Achieving End-to-End Security in the Internet of Things
Why it’s time to embrace carrier-grade Cellular IoT
EXECUTIVE SUMMARY

The new realm of possibilities enabled by The Internet of Things (IoT) arrives tempered with security concerns. Introduce millions of IP-enabled objects to the network, and you also expose a proportional number of vulnerabilities.

The media delivers a steady stream of news coverage about hackers taking control of end devices in the IoT network, including cars, refrigerators, baby monitors, and webcams. These incidents typically involve consumer devices that connect over Wi-Fi networks with user-configured password policies. The reality is that IoT security issues extend well beyond the end device.

Many early IoT implementations have yet to incorporate best practices to ensure end-to-end security. Successful IoT strategy requires a network that goes beyond consumer-grade mobile and Wi-Fi. As enterprises embrace IoT for their critical business applications, they must also respond to early lessons in IoT security. The Cellular IoT solution architecture addresses these concerns with a multi-layer strategy for keeping the enterprise secure while adopting the benefits of IoT.

SECURITY: FROM END DEVICE TO CLOUD

A recent report by HP Security Research documented a surprisingly high number of unsecured devices connecting to the Internet of Things (IoT). The report, which surveyed ten popular devices in common IoT niches, showed that as many as 80 percent of those devices lack basic security. And 70 percent use unencrypted network services, giving potential attackers unauthorized access to those devices and their cloud and mobile applications. Add to that the fact that networks connecting devices to the cloud are not sufficiently isolated, and what emerges is a picture of vulnerabilities throughout the connectivity chain.

Meanwhile, enterprises from a wide variety of vertical markets are currently tapping into myriad IoT-enabled opportunities. IoT networks are increasingly converging with enterprise networks, and as they do so, the vulnerabilities of IoT make their way to the enterprise, exposing businesses to a whole new wave of risks.

Diagram: Vectors of Attack in IoT

1 HP Security Research Report | Internet of Things Study, July 2014
Businesses that rely on mission-critical connected device applications can look to Cellular IoT—devices connected over the cellular network—for secure connections. And while total, ironclad security may be impossible to achieve with anything other than infinite funds, enterprises can gain a very high degree of security at a reasonable cost.

The Cellular IoT view of security covers four key layers for protecting an IoT deployment:

1. Device
2. Transport
3. Network
4. Application

This white paper discusses the security advantages of a Cellular IoT solution architecture, from the perspective of each of the four layers.

1. DEVICE SECURITY

According to the HP study, a key area of IoT vulnerability springs from weak passwords on devices with direct end-user access. Intrusions can also enter into the enterprise IoT infrastructure from spoofed or unauthorized endpoints. A simple way to remedy hacked passwords is to apply more stringent password policies in the device application. Proper authentication and authorization of devices connecting into network resources is a critical step in an overall security plan. However, most low-cost, low-powered devices cannot support sophisticated access control measures.

Securing devices with GSM standards

In the Cellular IoT solution architecture, a cellular-connected device equipped with a standard SIM uses hardware ciphering and encrypted key exchanges with trusted network authentication and authorization systems, allowing only authorized devices to connect.

The Global System for Mobile Communications (GSM) network authenticates the identity of the subscriber through the use of a challenge-response mechanism in this way:

- The network sends a random, 128-bit number to the SIM-equipped device.
- The device uses an authentication algorithm to compute a 32-bit signed response, which is based on the encryption of the random number using the individual subscriber authentication key
- Upon receiving the signed response from the subscriber, the GSM network repeats the calculation to verify the identity of the subscriber.

All of these tasks take place within the device and SIM hardware, drastically reducing the likelihood of a device being hijacked or spoofed—thus securing the network connection, too.
Preventing peer-to-peer vulnerabilities
Another advantage of a Cellular IoT implementation is the ability to prevent connected devices from communicating directly with each other. A network of devices increases the potential threat vector in proportion to the total number of networked connections. Preventing device-to-device (also referred to as peer-to-peer) communications reduces the risk of a compromised device interacting directly with another device in the IoT network and jeopardizing overall security. All communications in the Cellular IoT architecture—device-to-device and device-to-cloud—can be regulated from the network, significantly enhancing the overall integrity of the IoT deployment.

2. TRANSPORT SECURITY
Looking beyond the device, the HP report also describes vulnerabilities in data transmissions between a connected device and cloud applications. This situation usually results from weak or, in some cases, nonexistent data encryption, compromising the integrity and privacy of the data being sent. Attacks such as “man-in-the middle” and session hijacking are common methods for breaching the privacy of transmitted data.

End-to-end data encryption is a vital step toward avoiding such breaches. Today, many organizations use SSL and TLS credentials to ensure data integrity and privacy on the Internet. But many IoT devices lack the capability to support such application-level encryption.

Securing the transport network with GSM encryption
Cellular IoT addresses this challenge with an alternative solution: it provides GSM standardized encryption between the mobile network and the end device.

In the Cellular IoT scenario, a ciphering mode request from the GSM network initiates the encrypted communication. The GSM device uses a combination of ciphering keys and encryption algorithms on the SIM itself to securely transmit and receive data. The keys used are never exposed outside of the SIM hardware, and the true identity of the end device is never revealed—two factors that make this solution particularly secure.

3. NETWORK SECURITY
While encryption remains critical for companies to defend data integrity and privacy, keeping would-be intruders out of the enterprise and IoT network demands equal emphasis. To maintain network security, IoT implementations require either dedicated links or secure tunnels. While these methods remain important for connections between the enterprise data center and the GSM operator, they are typically not cost-effective for mobile devices. Dedicated links to mobile devices are expensive and impractical, as are sophisticated VPN clients for low-cost IoT devices.

Creating secure private networks with Cellular IoT
Cellular IoT provides a standardized and cost-effective approach to create private networks between the enterprise and its connected devices. Enterprises can use custom access point names (APNs) as a way to extend the local-area network (LAN) out to the remote device. This approach enables enterprises to allocate their own private IP addresses, and to specify additional levels of authentication and authorization beyond that provided by the GSM network, as described earlier.

What happens when a SIM card is stolen?
Inevitably, theft happens. Fortunately, preventive innovations in the Cellular IoT architecture can thwart intruders from gaining network access via an unauthorized mobile device. Here’s how it works:

The patented Jasper SecureSIM uses either a mobile device’s International Mobile Equipment Identity (IMEI, a unique identifier for cellular capable devices), or an enterprise-defined user ID and password. The first time the device connects to the network, the device’s IMEI or user ID is locked to the SIM.

The action of tampering or removing the SIM card to use it with a different, non-trusted device will raise a flag that can trigger a number of possible defensive actions. For example, the device in question can be barred from gaining network access, thus safeguarding the IoT infrastructure.
In essence, the Cellular IoT solution architecture enables an enterprise to extend its secure private network from the data center, across the mobile operator network, all the way to the individual devices.

4. APPLICATION SECURITY

Devices connect to IoT applications for command and control purposes, as well as for data exchange. Any breach of these applications or cloud infrastructure can lead to catastrophic repercussions across a company’s entire IoT deployment. For that reason, IoT applications and their cloud infrastructure must be engineered for total information security.

The process of ensuring information security is holistic and reaches beyond IT security, i.e., the technical aspects of designing a digital infrastructure. IT security comprises elements such as intrusion detection systems (IDS), firewalls, encryption, and authorization solutions—all of which figure prominently in the enterprise security landscape. However, even the perfect IT security measures can be foiled by a single act of malicious behavior.

Implementing information security for ubiquitous defense

Unlike IT security, information security requires secure practices in both digital and non-digital areas, which might include organization and documentation controls, physical security controls, legal protection, controls related to third-party entities, and human resources management. Adherence to standards such as ISO 27001 can provide a critical part of an overall strategy for ensuring information security in both IT and non-IT realms.

For the IT security framework to adequately protect the IoT application infrastructure, it must deliver proper identity management systems, role-based access, and access-control lists. Remote access must be confined to VPN-based connectivity only, with multifactor authentication. For IT environments that include cloud-based services and infrastructure, IT security needs to provide a robust multitenant design that carefully isolates each enterprise’s IoT transactions and data. Transactions must be protected against common attacks such as SQL injections, and each transaction should require validation. All data transmissions must be encrypted, and any data stored by a cloud-based service provider should comply with SSAE 16 (or the earlier SAS 70) standards.
Finally, applications themselves must support the ability to identify and analyze anomalous or suspicious behavior when it happens. They must be able to flag any irregular patterns in network and data transmission activities among devices or between devices, and the associated cloud applications should be removed from the network to prevent widespread disruptions.

**CONCLUSION**

The Internet of Things is already introducing new, technology-based competitive advantages for companies around the globe. Many of these early movers have adopted Cellular IoT to connect their assets and devices to the IoT cloud. By doing so, they have been able to avoid many of the well-documented security pitfalls.

End-to-end security architecture starts from the device and extends all the way to the cloud. Elements of this architecture are inherent in the Cellular IoT solution and include:

- Strong device-level access and authentication
- Encrypted data transport
- Separation of IoT traffic into private networks
- Comprehensive information security of cloud applications

The Internet of Things represents the next wave of evolution in the networked world, following major paradigm shifts set by the Computing and Internet revolutions. While security will always remain a primary concern, enterprises can look to Cellular IoT as a proven model to prevent their businesses from becoming tomorrow’s hacking headline.

---

**Cellular IoT powered by Jasper**

Jasper is the pioneer in cloud-based platforms for the Internet of Things (IoT) and the defining player in the Service IT category. The Jasper Platform empowers enterprises and mobile operators of all sizes to deploy successful IoT service businesses on a global scale. More than 1500 companies, including many of the world’s top brands, have chosen Jasper to fast-track their connected businesses. Mobile operator groups worldwide, representing 100+ network affiliates, partner with Jasper.

Founded in 2004, Jasper is based in Mountain View, California. For more information, visit www.jasper.com or follow us on Twitter @Jasper__IoT.