

Dynamic Message Signs – DMS Security Lockdown

Maybe you have seen it in the news: an increasing number of Department of Transportation dynamic message signs (DMS) are being “hacked.” The occurrence has been more prevalent recently, brought on in part, by hacker pranksters and perhaps their need to prove to us how simple the act really is. DMS devices are typically accessed remotely using a wireless cellular modem connected to the DMS control unit, which allows changes to be made to the sign’s message screen.

The wireless cellular modems used in DMS deployments on the roadside are designed to access the cellular phone network, typically using a Verizon or ATT network, minus the digital voice – this application only uses digital data. Cellular modems used for DMS applications are typically environmentally rugged, wireless data platforms designed to enable real-time (at 3G speeds), two-way communications with remote digital devices.

Wireless cellular communications networks are intentionally designed to operate in an open environment where ease of access and foolproof operation is the main objective. However, the tradeoff to using this type of open network is their predisposition to increased security breaches. A senior congressional representative recently admitted that there are several hundred (hacker) attacks against U.S. government, electrical-utility, and financial computer networks on a daily basis. Therefore, the dilemma is not *whether* a government network will be compromised, but rather *when*.

For remote DMS operations, the process is simple; users simply access the Internet through a service provider’s web site, type in the modem’s IP address, and you are “in.” DMS standards have been recognized as the most successful implementation of an Intelligent Transportation System (ITS) standard, the National Telecommunications ITS Standard Protocol for Dynamic Message Signs (NTCIP-1203 Object Definitions for Dynamic Message Signs). However, anyone can obtain the freely available open standard documentation, thus also knowing how to access the sign and change the sign messages. A recipe for easy tampering, perhaps, but the objective of any standard is to create an environment where technology is readily available and less expensive to adopt. We cannot fall back into the “proprietary technology” confinements of the past, which blame open standards for the problem.

Why be concerned?

DMS installations are a crucial part of the roadway system. Dynamic message signs are used to inform travelers of hazardous driving conditions, construction zone locations, and other public service announcements. Accordingly, the DMS system is also a critical part of a government agency’s transportation network. There is a popular belief today that our nation’s transportation network can be considered critical infrastructure, like our power grid or the water system. If any of these systems are tampered with, or are broken, our citizens’ health and safety can be compromised. One alarming statistic reports that more than half of road construction deaths are a result of workers being struck by vehicles, illustrating the importance of the public service a DMS system provides to drivers.

The consequences from tampering with DMS applications will, at minimum, compromise operational and administrative efforts. For example, a seemingly innocent prank can affect crime prevention if an “Amber Alert” is pre-empted, or can hamper emergency response efforts if a lane closure or detour notice due to an accident is blocked.

An Ironclad Approach to Securing the DMS Network

Recently, Econolite (www.econolite.com) and Uniloc USA (www.unilocusa.com) introduced a technology that changes the focus of protection from *keeping the bad guys out* to *only letting the good guys in*. The “good guy” strategy is based on the premise that asset owners have more control over who they would allow to access their critical systems than who they want to block. Furthermore, the strategy is based on the concept that systems communicate with systems and therefore the most important single factor for authentication should be between the systems themselves. This concept naturally evolves into a strategy of a *trusted-device network environment*.

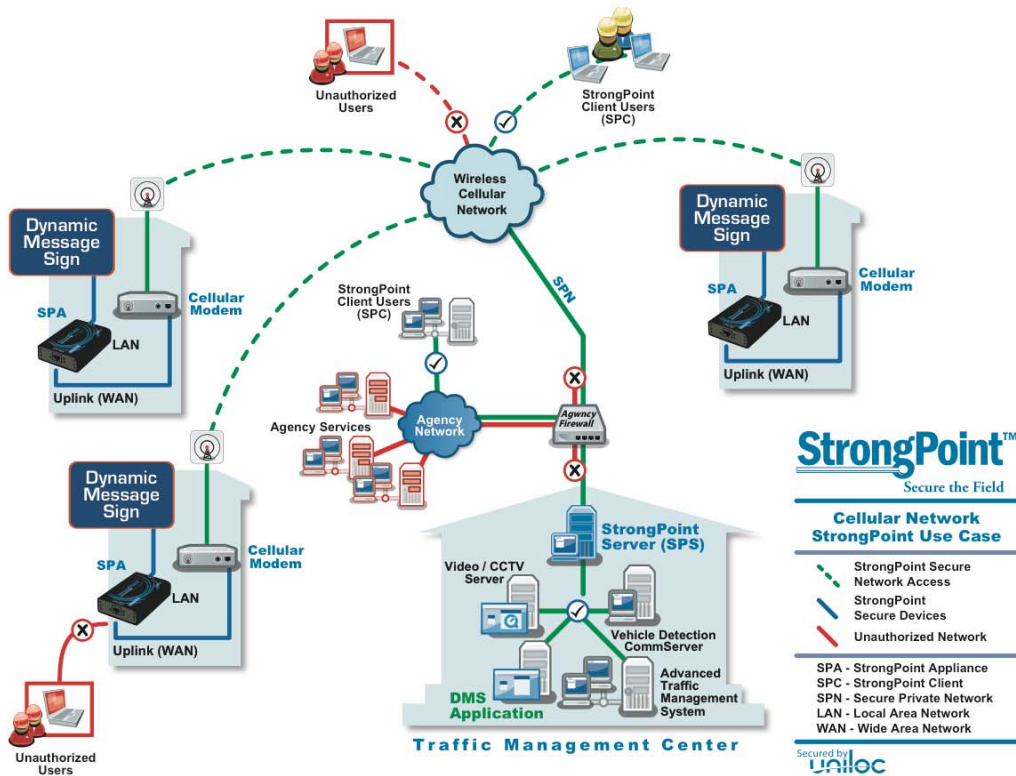
Access Control: *StrongPoint* network security allows an organization to define exactly who should have communications and control access to critical assets. It provides impenetrable authentication using Uniloc’s Physical Device Recognition (PDR) technology to grant access to authorized systems and communications networks. Client machines are “fingerprinted” and are the only ones allowed to communicate across an encrypted communications channel to critical assets on the network connected to *StrongPoint* security appliances.

Trusted-Device Network: The implementation of *StrongPoint* components, *StrongPoint* management server software, *StrongPoint* security appliances, and *StrongPoint* client software creates a “trusted device network” within which only authenticated devices are allowed to communicate.

For example, trusted-device networks can be established between individual transportation system components such as:

- Traffic cabinets located at signalized intersections or freeway ramp metering locations
- Dynamic Message Sign locations
- Vehicle detection system locations, including weigh-in motion sites and data collection installations
- Freeway CCTV camera locations
- Traffic Management Centers or Traffic Operations Centers
- Emergency Response Centers
- City utility facilities and other services managed by the Public Works Department

Trusted-device network environments can even be established by fingerprinting network infrastructure components so that only data flows between certain firewalls or switches for VLAN implementations.



Bi-Directional Security: The *StrongPoint*TM trusted-device network also provides the first application of bi-directional security. This means that only *StrongPoint*-trusted devices can connect to the *StrongPoint* network. *StrongPoint* appliances, located in the field, may only accept communications from the *StrongPoint* server and other *StrongPoint*-trusted devices. Specifically, *StrongPoint* manages authorized devices located in the traffic cabinet; unrecognized connections to the network from inside the traffic cabinet are blocked and immediately reported to traffic system operations personnel.

The *StrongPoint* appliance is a compact, hardened, hardware appliance that is deployed to protect an individual asset or a group of assets connected to the endpoints of a network. Security is provided by a specially engineered version of the Uniloc PDR technology embedded directly in the appliance.

The *StrongPoint* appliance automatically provides a secure private “link” between itself and the DMS device and the *StrongPoint* server. Uniloc’s unique challenge-and-response methodology continuously monitors the secure link and ensures ONLY authorized devices access the DMS. In other words, a *StrongPoint* secure communications tunnel is created within the existing wireless cellular bandwidth.

Device Fingerprints: Uniloc’s patented PDR technology uses the distinctive characteristics or device “DNA” of a computer to generate a unique signature or “fingerprint” for that specific computer. This device fingerprint becomes the authentication credential that is “locked” to that computer. The physical device-fingerprinting process is very adaptable and can be used to

generate both basic and highly complex signatures for virtually any device platform depending upon the application and security level required.



Uniloc's physical device fingerprinting can sample well over 10,000 different points within a computer system to generate a unique signature, targeting upon both naturally occurring component manufacturing imperfections and intentional configuration differences. Sampling points can include:

- Hard-drive damage maps
- CPU benchmarking
- Chip benchmarking on sound cards and video cards
- Silicon degradation and damage
- Serial numbers and MAC addresses
- Globally unique identifiers (GUID's).

Conclusion

As today's municipalities and state Departments of Transportation adopt more mainstream communications standards, it is imperative that traffic management networks bring security to the forefront of their implementation plans. Although technology may not be the 100% solution, technology should be a key component in the protection of these traveler information signs and message boards. More importantly, technology-based security solutions that do not require budget-busting expenditures, massive hiring, redesigning of communications systems, and extensive personnel can be the most effective and efficient way to give these communications venues the protection they need.

Econolite's partnership with Uniloc USA results in a unique security solution, which improves on commonly used security systems and creates a simple, but much more effective way to manage wireless communications networks and their critical infrastructure. As the wireless network expands and becomes more pervasive, authenticating the "good guys," and managing the network's "trusted-devices," makes a lot of sense.

About Econolite

In business since 1933, Econolite is a leading transportation solution provider and manufacturer of advanced traffic controllers (NEMA & ATC/2070), *Aries*[®], *icons*[®], *Centracs*[™], and *PYRAMIDS*[®] traffic management systems, *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.

About Uniloc

Uniloc USA is the technology leader in electronic Physical Device Recognition (PDR) for critical infrastructure security. The core technology platform driving Uniloc innovation is physical device fingerprinting, the company's patented method of uniquely identifying a user device, such as a PC or PDA, by the naturally occurring, inherent physical imperfections of that device, and then incorporating that physical device fingerprint into licenses or access credentials. Uniloc's technologies can identify devices with more comparable accuracy than human DNA. Uniloc is the inventor and holder of the seminal physical device-locking patent (U.S. 5,490,216) and has 9 related patents pending. Uniloc has applied its Physical Device Fingerprinting technical expertise to several vertical markets, including software publishing, network authentication, transportation, social networking, and DVD retailing. For more detailed information please visit www.uniloc.com.