Chapter 6
Responsibility for the Harm and Risk of Software Security Flaws

Cassio Goldschmidt
Symantec, Corp., USA

Melissa J. Dark
Purdue University, USA

Hina Chaudhry
Purdue University, USA

ABSTRACT

Software vulnerabilities are a vexing problem for the state of information assurance and security. Who is responsible for the risk and harm of software security is controversial. Deliberation of the responsibility for harm and risk due to software security flaws requires considering how incentives (and disincentives) and network effects shape the practices of vendors and adopters, and the consequent effects on the state of software security. This chapter looks at these factors in more detail in the context of private markets and public welfare.

INTRODUCTION

This chapter describes the current landscape of the responsibility for the harm and risk of software security flaws. We focus on software vulnerabilities for several reasons. Software assurance is critically important to information assurance and security and we believe it will be important for some time to come. While improvements in software security will be made, these will be incremental at best. Getting software right is still an art. No practical, formal methods exist to prove application security nor does a definitive authority exist to assert the absence of vulnerabilities. Small coding errors can lead to fatal flaws due to interactions among different components of complex software. The first portion of this chapter outlines who vendors are, their current practices to securing software, and overviews the forces that impinge on vendors' software security practices.

DOI: 10.4018/978-1-61692-245-0.ch006

While software is developed by vendors, it is deployed, operated, and sometimes adapted, by a myriad of adopters. Numerous decisions that adopters make have implications for the state of software security, for example, installation with default settings or patching practices. Given the interdependent nature of information systems, the role of adopters, their practices, and the forces that constrain their software security practices are also discussed. Special attention is given to how current practices in patch availability and deployment affect software security.

Despite best effort to build, deploy, and govern secure software, some portion of software vulnerability is inevitable, which brings us to the role of vulnerability disclosure. Vulnerability disclosure is about the sharing of vulnerability information: relevant issues include how, when, with whom, and how often vulnerability information is shared. This chapter discusses the role of vulnerability disclosure on the responsibility for harm and risk of software insecurity with a focus on how disclosure enables and constrains software security practices.

Producing robust software that is able to withstand attacks, work around hardware limitations, and even inform users about the potential security risks related to their choices is no longer seen by society as nice to have, it has become a requirement. Enacting this mandate, however, is far from clear. Improving software security is as much about economics, public policy, and social welfare as it is about abuse cases, error conditions, and testing methodologies. Who should be responsible for the harm and risk caused by security flaws?

BACKGROUND

One of the challenges in understanding who should ultimately be responsible for the harm and risk caused by security flaws is our lack of a full understanding of the nature of information technology risk. "As systems become more complex and interconnected, emergent behavior (i.e., unanticipated, complex behavior caused by unpredictable interactions between systems) of global systems exposes emergent vulnerabilities" (Computing Research Association, 2003, pg. 21). This complexity and emergence make risk assessment hard. Our existing mathematical/statistical risk models are based on independent failures, where "a component failure in one part of the system does not affect the failure of another similar component in another part of the system. This leads to especially beautiful and useful models of system failure that are effectively applied thousands of times a day by working engineers" (Computing Research Association, 2003, pg. 21). Unfortunately, these models are not transferrable to networked systems where failures are interdependent, not independent.

We need models that can account for dependencies between system components in a manner that sheds light on how the behaviors of system components interact to lead to system failure. Progress in interdependent risk measurement will enhance the effective management of investment. "Without an effective model, decision-makers will either over-invest in security measures that do not pay off or will under-invest and risk devastating consequences" (Computing Research Association, 2003, pg. 21). Interdependencies also pose considerable challenges when it comes to assigning liability, and formulating reasonable policy and associated compliance.

Despite our lack of understanding of the nature of interdependent risk, it is widely acknowledged that we are interlinked and the risk interdependent. Interdependent risk necessitates interdependent responsibility. In the words of Jane Addams (1910), "the good we secure for ourselves is precarious and uncertain, is floating in mid-air, until it is secured for all of us and incorporated into our common life" (pg. 116). Addams was awarded the Nobel Peace Prize in 1931 for her unwavering commitment to social improvement through cooperative efforts.