Global Knowledge®

Expert Reference Series of White Papers

Security and the Rise of Machine-to-Machine (M2M) Communications

Security and the Rise of Machine-to-Machine (M2M) Communications

Kerry Doyle, MA, ZDNet/CNet.com Associate Editor

Introduction

It's generally accepted that the machine-to-machine (M2M) communications sector is quickly moving from a period of market development towards commercial deployment. As a result, the need exists to offer secure connectivity and to assure customers on this point. That's because security issues are increasingly coming to the forefront as M2M solutions grow in complexity and are deployed throughout business-critical areas.

In fact, the possibility exists that the number of M2M connections in data centers across most industries has far outstripped the ability of those organizations to secure them. Such a misalignment between security and compliance can expose companies to undue risk because they face security threats that could severely compromise operations.

The automated, machine-connected world represents the next step in business technology's evolution. But despite the gains that M2M seems capable of achieving, are early adopters giving security the amount of attention it requires?

In this white paper, we explore the unforeseen risks prompted by M2M expansion and the Internet of Everything (IoE). We also assess possible barriers to secure functioning of M2M across a variety of sectors. Finally, we examine the problems posed by unchecked security threats as well as possible solutions that exist to mitigate those risks.

Internet of Everything (IoE) Security and M2M Connectivity

While there's been significant growth, we're still in the early stages of M2M productivity. The current M2M market consists largely of corporate/business deployments. However, the consumer segment is increasingly coming into focus as an area ripe for expansion.

Implementing M2M security is complicated because it's closely related to how processor-embedded hardware is designed and manufactured. The mass commodity manufacturing of sensor devices has little standardization and minimal regulatory requirements. This situation cuts across all industry verticals and geographies.

Cloud-based security is also at issue. That's because the IoE, which relies on wireless connectivity and, to some degree, cloud services, is an integral part of M2M functionality. At the moment, countless M2M-based transactions automate critical business and operational processes across a number of industries.

Data theft, network breaches, malicious mischief, and regulatory compliance are just some of the security issues that must be confronted. In the meantime, the integration of intelligent device (sensor) networking and M2M communication capabilities is creating what some have termed a "digital nervous system" that's ever-evolving and responsive.

In our hyperconnected, knowledge-intensive economy, digital technologies are improving production, distribution, and operations for all manner of physical goods, from high-tech equipment to basic machinery. The result is improved productivity/quality, increased workforce collaboration, and new levels of customer interaction and influence.

As we consider the security ramifications, it's important first to define and differentiate the two platforms. The Internet of Things (IoT) consists of the exchange of data between autonomous endpoints. Each uniquely identifiable device relies on IP connectivity and can transmit processing on a local or international scale. While not requiring human intervention, the IoT does provide management capabilities for monitoring and analysis.

The IoE, on the other hand, is more inclusive and entails a broader spectrum of devices. It also encompasses the networks that must support all the data that these sensor devices generate and transmit, requiring software and hardware to work in concert.

The IoE mines the intrinsic value derived from all these linkages and monetizes the increased connectivity and improved productivity. With so many more intelligent devices on the network edge, new security considerations and implementations need to be evaluated.

M2M and Business/Consumer Environments: Key Attributes

The growth and evolution of M2M and the IoE is increasingly based on applications and their ability to stitch together complex interactions and processes. In the past, M2M consisted primarily of low volume, low Average Revenue Per User (ARPU) sensor networks. Currently, increased mobile traffic, more devices and higher bandwidth applications are generating higher ARPU.

Another reason for growth is due to next-generation (4G) technology which provides exceptionally fast connection speeds. A range of M2M technology, such as automotive sensors, inter-device communication, navigation, and video (to name a few)—are all improved via the massive throughputs and low-latency periods provided by 4G LTE.

According to GMSA, the international mobility organization, global-wide M2M connections reached 195 million in 2013, growing at almost 40% per year between 2010 and 2013. Furthermore, M2M connections now account for 2.8% of all global mobile connections, double the 1.4% share recorded in 2010.

These figures are significant because consumer electronics, a projected key growth driver along with mobile devices, are increasingly reliant on fast connectivity. Investments by major carriers and providers in 4G LTE are targeted to capitalize on this growing segment. The potential for this new technology also extends to other vertical industries, including manufacturing, energy, and healthcare.

But as these capabilities continue to mature, standardization remains a crucial enabler for future M2M growth and wider IoE adoption. Without true "plug-and-play" capabilities, manufacturers risk unnecessarily complicating adoptions.

Standardization also needs to be applied across all aspects of the value chain, from manufacturers and hardware integrators to application developers. Overall uniformity reduces the cost of deployments and eliminates integration issues. Interoperability between devices and the ability to understand the "language" of others via standardization will only increase the number of M2M technologies that can be implemented. As a result, global M2M operator alliances will become increasingly important.

For example, automotive industries around the globe represent a key sector for M2M expansion. The multimedia experience enabled within cars extends to traffic information, navigation alerts, insurance telematics (how customers drive), and more.

In addition, the efficient roaming abilities provided by increased 4G coverage enable regional telecom operators to form the cross-border partnerships that provide coverage. For example, during auto breakdowns or in emergency situations, location and other data can automatically be transmitted and the closest authorities alerted.

Another area of potential growth is "Smart Cities," consisting of a collection of vertical services. Municipalities that invest in technology reflect efforts to improve the lives of citizens. For example, they can include thousands of strategically placed sensors that transmit data improving city processes and provide savings on a range of services.

While it seems inevitable that Smart Cities will eventually become a reality, adequate funding poses one barrier. The recent global economic downturn and austerity measures, especially in Europe, have slowed the trend. The questions relate to whether Smart City initiatives should be financed by central or local governments. In the meantime, related technologies such as big data analytics have been proposed as one way to identify other possible funding sources.

The term "Connected Life" represents a world where consumers and businesses use many different devices to interact via the IoE. A focal point of that contact is the home, enabled by sensors within the environment and wireless connectivity. For example, Google has made recent moves that should attract attention.

The company not only sold the hardware manufacturer Motorola to Lenovo, it recently acquired Nest, Inc., a company forging the way with wireless, sensor-based intelligence. Google is one among many major companies establishing the home-based concept of behaviorally smart, networked sensors uniting the physical and virtual worlds.

Finally, health-related telemetrics relayed via wearable technology represent only the beginning of future widespread deployment of M2M across the healthcare industry. Ultimately, the health vertical represents a valuable prospect for long-term growth. In the interim, regulations and entrenched healthcare industry practices could pose a challenge for establishing connections between eHealth and M2M. In addition, questions related to the security of personal information have also delayed adoptions.

The possibilities related to the growth of M2M—and the barriers—are typical of any radical, new technology. It's important to keep this in mind as we consider potential security weaknesses.

M2M Security Deficiencies and Solutions

As mentioned previously, security issues affecting M2M viability range from design and manufacturing concerns to cloud-based vulnerabilities and risks, including cyber-attacks. Recently, chipsets found in home routers, set-top boxes, and security cameras were infected by an Internet worm. Open source Linux distributions are commonly used in processors. The "Linux.Darlloz" virus, along with its variants, was known to have targeted a variety of sensor-based devices.

As the IoE becomes increasingly home-based, M2M-enabled devices, from toasters and fridges to home security, increase the number of attack vectors and opportunities for hackers.

Rapid adoption of network-connected devices that provide minimal security can be easily identified by cyber-criminals and other unlawful operators. Extrapolating such weaknesses to other M2M-enabled verticals, such as healthcare systems or the automobile industry, means that such security lapses could have severe implications.

Another widespread Internet-based infection with possible serious consequences for M2M functionality is the recent Heartbleed bug. A critical OpenSSL flaw such as this could easily expose a range of confidential data, jeopardizing M2M communications in any sector.

As a result, the need exists for increasing the numbers of available specialists. In general, M2M and the related automation it enables, is ineffective in terms of OpEx and ROI if an organization must train staff for every device that's connected. That's why increasingly sophisticated skill sets are necessary to maintain M2M systems and to ensure smooth functionality.

These new types of specialists include big data analysts, networking engineers familiar with emerging modalities such as Software-Defined Networking (SDN), and security professionals trained in diverse safety procedures.

In general, providing these capabilities also has implications for the design and production of M2M embedded devices. It's important not only to ensure that the technology is simple to use with easy public access in mind. It also requires uniformity in terms of design and manufacturing.

Traditionally, the focus of IT has been internal corporate processes. Over time, as the Web's dominance grew, IT became more concerned with devising ways to safely enable external connections. In the case of M2M, the reverse is true and open access is critical to effective adoptions.

However, that means security needs to be implemented at the design stage and not considered secondary. For example, the "Embedded SIM" specification enables "over-the-air" provisioning and management of SIMs in M2M devices.

Currently in the manufacturing process, SIM cards are inserted into the sensor device and hermetically sealed. In the traditional telephony market, the mobile operator bulk purchases devices and inserts its credentials on to the SIM. However, with M2M devices it's often a question as to where the pre-embedded SIM will be sold and operated.

The problems and risks associated with having thousands of disparate versions of device, firmware, and operating systems is almost too big to contemplate. Without standardization in place, different M2M manufacturers end up taking proprietary approaches to building M2M devices, which adds to the complexity.

In contrast, much of the software industry has arrived to the point where security is baked in to the development process at an early stage. Similarly, M2M device manufacturers need to be designing the controls within the hardware as well as within the software.

In terms of M2M encryption, Secure Shell (SSH) provides confidentiality and integrity of data as it flows through Internet connections. It is used by organizations, from financial institutions to cloud providers. While SSH is employed by companies to secure M2M processes, SSH key management in general is lacking.

Without adequate management of SSH keys in the network, theft and subsequent data breaches become all too real. Another means of security for M2M is the use of authorizations and enhanced "identity use."

Every M2M transaction is the result of one machine logging into another using an authorized identity and the exchange of data. To achieve effective security, companies must ensure that compliance and security initiatives fully account for onboarding, offboarding, and monitoring of machine-based identities and credentials.

Conclusion

Recent research by IDC has projected that close to 200 billion Internet-connected devices will be operational by 2020. Generally, it seems M2M and the IoE are set to gain wider adoption despite security concerns and data integrity issues.

Companies that rely on diverse smart systems use mobility, innovative networking (SDN, NaaS, etc.), advanced wireless (4G LTE), M2M, and the Internet of Everything (IoE) to facilitate these interactions. With this new approach, unprecedented levels of data are now accessible to a broad constituency of the workforce as well as to companies and their customers.

According to a recent McKinsey Global Initiative (MGI) report, we've entered a perfect storm in terms of digital trends. That is, a number of major IT developments are converging, interacting, and amplifying each other. These include mobile devices, cloud computing, social media, big data, analytics, and IoE.

Today, even SMBs or individual entrepreneurs can have a global reach and influence, expanding well beyond a capacity that was considered unreachable a few short years ago. Increased interconnectivity via M2M, the IoE, and smart systems holds profound implications for how business in the 21st century will continue to evolve.

In terms of M2M growth, key developments in security will be essential, from the design and manufacture of devices to more robust cloud security and ensuring the integrity of wireless data transmissions. Without these safeguards in place, organizations and industries that rely on M2M will continue to place themselves at risk.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge through training.

- Cybersecurity Foundations
- Introduction to Global Communications
- SDN Essentials: The Future of Networking

Visit **www.globalknowledge.com** or call **1-800-COURSES (1-800-268-7737)** to speak with a Global Knowledge training advisor.

About the Author

Kerry Doyle (MA, MSr, CPL) writes for a diverse group of companies based in technology, business, and higher education. As an educator and former editor at PC/Computing, reporter for PCWeek magazine, and associate editor at www.ZDNet.com, he has written extensively on high-tech issues for over 15 years. He specializes in computing trends vital to SMBs and enterprises alike—from virtualization and cloud computing to disaster recovery and network storage.