Securing the Insecure: Security Challenges Posed by the Internet of Things

Many organizations are experimenting with Internet of Things (IoT) deployments, ranging from automation systems and sensor networks to critical connected health-care solutions,

connected vehicles and industrial robotics. Such deployment scenarios can automate device management, improve efficiencies and reduce operational costs, while improving the customer experience. Opportunities exist in every business sector, and early adopters are racing to secure a first-move advantage.

However, the IoT brings several security challenges with far-reaching consequences. These challenges differ from those present in more conventional technology infrastructures. Unlike traditional cyber-security, which often results in data compromise, security challenges resulting from real-time IoT networks can have serious implications on human security and safety.

IoT System Security Challenges

IoT security challenges are categorized into a three-tier architecture:

• *Security of Devices:* It's vital that each device only does what it's intended to do, eliminating the opportunity for infiltration and reprogramming. Over-the-air update capabilities for software and firmware updates are essential for speed and efficiency, but can compromise the security of the system.

• *Security of Communications:* IoT communications occur over public, private, industrial and IT networks, and because several IoT devices have sensors with low computational power, providing data and network-based encryption falls on gateways. This results in the need to secure vast amounts of structured and unstructured data, while supporting various types of connections and device architectures.

• *Security of Cloud/Data Center:* IoT devices connect to the cloud remotely, and data from these devices is stored in the cloud. Securing these connections is critical, but requires one to secure every data packet individually—rather than the entire data store—because there are innumerable sources with varying levels of security.

IoT Device Security Challenges

As more devices populate IoT networks, the security challenge grows. According to Gartner, around 26 billion IoT devices will be connected by 2020. Key IoT device security challenges include:

• *Limitations of the Traditional Ring-Fence Concept:* A significant proportion of the security challenges surrounding IoT deployments stem from the nature of connected devices. Since these devices are periodically transmitting data, the traditional ring-fencing model (intermittently connecting roaming personal devices like smartphones, tablets, etc.) is proving to be a challenge. The small size, large-scale and distributed nature of IoT devices overwhelms such cybersecurity models.

• *Irregular Communication Patterns:* The sheer volume of IoT devices with irregular communication patterns can overwhelm many security tools. For example, the IoT goes beyond simple connectivity to connecting vast networks of increasingly smarter and more sophisticated devices which trigger contextually adaptive communication patterns. The conventional static models deployed in today's infrastructure are bereft of this context and hence unlikely to correctly handle such dynamic situations. In addition, the knee-jerk reaction of cybersecurity experts to deny access to ring-fenced assets further aggravates the situation.

• *Limited Compute Capability of IoT Devices:* Sensors and other monitoring devices have limited computational capabilities,

meaning security tools on computers cannot be installed, due to a lack of CPU power and data storage capacity. Additionally, many of these tools are not designed to readily accept updates and patches, or have configuration and security settings that cannot be updated.

The following examples illustrate the security challenges with IoT deployments:

• A critical condition may cause a medical IoT device to send an atypical pattern of data transmissions. This can trigger a traditional security system to quarantine the device, and prevent the data from reaching the doctor.

• A sensor network monitoring water quality of a water supply source may only communicate in result of altering conditions. If central controlling systems expect to receive data only in variable bursts, spotting malicious communications from hacked devices proves difficult. Malicious devices can replay legitimate communications to trick threat detection systems.

• Another security challenge stems from the many legacy systems still implemented within organizations. How can a company securely and efficiently link its 50-year-old mainframe and associated applications—that send unencrypted credentials and/or data using legacy protocols—to a new IoT infrastructure that draws from the cloud?

A new strategy is required.

IoT projects require IT teams to take a fresh, cautious approach to security, as conventional perimeter-based approaches have serious limitations, and deployment of sophisticated monitoring tools are unable to address all vulnerabilities. For this reason, new suites of trust models, detection heuristics, adaptive remediation techniques and tools must be sourced, deployed and managed.

The sheer scale of IoT devices requires real-time remediation following a detected threat. Significant changes must be made to threat-detection and -response technologies and procedures, so that security personnel remain informed without being deluged by inconsequential alerts.

On the regulatory front, an IoT-specific risk and governance framework is required for the successful rollout of IoT deployments. Government agencies must work with the private sector to ensure that suitable guidelines and laws are in place to guide deployments. As IoT devices permeate more areas, particularly sensitive places such as schools, hospitals, and homes, following security guidelines is vital.

The IoT has the potential to revolutionize the way many in which organizations function and transform the services and products they deliver to their customers. By addressing factors such as security, or invest in secure-by-design refactoring, the infrastructures created will be able to deliver on the large promises technology offers, without compromising safety and security.

GH Rao is the president of Engineering and R&D Services (ERS) at HCL Technologies. ERS provides services to product engineering companies dealing with aerospace, automotive, medical devices, consumer hi-tech and telecom from all over the globe. He joined HCL in 1980 as part of the R&D team that developed hardware subsystems for a range of micro/mini computers. GH went on to build business lines around core engineering services, and is also responsible for transforming and expanding the scope of services through comprehensive engineering services.

- ADVERTISE
- CONTACT

FOLLOW US ON

- Follow
- Follow
- Follow
- Follow

ABOUTCAREERSAUTHORIZED SERVICE PROVIDERSYour Privacy ChoicesTERMS OF USEPRIVACY POLICY