As more devices get networked, firms that build or connect them must ensure security

June 17 2011, By Victor Godinez

Telecom equipment maker Ericsson has famously predicted there will be 50 billion devices connected to data networks by 2020.

Those connected devices won't include just computers and smartphones, but cars, homes and industrial devices, constantly sending and receiving a flood of data.

That convenience comes with a potential dark side.

For hackers, cybercriminals and even armies, all those newly networked machines represent billions of new targets for mischief, thievery and assault.

"We understand that as our lives move into a completely digital connected world, it has to be secure and safe," said Geoff Hollingworth, Ericsson's Plano, Texas,-based head of Internet protocol services strategy for North America.

"It's no different than the real world, where you have to feel you can move down the street and not get attacked."

The security problem will be much broader than securing your laptop or even your smartphone.

Soon, the car in your garage, the electrical meter on the side of your home, the products you buy at the store, and the industrial controls at the

factory that made those products will all be connected to various networks and the Internet.

And each new networked device is a potential entry point for a hacker.

Addison, Texas,-based Revere Security Corp. develops security software for that new wave of connected devices.

About a year ago, the company moved from perfecting its algorithms to pitching its products to customers, which include everything from the U.S. military to power companies.

One of Revere's biggest opportunities is in the new wave of high-tech smart power meters.

"The industry is luckily moving toward security controls on smart meters," said Chris Hanebeck, vice president of product management and marketing at Revere.

Dallas-based power line operator Oncor has installed about 1.7 million digital smart meters in Texas over the last year or so, and its goal is 3.4 million by the end of 2012.

The technology has benefits for both consumers and electricity providers.

For example, if you have a smart meter, you can go to SmartMeterTexas.com to see nearly real-time data on your electricity usage.

And your provider can turn your power on and off with the flick of a software switch, rather than spending hundreds of dollars to dispatch trucks and technicians to individual homes.

But the high-tech meters are much more like minicomputers than the simple measuring devices they're replacing.

So Oncor now has to focus on digital security in a way it never had to before.

"When we started this project, from Day 1 we have foundationally built this with securing the system and securing the data in mind," said Oncor chief technology officer Mark Carpenter.

Carpenter said Oncor uses layers of security, including encryption, firewalls and data traffic monitoring, to keep bad guys from tapping into its meters.

"While no system is 100 percent impenetrable, we have designed our systems such that we can isolate events and situations to affect the minimum portion of the system, if they were to occur," he said.

Why would someone want to hack a smart meter?

Hanebeck at Revere said the motivation can range from simple vandalism - turning someone's power off - to economic sabotage against a power company or a full-scale cyber assault on a country.

And many of these new devices are being wirelessly connected, so an attacker rarely or never has to physically connect with the device.

All the damage is done over Wi-Fi.

Part of the challenge in securing this new wave of connected devices is that unlike PCs and now smartphones with beefy processors and memory to burn, hardware capacity is at a premium.

With a smart meter or a paper-thin radio-frequency identification chip slapped on a shipping pallet, the security has to be both lightweight and strong.

Another area where tech experts have had to rethink network security is in cars.

Ford Motor Co.'s Sync software, for example, pushes everything, from turn-by-turn driving directions to news and sports info, wirelessly to its cars.

So far, the company hasn't seen hackers trying to break into that data network.

But data security was built into Sync from the ground up.

Rich Strader, director of Ford information technology safety and security, said one way the company manages security is by keeping critical safety systems in a car on a different network from other functions.

"Some of these [systems] are dedicated to controlling critical functions of the vehicle - such as power train controls, safety systems, etc.," he wrote in an email.

"These dedicated computers can only be updated by an authorized Ford dealer to ensure a high level of safety and security for our customers. Our consumer-based systems - such as the part of Sync that controls the audio functions and performs voice recognition - can be updated by a USB interface."

Strader noted that it is possible to wirelessly push updates automatically to Sync-enabled cars without users noticing, but so far Ford has opted

not to do that, letting customers pick the updates they want to install.

Work in the auto industry has also begun on wireless networks that would be devoted solely to safety and traffic control.

For example, a car that has to brake abruptly in heavy traffic would send an instant alert to vehicles behind it, so each driver could know they might have to come to a sudden stop.

This "network for cars" would require an even heavier security focus, Strader said.

"Ford is part of a consortium of vehicle (original equipment manufacturers) that have been working with the U.S. Department of Transportation and the Department of Homeland Security to design vehicle-to-vehicle and vehicle-to-infrastructure communications that provide these capabilities reliably and affordably," he said.

"In addition, Ford plans to combine inputs from both the wireless network and onboard vehicle sensors to ensure proper behavior of our in-vehicle systems."

Hollingworth at Ericsson said many consumers are rushing to embrace the convenience of these new connected devices.

But unlike with computers and phones, the security of these new devices is almost completely out of the hands of the individual users.

So it's up to the companies building and connecting them to make sure they're safe.

"The benefits of connectivity are so large that people are trusting the technology, and we want to make sure that trust is well-founded," he

said.