

Proposal for Talk at RAID 2000

Company: Internet Security Systems

Type of presentation: Talk

Title: Visualization of Intrusion Detection Data

Topic Category: Innovative Approaches / New IDS methodologies and technologies
(among others)

Speaker: Tim Farley
Senior Researcher – X-Force
Internet Security Systems, Inc.
6600 Peachtree-Dunwoody Road
300 Embassy Row
Atlanta, GA 30348 USA
Tel: +1.678.443.6189
Fax: +1.678.443.6479

E-mail: tfarley@iss.net

Biography: See below.

Desired time: Any time that is available.

Abstract

Existing intrusion detection systems are known for their production of voluminous output. Much research has been done on methods of reducing output volume and/or dealing with the voluminous data. Despite this research, there is still a huge problem of dealing with false positives and other erroneous output from IDS products. Critical to the problem is the fact that experienced security professionals are rare, so most installations have few people with the skills necessary to adequately interpret IDS output.

Existing practitioners have largely focused on dealing with attack signatures on a case-by-case basis as they occur. The primary goal, naturally, is determining whether an attack has actually occurred and whether it represents a real threat to the protected network. After this data is analyzed, it is often reported on and simply filed in a historical database.

ISS believes that there is much to be gained by detailed analysis of historical intrusion detection data on a given network. Buried within these huge volumes of event data are patterns and relationships that often reveal subtle threats to the network. Among these are very low-speed attacks and attacks which are distributed amongst several source addresses. In addition, there are also long-term trends and other patterns that could be used to predict future threats. We merely need to mine this data for its hidden value.

Similar problems have existed for years in the analysis of large multi-dimensional databases. Many companies and research institutions have huge data warehouses full of data which are not adequately mined for their potential value. A large body of research exists on techniques in data visualization, or the graphical representation of these data sets in order to find previously unexplored patterns within them.

ISS believes these same techniques can be applied to historical intrusion detection data in order to provide valuable attack analysis. Results expected include both recognition of previously unnoticed attacks, as well as long term trend analysis of attack data. Correlation of attack data with vulnerability data also promises to better reveal the overall security posture of a protected network.

This talk will focus on work that has been done at ISS on a prototype called Security Visualizer. This prototype allows historical data from ISS RealSecure™ (as well as other ISS products) to be graphed and plotted in various ways. The purpose of this prototype has been to investigate which forms of data visualization work best on intrusion detection data.

Among the visualizations which will be discussed are:

- Network maps
- Event volume graphs
- Self organizing maps
- Scatter plots
- Geographical maps
- Abstract representations

Sample data and plots from actual attack databases will be shown and discussed. There will also be some discussion of future directions for this research and the current status of the Security Visualizer prototype.

Biography:

Tim Farley Senior Researcher – X-Force Internet Security Systems (ISS)

Tim joined Internet Security Systems (ISS) in September of 1997 as a senior software engineer on the RealSecure™ product team. In this role, Tim was involved in the development of the network sensor's detection logic and architecture, and pioneered the fusion engine concept now being developed at ISS. Currently Tim is a Senior Researcher with the ISS X-Force, working on data visualization prototypes.

Before joining ISS, Tim worked at several other major software companies, including Xcellenet and DCA (now known as Attachmate). Prior to that, Tim had worked at two of the pioneers of the "ShareWare" industry in Atlanta, Magee Enterprises (makers of "Automenu") and SemWare (makers of "QEdit").

Tim has also written a number of articles on technical topics for such publications as Atlanta Computer Currents, LAN Times, PC Techniques and Windows Developers

Journal. In addition, Tim has also contributed material to several books including "Undocumented DOS" and to several Internet Engineering Task Force (IETF) standards such as the Host MIB (RFC 1514) and the current Intrusion Detection Exchange Format working group. Tim is known as, and has been quoted as an industry expert in publications such as BYTE Magazine.

Tim attended Georgia Institute of Technology in Atlanta, Georgia.

end