Will IEEE 802.1X Finally Take Off in 2008?

Neal Leavitt

Security is always a key concern for network operators. They are thus always looking for effective new security tools to work with. Eight years ago, an authentication technology called IEEE 802.1X was supposed to be an important tool for local area networks.

802.1X provides a security framework by letting PCs, Internet phones, and other devices connect to a LAN only if they can authenticate themselves prior to network access.

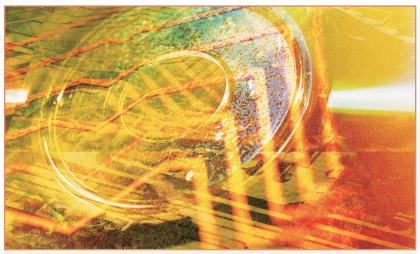
Despite its promise, IEEE 802.1X has never been widely adopted, although it has been used increasingly for wireless gateway-access controls.

"Adopters of 802.1X for authentication have run into capital costs, unexpected operational expenses, and security risks that can be expensive if not addressed properly," said Robert Whiteley, an analyst with Forrester Research.

Additional problems have included product in stability and potential users' unfamiliarity with the technology.

As is the case with many complex standards, vendor implementations are not always exactly the same and thus are not always completely compatible, particularly for advanced functions, said Scott Pope, Cisco Systems' security-product marketing manager.

However, Whiteley said, IEEE 802.1X's fortunes might be about to change. For example, vendors are working to correct the technology's



shortcomings. In addition, some experts predict that wider adoption this year of Windows Vista, which offers improved support for 802.1X, will spur increased deployment of the technology.

They also say the increased use of wireless networks, particularly for purposes requiring security, will spur more 802.1X use in mobile devices. And the OpenSEA Alliance is developing an open source 802.1X client that could promote a standards-based approach that would enable interoperability and encourage increased adoption of the technology.

It now remains to be seen whether organizations will more widely adopt 802.1X and whether proponents can continue improving the technology.

WHAT IS IEEE 802.1X?

The IEEE 802 LAN/MAN Standards Committee sponsored development of 802.1X. The IEEE ratified it as a standard in October 2001.

A revision, ratified in December 2004, incorporated minor changes to the original standard and added features to facilitate its use in wireless LANs.

Implementation

802.1X is more commonly used in wireless networks because of mobile technology's vulnerability to over-the-air signal interception. In addition, networks use 802.1X because it offers a convenient way to deliver cryptographic keys for wireless LANs, which typically provide security via encryption, noted Lisa Phifer, a vice president with network consultancy Core Competence.

"With wired LANs, we have better physical security. Hackers need to be inside a building to get access," said Lawrence Orans, an analyst with market-research firm Gartner Inc.

Major IEEE 802.1X vendors include Aruba Networks, Cisco Systems, Identity Engines, Juniper Networks, Microsoft, Nortel Networks, Hewlett-Packard's ProCurve Networking, and Trapeze Networks.

Under the hood

802.1X provides port-based authentication in wired Ethernet and Wi-Fi mobile networks. It also supports any technology the IEEE includes in its group of 802 local or metropolitan area network standards, such as WiMax (IEEE 802.16), according to Trapeze Networks principal engineer Matthew Gast.

The technology is typically implemented at the first point of connection to the network, noted Paul Congdon, chief technical officer of hardware vendor ProCurve Networking.

Components. 802.1X systems have three key components. A *supplicant* is typically software installed on a network endpoint—such as a PC, laptop, or Internet phone—that can access a network. Supplicants are provided as part of LAN adapters, which connect devices to networks; are sold individually; or are embedded within an OS. Windows XP and Vista, MacOS X versions 10.2 and later,

Published by the IEEE Computer Society

and several Linux implementations support 802.1X.

Authenticators, generally within wireless access points or Ethernet switches, are the devices in an authentication system that physically allow or block network access. The supplicant tries to connect to the LAN through the authenticator, which requests authentication credentials from the endpoint.

Authentication servers are usually enterprise Remote Authentication Dial-In User Service servers, although they can also be part of Active Directory servers, which provide central authentication and authorization services for Windows computers; or Lightweight Directory Access Protocol servers, which store information about a user's or resource's location on a network.

RADIUS provides network authentication, authorization, and accounting services, and is used by many organizations for access to various resources, including modem pools, DSL services, corporate virtual private networks, and wireless LANs.

With RADIUS, a user sends a network-access request to a network-access server. The NAS, which acts as a gateway, passes the request to the network owner's RADIUS server, which then asks for authorization via identification that typically consists of a username and password. Information in a RADIUS database also tells the system the level of access to resources that authenticated users should have.

Using RADIUS with 802.1X is convenient, said Core Competence's Phifer, because many companies already use RADIUS for other authentication purposes, and because interoperable implementations are widely available.

Also, use of a single, central server to handle authentication means network administrators don't have to configure each port or switch to do so, which could require considerable time and effort.

How it works. The 802.1X process starts when a supplicant connects to the authenticator while trying to access a network, as Figure 1 shows.

The system blocks all traffic from the client except that related to authentication. Upon detecting the access attempt, the authenticator prompts the supplicant to supply an identity.

The supplicant forwards its identity information and access request to the authentication server via the authenticator. They then exchange challenge/response messages, the number depending on the approach used. In some cases, the network not only authenticates the client, but the client also takes steps to determine whether it is connecting to a network it trusts. This adds traffic to the challenge/response process.

If satisfied with the supplicant's identification, the server informs the authenticator, which enables access by unblocking the LAN port. To establish security, the supplicant

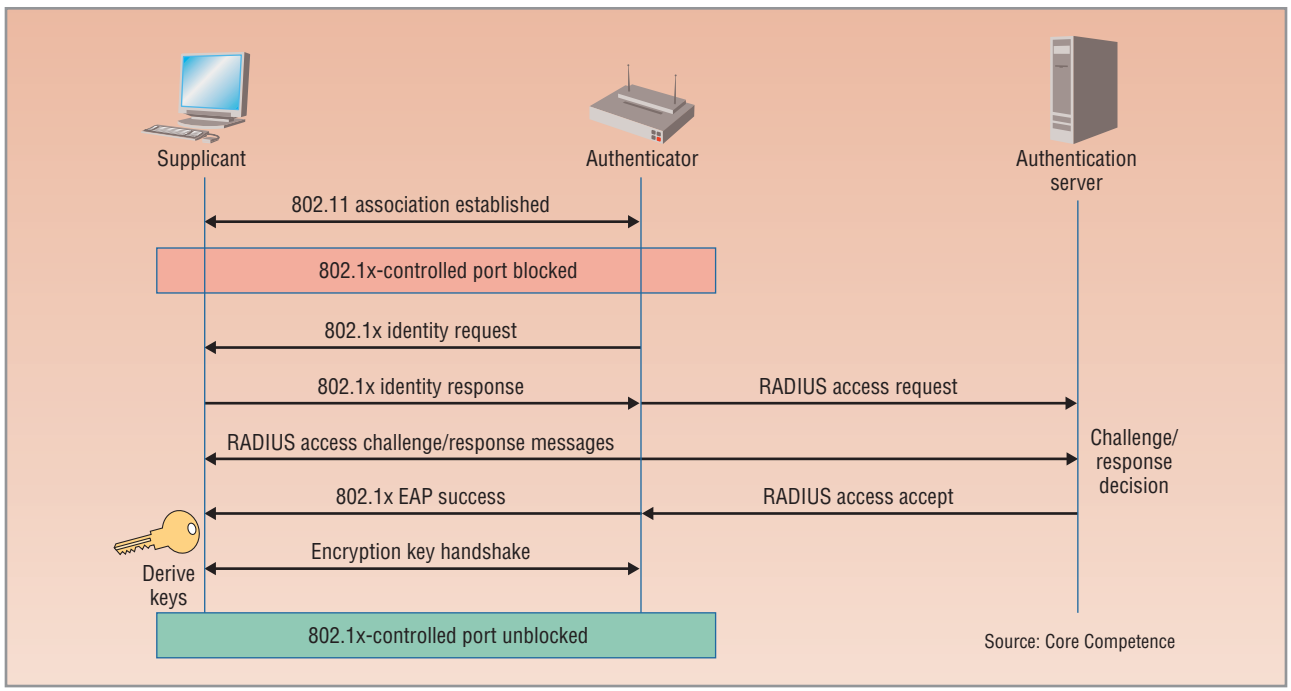


Figure 1. A typical 802.1X authentication process involves a device (the supplicant) trying to connect to a network; the machine that authenticates the supplicant (the authentication server), generally via Remote Authentication Dial-In User Service (RADIUS) technology; and the device that physically allows or blocks network access and handles communication between the other two elements (the authenticator). In this process, the authentication server asks the supplicant to identify itself. If satisfied with the identification, the server informs the authenticator, which enables access and passes on the necessary encryption keys.

and authenticator exchange cryptographic keys.

EAP. Typically, the supplicant authenticates itself via one of the many Extensible Authentication Protocol approaches.

EAP, usually implemented in wireless LANs, is not an authentication mechanism but instead provides an authentication framework. It provides some functions used in authentication and supports negotiation between the supplicant and authenticator as to the technique they will use. The technology supports mechanisms such as token cards, Kerberos, one-time passwords, digital certificates, public-key authentication, and smart cards.

IEEE 802.1X specifies how EAP packets should be encapsulated for transmission in LAN frames.

Miscellaneous. Network owners have the flexibility to choose the authentication approach used when someone tries to access the network. This lets them decide how much security they require and how much complexity they want to manage.

IEEE 802.1X generates and delivers single-use cryptographic keys for each session, noted Phifer. This avoids problems that occur with some security technologies—such as Wired Equivalent Privacy—that use one decryption key for all devices connecting to the same access point, Phifer explained. If hackers obtain the one key, she said, they could decrypt everyone's traffic until all devices are reconfigured.

When the supplicant logs off the network, it sends a message to the authenticator, which resets the port so that it blocks all nonauthentication traffic from connecting.

IEEE 802.1X functions the same on wired and wireless networks except that in the latter, it must support the transition of sessions from one access point to another when users are in motion.

802.1X'S DOWNSIDE

Despite its advantages, 802.1X also presents several potential problems.

Organizations must buy, install, upgrade, configure, and manage various network components—including supplicants, switches, and RADIUS servers—to implement 802.1X. This is a sometimes complex process that requires the expenditure of time and money and that becomes more difficult as an organization increases its deployment of the technology.

The need for ongoing supplicant configuration and management can cause unexpected operational costs, noted Seth Goldhammer, director of network-access-control product management for security vendor TippingPoint Technologies. Also, 802.1X changes the way a network is built and managed, requiring organizations to provide IT employees with training and support.

Several factors are contributing to the predicted increase in IEEE 802.1X adoption.

Some EAP types used by 802.1X systems have security vulnerabilities. For example, said Phifer, the Protected Extensible Authentication Protocol—an open standard proposed by Cisco, Microsoft, and RSA Security—can fall victim to man-in-the-middle attacks if users don't configure their PCs' network connections to check the certificate presented by the authentication server to ensure they reached the intended server. If they don't, an attacker could intercept 802.1X traffic, pretend to be an authentication server, and steal the user's password or the session's encryption keys.

According to Sean Convery, chief technology officer of network-security vendor Identity Engines, 802.1X works with so many authentication methods, users can have problems picking the most suitable one.

And providing 802.1X support to a network adds complex user-interface screens that many people aren't familiar with.

In addition, Convery said, several vendors have used proprietary extensions that have hurt interoperability and have made it difficult in some cases for organizations to use more than one vendor's products in their system. In addition, they may have trouble working with other users' systems if made by different vendors.

LOOKING UP

Several factors are contributing to the predicted increase in IEEE 802.1X adoption. For example, said Convery, "The technology's usability is being improved, new GUIs are being developed, and organizations such as the Wi-Fi Alliance have interoperability certification programs that ensure that implementations work well together."

Increased demand

Trapeze Networks' Gast said that as more new laptops ship with Windows Vista, more users will utilize its upgraded 802.1X capabilities, such as an improved GUI and a supplicant that has fewer bugs and is more stable.

Also, the increased use of wireless networks should drive increased demand for the security that 802.1X provides, said Convery.

And, Gast predicted, demand for 802.1x will grow as Internet telephony on wireless LANs improves in quality and becomes more popular. 802.1X can cache a single set of cryptographic keys and use them across access points as wireless users move around. This eliminates the need to produce new keys at each access point, which could unacceptably slow communications.

In some countries, government regulations require organizations to audit who is on their network. 802.1X can support this via RADIUS's accounting and logging capabilities.

OpenSEA Alliance

Some vendors have added proprietary extensions to their commercial 802.1X clients, which don't always work with other 802.1X systems.

The OpenSEA Alliance (www.openseaalliance.org; SEA stands for secure edge access) is trying to address this issue by developing an open source reference implementation of the technology that isn't tied to one 802.1X vendor, OS, or network technology, according to Convery, who is an alliance board member.

"This will allow testing, deployment, and rapid feature development by a larger community of participants than commercial products," he explained.

The alliance says it is trying to promote the use of standards-based 802.1X.

The OpenSEA supplicant is the result of an open source project and will be available for free to users. The licenses will be liberal enough for vendors to use the source code as a reference implementation and incorporate it into their products, noted Gast, who is also an alliance board member.

The organization says that compatibility resulting from the project could increase 802.1X adoption.

The group hopes to release the technology later this year.

802.1X is typically used by medium- to large-sized organizations, said Forrester's Whiteley, because of its complex network requirements and the additional skills necessary to use it. Moreover, these bigger organizations are more likely to need the increased security that 802.1X provides.

"Smaller organizations lack the same drivers," Whiteley added, "but will still move to 802.1X as it matures and becomes better integrated with operating systems, network infrastructure, and policy servers."

Therefore, predicted Core Competence's Phifer, during the next five years, 802.1X will be used on many more wired and wireless networks.

However, Trapeze Networks' Gast cautioned that to be successful in the coming years, 802.1X will have to be implemented correctly in many types of devices such as phones, PDAs, home entertainment equipment, and new products as they come along.

Nonetheless, said Convery, "We've reached a point where 802.1X can be reliably deployed for wired and wireless networks, and the security and regulatory environment we are faced with is demanding this kind of control."

Neal Leavitt *is president of Leavitt Communications (www.leavcom.com), a Fallbrook, California-based international marketing communications company with affiliate offices in Brazil, France, Germany, Hong Kong, India, and the UK. He writes frequently on technology topics and can be reached at neal@leavcom.com.*

Editor: Lee Garber, *Computer*, l.garber@computer.org