

VPNs, Dot-One-X and the Mailman

{ This column completes a discussion on wireless networking started in January. Broader product management topics return in March. }

When WiFi wireless networking first appeared, there was no effective security mechanism to protect one user's information from other eavesdropping WiFi users. Residential customers were not concerned, but corporate buyers were frightened off and the press jumped all over this story. This month's column looks at two alternate security models for roaming business users who may be in hot spots or visiting other companies.

WiFi exists at Layer 2 of the OSI model, also called the "link layer." In the absence of good link layer security solutions, some innovative products have appeared that borrow technology from the next layer up: Layer 3 or the "network layer." These have used VPN-style security (see below) to protect local wireless traffic from snooping and tampering.

Now, solid link layer security standards are emerging for wireless. This is good: to satisfy corporate road warriors, we'll want to use [link-level solutions for local WiFi security](#) and reserve [VPNs for long-haul protection](#). Here is a walk through the assorted pieces...

Catch Me Up on VPNs

Virtual Private Networks (VPNs) have been a standard part of remote security for a decade. They live at Layer 3, the "network layer," providing end-to-end authentication and encryption between specific endpoints - such as a remote laptop and a corporate firewall. This protects IP data from manipulation as it crosses many physical networks and providers en route. VPNs are how corporate email users keep their internal memos internal when traveling.

Looking for a real-world analogy, consider VPNs as a solution for love-struck teens who want to send mushy letters to each other. They know that letters will pass through many hands, including the postal service and parents at either end. By setting up a secret code in advance, our sweethearts can send letters • from mailbox to post office to mailbox • without grown-ups peeking. Julius Caesar used this same method for military dispatches from his far-flung campaigns.



Note that the secret code is unique to each [pair](#) of correspondents, and protects letters end-to-end. If you use such a code, all of your other mail arrives plain text, including whatever credit card bills and report cards may land in your mailbox.

Using VPNs for local wireless security means protecting data between your laptop (or PDA or Danger hiptop) and the local access point. Once there, all information is sent along the wire in clear text.

Dot-One-What?

Customers and vendors of networking gear crave standards. Newly arrived for WiFi is a link layer authentication standard called 802.1x and next is an improved encryption labeled 802.11i. (Ignoring the details, I'll refer to the combination as '.1x' and pronounce it 'dot-one-x'). This combination provides local security between the wireless end device and nearby access point. Each valid user is verified, allowed to send/receive, and has all data encrypted to reduce eavesdropping. Once through the access point and onto the wire, though, data is in the clear for downstream rascals to read or alter.



Again, returning to our mailbox analogy, .1x addresses a different problem than that addressed by VPNs. Imagine a neighbor who likes to read your mail, has x-ray specs able to see into your mailbox, and occasionally steals your letters before you get home. He might copy down your credit card number, swipe a party invitation, or censor teen heart-throb letters.

In our postal example, .1x specifically addresses the **local** delivery problem between the post office and your front door. Under .1x, your letter carrier would tuck all of your mail into a lead-lined briefcase, ring your doorbell, and give your letters to you **personally** after you show each other official photo IDs. Outgoing mail is slipped back into the briefcase for a safe return trip to the post office.



Note that all mail is protected (even advertising circulars) without involving the senders - but only on the delivery hop between post office and home. Evildoers at the post office could still steam open your credit card statement or steal invitations to White House galas.

The point of the exercise: these two technologies are for different things. VPNs are designed to protect **selected sensitive information end-to-end**, but ignore other destinations and non-IP traffic.

.1x defends **local traffic on the wireless link** and blocks unauthorized users • but defends us no further than the wireless access point. Snoopers further along the wire can still intercept my VPN-less data.

So What?

A variety of early WiFi security solutions have borrowed from Layer 3 to defend Layer 2.

In our mailman story, my household has to write every letter in a code that we share with the local post office, which decodes it before

sending it on. Likewise, every incoming letter and postcard is encoded at the local post office for us to decode at home.

For local security on a single bit of network, none of this matters much. I do think that market dynamics will drive WiFi vendors toward standard, low-cost implementations like .1x, which will be faster and cheaper, and we'll see a rush of .1x products in store by mid-year.

The major benefit, though, to having .1x protect wireless link layers is that it leaves VPNs available for end-to-end network security. Whenever I'm connecting to wireless networks away from my corporate home base, I want to VPN back to my email server (or order entry Internet, or whatever) without the local network owners peeking. In general, using VPNs for local wireless security prevents me from using them as well for remote security: tunneling one VPN through another is a mostly untested, inefficient proposition. I can't use my VPN for remote security if it's also in use for local security.

Back in Mailman Land, my household is now translating every letter into a special code shared with the post office, in order to thwart my nosy neighbor. This pre-empts our love-struck teen from using a different code to send secret letters to his honey.

There are also several technical advantages to .1x: it will cover non-IP traffic such as NetBEUI; it deters bandwidth thieves in your parking lot; and ARP attacks will be tougher. In addition, Microsoft has just begun its relentless rollout of nearly-standards-compliant .1x client for XP and Win2000.

Perhaps an Example

I'm sitting in my customer's office, preparing a major contract. She has graciously let me tap into her WiFi network, secured with a VPN-style client and routing all of my traffic to the public Internet. I'm anxious to check for last-minute strategy emails, verify her goods are in our warehouse, and scan for news about the competition. I don't want to send this across her company's network in the clear: I want a VPN tunnel back to my headquarters. Layer 3 WiFi security probably prevents this from working.

Sound Bytes

Arrival of 802.1x and 802.11i will put link layer security back into Layer 2, where it wants to be, and allow roaming WiFi users full freedom to VPN back home. This will allow more secure local connections - as well as secure remote connections for roaming business travelers, who are the primary financial supporters of hot spots.

"Product Bytes" is a monthly newsletter about product strategies for technology executives. To subscribe, send an email to subscribe@mironov.com. Back issues are archived at www.mironov.com.

Mironov Consulting specializes in early product strategy, technology planning, and customer requirements. Call if you think that emerging standards may bowl you over. All contents © 2003 by Rich Mironov. Product Bytes (TM) 2002. Contact rich@mironov.com or 650.315.7394.