How to fortify security in the era of Internet of Things

There is an increasing pace in adoption of Internet of Things (IoT) by businesses globally as it has proven to open new revenue streams through new smart offerings. The rising phenomenon of IoT in conjunction with the expanding cyber-threat landscape opens new avenues for attackers to go beyond the enterprise boundaries. There is much concern about the edge platform, which is often regarded as one of the weakest links in the IoT chain. Understandably, this link is attracting much traction from the hacker community. For example, in the case of connected medical devices, security researchers have demonstrated how a hacker can gain unauthorized access and hijack an insulin pump to deliver fatal doses to diabetic patients. Hence, in an IoT ecosystem, it becomes imperative to secure device authentication to ensure that only trusted devices connect to the IoT infrastructure cloud.

For enterprises, the common approach for securing communication between different systems today involves authentication by a password/certificate/key and secure network protocols. This approach has been derived from traditional Identity Management solutions, which are equipped for user/human identity and access. In this traditional approach, user identity lifecycle has achieved maturity in terms of alignment with business to follow business logic and to provide need-based access. But, in the case of IoT, device identity lifecycle is blurred with too many supply chain entities, device ownership issues, data ownership on device, device authentication and privilege access management on device. Hence, implementing a traditional approach is not feasible in the IoT model.

Combating the IoT threats

By being cognizant of a few key design principles while building the IoT solution, organizations can strengthen their cyber resilience controls to square up to any future IoT attacks. The design principles are as listed below:

Device ownership: The Original Device Manufacturer's (ODM) responsibility for secure design should be limited to first-time infusion of security keys. The ODM security key must be used for first-time connection and be replaced with another key while registering the device. This will ensure transfer of ownership from ODM to business owner.

Privilege access: Common pitfalls of using either default passwords or even storage of passwords must be omitted while onboarding. Agent-based software can be used to generate a random key which can be time/location-based to access devices. That will ensure that there is no exchange of password data across the wire to mitigate any packet sniffing over the wire. Each device needs to carry its own unique token-based privilege access.

Data security: Encryption should be on by default and wherever possible from edge to application interface over secure channels. IoT edge devices are constrained and may not have the necessary computing power to support secure communication. In such scenarios, random keys can be used to encrypt the data and decrypt at application end. So, even in the case of unsecure communication, data will stay protected.

Data privacy: With stringent data privacy laws, it becomes important to manage privacy data right from the source/edge. Privacy data components must be masked/hashed before they become part of the data stream that flows over the wire. This will save costs to protect the privacy data across all upstream components. The same key can be used to decrypt the data for legitimate use for authorized entities.

Automation: Considering the scale of IoT deployment where device volume is huge, it is not possible to manage operations manually. This is one of the practical challenges which drives IoT deployments to either use static keys/certificates or extend the expiry times to higher limits to balance operational overheads (renewal, expiry) - eventually lowering the security. Certificate renewal/expiry should be automated to initiate the change whenever device connects or initiates (push/pull) action within the renewal time window.

Integration capabilities: Having no common standards for IoT solutions during integration with underlying components, is a challenge. To overcome this challenge, the solution should have tighter integration capabilities with major cloud service providers (CSPs), device protocols, devices and internal/external certificate authorities. Logs/events should be integrated with event management platform sufficing audit and security event correlation capabilities. The scope the Computer Emergency Response Team (CERT) and incident response team must be extended to cover edge layer.

Device lifecycle: The device lifecycle must be maintained either physically or logically. If a device gets compromised, it should be blacklisted and keys should be revoked immediately, ceasing all access from this device. The hardware/software root of trust must be maintained within the device so that any anomaly should either encrypt or hash the entire device data.

Approach to a secure future

Businesses need to realize the urgent need for looking at security through the IoT lens, which will guide them towards the path of integration with their existing IT security systems. Unlike traditional user identity management, a combination of dynamic key algorithms and unique properties of device must be leveraged for any authenticated operation or secure data transfer in an IoT environment. Also, a combination of security principles, as discussed above, will ensure defense in depth and tighter integration with CERT, paving the way for digital cyber resilient response mechanisms.

About the author

Pankaj Anand
Cyber Security & Risk Services, Wipro Ltd.

Pankaj, a certified security practitioner, has been associated with Cyber Security & Risk Services practice for more than 20 years. During this period, he played various roles across multiple domains of cyber security, traversing through consulting, delivery, system integration, advisor and practice development. In his current role, he is responsible for developing IoT security solutions within Wipro. He engages with various Wipro teams/clients to ensure security in IoT solutions.

Wipro Limited
Doddakannelli, Sarjapur Road,
Bangalore-560 035, India

Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
wipro.com

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading global information technology, consulting and business process services company. We harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help our clients adapt to the digital world and make them successful. A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, we have over 160,000 dedicated employees serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.

For more information, please write to us at **info@wipro.com**

IND/BRD/AUG 2018-JUL 2019