HP slams 'sensational' reports about LaserJet printer hack vulnerability

November 30 2011, by Nancy Owano

(PhysOrg.com) -- Columbia University researchers have demonstrated how hackers can use printers not only to infect computer systems and steal information but to set printers on fire. Their claims were made this week in a demo at Columbia University's Intrusion Detection Systems Laboratory for msnbc. They report a security flaw in Hewlett-Packard (HP) printers open for exploit. While their experiments were only on HP printers, they said that they are just starting to sample other manufacturers' printers too.

As some observers explain the situation, we are in a computer equipment stage of embedded systems in printers, packed with Internet-connecting functions that make them operate more like computers.

Rewriting the printer's firmware takes only about 30 seconds, according to researcher Ang Cui, and a virus would be virtually impossible to detect once installed. Only pulling the computer chips out of the printer to test them would confirm an attack, Cui said.

Every time a vulnerable printer accepts a print job, it scans that job to see if it includes a firmware update. Older printers do not discriminate the source of the update; hackers can in turn intercept requests and plant their own updates. As one blogger described the potential mischief, the printer can be told to erase its software and hackers can install a “booby trapped” version.

The Columbia team sent standard print commands from a Mac and a PC running Linux and succeeded in tricking an HP printer into reprogramming itself.

The researchers have been working on the printer security project under grants from government and industry, according to reports, and they described the flaw in a private briefing for federal agencies. They also reported their findings to Hewlett-Packard.

Columbia professor Salvatore Stolfo, who directed the research in the Computer Science Department of Columbia University’s School of Engineering and Applied Science, said that these devices are completely open and available to be exploited. He and his team have been forceful in describing this as a serious matter for attention, involving a vulnerability that could impact millions of printers and other hardware.

In contrast, HP initially took a cautious view in response. Keith Moore,

chief technologist for HP's printer division, had said HP takes the Columbia findings seriously but initial research suggested vulnerability was low. He pointed out that the models tested were older models, and he would generally disagree that the threat is widespread. He said the company was reviewing the issue. But in a hard-hitting statement issued Tuesday, HP said, "*Today there has been sensational and inaccurate reporting regarding a potential security vulnerability with some HP LaserJet printers. No customer has reported unauthorized access. Speculation regarding potential for devices to catch fire due to a firmware change is false.*"

More information: msnbcmedia.msn.com/i/msnbc/sec … _printersecurity.pdf