JULY 2015
TELIT WHITE PAPER

M2M/IoT Cellular Data Security

Lawrence Miller, Principal Network Architect,
Telit IoT Connectivity

Historically most M2M communications were focused around proprietary protocols, private networks, leased lines and POTS. Some systems have moved to local LANs and TCP/IP. **Now they are moving to Internet access and cellular connectivity. Most efforts to date are focused on just getting things to work with only minimal consideration to overall system security.**

This paper will discuss ways to avoid some of the threats to M2M/IoT communications systems and ways to mitigate others.

CONTENTS

INTRODUCTION

Any discussion of security is dependent on context. This report will discuss security issues associated with migrating M2M/IoT communications to cellular technologies or creating a new M2M/IoT product using cellular communications. Historically most M2M communications were focused around proprietary protocols, private networks, leased lines and POTS. Some systems have moved to local LANs and TCP/IP. Now they are moving to Internet access and cellular connectivity. Most efforts to date are focused on just getting things to work with only minimal consideration to overall system security. Most cellular modems today connect directly to the Internet with less protection than the average home PC. Even products that do have some threat protection are still at risk of unanticipated data consumption. This paper will discuss ways to avoid some of the threats to M2M/IoT communications systems and ways to mitigate others.

HISTORY

THE TERM "MACHINE-TO-MACHINE" or M2M encompasses a rather broad range of activities. In general it refers to some kind of central processor or controller communicating with one or more remote sensors, actuators or other peripherals to perform some kind of automated function. This can be as simple as a home thermostat controlling a central furnace and air conditioner or it can be as complicated as computers at Johnson Space Center receiving telemetry from and tasking the Mars Rover. Since there is likely to be very limited cellular coverage on Mars, this discussion will be limited to more mundane activities here on this planet.

HISTORICALLY, PRE-INTERNET, the M2M industry did not put a lot of effort into security measures. Most connections were directly wired, either parallel or serial. Serial connections like V.35, RS-232, RS-422, RS-485, etc. were common. Security was physical. If there was an issue, it was resolved with a steel conduit or a cabinet. Around the same time companies were creating network technologies and protocols. Xerox and Digital Equipment Corporation developed Ethernet and DECnet. IBM created Token-Ring and SNA: Apple created Apple-talk. There were numerous others, all with little or no security considerations. Larger companies created private networks using these new network technologies and protocols over leased lines, ranging from analog phone lines through to digital T1 lines. The only real external security concerns were associated with "Plain Old Telephone System" (POTS) modems. At that time usernames and passwords were enough. With directories that were all paper, analog dialing and long negotiation times, any brute force attack would literally take forever. If someone did manage to get through, at speeds from 1200 to 9600 baud, there was plenty of time to trace the call. All of the phones were POTS lines; a trace not only discovered who had placed the call, but exactly where the call was placed. Making the prospects for anonymity, and not getting caught, fairly remote.

IN THE MID 1970'S The "Defense Advanced Research Projects Agency" (DARPA) funded a project to create a next generation network protocol to connect diverse networks and systems. In 1982, the US Department of Defense (DoD) declared TCP/IP the standard for all military networking. When Microsoft released Windows 95 with native TCP/IP support, it became the dominant protocol. In the mid 1980's, when the DoD, universities and defense contractors were busy interconnecting, "The Internet" was born, followed moments later by the first hacker.

CELLULAR DATA NETWORKS were created in the Internet era. Cellular devices, although they may have other services associated with the carrier's network such as SMS or eGPS, for data purposes are IP devices. They can communicate using almost any IP protocol that any other IP node (such as a PC) can use. Cellular modems have at least one IP address that is provided by the cellular carrier when the modem initiates a connection to the carrier's network. A common analog to this is the pre-broadband dial-up Internet connection where a computer, using a modem, would dial-up a service provider, authenticate and gain access to the Internet. This is essentially how cell phones, tablets and cellular modems work today, except without telephone wire and R2D2 sound effects.

SECURITY CHALLENGE

The challenge is to integrate historic, current and future M2M/IoT products and applications with cellular wireless technologies without becoming road kill on the Internet highway.

Technology is moving quickly and there are a lot of solutions and/or products to either adapt or replace traditional M2M devices and control systems. Discussion of these products is outside the scope of this paper. However, the vast majority shares a common design feature. The cellular modem is designed to register to a cellular carrier, establish a data connection, get an IP address, and gain access to the Internet via the carrier's network. They work this way because this is typically the only type of connection carriers offer the general public. However, there are a number of security and design issues associated with this type of connection.

INTERNET ADDRESSES

The carrier's network typically assigns a dynamic public address when the modem establishes a data connection to the network. As the term dynamic implies, the address will typically change at every connection. A public address allows mobile devices to communicate with servers on the Internet. It also allows systems on the Internet, some may be hostile, to communicate or try to communicate with the mobile device. This can lead to hostile attacks and unexpected wireless data consumption.

Some carriers provide a DNS (Domain Name System) lookup facility using a mobile device's phone number to return the current IP address. While this may, initially, be good for the user's application, it also means that the phone number can be used to track and attack a specific device.

Note: Fixed public addresses may be available from some carrier's on a limited scale and at additional cost. However, with the global depletion of IPv4 addresses it unlikely that there will be sufficient public IP address for any kind of sizeable deployment.

DEVICE BASED SECURITY

Present concepts of device security are of limited value for cellular data communications. Firewalls, usernames and passwords, and multi-factor authentication are designed to prevent un-authorized and/or malicious access into an IP node, system or device. While these techniques are effective at preventing intrusion into a cellular data device, they do not prevent the associated IP data traffic from reaching the device and consuming metered cellular data. Typical M2M data usage is less than 5MB per month. Brute force username/password attacks and repeated ports scans can consume 5MB and very quickly.

Denial of Service Attack (DoS)

A DoS attack is performed by sending so much traffic, from one or more sources, to a specific IP node, system or device that it causes the node to fail or sufficiently congest the network to the node so as to make the node unusable. This attack is notable in that it can both deny access to the node and cause very large data consumption and overages.

ABSENCE OF DEVICE BASED SECURITY

The previous section "Device Based Security" assumed that at least some level of device security was present. This is not always the case. Sometimes security is missing, unconfigured or misunderstood, leaving the device unprotected. When a legacy M2M device is connected to a cellular modem, it is not always clear what features or listeners are enabled in the TCP/IP protocol stack, for example FTP or Telnet. Once that modem connects to the carrier's network and the device is on the Internet, the automated scanners will find and exploit any openings. They will find them. Not long ago, just as a cursory test, an unprotected system was given a public address and put on the Internet. Within 60 seconds it had been found. Within 120 seconds it was unusable from the keyboard.

TRACEABILITY

Traceability is for accountability, it does not directly prevent any kind of attack or abuse. Tracing is used to identify the source of the attack or abuse. Unlike traditional telecommunications (i.e. POTS lines) the Internet provides ample opportunities for anonymity, which emboldens groups and individuals with less than honorable intentions since the chances of being traced or actually getting caught are very remote. With little to no disincentive, the rate and frequency of intrusion attempts is only going to rise.

REMOTE INITIATED CONNECTIONS

Cellular connectivity works well with a traditional client/server model where the client always connects to the server. With cellular connectivity, the modem establishes a data connection to the carrier's network and then the client application can create an IP connection to a server on the Internet. While some M2M/IoT solutions have been created or modified to operate in a similar fashion using scheduled or timed reports and check-ins, many M2M/IoT solutions require the server to have ability to initiate an IP connection to the remote device. A number of methods have been created to work around this problem that typically involve keeping the device continuously connected to the carrier's network and reporting the devices IP address to the server. There are several problems with this:

Increased Data Usage

IP connection resources within the carrier's network are valuable. The carriers set inactivity timers and disconnect devices that have not pass traffic for the configured timeout period. The only way to overcome this is to send some traffic slightly more frequently than the timeout period. This traffic usually needs to be initiated from the cellular device. It can be as simple as a ping or it can be a check-in to a server. These "keepalives" will consume billable cellular data.

Abuse of Carrier's Network

IP connection resources within the carrier's network are also finite. Most carriers have some kind of guidelines as to how they expect the network to be used. Some carriers actually publish them. Some, at their discretion, will require applications to be certified so that they do not adversely affect their network. The point being, applications that retain IP connection resources for extended periods of time and pass very little traffic can and have been considered abuse on some networks.

Extended Exposure to Internet Attacks

From a cellular security stand point using the Internet can be like a backwards game of "Whack-a-Mole." The objective is to connect, get an address, perform the required transaction(s), release the address and disconnect. The longer a node is active on the Internet, with the same address, the higher the likelihood that it will be found, attacked and possibly compromised. There are constant address and port scans on public addresses on the Internet. It is just a matter of time before an active address is found, interrogated and attacked.

DEVICE BASED VPNS (VIRTUAL PRIVATE NETWORKS)

VPNs are another way to overcome the remote initiated vs. host-initiated problem and also enable good data privacy, but they do not provide any security on the device. Device based VPNs can also be a technique for overcoming the inactivity timer. The timers for the VPN keepalive or Dead-Peer-Detection (DPD) are much shorter than the network's inactivity timers and may even cause enough traffic to avoid abuse consideration. However, that means a lot more billable data, which is a financial, not a security challenge.

SMS

SMS is a special case. It is not IP based and could be considered outside the scope this report. SMS is currently is not generally used as a vector for hacking. However, as more applications use it and more attention turns to smart phones, tablets and other connected devices, it will likely become a vector for malicious attacks. SMS can also be a financial concern. In the U.S., both Mobile Originated (MO) and Mobile Terminated (MT) SMS can be billable.

THREAT MITIGATION

Now that some of the challenges have been identified, the discussion changes to ways to mitigate or avoid these risks. As is usually the case with business this is a risk vs. reward situation. The drive to use the Internet provides for faster, cheaper deployments and access to previously unreachable areas. In return it opens your deployment up to a very hostile security environment. As might be expected, mitigating threats has a cost in time, complexity and dollars.

AVOID THE PUBLIC INTERNET

A wise man once said, "The best way to avoid a train wreck is to stay off of the tracks." If at all possible, stay off the Public Internet. Internet Protocol can be used without going out on the Public Internet. Get access to private APNs through M2M solution providers or, if your deployment is large enough to make it cost effective, get a private APN from one or more cellular carriers. An APN is effectively a bridge between the complexities of cellular IP data infrastructures and the ubiquitous wired IP/Internet infrastructure. The configuration of the APN controls all facets of the mobile device's interaction with the Internet. With a private APN carriers will allow some modifications to this interaction, like authentication and addressing.

PRIVATE IP ADDRESSING

Private IP addresses are defined in the Internet Engineering Task Force (IETF) RFC-1918. Private address space consists of 256 Class A networks (192.168.0.0 thru 192.168.255.0), 16 Class B networks (172.16.0.0 thru 172.31.0.0), and one Class A network (10.0.0.0). These addresses do not occur on the Internet and can be used privately for any purpose. Private addresses are not permitted on the Internet. For a node with a private address to reach the Internet its source address must be actively translated to a Public address. Private addressing aids security in that it requires a third component to be specifically configured to allow a privately addressed node to communicate with, or be attacked by, a node on the Internet.

HOST VPNS

Host VPNs connect one or more hosts to an M2M/IoT solution provider or a cellular carrier. The advantage to this type of VPN, as opposed to a device-based VPN, is that it typically encompasses all of the traffic to or from all cellular data devices for a given subnet or customer. This is a key component; it allows traffic to and from cellular data devices without the devices being directly accessible from the Internet. Cellular carriers tend to offer very limited VPN options in conjunction with private APNs. M2M solutions providers tend to offer more flexibility in VPN types and options without the complexity, or expense, needed to setup a private APN.

STATIC ADDRESSING

As was discussed earlier, many M2M/IoT applications have been and are based on a central controller or host connecting to or polling remote devices, which in this report, are cellular data devices. Static addressing, in this context, means that the device can always be addressed using the same address. So when a host attempts to connect, it can always use the same address. There are two basic ways to do this, static address and using static NAT (Network Address Translation; each has its own pros and cons.

Static Address

Static address is the simplest and most common. When a device connects to a carrier network, during the authentication process the device is always given the same address. The drawback to this is that all devices using a static address APN must always, for routing purposes, connect to the same carrier hardware that houses the APN. If that hardware is being serviced, fails or is otherwise unavailable, all devices on that APN will be disconnected and will remain disconnected until the APN hardware is available, or the APN and the routing are moved to replacement hardware.

Static NAT (Network Address Translation)

Static NAT is more complicated and unique to M2M/IoT solutions providers. When a device connects to a carrier network it is given a dynamic address. The address the device receives is tracked and a NAT entry is added to redundant locations within the M2M solutions provider's network so that the device will always be reachable using the same address. The most significant advantage to this is that when the carrier uses dynamic addressing, it can spread a single APN across a number of pieces of hardware. When a piece of hardware fails, the devices using it are disconnected and can reconnect immediately on anyone of the remaining units that the APN is using.

DEVICE-TO-DEVICE COMMUNICATION

This is one of those little loopholes that often slip past unnoticed. Typically, all devices within a single APN can communicate using IP addresses without leaving the carriers network and without transiting any kind of firewall or access control system. While this may not be a problem on a completely private APN, it is a big problem when using a shared or public APN. The good news is that most carriers can block it at the APN level for both shared and private APNs. Select an M2M solutions provider or carrier that blocks device-to-device communication. However, some applications may require device-to-device communications between specific devices. At least one M2M solutions provider that implicitly blocks all device-to-device communication offers the ability to allow communication between explicitly defined devices.

CONNECTION CONTROL

As the number of M2M/IoT devices increases, the chances and frequency of carriers enforcing network abuse policies will increase. Specifically, keeping devices connected to the network continuously and passing very little or no traffic for extended periods of time. This will likely take the form of reduced inactivity timers followed, eventually, by traffic volume over time equations. Anyway they do it, it will have an economic impact in the form of increased usage and device connectivity issues. Basically, connecting to a carrier's network for an extended period of time (hours, days, weeks) on the chance that a host might need to connect to it may not be a successful solution in the long run. The answer is to create or modify a solution so that the cellular data device only connects to the carrier's network when it is needed and releases it when it is no longer necessary. To do this, some method, or combination of methods, of connection wakeup needs to be used to establish the connection to the carrier's network. It is important to understand that this connection enables the device and host to communicate; it is not referring to the actual communication. The actual communication is controlled by the application and can be initiated in either direction. The common wakeup types are Event, Timed, SMS, and Dial.

Event Wakeup

This type of wakeup establishes a connection when one or more pre-configured events occur local to the cellular data device. Once connected to the carrier's network, the device and host can initiate IP communications in either direction.

Timed (or Scheduled) Wakeup

This type of wakeup establishes a connection at a predetermined time at the cellular data device. The time can be relative, a simple timer, or absolute, scheduled at a specific date and time. Once connected to the carrier's network, the device and host can initiate IP communications in either direction. If the clocks of the device and host are adequately synchronized using a common external source, like the cellular carrier's network clock, then it may be possible to have a host application that polls devices on a regular schedule and operates unchanged when communicating with a cellular data device.

SMS Wakeup

This type of wakeup establishes a connection when the device receives SMS from an external source. Once connected to the carrier's network, the device and host can initiate IP communications in either direction. SMS is a message protocol and can be used to signal many types of actions from many different sources. It is important that the SMS message uniquely indicates the desired action (from a specific source, contain a specific message, etc.…). It is also important to confirm the validity of the sender. The message should contain some kind of password or code to confirm that the sender is allowed to initiate the requested action. It is important to note that SMS does not guarantee delivery and, depending on the method sent, delivery time can vary from seconds to minutes to hours. In general the closer to the carrier's network the better.

Dial Wakeup

This type of wakeup establishes a connection when the device receives a voice call attempt from a specific source phone number. Once connected to the carrier's network, the device and host can initiate IP communications in either direction. This is the least secure and the most problematic method for remote signaling. The only advantage is that it tends to be very quick. The problems are significant. The caller-id can be easily spoofed. If it has a dial able phone number, can be called from anywhere. If it has a non-dialable number or no number it cannot be dialed at all. Auto redirect to voicemail can disable it. Some carriers simply do not like it and prohibit it by contract. In specific cases it might be useful, but it would be advisable to find a better method for general deployment.

With all of the wakeup types, it is important to include a shutdown process based on time, inactivity or an understanding of when the application has finished communicating so that there is an orderly disconnect from the carrier's network.

CONCLUSIONS

The communications environment for the M2M/IoT industry has changed and is continuing to change rapidly. With the introduction of the Internet into the equation, the security environment has become very treacherous. Considering all of the very interesting things that are already being connected, let alone all the things that have yet to be imagined, the number of very intelligent and determined people that will attempt to gain un-authorized access to absolutely everything, for both malicious and benign reason, will multiply rapidly. As stated earlier, getting off the Internet is effective for mitigating numerous security threats, but it may not be possible for some deployments, especially for consumer products. This report is only an introduction to the issues and mitigation practices to be considered.

A lot of M2M applications have, historically, been designed for unmetered or wired lines. Some current designs are based on the assumption that data will continue to be cheaper. The reality is that for the number of cellular data devices that are projected in the next few years to work with the available bandwidth and network resources, both devices and applications are going to have to make more efficient use of cellular networks.

M2M/IoT service providers, like Telit, can help.

BIOGRAPHY
LAWRENCE MILLER

Lawrence Miller is the Principal Network Architect at Telit Wireless Solution in Lincolnshire Illinois. He is currently responsible for the design of the Telit M2M IP Core infrastructure in North America. He has been working in network engineering and design for over 30 years with technology companies including Bausch & Lomb, General Electric, Siemens, Loral Aerospace, Lockheed-Martin, Ardis (Motorola) and CrossBridge Solutions, Inc.

www.telit.com

Telit reserves all rights to this document and the information contained herein. Products, names, logos and designs described herein may in whole or in part be subject to intellectual property rights. The information contained herein is provided "as is". No warranty of any kind, either express or implied, is made in relation to the accuracy, reliability, fitness for a particular purpose or content of this document. This document may be revised by Telit at any time. For most recent documents, please visit www.telit.com | Copyright © 2015, Telit

[07.2015]