Security

Network Security

The following sections describe the different categories of network security.

Identity

Identity is the identification of network users, hosts, applications, services, and resources. Examples of technologies that enable identification include Remote Authentication Dial-In User Service (RADIUS), Kerberos, one-time passwords, digital certificates, smart cards, and directory services.

Perimeter Security

Perimeter security ontrols access to critical network applications, data, and services so that only legitimate users and information can access these assets. Examples include access lists on routers and switches, firewalls, virus scanners, and content filters.

Data Privacy

The ability to provide secure communication is crucial when you must protect information from eavesdropping. Digital encryption technologies and protocols such as Internet Protocol Security (IPSec) are the primary means for protecting data, especially when implementing virtual private networks (VPNs).

Security Monitoring

Regardless of how security is implemented, it is still necessary to monitor a network and its components to ensure that the network remains secure. Network-security monitoring tools and intrusion detection systems (IDSs) provide visibility to the security status of the network.

Policy Management

Tools and technologies are worthless without well-defined security policies. Effective policies balance the imposition of security measures against the productivity gains realized with little security. Centralized policy-management tools that can analyze, interpret, configure, and monitor the state of security policies help consolidate the successful deployment of rational security policies.

A company's network is like any other corporate asset: It is valuable to the success and revenue of that company. More than ever, the corporate computer network is the most valuable asset of many companies. Therefore, it must be protected. Generally, middle- to large-size companies appoint a chief security officer, whose job is to develop and enforce corporate security policies.

Security threats present themselves in many forms:

- A hacker breaking into the network to steal confidential information or destroy corporate data
- A natural disaster such as a fire, tornado, or earthquake destroying computer and network equipment
- A disgruntled employee intentionally trying to modify, steal, or destroy corporate information and devices
- A computer virus
- An act of war or terrorism

Common security threats introduced by people include the following:

- Network packet sniffers
- IP spoofing
- Password attacks
- Distribution of sensitive internal information to external sources
- Man-in-the-middle attacks

Internet security is also a big concern given the exposure of corporate data resources to the publicly accessible Internet. Traditionally, you could achieve security by physically separating corporate networks from public networks. However, with corporate web servers and databases—and the desire to provide access to corporate resources to employees over the Internet—companies must be especially diligent in protecting their networks.

Another recent area for security concern is wireless networking. Traditional networking occurred over physical wires or fibers. However, the current trend is to provide networking services over radio frequencies. Companies are installing wireless networking in their buildings so employees can link to the corporate network from conference rooms and other shared locations from their laptop computers. Additionally, service providers are now offering public wireless Internet services.

Identity and Network Access Control

You can define identity terms of *authentication* and *authorization*:

- A computer or computer user identifies itself to the network or network resources.
- Authorization occurs after authentication. After the computer or user successfully identifies itself, the network or server authorizes the individual or computer to perform certain things with a certain level of access.

802.1x is a link layer protocol used for transporting higher-level authentication protocols defined by the Institute of Electrical and Electronic Engineers (IEEE).

One form of authentication occurs through the exchange of passwords. This form is generally a one-way transaction in which a user or computer identifies itself to a network or server.

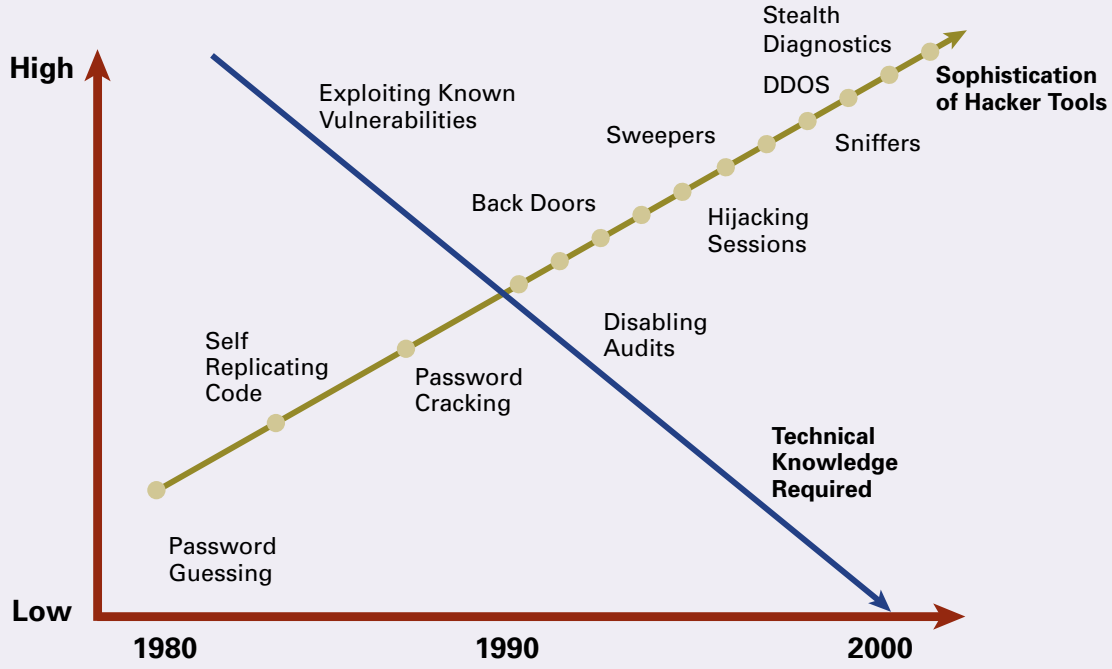
A popular method for securely identifying a machine or individual uses *digital signatures*. For example, if you send an e-mail to someone, he might want to verify that you were indeed the originator of the e-mail. Algorithms such as Secure Hash Algorithm (SHA), Message Digest 5 (MD5) (similar to checksum), and triple Digital Encryption Standard (3DES) encrypt and securely "sign" the message. Then, the sender and receiver match public and private keys. The combination of these methods allows both parties to trust (or not trust) each other when exchanging information.

At-A-Glance—Security

Why Should I Care About Network Security?

A company's network is like any other corporate asset: it has value, it is directly related to the success and revenue of that company, and, as such, it must be protected. One of the primary concerns of network administrators is the security of their network. Security attacks can range from malicious attacks to theft of information to simple misuse of company resources. Estimated losses attributed directly to network intrusions totaled more than $15 billion for 2001.

According to the FBI, the number of network attacks doubled from 2000 to 2001. They are expected to increase another 100 to 150 percent in 2002. It is believed that less than 50 percent of intrusions are actually reported. The majority of unauthorized access and resource misuse continues to come from internal sources. In addition, attacks from external sources continue to grow in number as less sophisticated hackers gain access to information and power tools designed for hacking. The figure below demonstrates this change.



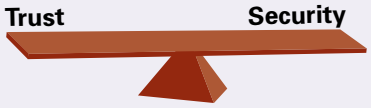
What Are the Problems to Solve?

Security must be an inherent part of every network design based on the principles of protecting from the outside (perimeter security) and controlling the inside (internal security). In other words, keep the outsiders out, and keep the insiders honest. You should think of the network performing the dual roles of "gatekeeper" (perimeter) and a "hall monitor" (internal).

At-A-Glance—Security, Continued

Balancing Trust and Security

Security and trust are opposing concepts. Trust is necessary for applications to run, but open access can expose a network to attacks or misuse. On the other hand, a very restrictive security policy might limit exposure but also reduce productivity. When security is a primary design consideration, you can determine a trust boundary on a per-user basis and strike the proper balance.



Establishing Identity

The first part of any security design is determining who is on the network. Without some knowledge of who the users are, you would have to make the network policies generic so they would likely be too open or too restrictive. Identity can include

- User identity based on password, smart card, fingerprint, etc.
- Device identity (e.g. IP phone) based on Internet Protocol (IP) or Media Access Control (MAC) address.
- Application identity based on IP address or Transmission Control Protocol/User Datagram Protocol (TCP/UDP) port number.

Identity is tightly linked with authentication. After you establish identity, you can apply, monitor, and enforce the proper policy for that user, device, or application.

Perimeter Security

Perimeter security refers to controlling access to critical network applications, data, and services so that only legitimate users and network information can pass through the network. You typically control access with access control lists (ACLs) enabled on edge routers and switches, as well as with dedicated firewall appliances. A *firewall* is a device that permits only authorized traffic to pass (according to a predefined security policy). Other tools, such as virus scanners, content filters, and intrusion detection systems (IDSs), also help control traffic.

Policy Management

As networks grow in size and complexity, the requirement for centralized policy management grows as well. Regardless of the existence of sophisticated tools, companies must employ a sound policy with clear guidelines for enforcement. Generally, middle- to large-size companies appoint a chief security officer whose job is to develop and enforce corporate security policies.

At-A-Glance—Security, Continued

Data Privacy

Much of the information passing through a network is confidential. Whether it is business-specific (engineering or financial) or personnel (human resources correspondence) information, it must be protected from eavesdropping. You can implement encryption and data privacy schemes in Layer 2 (Layer 2 Tunnel Protocol (L2TP)) or Layer 3 (IP Security (IPSec) for encryption), Multiprotocol Label Switching (MPLS) for data privacy). This type of protection is especially important when implementing virtual private networks (VPNs).

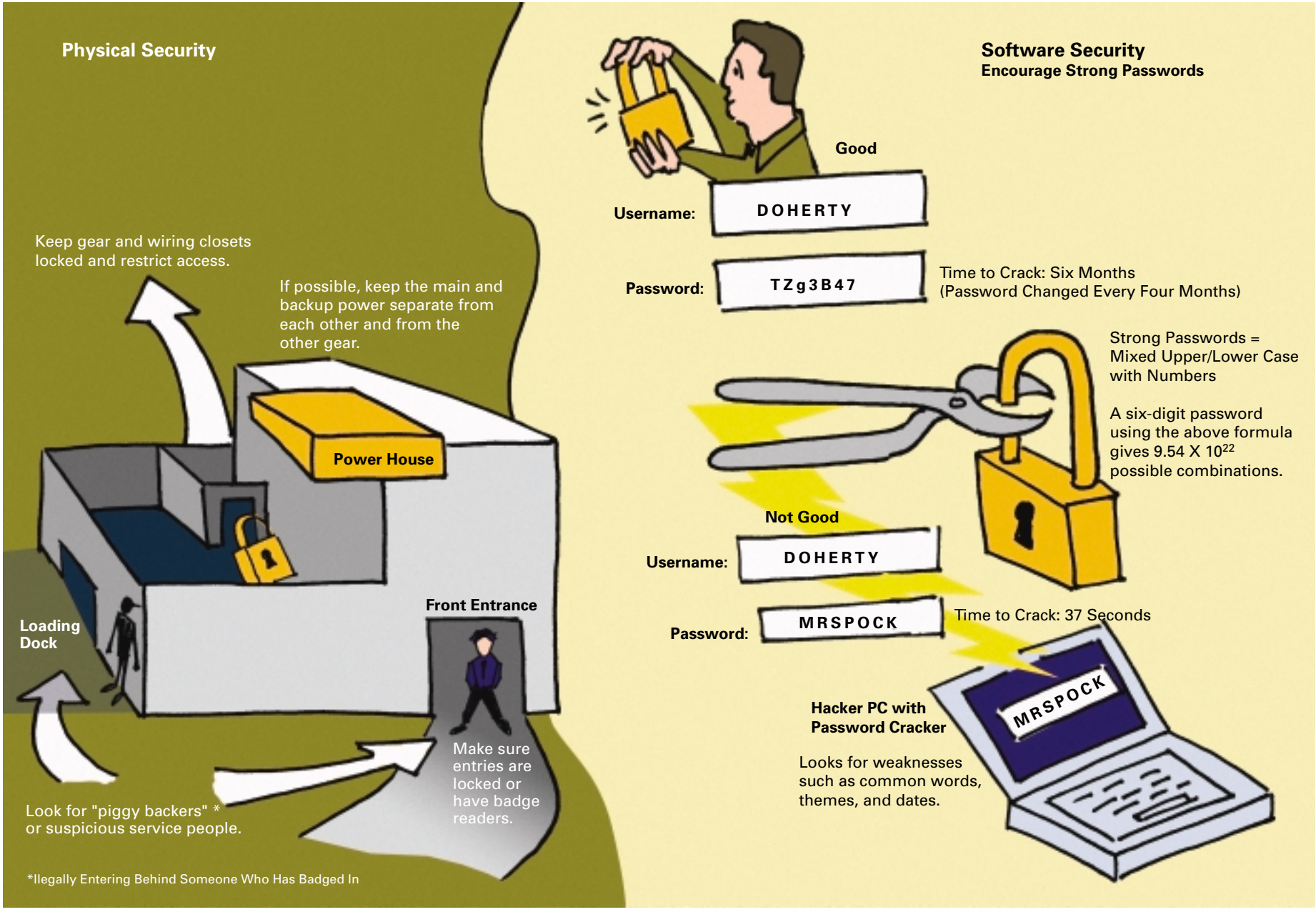
Security Monitoring

Enabling security measures in a network is not enough. Network administrators must regularly test and monitor the state of security solutions. Using a combination of network vulnerability scanners and IDSs, the network administrator can monitor and respond to security threats in real time.

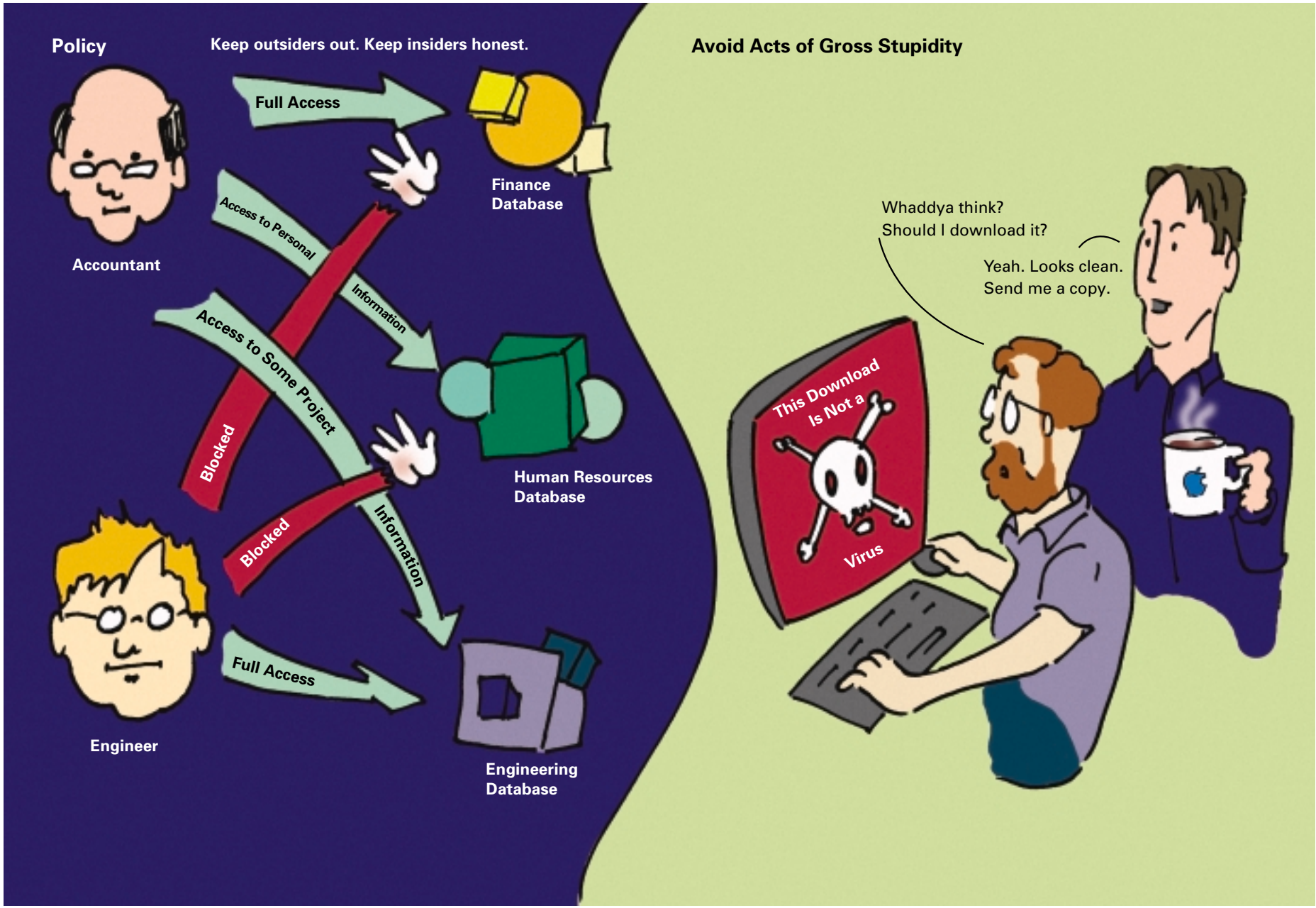
Top 13 Security Vulnerabilities

1. Inadequate router access control.
2. Unsecured and unmonitored remote access points, providing easy access to corporate networks.
3. Information leakage revealing operating-system and application information.
4. Hosts running unnecessary services.
5. Weak, easily guessed, and reused passwords.
6. User or test accounts with excessive privileges.
7. Misconfigured Internet servers, especially for anonymous FTP.
8. Misconfigured firewalls.
9. Software that is outdated, vulnerable, or left in default configurations.
10. Lack of accepted and well-promulgated security policies, procedures, guidelines, and minimum baseline standards.
11. Excessive trust domains in UNIX and NT environments, giving hackers unauthorized access to sensitive systems.
12. Unauthenticated services such as the X Window System.
13. Inadequate logging, monitoring, and detection capabilities.

Comparing Physical and Logical Security



Protecting Networks from Theft and Evil



At-A-Glance—Identity

Why Should I Care About Identity?

The majority of resource misuse and unauthorized access to traditional networks comes from internal sources. Identifying users and devices attempting to access the corporate network is the first step of any security solution.

Validating the *identity* of users and devices can also let network administrators provision services and allocate resources to users based on their job functions.

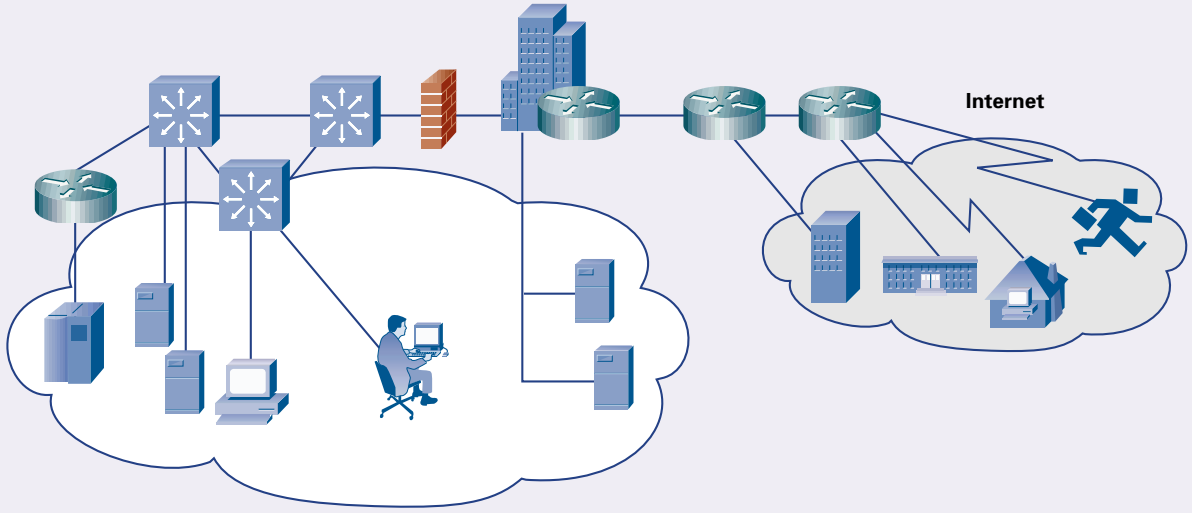
To be truly effective, the security policy must use identity in a way that does not disrupt business or make authorized access prohibitively difficult.

What Are the Problems to Solve?

A comprehensive network-security policy must keep the outsiders out and the insiders honest. Specific goals should be

- Preventing external hackers from having free rein in the network
- Allowing only authorized users into the network
- Preventing network attacks from within
- Providing different layers of access for different kinds of users

Network Security Policy Spans the Network



What Is 802.1x?

802.1x is a set of standards that describe a Layer 2 protocol used for transporting higher-level authentication protocols. It is language used to carry the information payload (e.g. name and password) between an endpoint (client) and the authenticator (server).

802.1x Header	EAP Payload

Extensible Authentication Protocol

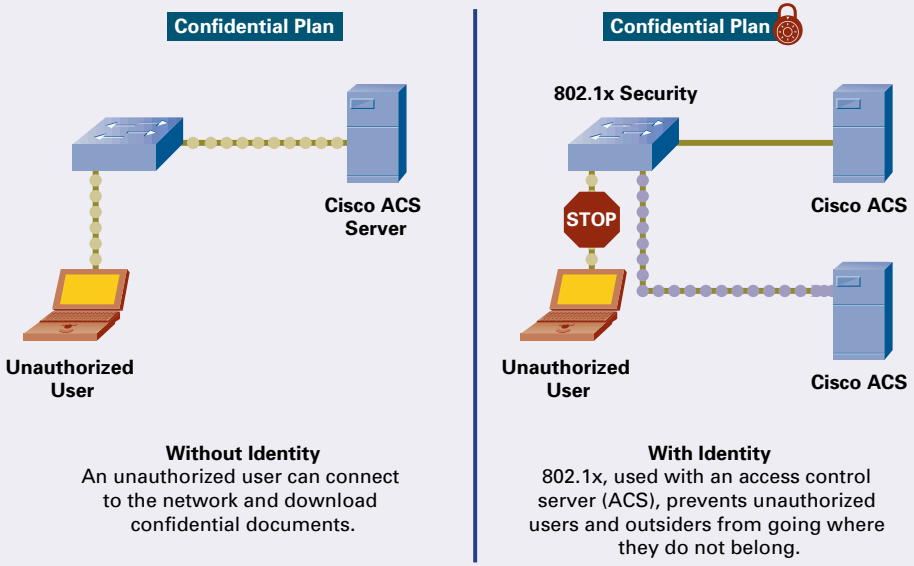
The *Extensible Authentication Protocol (EAP)* is a flexible protocol that carries authentication information. The authentication information can include user passwords or predefined security keys.

The EAP typically rides on top of another protocol, such as 802.1x or Remote Authentication Dial-In User Service (RADIUS), which carries the authentication information between the client and the authenticating authority.

At-A-Glance—Benefits of Identity

What Does Identity Do for Me?

Identity not only prevents unauthorized access, but it also lets you know who and where your insiders are. After you know who is on the network, you can apply policies on a per-user basis. This solid, comprehensive security solution actually enhances the usability of the network rather than reduce it. Some examples of the advantages of an identity-based security solution appear in the following figure.



Without Identity
An unauthorized user can connect to the network and download confidential documents.

With Identity
802.1x, used with an access control server (ACS), prevents unauthorized users and outsiders from going where they do not belong.

Preventing Unwanted Access

Limiting Access to Networked Resources

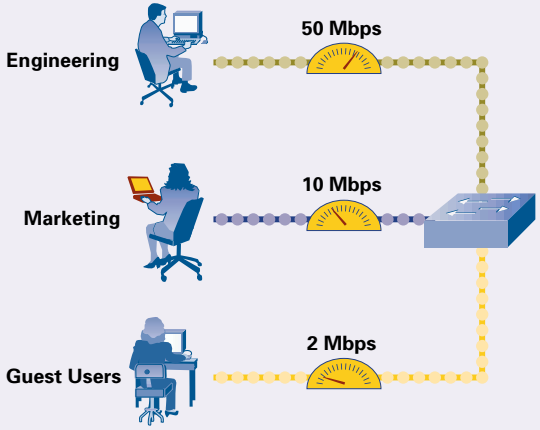
With Identity
By using 802.1x with extensions, you can specify which networked resources the user can access. For example, only managers have access to HR information.

Without Identity
Access to Human Resources databases and other sensitive material is available to all employees.

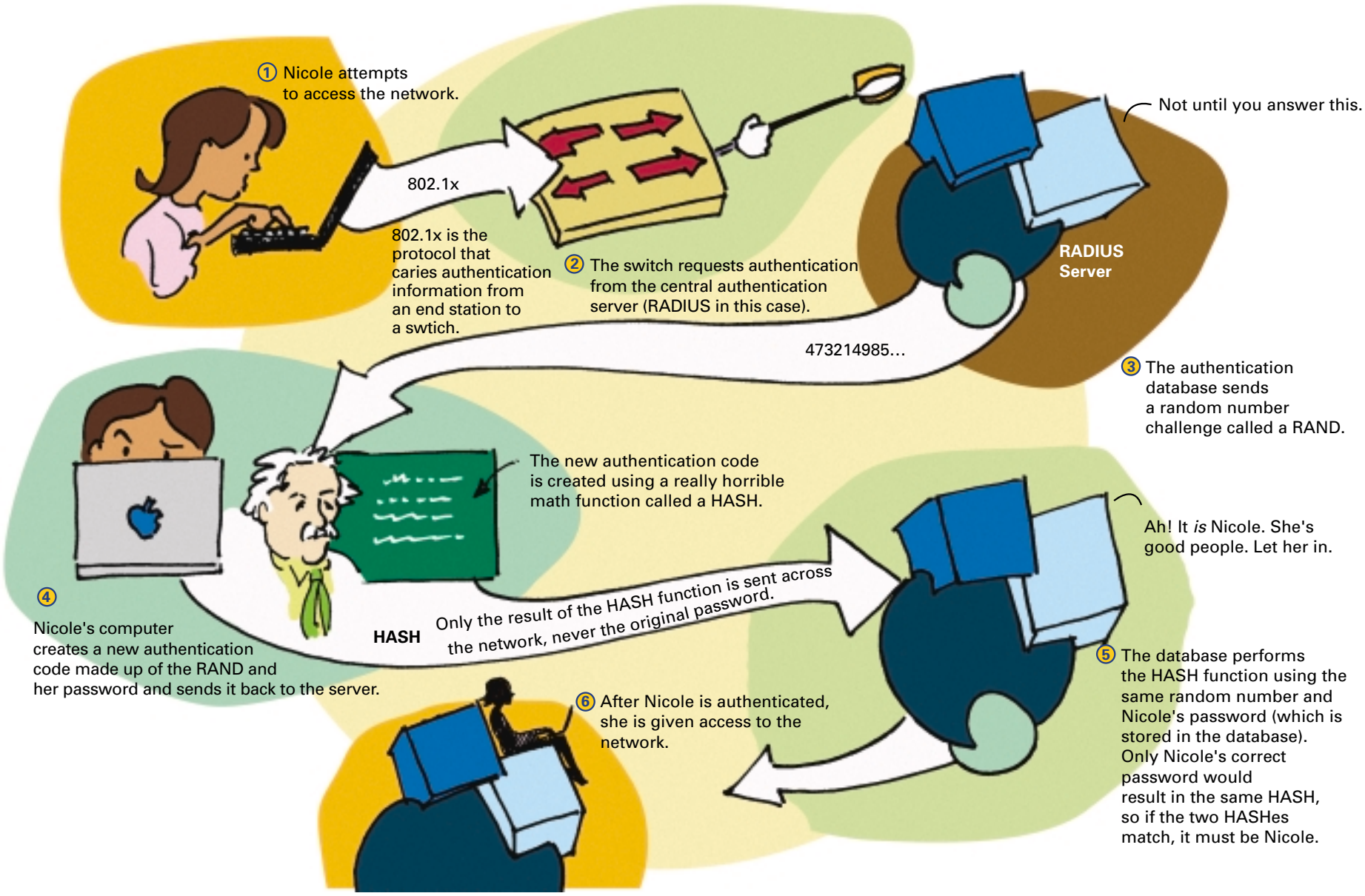
User-Based Service Provisioning

Without Identity
Hackers or malicious insiders might try to crash a network by overloading it with requests and traffic.

With Identity
By using 802.1x, the switch can allocate bandwidth and other services on a case-by-case basis. You can deal with an abuse quickly and easily.



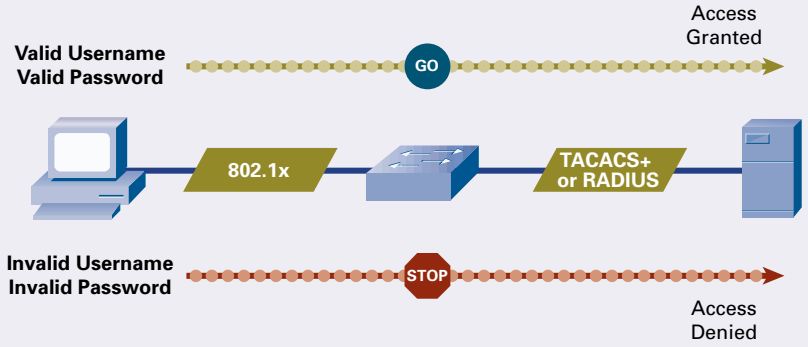
Authentication



At-A-Glance—Authentication Servers

Working with Authentication Servers

802.1x is only half of the identity story. A service must authenticate the information carried by 802.1x. This authentication can come from name and password validation using a RADIUS or Terminal Access Controller Access Control System (TACACS) server or from digital signatures confirmed by a third-party validation service such as public-key infrastructure (PKI).



RADIUS

RADIUS is a protocol that communicates between a network device and an authentication server or database. RADIUS allows a network device to securely pass login and authentication information (username/password), as well as arbitrary value pairs using vendor-specific attributes (VSAs). RADIUS can also act as a transport for EAP messages. RADIUS refers to the server and the protocol.

PKI

PKI provides identity authentication between two parties via a trusted third party. A PKI certificate is "proof" of identity signed by the third party. It is the network equivalent of a valid passport trusted by the customs agents of other countries. Just as a passport signed by the passport office states your verified identity and citizenship, a PKI certificate signed by a certificate authority states your verified identity and network associations. Unlike passports, PKI certificates can't be forged.