JISSec 7(3) 2011

Journal of Information System Security

www.jissec.org

Guest Editorial

Special Issue: Research Papers from the Annual Security Conference (April 7-8, 2010)

Greetings Colleagues,

This is the second of two special issues focusing on papers selected from the Annual Security Conference held in Las Vegas, Nevada. The three papers published in this issue of the Journal of Information Systems Security provide interesting research on network traffic analysis at small and medium size enterprises and a forensic. Thank you to all of the participants attending the Annual Security Conference.

The first paper in this issue, A Firewall Data Log Analysis of Unauthorized and Suspicious Traffic by John Week, Polina Ivanova and Sandy Week, analyzes suspicious traffic at a small Internet Service Provider. The paper reports on 7,478 attacks logged by a small business Internet Service Provider hosting 13 domains. On average, 276 attacks occurred per day. About one half of the attacks were common Windows RPC and SQL Slammer attacks. Slightly less than one half of those attacks came from ten networks and about 25% of those originated from ten hosts. Results suggest what actions can be taken to strengthen small business network security.

Next, Statistical analysis of Snort alarms for a medium-sized network by Kitti Chantawut and Bogdan Ghita, examines a medium size network and performs long term analysis of trends and recurring patterns of attacks. The study describes a number of characteristics including daily volume of intrusions and types of attacks. Results indicate a wide variety of intrusion attempts and reveal a cycle of correlated behavior. Interestingly, older successful methods appear to remain preferred attack methods long after their release. Similar to the first paper a large proportion of the intrusions were potentially generated by a small group of IP addresses.

The last work in this issue, Computer Forensics: Examining the Effectiveness of File Deletion by Mark B. Schmidt and Michael Condon, describes an experiment that puts the effectiveness of formatting a drive and

file deletion into question. In this experiment different ways of “erasing” files from a hard drive were examined. Research was conducted starting with the most basic, and common process and progressed by increasing the robustness and iterations of deletion techniques. The results help to evaluate the techniques in order to help ensure that a digital source is erased and private information will not be unknowingly distributed along with used hard drives.

We hope you’ll enjoy this special issue of JISSEC.

Alexander McLeod

University of Nevada, Reno