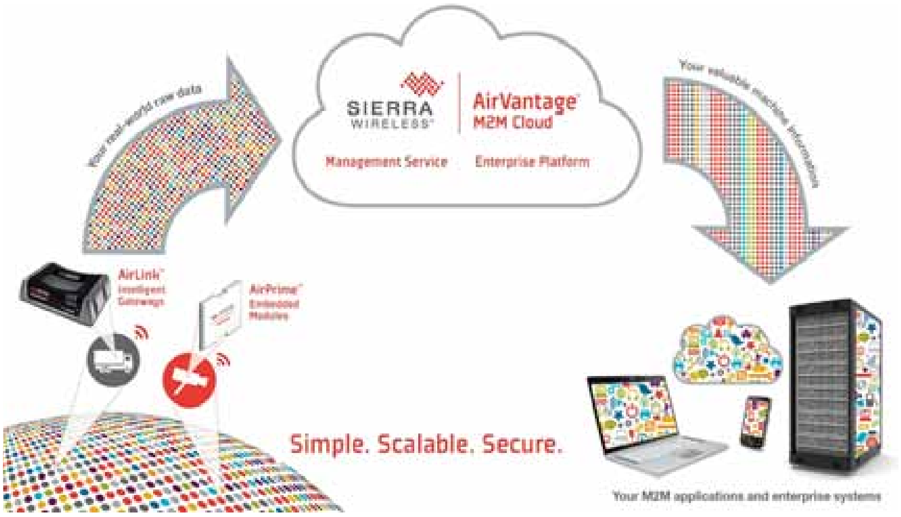
M2M security: considerations to address growing concerns

Security continues to be a hot topic in all areas of technology, including machine-to-machine (M2M) applications. Today, most analysts agree that the security risk is relatively low, primarily because M2M is still a growing space and hasn't reached a critical mass that would draw significant attention from hackers. However, M2M is growing very quickly. Cisco estimates that there will be 25 billion connected devices by 2015 and 50 billion by 2020, so security concerns will likely grow in the near future.


Your real-world raw data
SIERRA WIRELESS
AirVantage M2M Cloud
Management Service
Enterprise Platform
Your valuable machine information
AirLink Intelligent Gateways
AirPrime Embedded Modules
Simple. Scalable. Secure.
Your M2M applications and enterprise systems

In light of the threat, what should enterprises using M2M and OEMs developing M2M solutions be doing now to protect their applications? From a practical standpoint, the answer is to determine the level of threat and provide the right level of security for each specific device and application.

Enterprises and OEMs will use a variety of mechanisms and techniques to address threats in each segment of the M2M chain. Two key considerations for secure M2M deployments are trust and encryption.

Trust

The concept of trust in an M2M application is about verifying that commands or instructions coming in to a device or server are legitimate and coming from a verified source. The M2M cloud management platform, for example, must be able to verify that data coming from both deployed devices and enterprise applications can be trusted. The back-end enterprise application must use strong authentication to verify that it can trust data from the cloud management platform. And, the enterprise or M2M solution provider must be able to control access rights across all components of the system, and ensure that anyone accessing or configuring system settings is authorized to do so.

Embedded applications use the same concepts to assure trust as any other networked system: authentication and authorization.

Encryption

A secure M2M application needs to protect the transmission of private and confidential data. To do so requires data encryption and secure transmission technologies across multiple segments of the M2M application — between deployed devices, the M2M cloud management platform and the enterprise application.

If the M2M cloud management platform is operated by a third party, for example, an enterprise may wish to encrypt all data as it travels from device to cloud to enterprise application using a secure virtual private network (VPN).

On the other hand, a payment application requires a more sophisticated M2M gateway that can support the strongest possible encryption and transmit that data via a secure VPN. For applications that require maximum security, enterprises may prefer to use a private access point name (APN) network that contains only authorized devices in the application (i.e., no other devices use the network), and that does not connect to the Internet but links only with the M2M cloud via a VPN.

Finally, enterprises should use HTTPS to assure a secure connection whenever communicating with the cloud management platform and the enterprise application.

Conclusion

Security considerations for M2M applications are becoming more and more relevant as M2M continues to grow at an accelerated pace. In addition to the aforementioned details outlining the considerations of trust and encryption, secure M2M deployments need to be planned and deployed with robustness and upgradability in mind. When incorporated with effective trust and encryption mechanisms, long-term viability and security of M2M applications can be assured and stay in step with changing technology and new emerging threats.

As a starting point, enterprises or OEMs should work to achieve the "right" level of security for their M2M applications, both today and for the future. In doing so, they can drive forward the benefits of an effective M2M solution, while having the peace of mind knowing they've taken the right steps to avoid being compromised. ▲

Contact
Olivier Beaujard
Vice President Market Development
Sierra Wireless
OBE@sierrawireless.com
www.sierrawireless.com