Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 8, Issue 10

How Secure is M2M?

By: Jesse Cryderman

In August of last year, two researchers at an annual Black Hat security conference demonstrated some very clever and simple hacking with some very devastating results. They effectively stole a Subaru Outback by sending text messages from an Android phone.

It gets worse.

"I could care less if I could unlock a car door," researcher Don Bailey told CNN. "It's cool. It's sexy. But the same system is used to control phone, power, traffic systems. I think that's the real threat."

The automobile in question, like many others on the market, was equipped with remote starting and locking mechanisms, which are actuated through messaging from a GSM network. After sniffing authentication keys, Bailey and his cohort sent "authenticated" text messages to the vehicle, unlocking the doors and starting the engine. This process can be easily replicated on other similar cellular-linked M2M devices that do a lot more than protect cars, and it has.

Fast forward to November, when Pipeline reported on an alleged digital intrusion at an Illinois public water facility. According to an Illinois Fusion Center report, it appeared hackers gained control of a water utility pump, sent it a cyber poison pill, and disabled the pump. Since then, the FBI and the DHS rebutted the report, offering a rather compelling explanation that involved a worker accessing the control system while on vacation in Russia. Indeed a worker for the company that manages the control system was on vacation in Russia, and he did access the water plant at some point. However, security researcher Joe Weiss doesn't buy the DHS report; he stands by his original story, because, as he told Pipeline "control systems don't have cyberlogging and forensics." The DHS itself didn't respond to a request for comment on the incident, and a worker at the Curran Gardner Public Water District (where the incident occurred) told Pipeline "she could not comment" on the veracity of the original report. Was it just a false alarm? Regardless, the incident highlights a scary fact: SCADA systems that control utilities are online, and can be accessed from any country.

Commenting on this type of cyber terrorism, a McAfee researcher David Marcus wrote that "It is really no more difficult to attack a [Supervisory Control And Data Acquisition] SCADA network or system than it is to attack any other system." A hacker who claimed knowledge of a similar SCADA attack wrote of the stupidity of "connecting interfaces to your SCADA machinery to the Internet. I wouldn't even call this a hack, either, just to say. This required almost no skill and could be reproduced by a two-year-old with a basic knowledge of Simatic."

This is not science fiction--this is today's reality. As the "internet of things" goes online, questions of security and fraud move to the forefront. Particularly in light of recent high-profile attacks by Anonymous (who brazenly takes down government websites at will), cyberterrorism becomes much more frightening as a threat when critical infrastructures are exposed to infiltration and manipulation.

Both of these cases illustrate a major security problem facing M2M: machine-to-machine communication is inherently unattended, and unattended security is prone to attack. Additionally, "the number of M2M endpoints dramatically increases the attack surface," says Scott Swartz, CEO and founder of MetraTech. As we take a closer look at M2M, other security issues become apparent, a major issue being GSM itself. Surely carriers and vendors have already thought this through...or have they?

Is The Developing Digital World Inherently Unsafe?

"The research in security for M2M communications is still in its infancy," concluded a lengthy academic research paper published by researchers from the University of Waterloo and the University of Ontario in April 2011. "Despite the promising real-time monitoring applications and tremendous benefits, M2M communication is still in its infancy and faces many technical challenges," the researchers indicated.

Like web browsers and the Internet, it wasn't until after viruses and Trojans began to infiltrate our daily lives that security programs began to catch up. Similarly, each time a new digital platform is commercialized—smartphone, tablet—a new wave of cyber attack hits shore before security patches are released, and prevention and detection software is released.

Certainly, as M2M matures, better security will evolve, but until then, we are living in a developing country. Identifying key security problems is the first step in creating solutions.

M2M and GSM: An Unhealthy Marriage?

One of the biggest security issues facing M2M is the predominant network technology used to send M2M messaging is still GSM, which has considerable security flaws, compared to CDMA. Denny Nunez, Business Development Manager, Sprint, elucidated this threat. "The voice security hole has been exploited dozens of times over the years on GSM. Today eavesdropping over the GSM voice channel is done with relative ease and with under $100 in equipment costs. SMS has also been exploited in GSM M2M modules."

In fact, both examples at the beginning of this article were exploits of GSM networks.

"None of these examples have ever been successfully done on CDMA," continued Nunez. "This is thanks to the higher encryption level native in CDMA vs. GSM, and the spread spectrum technology inherent in its design."

The research in security for M2M communications is still in its infancy.

Scott Schwartz, CEO of MetraTech, agrees. "3G and 4G already offer better security than GSM/GPRS networks and if the device has the ability to encrypt the data, the connections are as secure as those that we use for online commerce and banking."

Although M2M will certainly evolve to communicate over 3G and 4G networks, today most M2M communication requires very little bandwidth and is still delivered over GSM networks. But that doesn't mean we're doomed until the next M2M network upgrade–there are security holes that can be closed.

Let's Get Physical

There are two points of attack on M2M communications: over the network, or physical attacks on the device. As I pointed out, M2M devices, by nature, are unattended, making physical attacks fairly easy. Also, many devices switch to sleeping mode in order to conserve energy, making detection of an attack difficult. Sadly, M2M devices aren't very well equipped to deal with physical attacks.

According to security experts, the security technology employed in the embedded hardware in most M2M devices is "from the 80s"—in other words, very easy

to hack. This is based on simple market dynamics: M2M devices must be cheap, highly available, and consume little power. In order to create a "trusted" connection, the devices contain authentication information. However, unencrypted flash memory in the devices themselves easily exposes the "secret keys" to an intruder.

Security researcher Hunz outlined the ease with which M2M devices can be physically attacked in a recent presentation. Hunz bought an asset tracking M2M device from eBay. When he looked inside, he found a PIN-protected SIM card. However, the device sent the PIN to the SIM card when it was powering up, making the PIN easy to "sniff" using SIMTrace. Hunz took the compromised SIM card from the device and put it in a cellphone that had the firmware patched to the IMEI of the M2M module. He began making phone calls. The SIM remained active.

If it ended here, this would be an example of SIM-fraud via M2M module. This is surprisingly quite common—recently an Australian woman was jailed for racking up nearly $200,000 on a SIM card she pulled from her smart meter. In Africa, a network of thieves pulled SIM cards from traffic lights to make thousands of dollars worth of calls. However, free calls and SIM-fraud is only one exploit; Hunz dug deeper.

He located a private internet of IP addresses (likely other similar devices) that updated regularly (likely moving cars). He then connected the M2M module to his PC, and spoofed the control surface to gain entrance into the vendor network, which had no rogue device identification parameter. Once "inside," he could have launched a passive attack to map out the network protocols, or an active attack to disrupt services provided by the M2M network.

Since physical attacks on M2M devices must be expected, the need for better device-side protocols is paramount. These include:

- Disabling debugging functions in M2M devices themselves.
- Encrypting the internal memory of microcontroller in the device.
- Eliminating signal pathways that send unencrypted data over external buses (USB, etc.)
- Building in circuitry that detects tampering or intrusion.

GSM, which is widely used for M2M, has considerable security flaws, compared to CDMA.

Physical security protocols are important whether a device is on a GSM network or a CDMA network, so carriers and M2M service providers should make every effort to ensure "secret" data is encrypted and properly handled through all touch points in the M2M communications chain.

Better Gateways and Encryption

Beyond physical device attacks, communications service providers who offer M2M solutions must also prepare for network-side attacks. As security expert Hunz wrote, "never trust the communications channel; always use extra sound encryption and authentication." For one, this means stronger gateways.

"CSPs should provide a gateway between M2M endpoints and M2M management platforms and any external interface," said Scott Swartz. "Consider the recent cell phone hacking scandals. Was the device hacked or the connection hacked? The industry must take into account what confidential information the endpoints contain and how to protect it."

In other words, even if a device is hacked, the gateway to the network must have robust authentication that prevents and detects unauthorized use and entry attempts, as well as logging and reporting mechanisms. Proper detection, logging, and reporting can contain an attack as a passive intrusion, before hackers are able to launch an active, damaging assault.

Additionally, communications channels used by M2M applications aren't usually encrypted by M2M service providers. As Denny Nunez at Sprint explained, "a concern is that many M2M applications also open up and utilize both the SMS and Voice channels. SMS and Voice are rarely ever encrypted by third-party M2M solutions and THAT is where a big security hole exists."

A Standard for Safety

While M2M solutions reside within a latticework

of overlapping standards that address various points along the machine-to-machine technological continuum, “There is no ISO standard for M2M security,” says Denny Nunez. There are M2M working groups that are certainly dedicating considerable time to creating security standards, but as of today, a M2M device doesn’t come with a sticker that verifies its compliance with, say, standards for encrypted security key handling in on-board memory. While security standards for M2M communications will certainly be developed, until they do, it is critical that CSPs who offer M2M diligently investigate the security protocols of devices, their third-party partners, and the level of encryption and authentication in their gateways and SMS/voice channels.

The Future is for the Machines

As I pointed out elsewhere in this issue the future of connected devices belongs to machines. Standing at the first stop on the road to the internet of things, we see M2M primarily being used for metering, asset tracking, and dynamic advertising. Although improving security of both the M2M devices and communications networks for these applications is crucial, the importance of M2M security will only increase as M2M applications evolves into active infrastructure management.

Scott Swartz summed up the challenges facing M2M service providers as applications move from simple monitoring and tracking to control: “The scary question is, “What M2M applications control things that are potentially dangerous vs. applications that are primarily benign?” I allow my home automation system to activate my alarm, but do I trust it to deactivate it? Not yet. Let’s hope that critical infrastructure providers use the same common sense until the security issues are sorted out.”