

SECURING TRANSPORTATION NETWORK INFRASTRUCTURE WITH PATENTED TECHNOLOGY OF DEVICE LOCKING – DEVELOPED BY UNILOC USA

Faraz Angha, Uniloc USA

3333 Michelson Drive, Suite 600, Irvine, CA 92612, USA

Tel. (415) 651-4297, email: faraz@unilocusa.com

Habib Shamskhov, DKS Associates,

Cyrus Minoofar, Alameda County Congestion Management Agency

ABSTRACT

In recent years, transportation systems' security has become a top priority for officials, specifically in highly congested areas. As technology advancement enables a myriad of information systems to combine different data sources, process and disseminate them to travelers and public agencies, it is critical to operate and maintain secure systems throughout. How do we prevent intruders from hijacking transportation systems? Alameda County Congestion Management Agency (ACCMA) has taken an unprecedented approach in studying innovative ways to ensure the integrity of these systems. Using patented technology of Device Locking, ACCMA initiated a proof of concept project to lock down ATMS platforms.

KEYWORDS

Security, ATMS, Network Management

SUMMARY

Advanced Transportation Management Systems (ATMS), are increasingly becoming more complex and sophisticated. Layers and layers of information from different data sources, transmitted into a repository, such as a Traffic Management Center (TMC), are stored, processed and disseminated into different channels. An amalgamation of various systems packaged into one. In a typical scenario, information is collected from various field devices and networks, and transmitted into a data center for processing and dissemination. In addition, commands are executed via computer systems to field devices to manage transportation networks.

Ever since September 11, 2001, transportation systems' security has become a top priority for key officials in the United States, specifically in highly congested areas, such as San Francisco Bay area. How easy is it for intruders to hijack a system, or how easily can someone hack into an AMTS system and turn the traffic signals all red and bring traffic to a stand still? How do we ensure the integrity of data and information? Initial studies were surprisingly telling how traffic signals and ATMS systems are vulnerable to security breaches with low level protection.

The East Bay SMART Corridors Program is a multi modal Advanced Transportation Management System (ATMS), which provides real-time traffic conditions to travelers and local public agencies. This local real-time conditions reporting allow transportation professionals to improve efficiency and safety of the regional transportation corridors while empowering travelers with information to make better travel decisions. The East Bay SMART Corridor Program started in 2000 with two of the major arterial corridors in the east bay portion of the San Francisco Bay Area – the Interstate 80, and the Interstate 880 corridors, with the recent addition of Grand Avenue/Mac Arthur Boulevard. The program started with a total corridor length of 40 Miles (64Km) of highly congested freeway. The Alameda County Congestion Management Agency (ACCMA) is the lead agency for the improvements in the Alameda and the western Contra Costa counties in San Francisco Bay area. ACCMA is managing plan, design, construct, inspect, operate, and maintain elements of the program on behalf of all 28 participating agencies.

As such, the ACCMA has taken an unprecedented approach to test the integrity of these systems. A demonstration project as a proof of concept was initiated with assistance from consultants DKS Associates, and Uniloc USA—a provider of digital security technologies for protecting networks, data and electronic content.

The goal of this project is to demonstrate means of securing sensitive portions of ACCMA's transportation network. The existing network provides information to and from member agencies to facilitate better management of their systems.

The project aimed to provide seamless security measures to these systems without introducing additional steps to users. This would ensure maintaining the integrity of information exchange between various systems within the network.

CONCEPT:

DKS and Uniloc engineers worked with ACCMA staff to formulate best approach to the project. This included ensuring the least amount of changes to the current infrastructure and allowing transportation professionals in member agencies to conduct their operations without changing their daily routines.

The concept project approach is summarized below:

- Develop work plan and concept of operations, including Functional Requirements acceptable to ACCMA and respected constituencies—cities and counties along the corridor.
- Develop Memorandum of Understanding (MOU) and secure agreement for demonstration of proof of concept.
- Conduct comprehensive security audit and a before study.
- Implement Uniloc netANCHOR software and conduct an after study to document the results

In order to identify high risk areas and target opportunities where total cost of ownership can be reduced through the introduction of Uniloc technologies, an overall system and network assessment was conducted following the ISO 17799 standard. The ISO 17799 specification for conducting a security assessment focuses on technical network and systems infrastructures and development, as well as personnel management and agency operating procedures. As Uniloc was charged with conducting an assessment of the network and technical operations of the ACCMA, only those sections of the ISO 17799 specification pertaining to these areas was addressed. Areas concerning personnel management and Asset Classification and Control were beyond the scope of this project.

During the initial audit, a few candidate systems within the ATMS network were identified for the project. This included the Video Detection System, The Radar dissemination system, and systems that exchanged information with Emergency Management Systems in Alameda and Contra Costa counties. For the initial phase, the Video Detection System was chosen, as the implementation process was deemed faster and more beneficial.

Uniloc has invented a patented technology based on *Device Locking*. Device locking is a simple yet powerful method of authentication and validation to securely protect devices and enterprise network systems. A device's digital identity, known as its "fingerprint," consists of a combination of machine

characteristics and properties that are generated using a set of proprietary algorithms.

Generating a device fingerprint consists of sampling non-user configurable properties coupled with a variety of additional parameters such as uniquely generated hashes and time sensitive values. Manufacturer parameters such as serial number, available memory size and type, chipset, bios and firmware versions, as well as dozens of additional values are addressable via operating system calls and low-level custom driver calls. The couplings of different methodologies for retrieving manufacturer specific parameters further protects fingerprinting by allowing the software to self diagnose. Through repetitive sampling calls, Uniloc security methodologies are able to detect and prevent hacking attempts and false positives.

IMPLEMENTATION AND RESULTS

As part of the project plan, it was decided that mirror systems will be used for the demonstration project. Initially Uniloc's netANCHOR enabled systems were implemented in mirror servers of ACCMA media servers. Media servers collect video feeds from various member agencies through the cameras that are installed throughout arteries and routes. These feeds are partially available to the public, and also used by agencies for traffic and safety monitoring and operations. Uniloc's netANCHOR can be installed on any operating environment, including, Microsoft Windows Server, LINUX, UNIX, etc. ACCMA utilizes Microsoft Media Server through Windows 2003 Server. netANCHOR does not require separate server infrastructure, and for this project the software was installed on the same servers as ACCMA's mirrored media servers.

Uniloc's netANCHOR software was used for locking down the candidate systems. The software enables secure information exchange through the patented technology of Device Locking. Using this technology, each field device, such as cameras, are fingerprinted and sampled to guarantee the integrity of the feeds. This way, systems operators ensure each feed is coming from the appropriate field device. Additionally, the systems and computers that use these feeds and interact with media servers are fingerprinted. This provides the means for only authorized devices to execute commands to the system. For instance, a computer at a member agency can view pre-designated portions of the video feeds, while another computer at ACCMA's headquarters, not only can view the entire system, but can also execute commands through the media server.

Having mirror systems provided adequate baseline to gauge effectiveness of the proposed security measures. This allowed DKS and Uniloc engineers along with ACCMA staff to compare systems side by side and draw a measure of effectiveness of netANCHOR enabled mirror servers.

To ensure usability and a measure of effectiveness, the following performance criteria was established by consultants:

- Resistance to hacking and impersonation
- Interoperability
- Adaptability of the Technology
- Permanence
- Susceptibility to circumvention
- Time required to implement
- User convenience
- Methodology costs (support and integration)
- System requirements

Uniloc netANCHOR Network Security Model

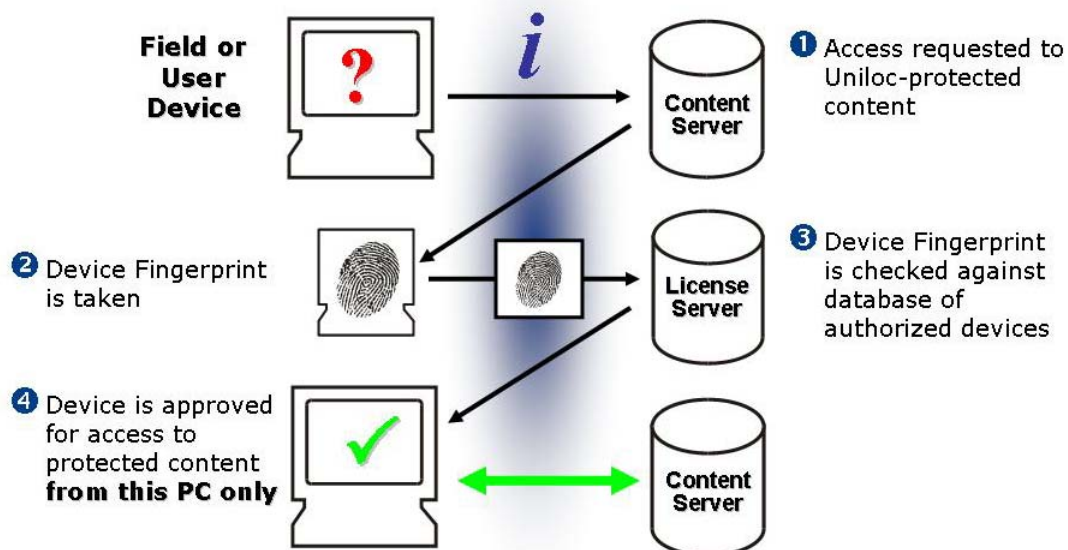


Figure 1 – netANCHOR Methodology

Finally, this method has been implemented in portions of the ACCMA managed systems to gauge its' effectiveness in an overall transportation systems environment. Uniloc technologies have been successfully implemented and operated in a variety of industries, such as, banking and finance, telecommunications, and software publishing.

While the pilot project is completed successfully, Uniloc will maintain netANCHOR enable servers throughout ACCMA's ATMS network until the end of 2006. The results of this demonstration project has been documented and submitted to ACCMA. Uniloc has provided a proposed solution, complete with an integration plan to ACCMA's ATMS system. Following the acceptance of the integration plan by ACCMA, Uniloc implemented the proposed technology into

ACCMA's ATMS network. Uniloc documented the steps taken for this process and presented the results to ACCMA.

This document serves as an official project result. Uniloc summarized the project and its' findings in a document that can be used as a security precaution for all 28 participating agencies within Alameda and Contra Costa counties. This document provided results from the ATMS network after the installation of netANCHOR. Furthermore, it outlined the benefits of the Uniloc enabled ATMS system in terms of potential security attacks. The document is currently going through final review. Upon acceptance the system will be incorporated into all 28 member agencies' systems as part of security enhancement of ACCMA SMART Corridor Program as part of Phase II of this project.

ABOUT ALAMEDA COUNTY CONGESTION MANAGEMENT AGENCY

The [Alameda County Congestion Management Agency \(ACCMA\)](#) was created in 1991 by a joint-powers agreement between Alameda County and all its cities. The CMA's goals, duties and composition make it easier for local governments to tackle the increasingly complex problem of traffic congestion. Established in 1995 in response to the need for improved mobility, the [East Bay SMART Corridors Program](#) (SMART Corridors) is setting a precedent for advancing transportation management systems in the Bay Area. Using existing resources, and costing significantly less than constructing new lanes, SMART Corridors improves traffic by implementing an Advanced Transportation Management System that uses cutting edge technology and is founded on key partnerships between agencies and jurisdictions. SMART Corridors achieves improvements in mobility and roadway safety. In addition, the program empowers users to make [SMART traveling choices](#).

ABOUT DKS ASSOCIATES

DKS Associates is a national transportation planning and engineering firm that provides state-of-the-art [consulting services](#) for all modes of ground transportation. DKS is an employee-owned company. Founded in 1979, DKS has become one of the largest specialized transportation engineering and planning firms in the United States. DKS provides technically innovative and institutionally sensitive [solutions](#) appropriate to the needs of each client.

ABOUT UNILOC USA

Uniloc USA (“Uniloc”) is the technology leader in electronic “device recognition” for securing networks, data and digital content. Device recognition is the method of uniquely identifying a user device, such as a PC, server, game console, smart phone or cell phone, by the naturally occurring, inherent physical imperfections of that device, and then incorporating that “device fingerprint” into access credentials or licenses. Uniloc’s technology can identify devices with more comparable accuracy than human DNA. Uniloc is the inventor and holder of the seminal device recognition patent (US 5,490,216), and has over 10 related patents pending. Uniloc has applied its device recognition technical expertise into several vertical markets including: software publishing, enterprise & government network security, web-based content, online banking & trading, and video copy control. For more detailed information, please visit www.uniloc.com.