Federal Highway Administration

Director, Office of Transportation Management

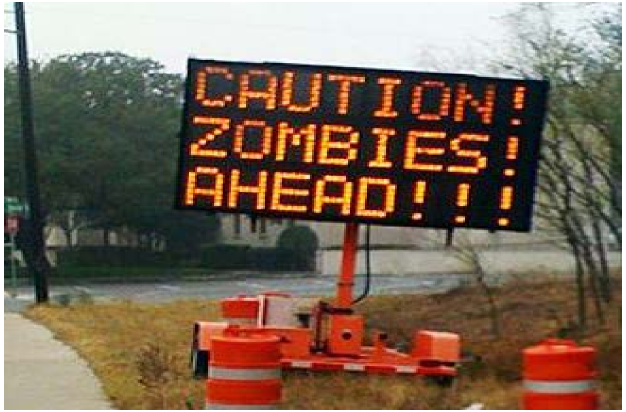
Transportation Systems Cyber-Security Framework

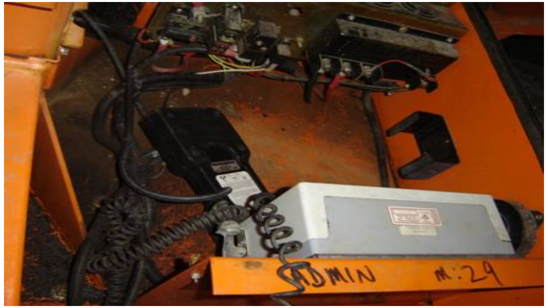
A process to

Monitor – Alert – Advise

Owner/Operators of ITS deployments

U.S. Department of Transportation
Federal Highway Administration



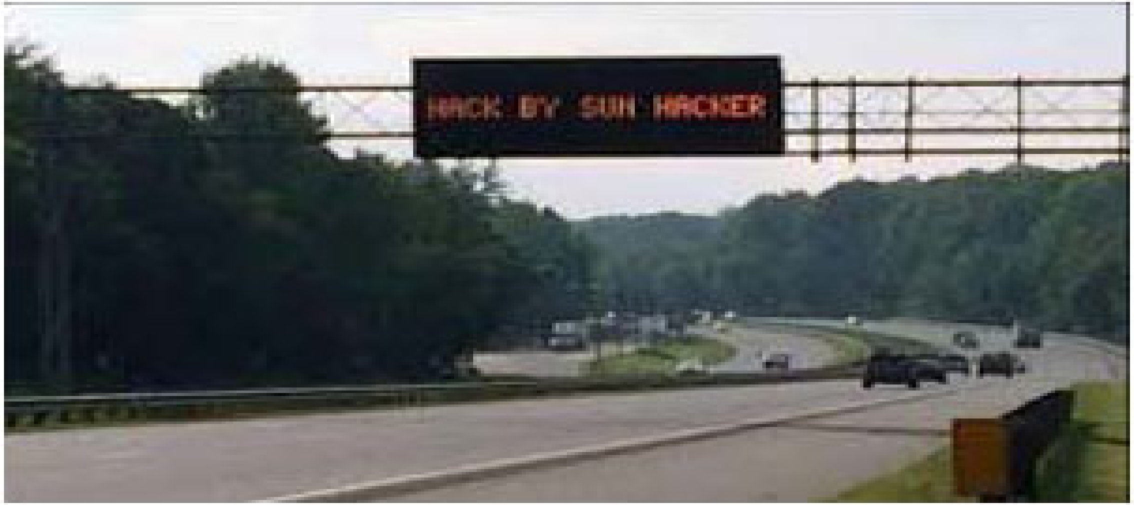


From just annoying

Unlocked or easily accessed control panels with uncomplicated or unchanged default passwords.

To becoming serious

DMS on publicly accessible IP address with an unchanged default password



Lesson Learned

- We need a better way to communicate and spread the word about incidents.
- IT Cyber Security experts do not have the domain knowledge of transportation system for proper threat assessment
- We're making old mistakes:
  - Poor configuration practice for wireless network
  - Poor practice to secure field equipment
  - Poor practice to patch vulnerabilities

Current

Proposed

Purpose

Provide transportation system owners/operators a resource for:

- Identifying, alerting, and advising on cybersecurity incidents specific to transportation systems and infrastructure
- Investigating potential system vulnerabilities
- Education and awareness training/information

Dimensions of Threat

- Malicious attack

- Non-malicious operational error
- Lack of system reliability
- Untrustworthy practices by the operator

Types of Impacts

- Misinformation
- Conflicting messages
- Defeating operational strategies
- Malfunctioning equipment
- Equipment damage
- Information theft
- Economic theft
- Data corruption
- Denial of service

Governing Assumptions

Make every effort to provide confidentiality of findings due to the sensitivity of:

- Inadvertently assisting cyber attackers through dissemination of unresolved vulnerabilities;
- Potential of shutting down information gathering within the ITS and owner/operator community due to receiving unfavorable and critical reports from media sources; and
- Work with existing organizations internal to the transportation industry and externally with the cybersecurity and ICS communities.

Organizational Platform

- Multi-organizational cyber security workgroup
  - Federal, State, and local / public & private sector

- Use the National Operations Center for Excellence for:
  - reporting and alert function
  - information and expert advice gateway, and
  - education/awareness portal.

Functions

Monitoring - Provide stakeholders a secure method to notify the CS WG of events, incidents, or vulnerabilities without exposing observed or suspected activities to the public. There are two reasons to have this more limited communication verses a list serve or other more public discussion forums; 1) assure confidentiality of the owner/operator who's system was attacked and 2) avoid exposing unresolved vulnerabilities. Regularly monitor other sources such as Homeland Security's ICS-CERT and MS-ISAC for attacks and advisory alerts. Provide these same resources with findings as appropriate while not violating confidentiality & exposure principles.

Alert - Develop an alert network of system owners, operating professionals, manufactures, and oversight/stewardship agencies (i.e. FHWA Divisions). This would be for quick reaction to on-going events and providing initial remedial advice. This might include directions on how to handle and distribute this information (e.g. confidential, general dissemination, etc.).

Advisory - Form expert sub-teams to develop/disseminate advice and solutions to attacks/threats, identify and manage needed research, and develop education and awareness products for stakeholder groups. Coordinate with other appropriate non-transportation specific organizations (ICS-CERT, MS-ISAC, DHS, etc.).

Beyond Roadway ITS Equipment and Deployments

- Personal Identifiable Information
- Tolling and Parking meters
- Transit Communication
- Freight Size & Weight inspection
- Border Crossing Inspection
- Connected Vehicles

Documents of interest

- Executive Order 13636—Improving Critical Infrastructure Cybersecurity
- 2014 National Strategy for Transportation Security: Report to Congress (not yet released)
- National Institute of Standards and Technology
  - NATIONAL CYBERSECURITY CENTER OF EXCELLENCE
  - Framework for Improving Critical Infrastructure Cybersecurity

Technical Support Available Now

- Self Assessment Tools - NIST
- Reports & Articles – ITSA, ITE, etc.
- Dedicated websites – TRB Cyber Security Resource Center
- Expert Advice – FHWA & USDOT VOLPE Center
- Relevant but non-transportation specific organizations - ICS-CERT, MS-ISAC, DHS

Membership: *Primary and secondary contacts/resources*

Federal Highway Administration (FHWA)

- FHWA Division Offices
- Other USDOT Modes and agencies (FTA, FRA, FMCSA, VOLPE Center, etc.)
- USDOT Cyber Security Action Team (Subgroup of the USDOT's Safety Council)
- Industrial Control System – Computer Emergency Response Team (ICS-CERT)
- U.S. Department of Homeland Security / Federal Bureau of Investigation

AASHTO

- State DOT's
- Toll Authorities
- Multi-State Information Sharing and Analysis Center (MS-ISAC)

NACTO

- City DOT's
- Department of Public Works

ITE

- Transportation Professionals
- Standards Development Organization

ITSA

- Equipment manufacturers
- Academia / Researchers

NEMA

- Equipment manufacturers
- Standards Development Organization

TRB

- Committee on Critical Transportation Infrastructure Protection

Way Forward

Actions

- Core organizations brief leadership and obtain by-in (AASHTO, ITE, ITSA, NEMA, FHWA)
- Coordination with USDOT Cyber Security Action Team and other USDOT modes (FHWA)
- Outreach to potential membership (AASHTO, ITE, ITSA, NEMA, FHWA)
- Coordinate with NOCoE (AASHTO, FHWA)
- Draft multi-organizational agreement/governance (AASHTO, ITE, ITSA, NEMA, FHWA)

Timeline

- Core organizations confirm commitment to move forward – Jan 2015
- Associated membership outreach effort – Jan/Feb 2015
- Charter/agreement/governance/responsibilities developed & in place – Summer 2015
- Advisory/Alert system activated – Fall 2015
- Research roadmap established – Winter 2015
- Awareness and Education activities defined – Winter 2015

Questions