Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 9, Issue 6

Mole in the Machine? Unique Security Challenges of M2M Connectivity

By Jesse Cryderman

Anyone with a finger on the pulse of telecommunications will tell you that a seismic shift is occurring, and it's bigger than 4G or VoLTE. This change will predominantly occur over 2G, WiMAX and Wi-Fi, and it has very little to do with customer experience management (CEM). That's because the connected future belongs to machines, and machine-to-machine communications (M2M) will eventually outnumber human connections by a substantial margin. The applications for M2M are limitless: from vending machines to healthcare devices to home appliances and public safety systems, nearly everything that can benefit from connectivity will. That much is certain.

What is less certain is what will transpire between today and the Jetsons-like future that awaits us. Will user configuration errors turn a "make more ice" command intended for a "smart" refrigerator into a poison pill for a home network? Will hackers infiltrate public safety networks or use SIM cards from unattended devices to perpetrate fraud? M2M is still a nascent technology, and security concerns are one major piece in the puzzle that must be addressed before the technology moves forward into a secure and profitable automation and virtualization solution.

Welcome to the machine

When industry leaders like John Horn, president of Raco Wireless, say, "Machines are going to rule the world," they are hardly joking. Current M2M use cases like telematics and fleet management, security, smart grids, and dynamic advertising are just the beginning of a trend that will generate billions of dollars for mobile network operators (MNOs). The latest white paper from Machina Research forecasts the following developments by 2020:

- 2.1 billion cellular M2M connections;
- 3.6 billion additional M2M connections where cellular connectivity can add value;
- an addressable market for mobile operators totaling $373 billion.

The market is certainly ripe, but it won't blossom without advanced security, and it isn't as easy as just porting security solutions that worked in the cellular domain. In an academic white paper entitled "Security and Trust for M2M Communications," the authors noted that M2M "threats may not be fully addressed by use of security technology and methods adopted in existing wireless devices, cellular networks, or WLANs."

At the same time, MNOs who want to rule the M2M space must move quickly, as the ecosystem is broad and encompasses possible players in many industries, not the least of which are Internet-based companies like Google. "Ensuring end-to-end security is going to be [a] significant industry challenge, and those who move quickly will reap the greatest benefits," predicted Frost & Sullivan in a recent white paper. Closely examining the security challenges of M2M will enable MNOs to be the early birds and build safe, reliable, high-value M2M platforms.

Machining digital security

On an abstract level, there are essentially three pillars to any digital security solution:

- Confidentiality: Only authenticated parties and systems should have access to information.
- Integrity: Data must be safeguarded from modification as it moves through the network.
- Authenticity: The source of data moving through the network must be genuine, identifiable and logged.

There are several reasons why M2M connections present unique security concerns compared to common computing or cellular security. First and foremost, M2M ostensibly removes one of the biggest security threats from the equation: the human end user. Network compromises caused by either accidental or intentional errors on the part of a human are arguably the most significant security threats. In the cellular network "most of the risk is the user," says MTS CIO Frederic Vanoosthuyze. A machine, on the other hand, is incredibly good at following its own security policies. But unlike a cellular phone or a tablet, machines are, for the most part, unattended, and present an easy opportunity for attack. Many analysts and academics point to the unattended nature of M2M communication as its biggest risk.

Second, a central tenet of security is that the more points of entry there are, the greater the risk. It's simply a numbers game: Even if all the doors are made of steel, a house with 1 door is easier to defend than a house with 20. Likewise, managing a million devices — or attack points, depending on how pessimistic you are — is difficult, but ratchet that number up by a factor of 10 and you get an idea of the increased risk M2M presents.

Third, data in the M2M network isn't inherently encrypted or managed like data in the cellular network because there are numerous providers and numerous transfer protocols. Machines will do a great deal of talking in the future over unregulated spectra like Wi-Fi. "Non-cellular will account for about half the market," says John Horn of Raco Wireless. "Wi-Fi needs a specific security solution."

Fourth, M2M security means different things to different parties. A simple home automation system might be designed with simple security — hardware-based security and software-based monitoring and control. Healthcare and financial institutions, on the other hand, are governed by strict confidentiality and security laws, so M2M security solutions in these industry verticals are much more robust. The TIA has drafted M2M standards, but the industry has yet to adopt a unified view of what constitutes M2M security. In fact Machina Research predicts that greater standardization is one of the top 10 drivers for the M2M revolution.

"Ensuring end-to-end security is going to be a significant industry challenge, and those who move quickly will reap the greatest benefits."

The M2M security platform

There are three elements that must be addressed to create a secure M2M platform: device-level security; data security in the network and gateway; and application security.

Device security

According to the TIA's TR-50 standards committee, devices in the M2M ecosystem are vulnerable to six types of attacks, such as configuration attacks, data and identity attacks and protocol attacks. There's a reason why so many attack scenarios originate from M2M devices: Most of them aren't built with the power to perform advanced encryption. By nature, M2M devices are designed to be cheap and produced in large volumes; one security researcher I spoke with for the March issue of Pipeline said the security in most current devices is weak and easy to crack.

It is critical that volatile data is encrypted and erased following a session, including authentication tokens, login procedures and session data. In order to prevent attackers from accessing and modifying EPROMs or sidejacking to view and exploit data transmission between a device and the network, devices should have some type of intrusion detection system that works even in sleep mode, not to mention an emergency policy control that removes the device from the authenticated network.

Luckily, there are several hardware solutions on the market. Gemalto has created a version of the SIM card specifically for M2M devices called the MIM, or machine identity module. Another option is the use of a coprocessor or modular hardware device to manage encryption and authentication, like Amphion devices from the Ei3 Corporation.

Network and gateway security

Devices in the M2M ecosystem can control mission-critical systems like power and public safety, so the network and gateway considerations are greater. Going beyond the traditional peer-to-peer connectivity of the Internet, secure connections to and from an M2M device are essential.

"We lock the solution down with a VPN [virtual private network] and an APN [access point name] into the carrier network," explains John Horn. This is a good model for any operator interested in the growing M2M space; when you consider the applications of M2M, from retail sales enablement to portable healthcare monitoring devices, a secure VPN + APN connection is the best option.

Application security

Porting applications from the cellular or Wi-Fi environment to the M2M ecosystem is a quick way to play, but it's also unwise. For all of the reasons we've already covered, M2M has a unique set of security issues. Applications in the M2M ecosystem must be written with M2M security needs in mind, and platform providers should audit their third-party developers to ensure there are no doors left open.

Opportunities for CSPs

CSPs stand at an advantageous spot on the M2M landscape because they have a proven ability to build and maintain secure networks. As Frederic Vanoosthuyze of MTS pointed out, "All mobile operators built a high level of security into their networks in order to achieve high levels of reliability." This is especially true in CDMA technology.

Scott Swartz, CEO of MetraTech, outlined just how secure modern cellular connectivity can be: "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."

Of course, most M2M devices aren't running on 4G networks: this bandwidth has been reserved for high-ARPU services like mobile video. Instead, mobile operators are repurposing 2G spectrum, which is more penetrable by malicious attack. Therefore, in most instances the need for better device-side protocols is paramount. These include:

- Disabling debugging functions in M2M devices themselves.

Unlike cellular phones or tablets, M2M devices are unattended, making them more vulnerable to attack.

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

Additionally, Denny Nunez, business development manager of M2M Security at Sprint, explained that security measures from partners must be examined. "SMS and Voice are rarely ever encrypted by third-party M2M solutions, and that is where a big security hole exists."

Even with the risks, building and marketing a secure, reliable M2M platform is becoming a top business priority for many CSPs; Telefonica, Vodafone, Deutsche Telekom, Sprint, and many others are all highly active in M2M. Global CSPs have also partnered to benefit from their combined scale and accelerate time to market. The best example was seen in July, when KPN, NTT Docomo, Rogers, Singtel, Telefonica, Telstra, and Vimpelcom combined forces to create a seamless, global M2M platform. The alliance is providing a global product featuring a unique SIM, as well as a united Web interface and centralized management of status and usage of M2M devices globally, via the Jasper Wireless Control Center. Notably, nothing of this scale in M2M has been announced by U.S. mobile operators.

Opportunities for BSS/OSS providers

Companies traditionally identified as BSS and OSS providers will greatly benefit from the M2M ecosystem, provided they can adapt their solutions for the new market. Piotr Machnik, EVP of Comarch, believes that "new business models like B2B and B2B2C ecosystems with multipartner value chains and all-IP services can't be managed in the old-fashioned style, typical for OSS/BSS silos." Raco Wireless's John Horn agrees: "You are going to see entirely new systems, tools and support solutions come out of this."

The M2M management and security platform must manage hundreds of millions of devices while efficiently reporting, billing and logging on the individual device level. M2M management, security and billing solutions will have to take into account the massive volume of authenticated devices, while at the same time they must be able to function very efficiently, as the ARPU for M2M transactions is small. It's a unique challenge.

Foundation for the future

Luckily, there is still time to build a secure and profitable foundation for the future. Recent reports indicate M2M hasn't gained ground as fast as analysts had predicted, quite possibly due to the fact that security still must be ironed out and standards have yet to be universally applied. However, the market will undergo many changes in the near future as venture capital flows in and consolidation occurs at the top. There is still plenty of room for both niche players and tier 1 CSPs to differentiate, and security is a great place to start.

"You are going to see entirely new systems, tools and support solutions come out of this."