspiration in certain cases from natural or biological processes.

Key Words: Diversity, Security, Environments

Introduction

The notion of resource constrained environments is tightly coupled with the growing field of information and communication technologies for development. Resource constrained environments however, are not a peculiarity of developing nations only but more generally of geographic locations where access to technological infrastructure is limited. For instance, in remote areas access to water, transportation, and electricity is sometimes hindered by factors that include cost of connection, low population density, and the infrastructural cost. In these cases, it is often not feasible cost-wise to set up the required infrastructure to make the service available to the population. Therefore, we define resource constrained environments to be areas in which convention methods of technology distribution are hindered by environmental and cost factors. Consequently, providing or implementing technological solutions in these environments requires that one step back and re-evaluate the options in order to find effective methods of addressing the challenges that emerge in the affected areas.

In this chapter and book in general, we focus specifically on the problems of implementing security solutions in resource constrained environments. Factors such as bandwidth limitations, power outages, limited access to information technology, make implementing security solutions in

conventional ways challenging. For instance, the popularity of smart phones in emerging economies has resulted in an increased access to social networking media. However, oftentimes the laws on privacy in these countries are quite different from what they are in the United States where the application was designed and implemented. When information gets leaked or exposed to unauthorized parties it is difficult if not impossible to prosecute the malicious user. The problem is further compounded by the fact that the lack of proper security regulations or legislature is creating a growing danger of what has been termed the "tsunami of information insecurity"(Goodman and Harris, 2010).

As Goodman et al. (Goodman and Harris, 2010) point out, cellphones are more affordable and accessible than regular computers are in most African countries. There several reasons for this, but two of the most cited ones include portability and usage simplicity. Frequent power outages make the idea of a small, low-power intensive device that can guarantee communication anytime and anywhere, attractive. Likewise, the usage simplicity of cellphones has addressed an issue that regular computers have struggled with for decades, that is ensuring that the device is simple enough to use irrespective of the education or tech savvy-ness of the user. Cellphones however are rapidly evolving and some of the current smartphones, though considerably more expensive than the first generation of cellphones, can by themselves operate as though they were mini-computers.

Using cellphones to access the Internet has also become a common practice in recent years and with this the host of privacy and security problems that emerge naturally in this environment. Lack of proper knowledge of or inability to pay for expensive security enforcing applications, is creating a growing situation of information insecurity for the users of these devices.

In this chapter we consider two cases of information insecurity scenarios that are created by factors such as constraints in resource availability, and social media access on mobile devices, due to their popularity in Africa. The rest of the chapter is structured as follows, in Section 2, we discuss factors such as power outages and bandwidth limitations in resource constrained environments. We evaluate the impact of these factors on information security and highlight some potential solutions for addressing these issues. In Section 3, we consider the issues such as the following:

1. Social media use on mobile phones amongst teenagers, and how privacy breaches can be exploited for bullying, and harassment.

2. Personal healthcare data management on mobile devices and the challenges of adopting standard electronic healthcare management systems in developing countries.

3. Enforcing privacy preservation on crime data via anonymity algorithms.

We offer concluding comments and discuss avenues for future work in Section 4.