Chapter 20
Establishing Reasoning Communities of Security Experts for Internet Commerce Security

Andrei V. Kelarev
University of Ballarat, Australia

Simon Brown
University of Ballarat, Australia

Paul Watters
University of Ballarat, Australia

Xin-Wen Wu
University of Ballarat, Australia

Richard Dazeley
University of Ballarat, Australia

ABSTRACT

The highly sophisticated and rapidly evolving area of internet commerce security presents many novel challenges for the organization of discourse in reasoning communities. This chapter suggests appropriate reasoning methods and demonstrates how establishing reasoning communities of security experts and enabling productive group discourse among them can play a crucial role in successful resolution of problems concerning the implementation, integration, deployment and maintenance of flexible local security systems for defense against malware threats in internet security. Local security systems of this sort may combine several ready open source or commercial software packages behind a common front-end and may enhance and supplement their facilities with additional plug-ins. To illustrate the diverse character of challenges the reasoning communities in internet security are likely to be faced with, this chapter concentrates on defense against phishing attacks. This example was selected as it is one of the newest and most rapidly changing application domains for the principles of organizing reasoning communities. The major group discourse methods suggested for the reasoning communities of security

DOI: 10.4018/978-1-60960-091-4.ch020
INTRODUCTION

This chapter is devoted to the development of methods for group discourse in the reasoning communities of security experts responsible for all stages of the implementation, integration, deployment and maintenance of flexible local security systems for defense against malware threats. In particular, we are looking at creating a fairly small and very flexible system to defend against phishing attacks, which may be applicable to other internet commerce security tasks, and which is adjustable enough to take into account local requirements in order to address the local information security needs of various organizations and make it easier to use uniform anti-phishing packages available on the market. For successful use of a highly flexible security system of this sort it is essential that it be supervised and guided by a small specialized group of local system administrators and security experts. The main aim of this article is to set up a framework for discourse in the reasoning communities of security experts in order to enable robust supervision of adjustments to all parameters of the local security system, as well as suggest directions for future research on associated reasoning.

There are serious differences in the operation of various organizations, their email correspondence and patterns of email usage by individual staff. Substantial differences among numerous organizations lead to the diverse character of security threats they are faced with. This provides motivation for creating a flexible system capable of complementing large uniform anti-phishing tools available on the market. It is best to include one or more ready open source or commercial programs in the system, because these products have already been thoroughly tested and have been developed and improved for many years. Such systems can be installed centrally as well as for each individual user to take care of personal preferences. These security packages can apply a number of methods well-known in the defense against phishing. The major steps and algorithms involved in the systems include pre-processing of email messages, feature selection, classification and clustering of messages, and preparation of evidence for evaluation.

On the other hand, the installation, integration and management of several already existing large uniform programs could benefit from the development of a combined convenient front-end simplifying the configuration tasks and providing additional facilities. The effectiveness of operation of the combined local system can be further fine-tuned by developing appropriate plug-ins. This would involve various mechanisms and parameters which can be monitored and adjusted as the operating environment and current threats evolve.

The implementation, integration, deployment and maintenance of a flexible local system of this sort is impossible without successful resolution of a variety of problems by a specialized reasoning community of security experts managing these tasks. There are numerous aspects of the system which need to be monitored and adjusted. The group discourse methods for the reasoning community considered in this chapter aim to enable the reasoning community to handle all of these tasks effectively and resolve various issues re-

experts in this chapter include the Delphi Method, the Wideband Delphi Process, the Generic/Actual Argument Model of Structured Reasoning, Brainstorming, Reverse Brainstorming, Consensus Decision Making, Voting, Open Delphi and Open Brainstorming Methods. The Delphi Method and Wideband Delphi Process are suggested as tools for organizing a cohesive reasoning architecture, for coordinating other methods, and for preparing and allocating other methods to particular issues.