Network Security Presentation Follow-up

Sources:

The background for the "isolated networks" map came from a variety of sources. It developed most quickly after conversations at the Dartmouth Unleashed conference where I spoke with a number of Academic IT folks, including David, the lead sys admin at Colby-Sawyer, Harold, the tech services manager at Holy Cross, and Donald, a conference presenter and wireless project lead at West Point. Their stories were echoed by many others during conference, and seemed to establish the "best practice." That many institutions had arrived at similar plans after long re-engineering processes, some involving name brand consultants, only confirmed that point in my mind.

The case for "clientless" authentication also comes from a variety of sources. Every example that matches our service model uses some form of clientless authentication (if authentication is required at all). They do this because it meets these three requirements at the lowest cost:

- Access control
- Data security (with the use of application layer security)
- Low client impact and low client requirements

An example comes from Simmons in Boston. David says they chose clientless authentication (via NoCatAuth) because it met those requirements better than any other mechanism they could identify. These views are shared separately by David from Colby-Sawyer, where they are now testing a commercial clientless authentication product from Vernier Networks. Vernier isn't the only vendor in this market; Bluesocket and others also offer wireless gateway products.

I have found one example of 802.1x authentication in higher-ed. Donald, from West Point, selected an early, proprietary implementation of 802.11i (with 802.1x authentication), but only because of West Point's unique service model. The first difference is technical, all student computers are government property and the school specifies uniform software and hardware for them, beyond that, however, West Point has very little competition and its computer policies or limitations are not a factor in student enrolment.

Alphabet Soup:

I was not specific in my presentation about the capabilities of WPA. WPA is a name applied to two related standards:

The first, an interim security standard, specifies the use of 802.1x authentication with a WEP key distribution mechanism and is generally compatible with current 802.11b client hardware. However, it continues to depend on WEP and has all the vulnerabilities of WEP.

The second standard, the IEEE's as yet incomplete 802.11i, defines a much more robust set of security enhancements to wireless networking (it does block encryption, instead of WEP's stream encryption, and each client has a different key), but is incompatible with existing hardware. The standard is expected to be completed early in 2004, with hardware based on that standard hitting the market in 2005.

Some single-vendor solutions, like the one selected by Donald from West Point, do offer some of the capabilities of 802.11i now, but support and compatibility is limited.

My conclusion: we should revisit the wireless security question in 2005 to review adoption of 802.11i for 2006 deployment, but the interim WPA standard available now offers little to improve wireless security and does nothing to address the serious vulnerabilities in our wired network.

The Money Question:

Clientless authentication puts the burden of security on equipment at the center of the network and depends on inexpensive edge devices, while 802.1x requires expensive and complex edge devices. Because of this, growth is less expensive with clientless authentication.

To deploy a proprietary implementation of 802.11i now (because anything less than that would not meet our security needs and interoperable 802.11i equipments won't be available for some time), we'd face enormous costs in upgrading our existing base of client devices to meet the compatibility requirements.