Paper Submission for the
Second International Workshop on the
Recent Advances in Intrusion Detection

Topic Category: Practical Considerations

Intrusion Detection for Telephony Signalling

David Gorman
Electronic Systems Division
GTE
9790-H Patuxent Woods Drive
Columbia, MD 21046
Ph: 301-310-0314
Fax: 301-310-0125
david.gorman@gsc.gte.com

Mary Ruhl
National Security Agency
9800 Savage Road, Suite 6516
Fort Meade, MD 20755
Ph: 301-688-0292
Fax: 301-688-0289
mkruhl@alpha.ncsc.mil

Abstract

The Public Switched Telecommunications Network (PSTN) has becoming increasingly dependent on Signalling System 7 (SS7) due the drive to provide new services, such as Calling Name ID, Local Number Portability, the migration of other services to regional and national databases (e.g., E800, Calling Card, and eventually E911) and deregulation. Additionally, the explosion in the mobile communications has created an even stronger dependency on SS7. The SS7 network controls the modern U.S. telecommunications infrastructure and continues to evolve to support advanced network services, such as Advanced Intelligent Network (AIN) and wireless services. Attacks against the SS7 network could disrupt, modify, or deny service within the PSTN, affecting the capability to process or complete calls. The goal of this project is to expand defensive measures for attacks against the SS7 protocol.

This project specifically focuses on investigating and developing detection capabilities for message insertion attacks against the SS7 network that could disrupt or deny telecommunications services. The types of postulated attacks include:

- brute force messages to tear down calls;
- messages to take circuits out of service;
- inability to set up/tear down calls;
- messages to take signaling links out of service;
- isolation of services such as database features.

This project is an outgrowth of the DARPA funded KingsMen project. The work performed under KingsMen identified potential vulnerabilities within the SS7 network and developed a proof of concept intrusion detection tool. The original KingsMen work was based substantially on analysis of the ANSI standards and on previously collected signaling traffic. Therefore, one of the main purposes of the work continuing under this project is to validate previous work and verify detection methods.

Most of the network protection interest by the telephone industry is, of course, concentrated on fraud and on the revenue bearing aspects of service disruptions. As a result of this interest, new techniques of network monitoring have been introduced. These new tools are applied on signalling links used to control the telephone network. Monitoring the signaling links is a departure from the traditional method of directly monitoring the network elements for both Operations and Maintenance (O&M) and security purposes. These new tools are still primarily designed for the O&M and fraud applications. However, the infrastructure being put into place for monitoring of the signalling links provides the foundation for a new type of telephony intrusion detection techniques. These techniques, are based on the ability to directly monitor the SS7 Links. Intrusion detection is based on the real-time monitoring of message traffic on each signalling link for:

- evidence of intrusions for service disruption;
- SS7 messages and message fields of interest, which indicate possible intrusion threats to the SS7 network infrastructure;
- attack signatures;

- anomalous network responses.

The current intrusion detection method employs a rules base of anticipated attack signatures and network responses to such attacks. We intend to explore the use of a statistical analysis engine. Ultimately our goal is to fuse the two methods. The statistics engine is desired to provide a tip-off to unanticipated attacks and perhaps, a correlation to rules firings to establish a confidence level on the anomalies.

Due to the obvious destructive nature of the attack scenarios, “livefire” testing is not an option on an operational network. The validation testing will be performed in a lab environment. Efforts are underway to build the lab and provide adequate testing tools and methodologies.