Brought to you by:

pelion
an arm company

IoT Connectivity Security

for dummies®
A Wiley Brand

Secure device identity

Safeguard data in transit

Work with secure partners

Pelion Special Edition

Lawrence C. Miller

About Pelion

Pelion was originally founded as an incubation unit within Arm, the world's leading designer of key technologies at the heart of computing. Now a wholly owned subsidiary of Arm, Pelion is forging its own path in the IoT revolution, building on a solid foundation of device expertise. Pelion wants to break down barriers to IoT adoption for anyone looking to revolutionize their industry. With Pelion simplifying the development, deployment, and management of IoT solutions, innovators can focus on what they do best and leave the technological details in safe hands.

Pelion's Connected Device Services offer a flexible, secure, and efficient foundation spanning connectivity, device, and data management. It accelerates the time to value of IoT deployments by helping partners easily connect trusted IoT devices on global networks, invisibly administer them, and extract real-time data from them to drive competitive advantage.

Find out more at **pelion.com.**

IoT Connectivity Security

Pelion Special Edition

by Lawrence C. Miller

for dummies®
A Wiley Brand

IoT Connectivity Security For Dummies®, Pelion Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-119-60687-1 (pbk); ISBN 978-1-119-60690-1 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

We're proud of this book and of the people who worked on it. Some of the people who helped bring this book to market include the following:

Project Manager: Martin V. Minner

Senior Managing Editor: Rev Mengle

Acquisitions Editor: Ashley Coffey

Business Development Representative: Karen Hattan

Production Editor: Mohammed Zafar Ali

Introduction

Any time a device is connected to the Internet, it's at risk of being breached. Today, billions of devices are being connected to the Internet. As a result, the attack surface has grown, making it exponentially larger, more complex, and more challenging to secure. But like any other breach today, a successful Internet of Things (IoT) breach requires network connectivity. Thus, the key to securing IoT devices is to secure IoT connectivity.

About This Book

IoT Connectivity Security For Dummies consists of six chapters that explore IoT connectivity vulnerabilities (Chapter 1), device integrity (Chapter 2), how to protect data in transit (Chapter 3), IoT security management (Chapter 4), the secure connectivity ecosystem (Chapter 5), and keys to securing IoT connectivity (Chapter 6).

This book focuses on cellular IoT security rather than Wi-Fi and other protocols that are commonly used for IoT connectivity.

Foolish Assumptions

In this book, I assume you work for an enterprise that is considering an IoT deployment and that you have at least a basic understanding of IoT and some of the potential challenges to security, but that you'd like to learn more about IoT connectivity security.

Icons Used in This Book

Throughout this book, I occasionally use icons to call out important information. Here's what to expect.

This icon points out information you should commit to your nonvolatile memory, your gray matter, or your noggin.

If you seek to attain the seventh level of NERD-vana, perk up! This icon explains the jargon beneath the jargon.

Beyond the Book

If you find yourself at the end of this book thinking, "Gosh, this was an amazing book — where can I learn more?" just go to `https://pelion.com/product/connected-device-platform/`.

IN THIS CHAPTER

- Identifying physical security threats
- Keeping IoT software secure
- Securing the end-to-end connection lifecycle

Chapter 1

Recognizing IoT Connectivity Vulnerabilities

In this chapter, you explore Internet of Things (IoT) connectivity vulnerabilities associated with communication, physical security, the connection lifecycle, and the software components of IoT devices, and why it's important to identify vulnerabilities early in your IoT project to avoid deployment delays due to potential security issues.

Communication

Cellular networks including 3G, 4G, and 5G are ubiquitous for long-range mobile communications and are thus ideally suited for IoT device communications.

Cellular networks provide distinct security advantages over other IoT network options, such as Wi-Fi. However, because IoT devices typically transmit data beyond the network to the Internet, security cannot be assumed. Vulnerable cellular network components include:

- **Signaling System No. 7 (SS7) nodes:** Developed as a set of telephony protocols in 1975, SS7 now provides connection for roaming between cellular networks. Although newer technologies are being adopted, many roaming and older networks still rely on SS7. Vulnerabilities enable routing paths to be manipulated, transmissions to be intercepted, and locations to be tracked in real time.
- **Baseband processors:** The CPU, memory, network interface and media processor in mobile and IoT devices are referred to as the *baseband processor.* Vulnerabilities in the hardware, firmware, and software of these devices can be exploited.

Securing SS7 nodes and base station vulnerabilities is the purview of telcos and mobile network operators (MNOs). IoT device manufacturers developing and deploying IoT solutions should instead focus on securing connectivity in their IoT devices.

Physical

Attackers often use physical properties of the system-on-chip (SoC), such as timing or voltage, to extract information or induce bad behavior. If the base layer of silicon fails, allowing data to leak out or to be easily accessed, the entire system security becomes at risk.

An intruder may attempt to tamper with an IoT device to take control of the device, alter its functionality or behavior, steal data collected by the device, or use the device to pivot to other networks. The intruder often attempts to tamper with the device's communications components, such as the subscriber identity module (SIM).

Hardware hacks are much harder to perpetrate than software hacks. Moreover, a software attack can directly reach thousands of IoT devices, whereas a hardware attack is generally more limited.

Software

Even the most robust security schemes and cryptographic architectures are susceptible to physical attacks, and this type of attack is gaining traction as new automated tools make it easier to perform. The risk with a physical attack is the scalability factor: Extracting information from one device, such as keys or source code, allows an attacker to conduct a large-scale software attack.

As with computer software, vulnerabilities are inevitably discovered in IoT device software and must be patched and updated in a reliable, timely, and effective manner. A challenge with IoT devices is that they cannot be easily upgraded to mitigate issues. Although there have been spectacular breaches against IoT devices, such as Mirai, Chalubo, Torii, and Demonbot, many other software vulnerabilities are susceptible to traditional breaches, such as buffer overflows that exploit memory flaws.

Though the computing industry must respond to new vulnerabilities, software must also address traditional issues such as default user identifiers and passwords.

Connection Lifecycle

Security of IoT devices is too often an afterthought. Vulnerabilities must be addressed throughout the device lifecycle. This includes secure deployment, ongoing or continuous monitoring, over-the-air (OTA) updates, remote management, deprovisioning, and human access to the connectivity management platform.

To achieve end-to-end security throughout the connection lifecycle, security must be a primary design consideration in IoT devices — as fundamental as any other parameter. There should be a strong focus on tight mechanisms for device authentication and integrity, as well as minimizing the potential attack surface.

IN THIS CHAPTER

- Authenticating devices and connections
- Establishing the "new perimeter"
- Providing authentication and authorization services

Chapter 2
Securing Device Identity

In this chapter, you learn about the importance of secure identity management for the devices in your Internet of Things (IoT) deployment.

Ensuring Device and SIM Authenticity

Ensuring the authenticity of devices connected to your IoT platform and the subscriber identity modules (SIMs)

in those devices is crucial to maintaining the confidentiality, integrity, and availability of your IoT ecosystem.

Digital certificates, unique device credentials, and virtual private network (VPN) connections can help the enterprise verify the authenticity of IoT devices to the centralized management point.

Embedded SIMs (eSIMs), discussed in Chapter 4, can help to significantly reduce the risk of removal or replacement of the SIM card in a device, helping to further ensure the authenticity of devices connecting to your platform. An eSIM, which is directly soldered within the device, is much harder for an attacker to locate, remove, or replace, than removable form factors, thereby improving IoT security with a hardware-integrated solution.

Verifying Identity

With the proliferation of cloud computing and mobile computing, traditional network perimeters have become largely indistinct. Identity has become the foundation for controlling how and if a device connects to the network, and which services can be accessed by a subscriber. Verifying an IoT device is crucial to the security of the ecosystem within which it operates as well as the authenticity of the data it is gathering and passing back across the ecosystem.

A device can be verified with its International Mobile Equipment Identity (IMEI), which uniquely identifies the device and is essentially a make, model, and serial number for the device. The IoT SIM Applet For Secure End-to-End Communication (SAFE) is a recommendation of the Global System for Mobile Communications (GSMA) to leverage the advanced security and cryptographic features in a SIM to function as the hardware Root of Trust in an IoT device. Although IoT SAFE does not identify the device, it allows you to verify the trustworthiness of the device.

Enabling more secure network access pairing requires a combination of subscription identification coupled with hardware identification. An entity on the network, known as an Equipment Identity Register (EIR), matches the IMEI of a device with the International Mobile Subscriber Identity (IMSI). The EIR is typically a component of the cellular network and is closely integrated into the Operations Support System (OSS) and Business Support System (BSS) that has close insight into both device and subscriber IDs, as well as integration with a central blacklisting service. However, use of this capability has to be carefully approached because blocking or flagging subscriber access as suspicious, in cases where the IMEI doesn't marry up with the subscriber ID, can have ramifications.

Authenticating and Authorizing Access

The Third Generation Partnership Project (3GPP), that is, the world umbrella standardization body for cellular connectivity, includes a complete mechanism by which session keys are derived from the network authentication process. This process protects radio communications from the device to the first network equipment that it connects to — the Evolved Node B (eNodeB) on a 4G network or Next Generation Node B (gNodeB) on a 5G network.

Centrally managing the ongoing authentication and authorization of devices at scale can be a major challenge in enterprise IoT deployments. A secure connectivity management platform (CMP), discussed in Chapter 4, can provide authentication and authorization services, including generating and validating access credentials; issuing, validating, and revoking security certificates; exchanging security keys; and establishing a secure virtual private network (VPN) from enterprise environments to IoT connections.

IN THIS CHAPTER

- Securing end-to-end IoT communications
- Protecting the confidentiality and integrity of data in transit
- Ensuring a robust, highly available connectivity management platform

Chapter 3

Protecting Data in Transit

In this chapter, you learn about secure connectivity requirements, how to protect the confidentiality and integrity of data in transit, and what to look for in a connectivity management platform to ensure a highly available Internet of Things (IoT) solution.

Ensuring Secure End-to-End Connectivity

The IoT introduces new challenges associated with secure end-to-end connectivity. For example, IoT devices connected to each other can be different from one another in terms of characteristics and communication technologies, making it harder to establish secure sessions and secure communications. IoT devices often connect to their reciprocal management server or ecosystem over cellular networks including 3G, 4G, and 5G, and other newer emerging technologies such as Low-Power Wireless Area (LWPA) Networks.

As with most IoT technologies used, cellular technologies also have vulnerabilities and new vulnerabilities will inevitably be discovered across the full range of IoT connectivity options. Network operators implement security in their cellular networks in the following ways:

- Including fraud detection as a component of the mobile network to track and trace unwanted behaviors and miscreant activity, thereby adding to their overall security
- Uniquely identifying endpoint devices on the network using an international mobile equipment identity (IMEI)

- Using network and country codes to identify different networks
- Encrypting network traffic, providing private networks (including virtual private networks), and creating dedicated networks
- Ensuring high availability by using licensed spectrum, implementing standard network technologies, and building resilient network topologies

Enterprises (as deployers or consumers of the IoT ecosystem and data), device manufacturers, and network operators must ensure that secure end-to-end connectivity is a fundamental part of their IoT designs. This includes ensuring only authenticated and authorized devices can connect to the IoT platform and that the platform, in turn, can only communicate with properly authenticated and authorized endpoints. This is particularly important because IoT devices may connect to multiple public and private clouds, as well as edge clouds and different provider networks in the IoT ecosystem.

End-to-end communications can be secured via a VPN with robust key management capabilities and/or by separating IoT traffic from the public Internet over a dedicated network. Whether communicating over a VPN or dedicated network, Transport Layer Security (TLS)/Datagram TLS (DTLS) should be used to secure end-to-end traffic. Enterprises and device manufacturers must also

ensure that their devices can be supported from a remote management platform with robust capabilities. For example, reliably installing security patches and protocol updates over the air for devices already deployed in the field.

To establish a data connection with a network operator, a mobile device must be configured with an access point name (APN). The APN maps to a specific configuration set that can include functions that can ensure a secure entry point between the cellular network and another network, such as a private corporate network. For general users, the APN is usually configured to be open to general Internet access, but it still protects a device from unsolicited requests from the Internet towards a device. The network operator may use the APN to determine the type of data connection that should be created. For example, the APN may be used to define what security methods to use for the connection.


REMEMBER

Some network providers can create "private APNs" that allow authentication to be controlled on a per-SIM level and updated dynamically.

Encrypting Data in Transit

Data transmitted and received by IoT devices must be encrypted to protect its confidentiality and integrity. Although certain IoT applications may not generate or

process particularly sensitive data, intruders may be able to glean information from the aggregation of this data that helps perpetrate a breach against a target. For example, a power meter may provide an intruder with enough data to determine if someone is at home or not, or when they are likely to be home, based on their power consumption patterns.

Additionally, ensuring the encryption of data in transit assures its integrity and validity upon arrival. This can be data gathered by the device (for example, environmental data or electrical power usage) or software updates and security patches destined for the device, ensuring malicious code is not installed and the device is not compromised.

Data in transit should be encrypted using the most current version of the Transport Layer Security (TLS) protocol.

Transport Layer Security (TLS) is commonly, though incorrectly, referred to as Secure Sockets Layer (SSL) encryption. All versions of SSL have now been deprecated and replaced by TLS.

Data in transit should also be encrypted from end to end — from the device, across the communications service provider (CSP) networks, to the data center and system where the data is ultimately hosted for use.

The 3rd Generation Partnership Project (3GPP) standards define the mechanisms for authentication and confidentiality between the device and the base station, as well as the interfaces from the base station back to the network operators' infrastructure core and the Internet gateways. Authentication occurs with credentials held in the Home Subscriber Server (HSS)/Home Location Register (HLR), which sits in the heart of the core network. Numerous security methods and controls are used to ensure the entirety of the mobile network infrastructure is a private network and protected against external attacks. In comparison, a web browser session may be encrypted using Transport Layer Security (TLS), whereas an IoT device doesn't have any end-to-end session encryption unless it is set up explicitly.

REMEMBER

In addition to the 3GPP security standards and the network operators' security deployments, ensuring that data is encrypted end-to-end provides additional security and protects against any momentary degradation or breaches in security at any point.

IoT Subscriber Identity Module (SIM) Applet for Secure End-to-End Communication (SAFE) is a Global System for Mobile Communications Association (GSMA) recommendation that leverages the SIM to protect the device's credentials, just like the network credentials themselves. IoT SAFE advocates using the SIM as the hardware Root of Trust in an IoT device to establish "end-to-end,

chip-to-chip security." It uses the SIM as a mini "crypto-safe" to establish a Datagram TLS (DTLS) session with an application server or cloud and mutually authenticate the device and server/cloud.

Providing Resilience

Your IoT connectivity management platform also needs to provide resilience to maximize uptime and ensure that critical devices can reliably and securely reach and interact with your IoT ecosystem. In the event of a failure, you need to maintain the security of your critical applications and devices until they can be returned to their normal operating state. When considering different connectivity management platforms and partners, look for the following features and capabilities:

- Redundant, geographically dispersed Tier 3 (or Tier 4) data centers with 99.982 percent uptime (no more than 1.6 hours of downtime per year) and N+1 fault tolerance providing at least 72-hour power outage protection
- Multiple partner networks with different transit providers and Internet providers providing failover capabilities between diverse links with sufficient capacity to handle full traffic loads individually

- Redundant, load balanced Packet Data Network Gateways (PGWs) capable of handling full traffic loads
- IPSec VPN routing and hot failover for maximum reliability and seamless failover of services between sites
- Successful completion of an International Organization for Standardization (ISO) and International Electrotechnical Commission (ISO/IEC) 27001 security standards audit

IN THIS CHAPTER

- Managing secure IoT connectivity at scale
- Exploring remote provisioning capabilities
- Enabling proactive monitoring and alerting

Chapter 4

Managing IoT Connectivity Security

In this chapter, you learn about connectivity management platforms and how they help enterprises securely manage their IoT deployments.

Connectivity Management Platform (CMP)

Making a reliable, secure connection available is critical to IoT deployments, which are complex environments with potentially hundreds of thousands of connected devices. An IoT connectivity management platform enables secure remote connectivity for IoT deployments at scale.

Without a connectivity management platform (CMP), large IoT deployments cannot be efficiently managed, for example, in the event of a breach that requires visibility and control to identify, contain, mitigate, and recover the affected IoT devices. Other important reasons to manage your IoT deployments with a CMP include:

- Managing devices across networks and providers at scale is challenging; having a consistent interface and integration allows easier device updates.
- No insight into connectivity status means you do not know if your critical assets have gone offline and whether it's due to a malfunction, a breach, or some other issue.
- Lack of statistical data and analytics means you don't know if your asset has overconsumed data and you can't efficiently identify issues with connections that aren't functioning correctly.

The ideal CMP is an interface that should provide enterprises with the ability to:

- **Manage the lifecycle of a connection:** Activate, deactivate, bar, or unbar a subscriber.
- **Monitor subscriber activity and performance, preferably in an automated fashion:** How much data has been used on a device or account?
- **Manage inventory:** Order new subscriber identity modules (SIMs) and embedded SIM (eSIM) profiles, or manage existing stock.
- **Manage billing:** How much does each connection cost? What was my bill this month? How much did my overage cost?
- **Allow easy access to devices over a single network interface:** Allow updates for devices regardless of mobile network.

Provisioning and Deprovisioning

Remote eSIM provisioning provides the ability to download, enable, disable, and delete network operator profiles for devices over the air.

REMEMBER

An eSIM is embedded (that is, directly soldered) within the device at the point of manufacture.

Remote eSIM provisioning opens the door to a range of use cases that cannot be supported by conventional SIMs. For example, it allows a device manufacturer to insert or embed an eSIM at the point of assembly. When the device is turned on, provided the correct configuration is in place, it can connect to a local cellular network, making the device ready to use immediately regardless of where it has been deployed. Instead of holding SIM cards for multiple network operators across the globe and coordinating which card should be inserted into which device, every device can use the same type of physical eSIM and have the correct profile applied in the field. If the network operator profile on a deployed device needs to be changed, it can be downloaded to an available memory slot on the eSIM and enabled over the air. This capability is a significant enhancement, especially when compared to conventional SIM cards, which require a SIM to be physically swapped for a network change.

In short, remote eSIM provisioning allows manufacturers to drastically simplify their supply chain and reduce the high cost of inventory, while providing customers with devices that can be connected out of the box. It also provides the capability to manage connectivity by downloading and enabling the SIM profile for a new operator's subscription for an IoT device deployed in an inaccessible location. The CMP must have an awareness of this type of

SIM and SIM profile deployment mechanism as well as integration with the relevant remote SIM provisioning platforms.

Managing Human Access

Human access to physical IoT devices introduces the risk of tampering. Often, such tampering involves replacing or removing the SIM card to take control of the device, steal data, or otherwise compromise functionality.

Technologies such as eSIMs help to reduce the risk of tampering because the SIM is embedded during the manufacturing process into a sealed enclosure. It is extremely difficult to tamper with or remove an eSIM without causing significant damage to the device.

Access to the connectivity management platform must also be controlled, including the permissions assigned to authorized users for specific systems. The CMP provides visibility and control of the entire IoT device estate, so controlling access to this functionality is crucial.

Monitoring and Alerting

A connectivity management platform also enables real-time monitoring of devices deployed at scale, which helps enterprises proactively troubleshoot device issues. Alerting capabilities ensure that corrective action can be taken

immediately when a device goes offline or otherwise experiences issues.

Monitoring and alerting provide visibility across your network environment so that you know when your subscribers or devices are behaving in unexpected, unauthorized, or potentially malicious ways.

Beyond monitoring and alerting, remote troubleshooting capabilities provide functionality that includes refreshing SIMs and disconnecting or reconnecting devices on the network. In this way, you can triage the scale and cause of suspicious device activity without having to send out a field engineer or deactivate a device when a power failure or network outage causes a temporary issue. This enables a more rapid response that you need to send out a field engineer by ensuring that basic troubleshooting has been completed, and the right engineer with the right tools and resources is deployed. In locations where an engineer can't physically access the device, a connectivity management platform ensures you can remove the defective or altered device from the network.

Automation rules can potentially be used to address issues before they affect the business. For example, a subscriber who has not connected to the network for 15 minutes may have a device that has been tampered with. A connectivity management platform with automation functionality can send alerts or remotely block the SIM from reconnecting to prevent an intruder from running up usage charges or otherwise using the device for unauthorized purposes.

IN THIS CHAPTER

- Identifying technical and business requirements
- Ensuring your partners can work together
- Addressing ongoing management issues

Chapter 5

Working with Secure Connectivity Partners

The Internet of Things (IoT) has lots of moving parts such as software and hardware updates, evolving accreditation and certification requirements, and new technologies and features being added and implemented. You need a strong partner ecosystem to help bring your IoT solutions to market. In this chapter, you explore some of the considerations that will allow

you to identify partners that can help you successfully deploy IoT solutions today and in the future.

Defining Partner Requirements

As you identify potential partners, ensure you are drilling into your actual needs rather than just discussing technology. Make sure you've discussed specific requirements for your IoT solutions that will potentially affect your success and ongoing costs, such as:

- What are your expected data consumption needs?
- Where will your devices be located?
- What specific power consumption needs do you have and what is the impact of connectivity management?
- Do you need permanent or on-demand data? Permanent connections require greater resilience in order to ensure continuity of operations.

Also, consider the strength of the various partners with whom you are talking. For example:

- Do they have expertise in your specific field or industry?
- Do they have a proven track record of innovation and success?

Enabling Integration and Interoperability

Your partners must be part of a strong ecosystem to deliver an end-to-end solution that meets all your needs. Your secure connectivity partner needs to enable integration and interoperability. Look for the following:

- A low barrier to entry and a feature-rich toolset that allows you to quickly deploy connected solution sets
- A high-speed network with large geographic reach to connect to mobile operators both internationally and domestically to support different use cases. Some NarrowBand IoT (NB-IoT) devices, for example, will only require minimal quantities of data to be exchanged.
- Trusted networks operating on licensed spectrums and compliant with Third Generation Partnership Project (3GPP) standards
- N+1 service resilience with network interconnects from different transit providers, Internet access from different service providers, and power from different power suppliers/grids, where possible
- Secure virtual private network (VPN) connectivity and tunneling provided over open protocols such as Internet Protocol Security (IPSec)

- Integration with public cloud providers such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP)

Considering Ongoing Management Issues

Look for a secure connectivity partner that will help you address ongoing management issues. This includes simplifying management of your device deployments at scale across multiple partners. Consider the following:

- What assurances have you been given to ensure devices will remain secure once they are deployed?
- Can your partner consolidate mobile network operator (MNO) contracts and bills into a single relationship?
- Can your partner demonstrate how the performance of multiple deployed devices is streamlined into one manageable view?
- What tools does your partner provide to help ensure complete visibility of your deployments and what monitoring, auditing, and compliance verification capabilities are available?

IN THIS CHAPTER

- Identifying vulnerabilities and controlling access
- Making devices secure by design
- Enabling security intelligence and ensuring compliance

Chapter 6

Seven Keys to Secure Connectivity

Here are seven keys to ensuring secure Internet of Things (IoT) connectivity:

- **Map your attack surface and derive a threat model.** Consider how vulnerabilities can be exploited across a range of attack surfaces and methods throughout the life cycle. Identify vulnerabilities and ask how your connectivity partner can help.

  As an Arm company, Pelion encourages innovators to look into Arm's Platform Security Architecture

(PSA) certification. It defines ten security goals to provide standardization over how secure IoT devices are designed. The four-stage process starts with the "analyze" phase where the developer analyzes threats and assets in the IoT application and identifies key security objectives to be implemented in the device, hardware, and software.

- **Control access to trusted networks.** Make use of established device identity and authentication procedures so that only known devices can connect to trusted networks.
- **Design and build for resiliency.** Have resilient infrastructure so you don't lose connectivity if something goes wrong.
- **Ensure end-to-end security.** Ensure traffic is routed securely and encrypted as it travels from the device across networks to your management platform and cloud.
- **Leverage artificial intelligence (AI).** Use AI to proactively monitor, alert, and implement mitigation measures on the network.
- **Control access to your connectivity management platform.** Create a clear policy detailing who has access and what they can do.
- **Ensure security and privacy compliance.** Is your partner compliant with all the required data protection and handling regulations in all the territories where you plan to operate?

pelion

422% ROI for **IoT Connectivity**

The Total Economic Impact of Pelion Connectivity Management, a commissioned study conducted by Forrester Consulting on behalf of Pelion

Measuring ROI is still a struggle for enterprises looking to prove the value of IoT. In their study examining Pelion Connectivity Management, they found benefits totalling $421,080 USD.

- Reliable and robust cellular connectivity delivered on an international basis
- Resilient network infrastructure that delivers optimum levels of security
- Connectivity management capabilities

FORRESTER

Learn more at
pelion.com/resources/economic-impact-iot-connectivity

Secure your IoT connectivity

Any time a device is connected to the Internet, it's at risk of being breached. Today, hundreds of billions of devices are being connected to the Internet of Things (IoT). As a result, the attack surface has grown exponentially larger, more complex, and more challenging to secure. But like any other breach today, a successful IoT breach requires network connectivity. This book is your guide to securing IoT devices through secure IoT connectivity.

Inside…

- Identify vulnerabilities
- Ensure secure end-to-end connectivity
- Protect confidential data
- Manage IoT security at scale
- Provision devices remotely
- Enable proactive monitoring

pelion
an arm company

Lawrence C. Miller has worked in information technology for more than 25 years. He has written almost 200 For Dummies books.

Go to Dummies.com™
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-119-60687-1
Not For Resale

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.