Press Release

For Immediate Release **Date: September 2, 2010**

StrongPoint® Safeguards the Intelligent Transportation Systems (ITS) Network

Anaheim, California — Econolite's *StrongPoint* network security appliance was recently the subject of an intelligent transportation systems (ITS) network vulnerability assessment (NVA) and penetration test (PT) performed by Sword & Shield Enterprise Security, Inc. Tested in a typical advanced traffic management system (ATMS) network configuration, *StrongPoint* was proven to safeguard the integrity of customer systems and information from internal and external threats.

Sword & Shield's full battery of tests, conducted using "zero knowledge" scenarios to replicate an outside hacker, and "full knowledge" scenarios to represent a malicious or disgruntled insider/employee, determined that none of the *StrongPoint* hosts identified on the system had vulnerabilities from unauthorized field network access. In addition, *StrongPoint*'s overall network security position was found to be "strong" due to its firewall gateways, virtual private network (VPN) tunnels, two-factor authentication, and an intrusion detection system (IDS) – critically important for the highly networked environments of emerging ITS solutions.

StrongPoint's point-and-click graphical user interface (GUI) management console was also part of the evaluation process. The Sword & Shield assessment team found the *StrongPoint* GUI intuitive, making it easy for basic-level computer users to quickly navigate through the entire application quickly, including understanding and executing configuration, monitoring, and network management functions.

StrongPoint leverages traffic network security technology, based on the strategy of a trusted-device network environment that was jointly developed by Econolite and Uniloc USA - the leader in device-based identification. The trusted device network approach provides an organization with a higher level of control over critical system access. As a result, *StrongPoint* provides authentication using Uniloc's Physical Device Recognition (PDR) technology to grant access to authorized systems and communications networks. Authorized computers are "fingerprinted" and are the only devices allowed to communicate across an encrypted communications channel to critical assets on the network. The *StrongPoint* security appliance creates a secure, virtual-network layer connection between the traffic management system and the communications network endpoints. Additional information about *StrongPoint* is available at http://www.econolite.com/products/networks/networks.asp?product=strongpoint

About Econolite

In business since 1933, Econolite is a leading transportation solution provider and manufacturer of advanced traffic controllers (NEMA & ATC/2070), *Centracs*™ and *Aries*® Advanced Transportation Management Systems (ATMS), *Autoscope*® video vehicle detection systems, arterial systems masters, vehicle and pedestrian signals, traffic control cabinets, data collection and management services (*DCMS.2*), Intelligent Intersection™ technology, and a full line of transportation maintenance services. Econolite is committed to employing advanced technologies that reduce traveler time, ease congestion, enhance transit operations, provide safer mobility, and improve quality of life.

Press Release Contact: Frank Provenzano, Director of Public Relations,
714-630-3700 ext. 296, or marketing@econolite.com

ECONOLITE
Solutions that Move the World®

- Approved for Immediate Release -

About Uniloc

Uniloc offers a patented Physical Device Recognition (PDR) platform that authenticates the true identity of devices that attempt to access high-value technology assets. Uniloc provides a patented method of uniquely identifying a user device, such as a PC or portable device, using the naturally occurring, inherent physical characteristics of that device. Uniloc has applied its expertise in Physical Device Recognition to several markets, including software and game security, identity management, and critical infrastructure security. For more information, visit www.uniloc.com

About Sword & Shield

Sword & Shield was founded in 1997 with the goal of providing information security products and solutions. The company also provides risk, compliance and security assessments, as well as computer forensics and eDiscovery services. While Sword & Shield maintains an IT security focus, the company works with its sales agents to provide a variety of IT products to federal agencies through its SEWP program. More information about Sword & Shield can be found at: http://www.sses.net/

# # #

Note: *StrongPoint is not designed to be used in lieu of appropriate physical field security measures, or an organizationally approved and distributed network security policy.*

Press Release Contact: Frank Provenzano, Director of Public Relations,
714-630-3700 ext. 296, or marketing@econolite.com

ECONOLITE
Solutions that Move the World®

- Approved for Immediate Release -

MEMORANDUM OF TESTING METHODS

TO: JIM LESLIE, ECONOLITE

FROM: SWORD & SHIELD ENTERPRISE SECURITY, INC.

DATE: JULY 30, 2010

RE: STRONGPOINT NETWORK VULNERABILITY ASSESSMENT AND PENETRATION TEST

Engagement Overview:

Sword & Shield Enterprise Security, Inc. (hereinafter referred to as Sword & Shield) conducted a network vulnerability assessment (NVA) and penetration test (PT) against specified targets within a test environment provided by Econolite technical staff. The overall objective of the assessment was to review and analyze Econolite's system of application controls to ensure effectiveness in safeguarding the integrity of customer systems and the protection of information.

Econolite's StrongPoint network hardware/software solution is designed specifically for use in securing traffic networks using Uniloc's unique Physical Device Recognition (PDR) technology as a means of creating secure communication tunnels between a traffic management center and field device locations such as traffic cabinets.

Approach:

Sword & Shield tested to verify StrongPoint's capability in providing security against unwanted/unauthorized access into the secure network. General threats to a networked environment include interception, modification, fabrication, and interruption of communications. The assessment team focused on identifying three distinct threat vectors against the typical traffic network:

1. Physical access to a traffic cabinet.
2. Compromise of a field network.
3. Municipality employee threat.

The identified threat vectors imply a varying degree of knowledge about the environment. Testing was performed using both "zero knowledge" and "full knowledge" approaches. "Zero knowledge" testing was launched without any information about the network being tested. Testing with "full knowledge" is the "inside-out" approach wherein testing was launched from a network with extensive information about the type of system under test. Tests were attempted from both invalid and valid (assumed identity) connections.

To accomplish this task, the team performed the following:

- Conducted a network vulnerability assessment to identify vulnerabilities that could be exploited by unauthorized external users or internal users with malicious intent.
- Attempted to penetrate existing security controls and gain entrance to the internal traffic network or data through external and internal test points.

Assumptions:

There was a battery of tests carried out from points typically used by the three distinct threat vectors. Specifically the following types of intrusion protection were validated:

1. Physical access to a traffic cabinet:
   Connection from behind any StrongPoint Appliance (SPA) to its local area network (LAN) port(s).

   Note that for a connection behind an SPA on its LAN, it was a simple hub/switch operation and, therefore, communication was open between devices connected on the SPA's LAN.

   A. Tested the ability to access, alter and/or manipulate the SPA in the cabinet.
   B. Tested the ability to access, alter and/or manipulate any *other* SPA in the system.
   C. Tested the ability to access, alter and/or manipulate devices connected behind any *other* SPA.
   D. Tested the ability to access, alter and/or manipulate the StrongPoint Server (SPS).
   E. Tested the ability to access, alter and/or manipulate any computer connected behind the SPS.

2. Compromise of a field network:
   Connection from any point within the network connecting the SPS to the SPAs; in this case, to the hub/switch in between the SPS and SPAs.

   A. Tested the ability to access, alter and/or manipulate any SPA in the system.
   B. Tested the ability to access, alter and/or manipulate devices connected behind any SPA.
   C. Tested the ability to access, alter and/or manipulate the SPS.
   D. Tested the ability to access, alter and/or manipulate any computer connected behind the SPS.

3. Municipality employee threat:
   Connection from behind the SPS.

   A. Tested the ability to access, alter and/or manipulate any SPA in the system.
   B. Tested the ability to access, alter and/or manipulate devices connected behind any SPA.
   C. Tested the ability to access, alter and/or manipulate the SPS.

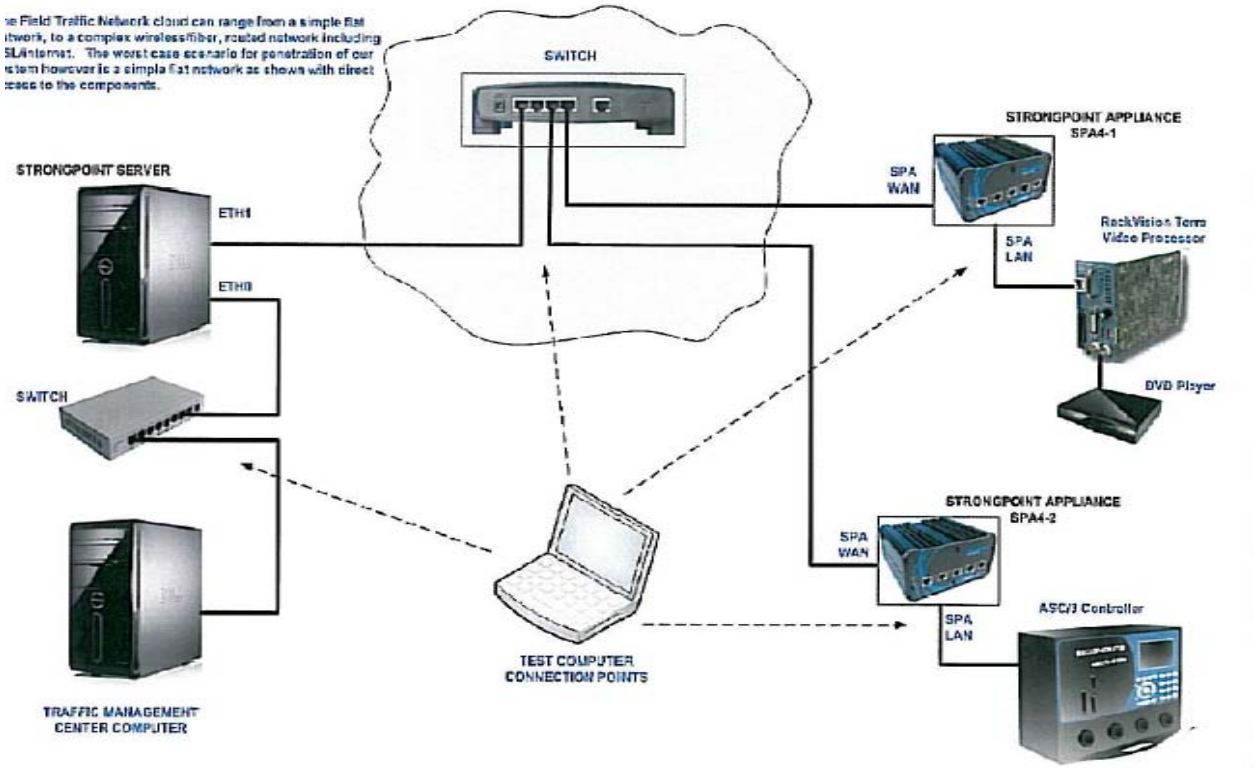

Figure 1: Penetration Test Setup

All testing was performed on a statically deployed system, with typical traffic being generated during the testing period. StrongPoint Application Gateway restrictions were implemented on the test appliances. Even though the StrongPoint system has intrusion detection (IDS) capabilities, it was assumed that these would not intervene/be incorporated into the testing and no manual countermeasures against the testing team were taken during the testing period. StrongPoint client software was also provided to the test team for evaluation.

Methods Utilized at Each Test Point:

Network Packet Sniffing:
Sniffing involved capturing LAN traffic for useful and/or compromising information, such as access credentials. This was often performed in conjunction with address resolution protocol (ARP) poisoning.

Network Service Vulnerability Scanning:
Network vulnerability scanning involved checks for known vulnerabilities on the network. This testing evaluated responsive system and individual devices for known weaknesses in security mechanisms. The results of automated tests were manually reviewed to eliminate false positives.

Host Vulnerability Scanning:
Host vulnerability scanning involved checks for known vulnerabilities on an individual host using administrative credentials. This testing evaluated individual devices for known weaknesses in security mechanisms at the host level.

Web Application Scanning:
Web application scanning involved checks for known vulnerabilities on web sites at their application levels. This involved both authorized and unauthorized credentials.

Database Scanning:
Database scanning involved checks for known vulnerabilities on databases at their database levels. This type of testing was not able to be performed due to access restrictions to any databases.

Network Service Exploitation Testing:
Service exploitation testing seeked to determine if security mechanisms on network services could be bypassed. It involved using the results from the various forms of sniffing and scanning (i.e., exploitable weaknesses) and attempted to bypass security mechanisms.

Credential Bruteforcing:
Credential bruteforcing involved extensive automated checks for weak credentials used to access services on the network.

Spoofing:
Spoofing involved utilizing methods to assume authorized identities to gain access to communications over the network.

Conclusion:

The Sword & Shield assessment team used various testing methods at different network points to attempt to identify and exploit vulnerabilities against the StrongPoint security system. Overall, the security posture for the Econolite system was strong due to its incorporation of stateful firewall gateways, virtual private network (VPN) tunnels, two-factor authentication, and an IDS. All of these are recommended security measures for a networked environment.

Signed: Dave Shackleford
Director, Security Assessments