Proposal for Talk at RAID '99

Company: Internet Security Systems

Type of presentation: Talk

Title: Lessons Learned in Commercial IDS Development & Deployment

Topic Category: Practical Considerations / Case Studies (among others)

Speaker: Tim Farley
Software Engineer
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

The process of enhancing, marketing, deploying and supporting a commercial software product is very complex. This process often presents developers with many challenges that were not anticipated in the early design and research of their product. Responding to these challenges results in stepwise product enhancements that benefit all customers. Experience has shown that these enhancements result in product design decisions that are rarely arrived at in non-commercial research projects.

The development of commercial intrusion detection software is no exception to this phenomenon. In the process of developing its industry leading intrusion detection system RealSecure™, Internet Security Systems (ISS) has learned many lessons about the development of fast, reliable and accurate intrusion detection technology.

This talk will attempt to cover some interesting highlights of this process at ISS. Some of the highlights will include:

- Choosing which signatures to implement.
- Finding the right balance between false positives and false negatives, when detection signatures are not clear-cut.
- Designing attack signatures to be deal with mutating attacks in the field, and adapting them as new mutations are discovered.
- Anticipating support issues which will arise surrounding particular attack signatures, particularly the diagnosis of false positives.
- Designing detection logic that can deal with dual routed networks.
- Deploying network intrusion detection systems in networks with switching technology.

Specific examples relating to ISS RealSecure will be presented, along with the solutions that were used. Emphasis will be placed on problems that were unanticipated in the early design phases, or which were thought to be rare situations in reality.

Tim Farley
Senior Software Engineer - RealSecure Team
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, Currently, Tim is involved in the development of the network engine's detection logic and architecture, and soon he will be project leader for the upcoming Fusion engine.

Before joining the ISS team, Tim worked at several other major software companies, including Xcellenet (now known as Sterling Commerce) 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.