



Unmonitored net links are open doors ignored by security apps

By Kevin Fogarty, News Director
Apr 2007 | SearchSecurityChannel.com

There are a lot of unappreciated risks within information security, but some channel companies are pointing out that an IP phone, uninterruptible power supply, HVAC system and other smart-but-not-too-smart devices could pose threats security systems aren't prepared to counter.

Despite their relatively low priority on the security hot list, uncontrolled networked devices present a trusted, high-bandwidth doorway into a secure network for anyone able to plug into those connections or pretend they have.

"The two most common security questions customers ask me are 'What do you do about [Media Access Control \(MAC\) address](#), [spoofing](#) and [port swapping](#),'" said Bob Durkee, VP of sales and business development for endpoint security application provider Great Bay Software Inc. in Greenland, NH. Vulnerable devices include fax/scanners, uninterruptible power supplies, inter-switch links, wireless access points and other devices that are connected to the network but are unable to authenticate using 802.1x and the Extensible Authentication Protocol (EAP).

However isolated or low priority, physical network connections live inside the trust envelope of the corporate network, so devices attached to them -- the original printer or a hacker pretending to be the printer -- only needs to request an IP address from the [Dynamic Host Control Protocol \(DHCP\)](#).

"The devices being swapped and spoofed most often are printers and IP phones, because they give you their MAC addresses just by hitting a button," Durkee said. "A printer could turn into a Linux workstation and you might not know that."

"It's not so much that someone's going to get into your network through a printer," according to Robert Ayoub, analyst at [Frost & Sullivan](#). "It's more that a hacker could exploit a medium- or low-priority system, and from there jump to a printer running an unpatched Linux kernel, or another device. It's getting that foothold and then a hopping to a place where they can mount a real attack."

Great Bay is working with both [Cisco Systems Inc.](#) and [Juniper Networks Inc.](#) to integrate its -- [Beacon](#) and [Endpoint Discovery](#) products into the networking vendors' [Network Access Control \(NAC\)](#) products to locate non-EAP devices as well as the PCs, servers and other OS-running hardware that NACs are designed to control.

As recently as 2005 Frost & Sullivan limited its definition of "endpoint" PCs running firewalls or other security applications -- leaving out servers, routers and unmanaged devices such as printers and other network-connected but non-IT-related systems. In a report on the worldwide Network Access Control (NAC) market late last year, however, Frost & Sullivan had changed tacks, to follow "organizations [that] are realizing the need

to enforce granular network access to eliminate risks involved when using unmanaged endpoints."

The market for security on unmanaged endpoints was \$85 million in 2006 and could rise as high as \$600 million in 2013. Great Bay fills a hole in those security products that not only created an opening for intruders, but an administrative headache as well, according to Jay Kirby, VP and chief sales officer at integrator [Troubadour Ltd.](#) in Houston, Texas. "If you take a network printer -- one that does not authenticate -- and you move it from a port on the second floor to the fifth floor, through a traditional NAC deployment, you may not see it and it may not be available," Kirby said.

Using Great Bay products to discover those devices helped Troubadour -- Cisco's Global Security Partner of the Year 2006 -- close holes in the networks of large healthcare clients such as Baylor College of Medicine and Driscoll Children's Hospital, and improve control of their networks.

"In the first meeting a client will say they know everything that's attached to their network; in the second meeting, they'll say 'OK, we don't know everything,'" Kirby said. "But when the NOC team sees they can drill down in the net and see something that turns out to be an AP that's not on their standards list, they'll say 'I always wondered what that was.' When you've got 16,000 devices on the network, you don't know every one."

Security consultants do try to identify undersecured machines during vulnerability audits, and some asset-management vendors are beginning to bridge the gap between asset management and security, Ayoub said. But there are few tools specifically designed to identify and lock down low-priority machines that could become entry points, he said.

The Great Bay products are not scanners and are not inline network inventory managers, Durkee said. They can gather data by monitoring network traffic at Layer 2 or Layer 3, but get the best information by tapping into the DHCP request stream, he said. "We're only seeing the DHCP, not having to reply to it, and that gives us fantastic information," he said. "Every device that attaches [to the network] needs to make this request, and if the IP address lease time is seven days, we will see every device that requests an IP within three-and-a-half days, the half-life of that license."

The products can also monitor traffic from devices using [NetFlow](#) or [Simple Network Management Protocol \(SNMP\)](#) management traffic, or do more active profiling by sending out a small number of packets to identify if a particular port on a particular device is open.

"If we see you have port 900 open, that increases our confidence that you're a printer, and we can shut that down if we want," Durkee said. "We can go into the IP phone server or print server and can see who the print server is talking to for print jobs. By inference that can increase our confidence that all it's talking to is a printer or an IP phone, rather than something else."

That data is collected in a database either the solution provider or the customer can use to maintain a continuous, accurate inventory of what devices are on the network and what security risk they might pose.

"It's helping us shorten the implementation of NAC deployments in large environments," Kirby said.

It's also helping close deals and increase the profit on them, he said. Great Bay products may only make up 10% of a total security deal -- maybe \$40,000 or \$50,000 with a typical mid- to large-sized customer -- but they answer questions for customers that would be very difficult to answer otherwise, Kirby said.

Plus, they come with "a very nice margin from Great Bay," according to Kirby, who wouldn't elaborate.

Troubadour is a Platinum partner in Great Bay's channel program, however. Platinum partners typically get a 40% discount on the list price of Great Bay gear, according to Durkee, who estimated his products could make up 15% to 20% of a NAC deal. Gold partners get 20% discounts.

Let us know what you think about this story; e-mail [Kevin Fogarty, News Director](mailto:Kevin.Fogarty@NewsDirector.com).