Changing the way the world thinks about computer security.


ABSTRACT

Small changes in an established system can result in larger changes in the overall system (e.g., network effects, emergence, criticality, broken Windows theory). However, in an immature discipline, such as computer security, such changes can be difficult to envision and even more difficult to appreciate, as the immature discipline is likely to lack the scientific framework that would allow for the introduction of even minute changes. (Cairns, P. and Thimbleby, H., 2003) describe three of the signs of an immature discipline as postulated by (Kuhn, 1970):

a. squabbles over what are legitimate tools for research
b. disagreement over which phenomenon are legitimate to study, and
c. inability to scope the domain of study.

The research presented in this document demonstrates how the computer security field, at the time this research began, was the embodiment of these characteristics. It presents a cohesive analysis of the intentional introduction of a series of small changes chosen to aid in maturation of the discipline. Summarily, it builds upon existing theory, exploring the combined effect of coordinated and strategic changes in an immature system and establishing a scientific framework by which the impact of the changes can be quantified.

By critically examining the nature of the computer security system overall, this work establishes the need for both increased scientific rigor and a multidisciplinary approach to the global computer security problem. In order for these changes to take place, many common assumptions related to computer security had to be questioned. However, as the discipline was immature, and controlled by relatively few entities, questioning the status quo was not without difficulties.

However, in order for the discipline to mature, more feedback into the overall computer security (and in particular, the computer malware/virus) system was needed, requiring a shift from a mostly closed system to one that was forced to undergo greater scrutiny from various other communities. The input from these communities resulted in long-term changes and increased maturation of the system.

Figure 1 illustrates the specific areas in which the research presented herein addressed these needs, provides an overview of the research context, and outlines the specific impact of the research, specifically the development of new and significant scientific paradigms within the discipline.

Item Type: Thesis (PhD)
Additional Information: Context document, submitted in partial fulfillment for the degree of Doctor of Philosophy.
Research Areas: A. > School of Science and Technology > Computer and Communications Engineering B. > Theses
Item ID: 7995
Depositing User: Devika Mohan
Date Deposited: 11 Jul 2011 10:28
Last Modified: 02 Apr 2019 11:04
URI: https://eprints.mdx.ac.uk/id/eprint/7995

ABSTRACT

Small changes in an established system can result in larger changes in the overall system (e.g., network effects, emergence, criticality, broken Windows theory). However, in an immature discipline, such as computer security, such changes can be difficult to envision and even more difficult to appreciate, as the immature discipline is likely to lack the scientific framework that would allow for the introduction of even minute changes. (Cairns, P. and Thimbleby, H., 2003) describe three of the signs of an immature discipline as postulated by (Kuhn, 1970):

a. squabbles over what are legitimate tools for research
b. disagreement over which phenomenon are legitimate to study, and
c. inability to scope the domain of study.

The research presented in this document demonstrates how the computer security field, at the time this research began, was the embodiment of these characteristics. It presents a cohesive analysis of the intentional introduction of a series of small changes chosen to aid in maturation of the discipline. Summarily, it builds upon existing theory, exploring the combined effect of coordinated and strategic changes in an immature system and establishing a scientific framework by which the impact of the changes can be quantified.

By critically examining the nature of the computer security system overall, this work establishes the need for both increased scientific rigor and a multidisciplinary approach to the global computer security problem. In order for these changes to take place, many common assumptions related to computer security had to be questioned. However, as the discipline was immature, and controlled by relatively few entities, questioning the status quo was not without difficulties.

However, in order for the discipline to mature, more feedback into the overall computer security (and in particular, the computer malware/virus) system was needed, requiring a shift from a mostly closed system to one that was forced to undergo greater scrutiny from various other communities. The input from these communities resulted in long-term changes and increased maturation of the system.

Figure 1 illustrates the specific areas in which the research presented herein addressed these needs, provides an overview of the research context, and outlines the specific impact of the research, specifically the development of new and significant scientific paradigms within the discipline.