Ensuring a secure Internet of Things

Written by: Leonard Cali, Senior Vice President, Global Public Policy, AT&T

Last update: 20 March 2017

© Alamy

The rapid rise of a new generation of connected, intelligent devices–collectively known as the Internet of Things, or IoT–is more than just the latest digital enabler to impact organisations of all sizes. The IoT presents vast opportunities for governments and businesses to improve internal efficiencies, serve their customers or constituents better, and enter new markets or provide new services. Such services will transform the way we work and live every day. As the IoT develops, it is essential that security-by-design be a core feature of the connected device ecosystem.

You can see promising innovation in the automotive, shipping, industrial, healthcare, home security and smart city sectors, just to name a few. Take, for example, a wristband fitness tracker or health monitor. Such an item can be a purely personal device for tracking one's daily exercise; or it can be used for medical purposes to determine a diabetic's insulin demand. In either case, appropriate security practices are vital. And each member of the ecosystem as well as government has a role to play in ensuring effective security protections

that take a holistic view of the threat management environment. Effective threat management involves many interrelated efforts.

First, the device itself must be secure–especially if the device is used to track sensitive medical information like insulin demand, rather than just the number of steps taken in a day. To ensure device security, it is essential that security issues be considered from the very beginning of device design, and should not be an afterthought or bolt-on solution. Furthermore, this design must permit security to be ensured over its complete lifecycle. Although device security is often achieved using hardware based solutions, it may also be implemented through commercial arrangements that involve co-operation with network operators or applications providers.

Second, the device's operating and applications software must be secure against unauthorised attempts to reprogramme or disable it. Possible solutions include the use of encryption or code signing. And because one may never know all future security threats, it is vital that device and applications providers be able to securely update the software on the device to patch vulnerabilities and security gaps as they evolve. Otherwise, older devices could become unacceptably insecure. Further, since IoT devices are commonly deployed in remote locations, update capabilities such as Firmware-Over-The-Air will be crucial. User data stored on-device needs to be secured, too–perhaps via on-device data encryption so even if the device is breached, the data stored on it remains secure.

Security in networks over which IoT devices communicate is also vital. It does not matter whether these networks are wired, or wireless wi-fi or mobile cellular, customers will demand that they be secure to ensure that data passes reliably between the device and its applications provider. One way this may be achieved is through a secure transmission service such as AT&T NetBond® to link devices to their cloud-based applications servers without exposing their traffic to congestion or online threats like DDoS (Distributed Denial of Service) attacks that exist on the public Internet.

Finally, the computer server managing the device's application must not be a weak link in protecting the integrity of the service. Regardless of whether this server is the application provider's own machine or one located "in the cloud," it must be secured using robust intrusion detection and prevention systems, and firewalls to prevent unauthorised access.

With security being one of the biggest priorities for IoT deployment, effective government partnership with the private sector will be key. This may take several forms. One is that government agencies may convene industry groups to develop cross-sectoral (e.g., device, network, applications) practices and expectations for IoT security. Furthermore, government may assist by providing clear interpretations and advance guidance as to what its general security laws and

regulations require for IoT systems and ensuring these requirements are consistent across all units of government and ecosystem participants.

Finally, governments will themselves be deploying IoT solutions for initiatives such as smart cities, smart transportation or effective health care. Given the pervasiveness of these applications, governments will need to collaborate closely with IoT providers to understand security risks associated with their applications and create a framework for shared knowledge. Working together, government and industry can accelerate innovation in IoT and in IoT security.

The IoT is growing exponentially and the need to secure its ecosystem end-to-end is an absolute necessity. This requires a bottom-up holistic approach to security design and implementation in which each ecosystem participant does its part. Continuing close partnership between the public and private sectors is also important to ensure that IoT security innovation continues and solutions are shared across industry and IoT system users. By following this path, the most valuable years of the Internet will always lie ahead of us.

Visit www.ATT.com