Study Shows Thousands of Consumer Internet Connectivity Devices Are Vulnerable to Attack

October 26 2009

Columbia's Intrusion Detection Systems Lab, led by professor Salvatore J. Stolfo (center)

(PhysOrg.com) -- Following news reports that 65,000 modems and wireless routers used by Time Warner Cable customers are vulnerable to attack by hackers, a Columbia University expert on computer security and privacy has found that software flaws in embedded devices like routers, webcams and Voice over Internet Protocol (VoIP) phone adapters are far more widespread than previously known.

Salvatore J. Stolfo, a computer science professor and director of the Intrusion Detection Systems Lab at Columbia's Fu Foundation School of Engineering and Applied Science, presented "Brave New World:

Pervasive Insecurity of Embedded Network Devices" at a computer security conference in France last month.

In the paper, co-authored by graduate students Ang Cui, Yingbo Song and Pratap V. Prabhu, Stolfo recounts how he and his team scanned thousands of consumer and business devices around the world and found that a high proportion of them were unprotected. Their ongoing research began in December 2008.

"Many thousands of unsuspecting people world-wide have this problem," says Stolfo. "Many of these devices are easy targets for just about anyone with mal-intent. One can 'log in' to your home router and plant software in it, much like a virus, and record your network traffic or alter it; record phone conversations, or do just about anything nasty one can imagine."

While scanning devices in North America, Europe and Asia, Stolfo found that certain types of consumer devices publicly accessible over the Internet have vulnerability rates as high as 41.62 percent. Among VoIP phones, the vulnerability rate was one in five. He and his colleagues, through an outside group, are contacting the Internet service providers who supply connectivity to those vulnerable devices. The ISPs, in turn, will warn the customers. An additional step may involve alerting vendors of the devices.

Like PCs, embedded devices contain software. This software is used to route messages in and out of one's home or office. Vulnerability is introduced into the device when users fail to properly configure it before plugging it in. To protect themselves, consumers need only read their instruction manual and follow the directions telling them how to go online and set up their machine so no one can break into it.

Provided by The Earth Institute at Columbia University (news : web)