SupplyChainDigest™
Your First Stop for Supply Chain Information

Near Total Lack of Security in San Francisco Toll Tags Highlights Potential RFID Privacy Risks

Incredibly Easy to Hack, Says One Expert; No Encryption being Used; Surprised "Free" Toll Tags Haven't Hit the Black Market Yet

SCDigest Editorial Staff

Experts at computer security firm Root Labs have found that at least one auto toll system based on RFID tags – the FasTrak system in San Francisco – uses little or no security and is therefore subject to many hacking, theft and privacy problems for Bay area drivers. It also highlights that various privacy-related issues with regard to RFID-based systems are not likely to go away soon, especially in systems not well architected to prevent such concerns.

Like many toll systems nation-wide and around the globe, the FasTrak system uses an RFID transponder, typically placed on a car's windshield, to identify a vehicle as it approaches a toll booth. The identification number on the tag is read, allowing the vehicle to pass successfully through the toll booth area and adding the cost of the toll to the user/vehicle's account.

The Root Lab analysis found the tags used in FasTrak do not employ any encryption, even though there's a "placeholder" for an encryption key, according to **Nate Lawson**, a principal at the firm. He says for that and other reasons, tags could be copied or created with relative ease. This could enable, for example, someone to read the number off of another car's tag, and then write that number to a different transponder that would then be accepted at the toll booth and debit the first driver's account.

"It's trivial to clone a device," Lawson said at a recent security conference. "In fact, I have several clones with my own ID already."

He also said he is surprised a black market for cloned or copied devices hasn't already emerged.

"It amazes me there has not already been widespread fraud, cloning, and selling of 'free transponders' that" were hacked and reprogrammed," Lawson said. "There's nothing there technically to prevent it."

"It amazes me there has not already been widespread fraud, cloning, and selling of 'free transponders' that were hacked and reprogrammed," he said. "There's nothing there technically to prevent it."

The vulnerability could lead to all sorts of problems. In addition to some drivers escaping the tolls, the drivers whose IDs were copied would then face toll charges that perhaps far exceed their real use; they would have to argue or prove that the charges weren't theirs. In addition, criminals could theoretically copy their IDs to another vehicle to provide an alibi for the time of a crime.

Lawson also found that transponder IDs were stored in writeable memory. That means a hacker could change or alter any specific ID. That could then simply prevent a legitimate user/account from successfully passing through a toll station as an act of mischief.

It is unclear whether other toll systems have similar vulnerabilities. However, earlier this summer students at MIT apparently identified a number of security flaws in Boston's subway system, includ-

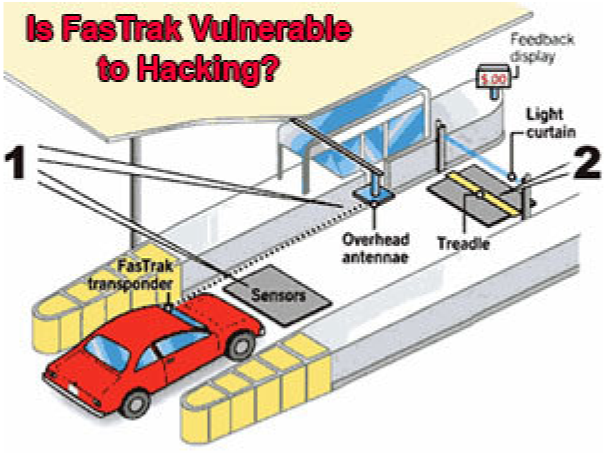
Near Total Lack of Security in San Francisco Toll Tags Highlights Potential RFID Privacy Risks (Con't)

ing the ability to copy RFID tags some use to access the train stations.

As the FasTrak system add tag readers along highways for other applications, such as tracking commute times, Lawson says he developed a simple "sniffer" that can easily pick up the communications between the transponders and the readers, typically attached to light poles. It would be easy, therefore, for a hacker to quickly acquire hundreds or thousands of valid ID numbers that could be cloned onto other transponders. Hackers could also simply walk up to any car with a tag and grab the transponder ID with a portable interrogator.

While FasTrak offers an aluminum shield that drivers can put their transponders in between toll booths to block on-road transmissions, many say the devices are clumsy to use and might even present a road danger as drivers try to put the transponder inside the shield while on the road. Root Labs has developed a different approach, using a "daughter-board" that is attached to the transponder and enables it to be powered on or off with the push of the button, allowing control of when the tag will transmit data (for example, only when nearing a toll station.)

The news caught The Bay Area Metropolitan Transport Commission (MTC) by surprise, and while officials stated they believed the system was secure, they are working with the provider of their technology to investigate the claims. In the past, MTC has said the data on the tags was encrypted, which Lawson disputes.



MTC also said it is beefing up general security technology in its systems. For example, if a cloned tag is identified (say from a customer complaint over charges) the system would alert officials the next time it saw that tag passed though a toll booth and take a picture of the vehicle and license plate.

But, the whole subject illustrates that we are still probably early in the curve of these sorts of issues with regard to RFID – and that consumers may need to do more due diligence than they might prefer to keep in control of their own "identity management." (See **Are We Entering a Period of Consumer "Identity Management?"**.)