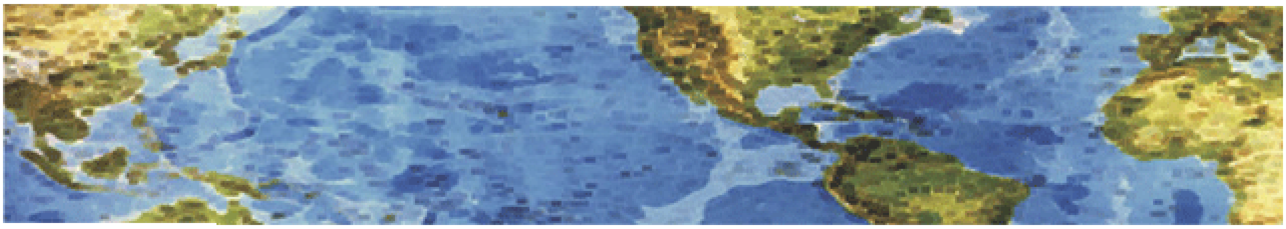
HALL ASSOCIATES



Risk-Based Decision Making Commentary
22 August 2014 Newsletter

Security researchers at the University of Michigan have not only hacked traffic light signals in real life, but also claimed that it’s actually shockingly easy to perform by anyone with a laptop and the right kind of radio. If we compare the traffic light hacks in movies and real life, **the reality is much easier.**

In a paper study published this month, the security researchers describe how a series of major security vulnerabilities in traffic light systems allowed them to very easily and very quickly seize control of the whole system of at least 100 traffic signals in an unnamed Michigan city from a single point of access. Researchers took permission from a local road agency before performing the hack, but they did not disclose exactly where in Michigan they did their research.

> ‟*Our attacks show that an adversary can control traffic infrastructure to cause disruption, degrade safety, or gain an unfair advantage.*

SECURITY HOLES IN TRAFFIC LIGHT SYSTEMS

The team said that the networked traffic systems are left vulnerable to three major weaknesses: *unencrypted radio signals, the use of factory-default usernames and passwords, and a debugging port that is easy to attack*. This left the network accessible to everyone from cyber criminals to young hackers. In an effort to save on installation costs and increase flexibility, the traffic light system makes use of wireless radio signals rather than dedicated physical networking links for its communication infrastructure - this hole was exploited by the researchers. Surprisingly, **more than 40 states currently use such systems** to keep traffic flowing as efficiently as possible. The researchers say that anyone with a laptop and a wireless card operating on the same frequency as the wirelessly networked traffic light — in this case, 5.8 gigahertz — could access the entire unencrypted network.

This system’s control boxes run VxWorks 5.5, a version which by default gets built from source with a debug port left accessible for testing. This debug port allowed researchers to successfully turn all lights red or alter the timing of neighboring intersections — for example, to make sure someone hit all green lights on a given route. A more worrying part is the ability of a cyber criminal to perform denial-of-service (DoS) attack on controlled intersections by triggering each intersection’s malfunction management unit by attempting invalid configurations, which would put the lights into a failure mode. *(Would make it easier to get away from a robbery, perhaps?)*

SOLUTION TO PROBLEM

The research team called for manufacturers and operators to improve the security of traffic infrastructure. It recommended that the traffic-system administrators **should not use default usernames and passwords**, as well as they should stop broadcasting communications unencrypted for “casual observers and curious teenagers” to see. Moreover, they also warned that devices like voting machines and even connected cars could suffer similar attacks.

Does Google have the right to scan user emails?

A person (see actual article for more details) has been charged with possessing child pornography, after the National Center for Missing and Exploited Children **received a tip from Google**. While it’s clear that the end result of this is positive – he’s being prosecuted for the heinous crime he’s committed – we have to ask, **do email platforms have the right to scan user emails if it helps to combat crime?**

Technically, whether or not they have the “right” depends on the terms of service between the user and that service as well as the laws governing that country. In the US, this is a complicated issue due to other US Federal laws that compel ISPs to help combat child pornography. Despite the horrific nature of these specific crimes, I don’t think Google has the “right” to scan user’s information. The general public has an understanding and expectation of how privacy works in the “real” world. For better or worse they’ve carried those same expectations into the online world.

This means that society expects online privacy to work in a certain way, regardless of the wording and details buried in user agreements and privacy policies. **These are not read, and these are not understood** – there is no meeting of the minds. So again, for better or worse, these expectations for privacy in the real world is how “we the people” expect and want online privacy to work. These expectations are not being met by things like online tracking and the scanning of emails and cloud content.

There are three types of scanning that email, cloud, and calling (VOIP) services do, such as parsing the content of Gmail messages to display ads, looking at user activity to optimize ‘free’ services, and pro-actively scanning content to identify criminal activity (plus a fourth which is providing access directly to law enforcement and governments at their request).

1. No right to scan for a crime. Both Gmail and Microsoft’s Cloud Storage have been known to proactively scan users’ content for evidence of criminal activity. In the US, society would expect the 4th Amendment’s protections against search and seizure to guard the privacy of their communications (not unless they have a warrant or other specific legal measures).
2. “Limited” right to scan content for Ads. I think at this point most people have some understanding that free email and other platform providers are scanning their content in order to display ads. But they would be shocked at the depth of the profiles that are assembled. Companies also have no right despite whatever clever agreements they’ve come up with to use this type of data for any other purpose. That would break the “context” of the exchange between the ad and the use of the free service
3. “Limited” right to scan usage for service optimization. Like ads, many people do understand that service providers look at metrics around how they use the services. Nominally this is done to “improve” the services provided and their service delivery. It also usually includes figuring our how to cross market additional services.

Users can take steps to protect their privacy when using free platforms like Yahoo, Outlook or Gmail. However they need to decide how much convenience they are willing to sacrifice, and how much information they are willing to share. Here are some things they can do right now to protect the content they entrust to these service providers:

Encrypt the content of your email messages. Users can keep free email providers from successfully scanning the content of their emails by first encrypting their emails before they send them. Tools like EnigMail for FireFox or GnuPGP will provide strong encryption. But they can be tricky to use, and you should use them to encrypt your email content outside of gmail.google.com (as it could save drafts while you are composing your email.)

Encrypt your files for cloud storage. Any files or images that you want to store on a cloud service you can also encrypt before they are uploaded to the cloud. Note this won’t work with sites like Flickr, but rather with cloud storage services that work like “hard drives” such as SkyDrive or Dropbox. You’ll have to be sure to decrypt and re-encrypt these files each time you use them.

http://www.abine.com/blog/2014/google-right-scan-user-emails/