WHITE PAPER

mobotrex™
MOBILITY & TRAFFIC EXPERTS

Signal Cabinet Peace of Mind

By Ben Ziegler,
Manufacturing Engineer
December 28, 2015

If you've had nagging thoughts about our industry's traditional #2 key/lock cabinet standard, take heart. The key, which can be purchased on eBay for a mere $6, is about to be fortified with a customized electronic lock and tracking software.

"There is much more public exposure than initially meets the eye," said MoboTrex Engineer Ben Ziegler. He recently worked with one Department of Transportation customer to secure and track access to its traffic signal cabinets. The MoboTrex system solution gives:

- Temporary access to qualified contractors and agencies for a specific duration.
- Works with RFID badge card reader or keypad.
- Grants individual user IDs so that the system tracks who specifically enters the cabinet, and when and how long the event occurred.
- Frees up inspector's time to supervise multiple projects.
- Reduces agency liability of untrained individuals accessing traffic systems.

"In the case of one of our customers, significant physical damage had taken place and they had no idea who should be charged back for the replacement costs," Ziegler said.

Ziegler researched potential solutions that adapted security industry technology. He built a hardened version with a custom lock, supporting that #2 key. The key is disabled by the electronic lock until the system gets a PIN code or card read. Ziegler's system can be set up to use existing building access cards.

A controller, electronic panel and key pad were specially designed for the signal box. He then integrated software running the individual cabinet locks into the network. The system is available as a stand-alone addition for cabinets now in use or may be specified for new equipment.

Why Be Concerned?

Simply put, more and more "stuff" is connecting inside that signal cabinet. As Intelligent Transportation Systems are more widely implemented, even more DOTs may find good reason to secure access to signal cabinets. Consider what may be inside or connected to the cabinet:

- Signal controllers
- 900 MHz Wi-Fi and GPS cell services
- Cameras
- Variable speed signs
- Emergency pre-emption systems

"The traditional industry #2 key is readily accessible, easily copied and widely available to former employees, contractors, third-party vendors and other municipal agencies," said Ziegler. "The root of the problem is that without an actively monitored data log, you can only guess who may have been in your cabinet."

As a practical matter, a DOT could not only experience damage to its equipment, there is risk for timing changes and equipment theft. By physically limiting access to the cabinet, this additional step helps indirectly secure access to communication switches and various networked equipment. Since most cabinets frequently share municipal fiber, a new layer of security is welcome since fire, police and even healthcare agencies may be on the network.

5 Ideas for Keeping Pace with Technology

"Our industry is rapidly adapting technologies from other industries. That's exciting," said Ziegler. "However, many of those industries' security best practices have not transferred to us just yet."

He notes that the size of municipality or agency doesn't indicate the level of sophistication. He works with a small municipality that is very vigilant.

1. **Establish a baseline for the new normal.** Is the inventory of devices up to date? What does normal look like for your operation? Will you understand if there is a change?
2. **Are your devices updated on a regular schedule?** Your maintenance procedures may need to be tweaked as technologies are added.
3. **How often are your networks updated?** Have you established standard opportunities for updating?
    - As a service tech is in a signal box for repairs.
    - Auditing during a special event such as stadium games, rush hours or major construction projects.
    - Have you set a quarterly or annual audit?
4. **Are you reaching out to sister agencies?** Who owns the traffic camera? Inter-agency coordination for maintenance may be needed. Will your agency and others served on the same strand within the fiber network, have enough room as ITS is implemented?
5. **What resources are available to notify you of a change?** Do you have a security system that alerts you to changes? Is there staff available to monitor the alerts?

About Ben Ziegler

Ben has worked for MoboTrex for four years and serves as Manufacturing Engineer. He designs and deploys wide area networks for MoboTrex customers. He holds a Bachelor of Science degree in mechanical engineering from the University of Illinois at Urbana-Champaign.