The MobilityHub
SECURING DATA & APPS.

John Edwards

M2M Networks the New Battleground

John Edwards, Technology Journalist, 4/17/2013

Bio Email This Print Comment 13 comments

A fresh attack vector is emerging to engage the interest of cybercriminals -- machine-based Internet networks.

Machine-to-machine (M2M) networks are popping up all over the place, allowing food and beverage suppliers to monitor vending machines, manufacturers to control production lines, and retailers to track pharmaceutical shipments. M2M is also used to monitor automated toll payments, smart utility meters, and various types of security networks. Cyber criminals would like to get into all of these systems, and many others, to steal funds, gain physical access to unauthorized locations, and create a general state of havoc.

Growing concern

Security experts have always considered M2M network protection a low priority. Until recently, M2M systems were mostly limited to pilot projects and other small-scale deployments. But as more M2M networks come online and begin handling a growing number of important tasks, cyber criminals are finding multiple ways of worming themselves into the systems.

Brute force network intrusions and stolen codes are just a couple of the ways lightly defended M2M networks can be compromised. Complicating M2M network security is the fact that, unlike computers, smartphones, tablets, and most other human-operated Internet systems, M2M devices usually feature restricted processing, storage, and power capabilities, making them harder to secure against cyber criminals.

Serious attacks are already underway. A series of intrusions launched against smart meter installations over several years may have already cost one US electric utility hundreds of millions of dollars annually, the FBI revealed in a cyber intelligence bulletin published back in May 2010.

Is anybody home?

A National Science Foundation report on smart meter attacks, published by the Association for Computing Machinery in October 2012, noted that spoofing and reverse engineering make it relatively easy for anyone with the requisite knowledge to communicate with commonly deployed electrical meters. With little more than a desktop computer and an Internet connection, the study's researchers were able to look into meters to examine a home's electrical consumption in an effort to determine when people were inside or away. By tapping into homeowners' set-top cable boxes, the researchers were even able to see which TV channel people were viewing.

Many security experts also worry that M2M attackers may be in the process of learning some

tricks from their web counterparts. DDoS attacks, for example, may actually be more effective against M2M network devices than against websites. With only limited onboard capabilities, it wouldn't take much of an attack to effectively freeze a device and render it inoperable. Furthermore, in the case of battery-operated M2M devices, which are becoming increasingly common in agriculture and other applications without practical access to commercial power, a DDoS attack could be designed to intentionally overburden the processor, prematurely draining the device's battery and knocking the unit out of service.

Security has not posed a major challenge to M2M network makers or users so far. Yet, as M2M data becomes increasingly engrained into more systems, solution providers will need to demonstrate their total commitment to hardened security.

Related posts:

- Ransomware on the Rise
- QR Codes: The Latest Hacker Entry Point
- Malnets Become the Biggest Mobile Threat