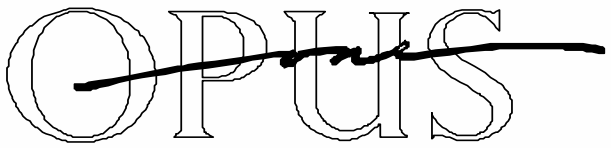
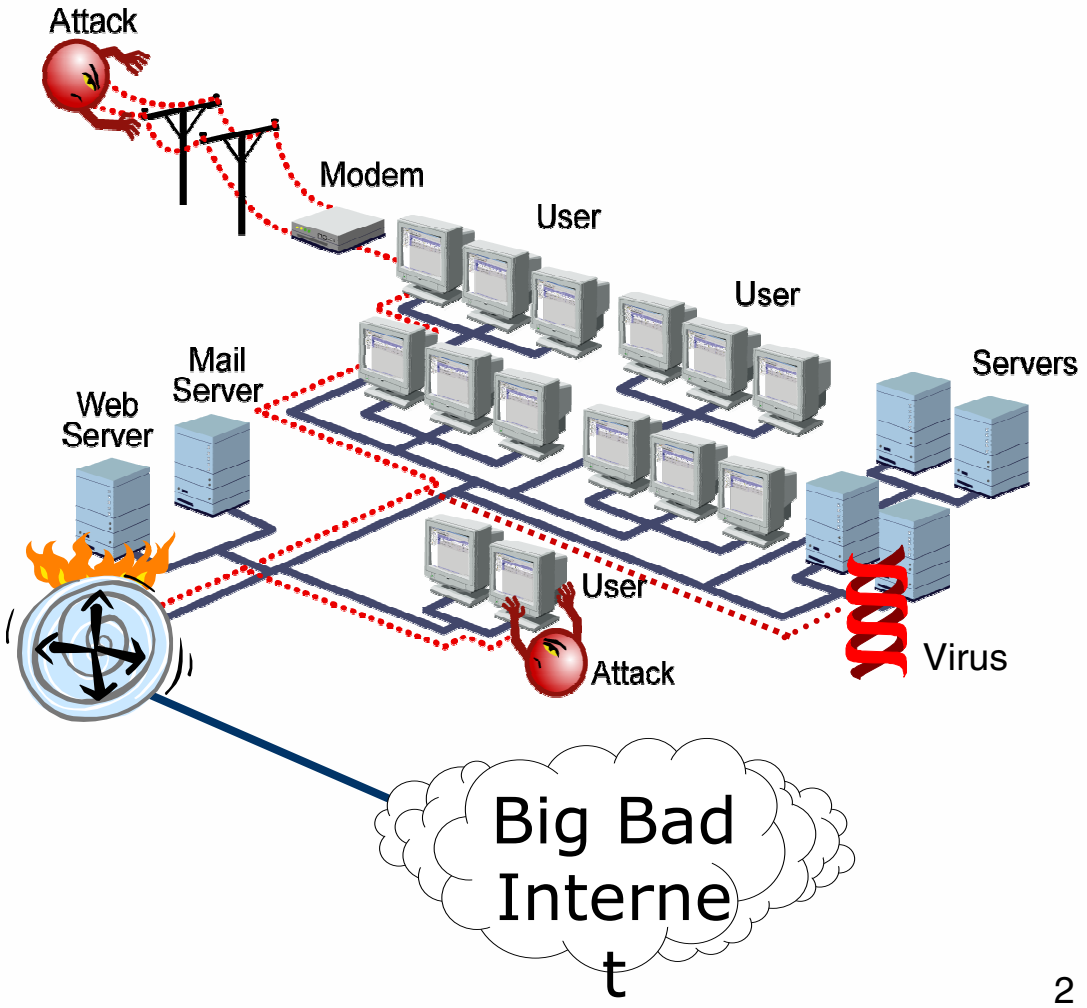
Layered Access Control-Six Defenses That Work

Joel M Snyder
Senior Partner
Opus One, Inc.
jms@opus1.com

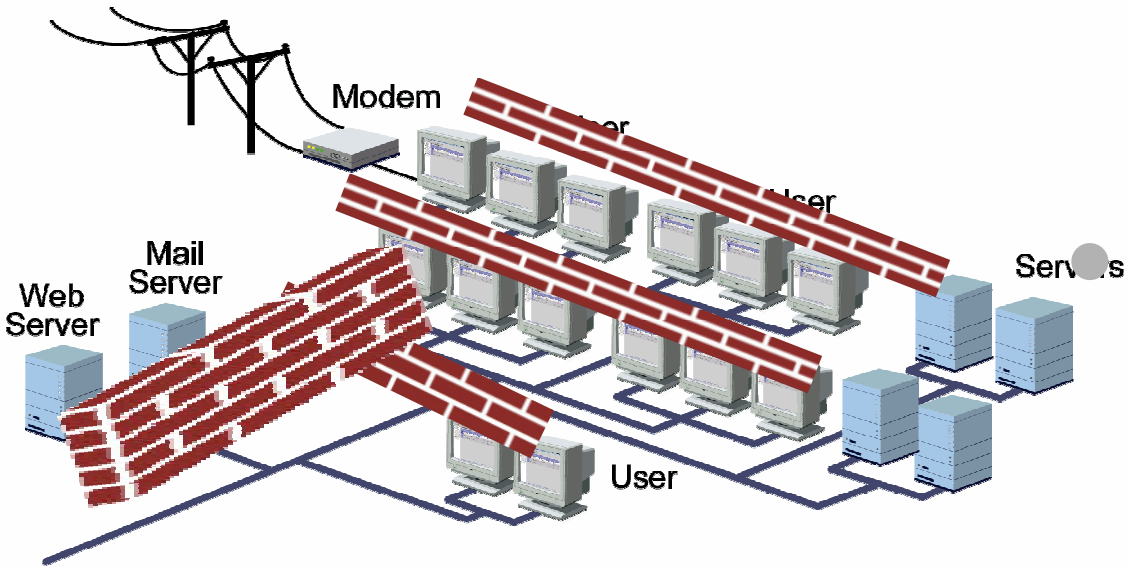


Perimeter defense has its flaws

- **"Protecting your network with a perimeter firewall is like putting a stake in the middle of a field and expecting the other team to run into it."**
- **#include <statistic on insider break-in percent>**
- **"If your position is invisible, the most carefully concealed spies will not be able to get a look at it." (Sun-Tzu)**



Defense-in-Depth is the alternative



- **Make the network "crunchy," not soft and chewy throughout**
- **Turn the network inside-out: the security is on the inside, not on the outside**

Here are Six Strategies you can use as guideposts for Defense in Depth

Strategy 1: **Authenticate and Authorize all Network Users**

Strategy 2: **Deploy VLANs for traffic separation and coarse-grained security**

Strategy 3: **Use stateful firewall technology at the port level for fine-grained security**

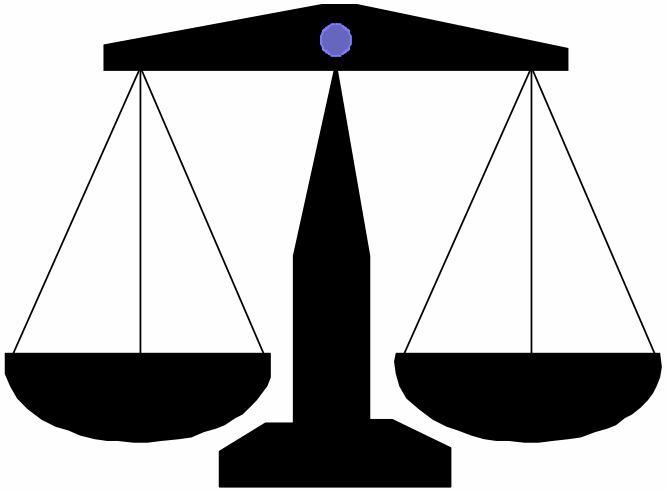
Strategy 4: **Place encryption throughout the network to ensure privacy**

Strategy 5: **Detect threats to the integrity of the network and remediate them**

Strategy 6: **Include end-point security in policy-based enforcement**

You are not being given the Holy Gospel

- **These are strategies that you can mix and match as appropriate to your own network and your own requirements!**

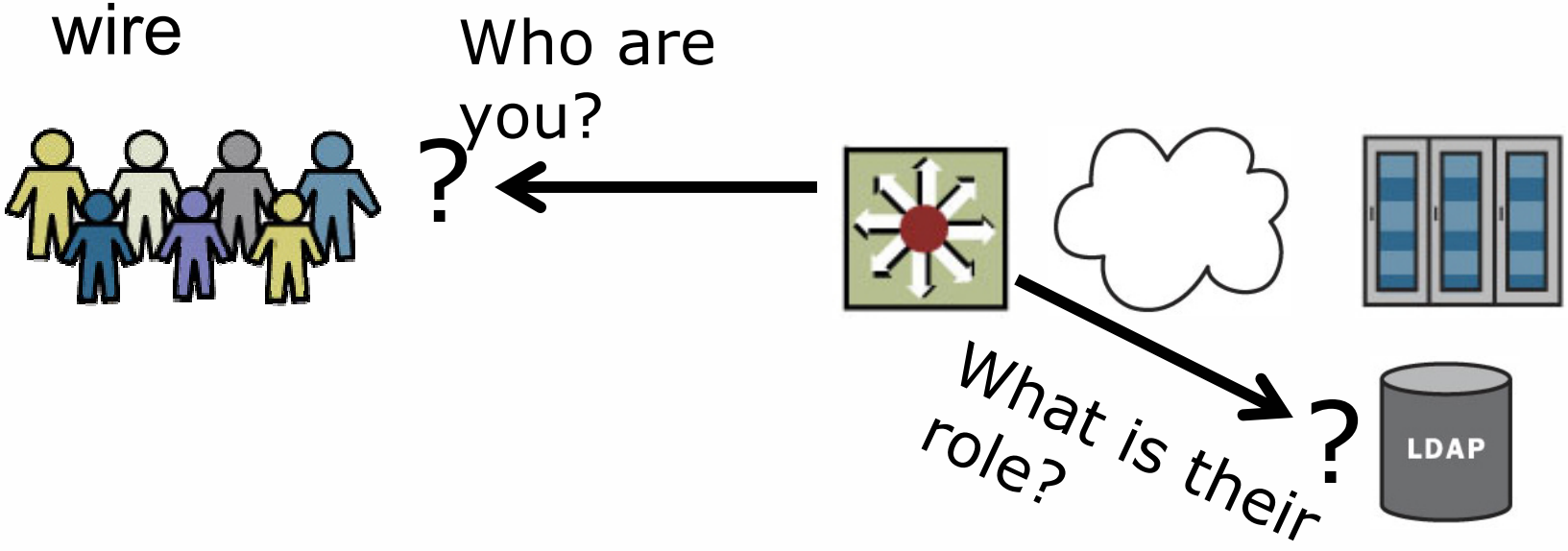


How "secure" is this network? Is it "more secure" than it was? Is it "secure enough" for our business?

- **Adding defense in depth to a network is as much policy and procedures as it is hardware and software**

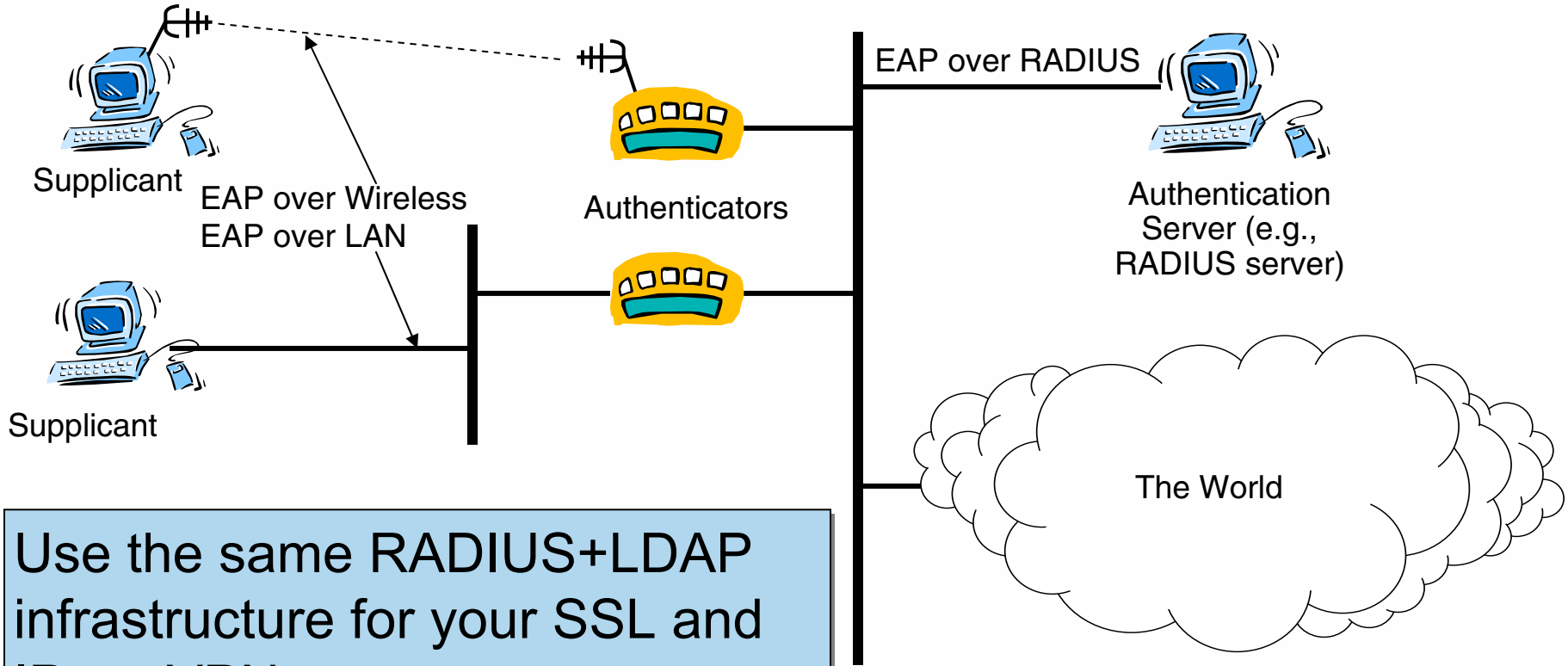
Strategy 1: Authenticate and Authorize all Network Users

- You need to know who is on the other end of the wire



Once you know *who* you can define *authorization*

802.1X Provides a standards-based approach for authentication and authorization



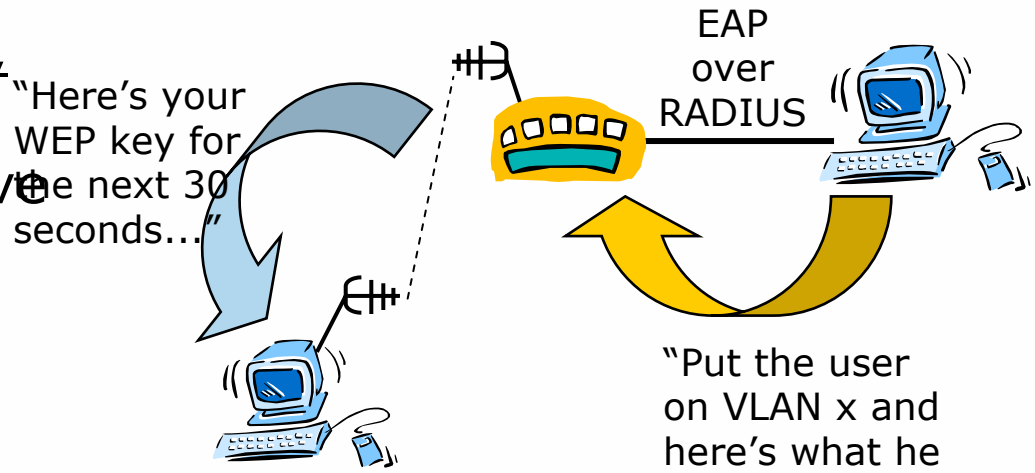
Use the same RADIUS+LDAP infrastructure for your SSL and IPsec VPN users

802.1X on every port adds security

- In the wireless environment, 802.1X is absolutely required
  - 802.11i and WPA (Wi-Fi Protected Access) use 802.1X
  - Pure 802.1X for authentication solves most WEP problems
- In the wired environment, 802.1X adds security
  - Microsoft and Apple give it to you for free

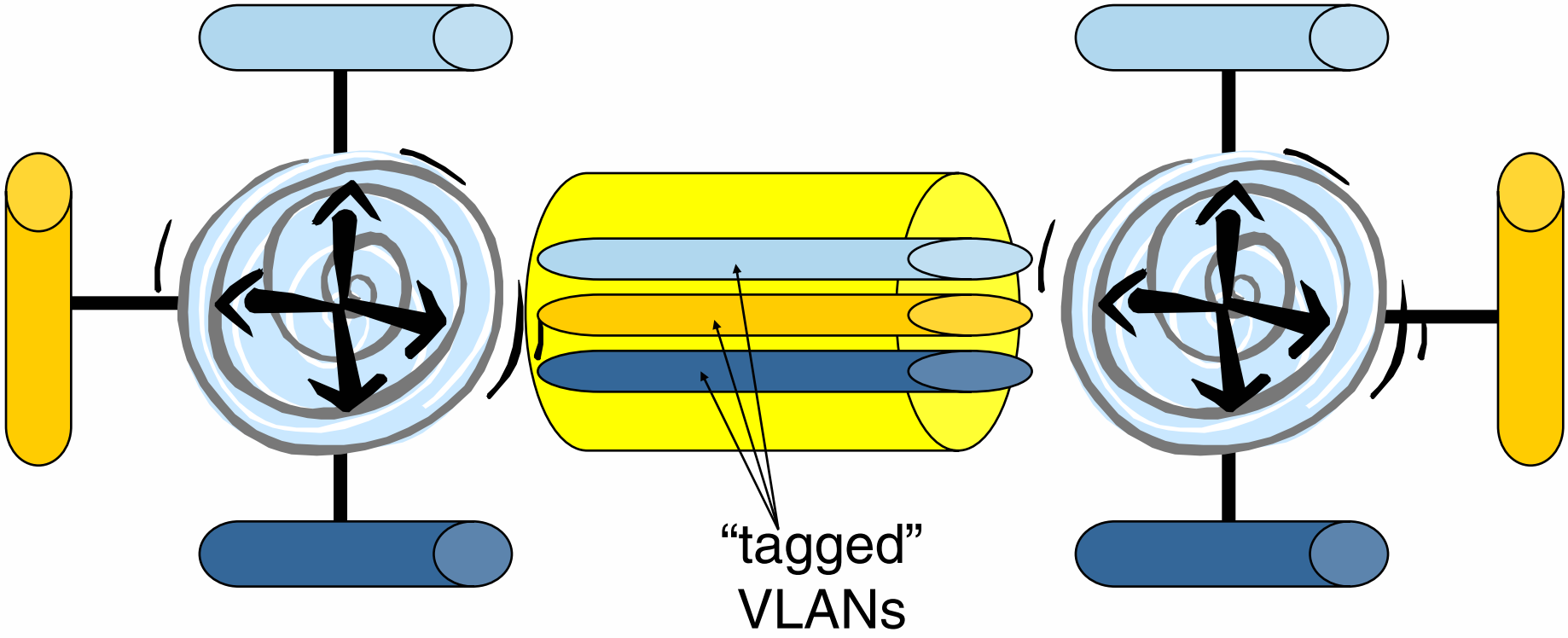
Captive Portals are so very 20th century…

- 802.1X ties to RADIUS which means…
  - You can use RADIUS to push authorization information to wired and wireless equipment
    - VLANs & Filters



Strategy 2:
Use VLANs for coarse-grained security

- **802.1q VLANs are present on all modern switches**



VLANs can be used as security barriers

- **"Coarse Grained" means you don't want too many of them**

Enterprise VLAN Assignments
Outside the firewall
Trusted Internal User
High Security Zone
Remediation Zone
VoIP Services

Using VLANs for security has its risks

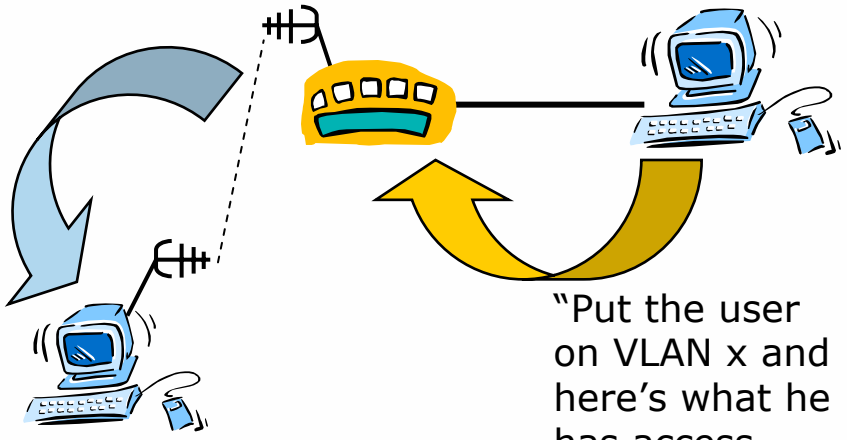
- If packets jump from one VLAN to the other… the game is over
- Management of switching infrastructure is now as important as management of firewalls
- Your switches are your weak links
  - Attacks
  - Bugs

Key to successful use of VLANs is dynamic assignment

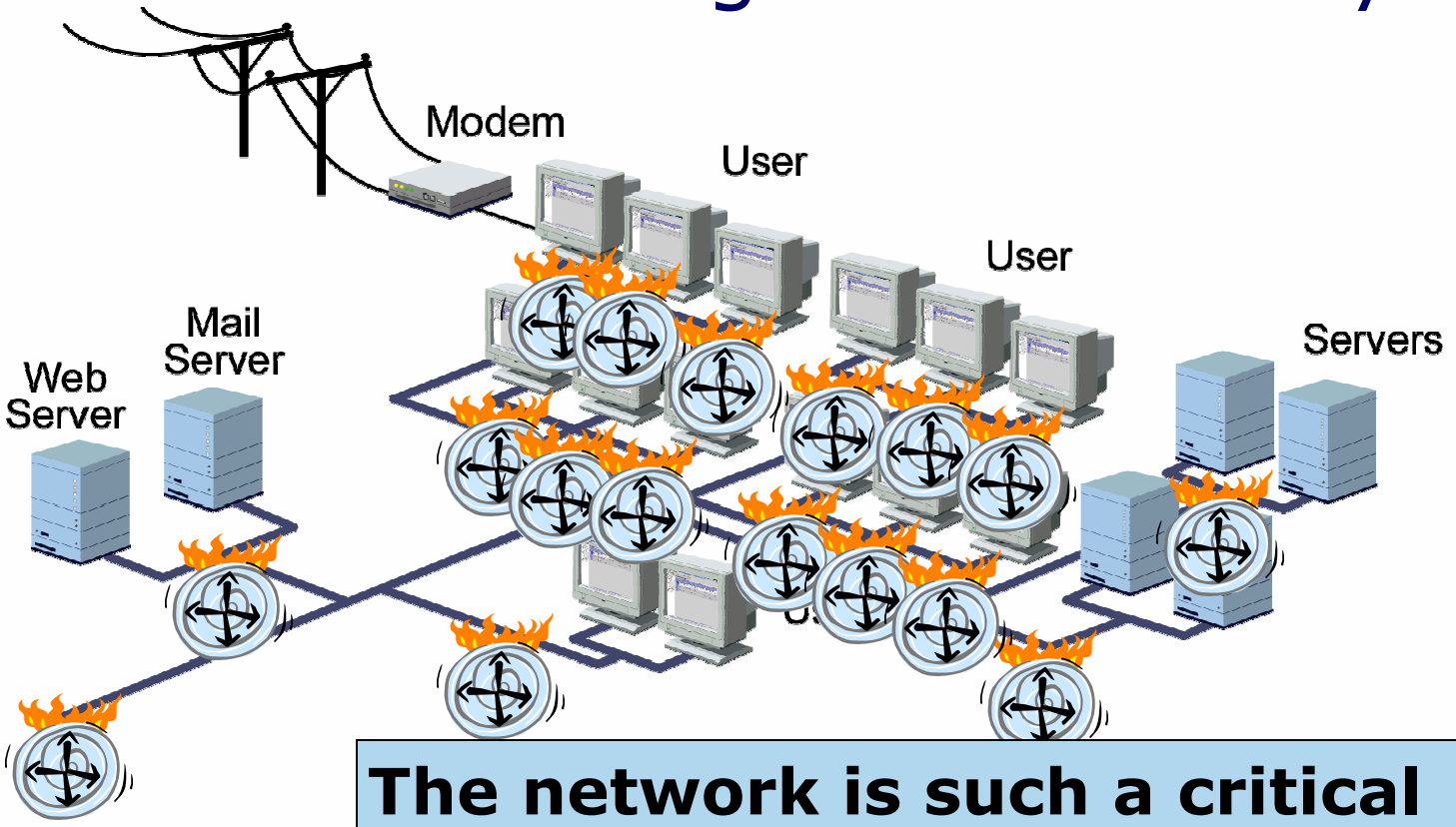
If you have authenticated your users…
… you can have authorization information …
Which Tells You What VLAN They Go On!

Other Strategies

- based on end-point security status (see strategy 6)
- based on lack of authentication



Strategy 3:
Use firewalls for fine-grained security



The network is such a critical resource, it needs to be protected down to the port level

Management and Economics challenge the use of Firewalls within the Network

How are you going to define policy?

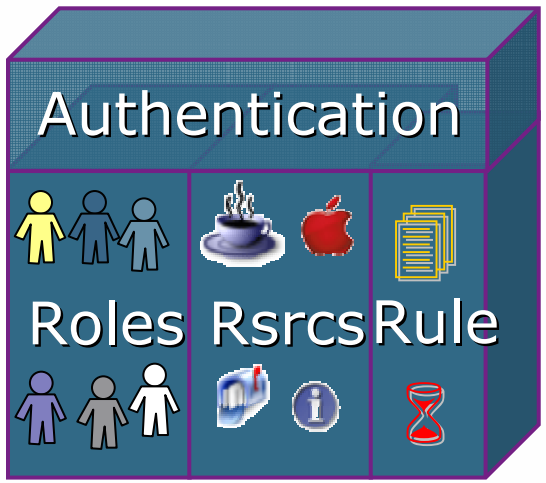
- **How are you going to bind policy to an authenticating user?**
- **Answer: role-based management of users**

How can you afford to buy a thousand ports of firewall?

- **How can we get firewalls with dozens and hundreds of ports in them?**
- **Answer: the price is coming down faster than you can imagine**

The Key strategy for Internal Firewalls: Use Role-based and Resource-based Policy

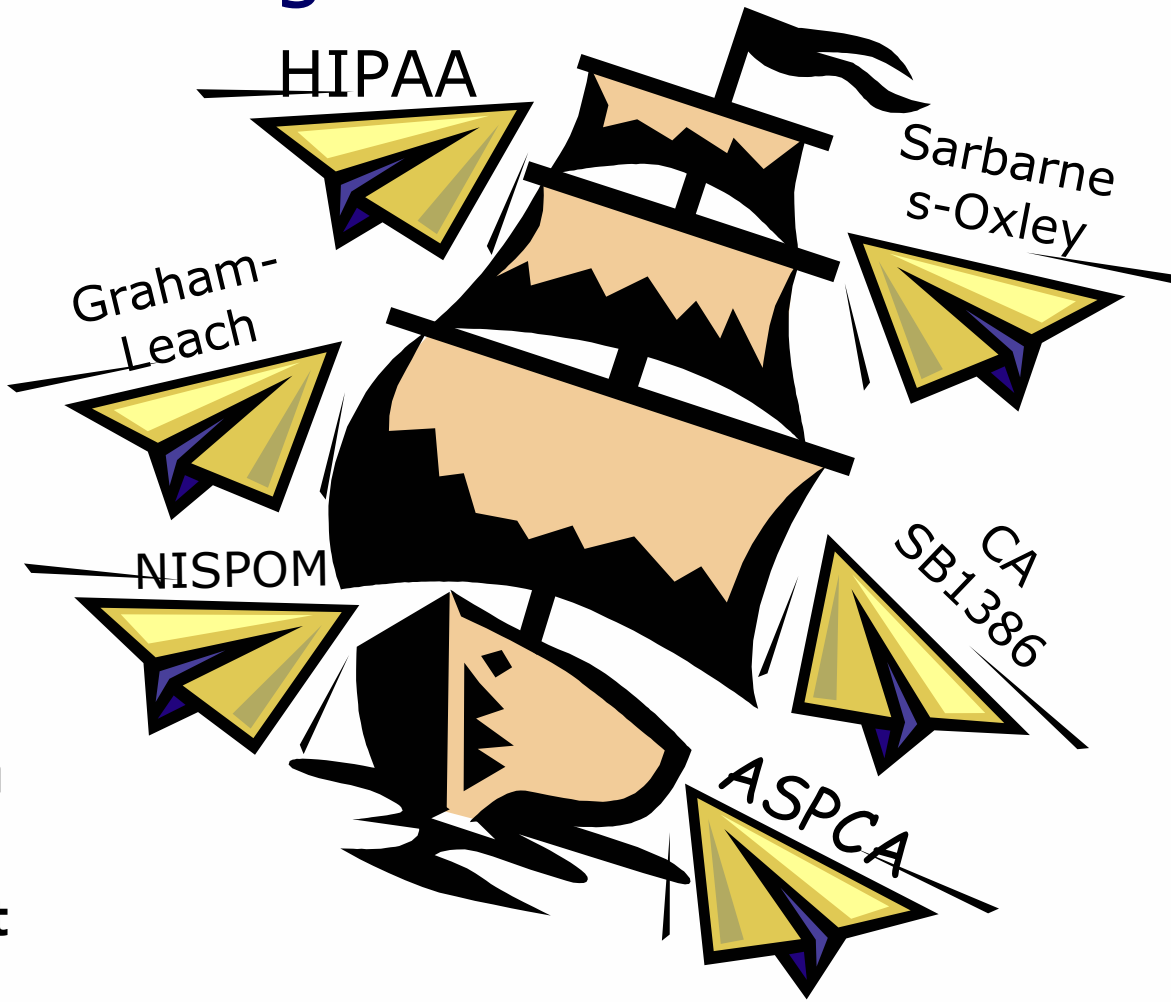
- **Define policy first**
- **Define policy first**
- **Define policy first**
- **Start with your wireless network as a test of the technology**



- **Use a combination of port-based firewalls and VLANs as appropriate**
- **If an "intermediate" solution is right for you, jump on it!**

Strategy 4:
Place encryption throughout the network

- **Wireless Network?**
  - **You should be encrypting!**
- **Remote Access Network?**
  - **You should be encrypting!**
- **Wired network in a building?**
  - **You still might want to encrypt!**

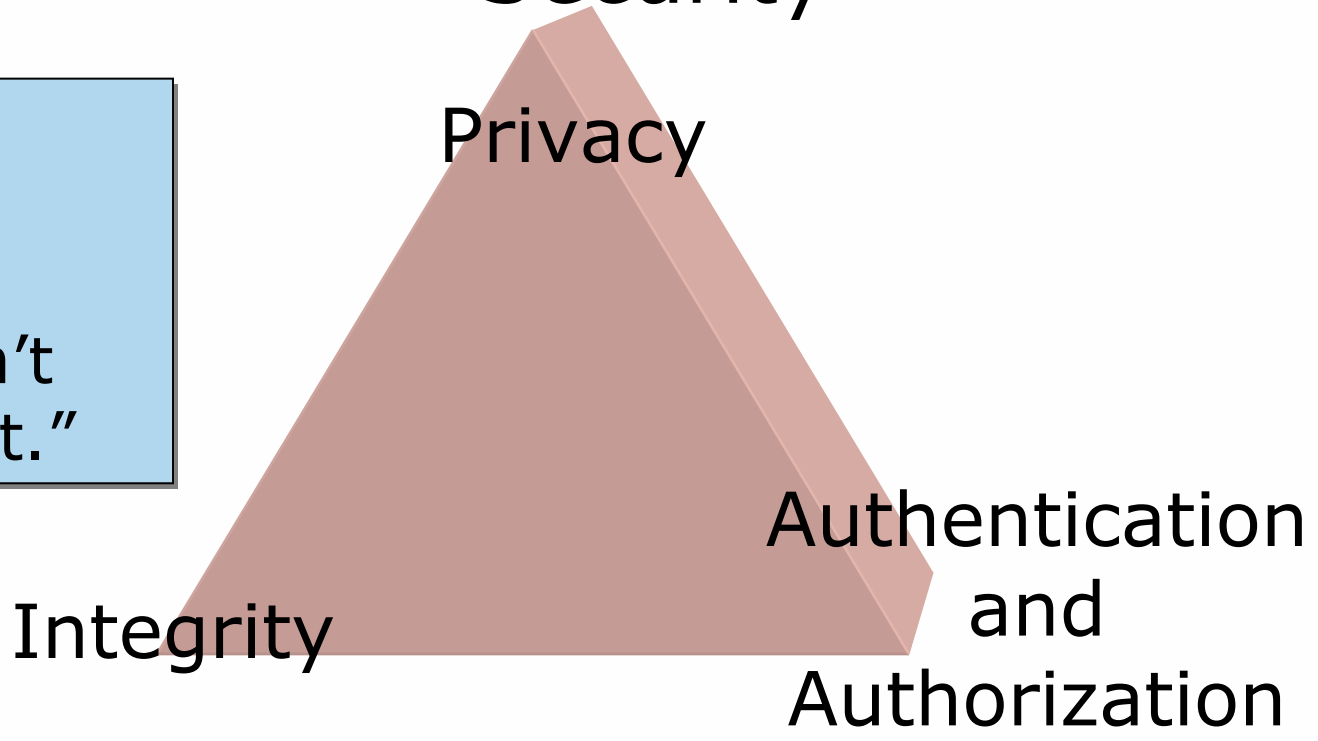


Encrypt where needed and in the right way

Environment	Common Solutions
All Wireless	802.11i combined with 802.1X using either TKIP or AES encryption; VPN protocol to VPN concentrator
Server to Server Wired	IPsec in transport or tunnel mode between servers or server farm subnets
Client to Server Wired	Application Layer Encryption (SSL); link-layer encryption in building
Client to Remote Access Server	VPN protocol such as IPsec or SSL to corporate VPN gateway

Strategy 5:
Detect threats to the network and remediate

The Rodney Dangerfield Corollary: "Integrity don't get no respect."



Detecting threats seems to be on everyone's mind

Detection and remediation can ensure network integrity

Key strategy: Identify greatest areas of risk and concentrate on those first

- **Example: trojan horses, viruses, and malware**
  - **Enormous risk**
  - **Enormous potential for loss**
  - **Risk of infection is high**

Key strategy: Focus on technologies that have the lowest cost (capital and operations)

- **Example: firewalls with built-in IPS technology**
  - **Low cost**
  - **Moderate tuning**
  - **Operationally easy**

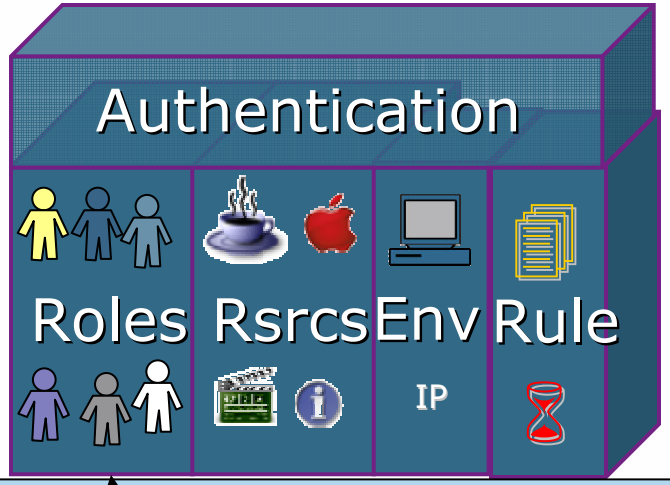
Strategy 6: Include end-point security in policy

- **The hot topic for 2005 is "End Point Security"!**

This issue came to the front with SSL VPN and now everyone is on the bandwagon

Vendor	Buzzword
Cisco	CSA + CCA + CTA + Network Admission Control
Check Point	Total Access Protection
Microsoft	Network Access Protection
Juniper	Juniper End-Point Defense Initiative

End point security adds a column to the access control tuple



Derived zone based on various attributes.
Like groups, but based on security posture assessment.

Your guideposts for adding Defense-in-Depth

Strategy	Technology
Authenticate and Authorize everyone	**802.1X, RADIUS + LDAP**
VLANs for traffic separation and coarse-grained security	**VLANs, 802.1X**
Stateful firewall for fine-grained security	**High-density firewalls, 802.1X**
Encryption for privacy	**802.11i (Wireless); IPsec/SSL/TLS (Wired/remote access); others…**
Detect Threats and Remediate to insure integrity	**IPS/IDS and derivations (IPS-in-firewall, *e.g.*)**
Add end-point security to policy enforcement	**In flux. Watch closely.**

Audience response

- **Questions?**