



ARCHITECTS OF AN INTERNET WORLD

Smart Cards, Biometrics and Tokens for VLANs and Subnet Access



Jeff Hayes

Director, Security Programs
Alcatel e-Business Networking Division
<jeff.hayes@alcatel.com>



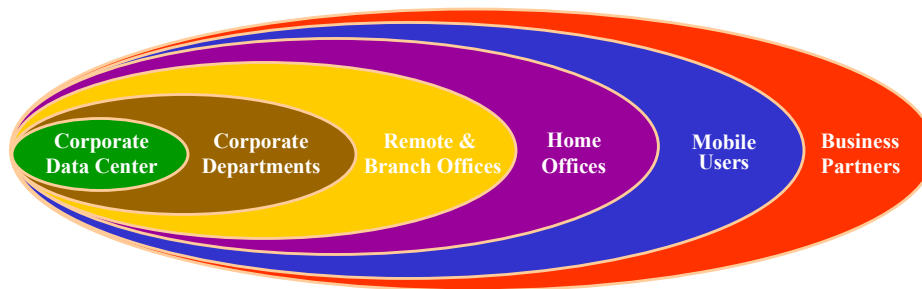
Agenda

- LAN Access Issues and Requirements
- Authentication vs Authorization
- Strong Authentication
 - Tokens
 - Smart cards
 - Biometrics
- Tying it all together
- Case Studies



LAN Access Issues and Requirements (1)

- Networks are topographically layered
- However security usually does not follow this model
 - Most networks follow the “crunchy on the outside, chewy on the inside” mantra
- As applications are accessed on a least-privileged basis, network access should follow suit

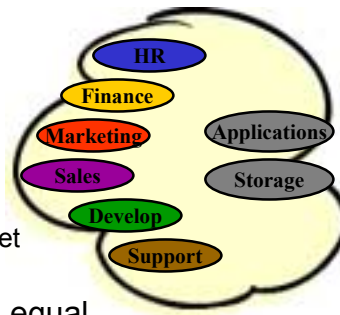


ACSAC 12/01 – slides 3



LAN Access Issues and Requirements (2)

- Most networks are segmented
 - Flat networks implement VLANs
 - Control broadcasts
 - Simplify management
 - Routed networks implement subnets
 - Logical partitioning, better control
 - Often use VLANs within the subnet
- All LAN segments are not created equal
 - Differentiated user groups
 - Family jewels
- Some users require mobility
 - Intra-campus mobility (job driven)
 - Ad hoc connections (temps, visitors, contractors)



ACSAC 12/01 – slides 4



- Network access for the local users starts at the switch port
 - If I have access to the switch port, am I allowed to access the network?
 - What damage can I do with an active LAN port?
- The switch port can limit access to
 - Ports (IEEE 802.1X)
 - VLANs (IETF 802.1X RADIUS usage guidelines)
 - Subnets (dynamic IP rules / Authenticated ACL)



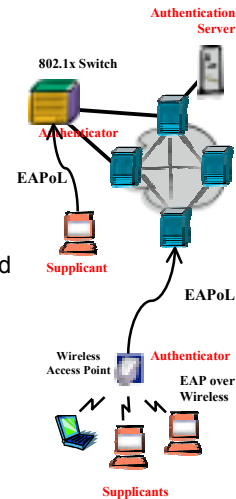
- Authentication = identity assurance
 - Smart cards, biometrics, tokens provide strong authentication
 - You have proven to me that you are who you say you are
- Authorization = access privilege
 - RADIUS, DIAMETER, and LDAP-based Directory Servers provide authentication and authorization (and accounting) - AAA
 - I know who you are, now you can only do the following, and I will track what you do and when you do it
- AAA provides fine-grain access control within a finite domain of control
 - Hosts
 - Applications
 - Networks

Implement network access based on a layered approach



Port-Based Network Access 802.1X

- User's device is granted access through the switch port after the user authenticates
- Defined by IEEE 802.1X
 - supplement to IEEE 802.1D
 - IETF defines RADIUS usage guidelines
 - Works with Ethernet and wireless networks
- Based on the all or nothing notion
 - If port is 802.1X port, then authentication is required prior to opening port for normal communication
 - If port is not 802.1X port, port is open by default
- Requires a client application
 - Microsoft XP
 - other 3rd party clients for non-XP systems
- Secure password
 - MD5
 - EAP / TLS

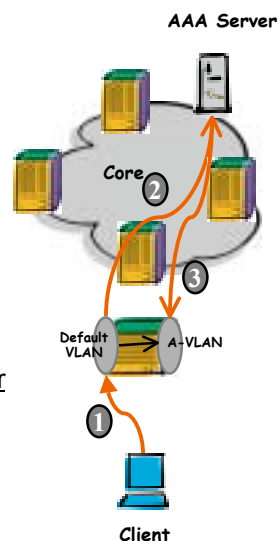


ACSAC 12.01 – slides 7



Authenticated Layer 2 Access VLAN

- User's device is granted access to a specific VLAN through the switch port the user's device is attached after the user authenticates
- Grants permissions based on the user's identity, not on the device characteristics
 - The user's MAC is moved from the default VLAN to an authorized one
- Leverages common AAA systems
 - RADIUS, DIAMETER, LDAP DS
- Supplement AAA system with strong 2-factor authentication techniques
 - Smart cards, Biometrics, Tokens
- Requires client software
 - Shim software or HTTP/Java
 - Must deal with boot issues (DHCP)

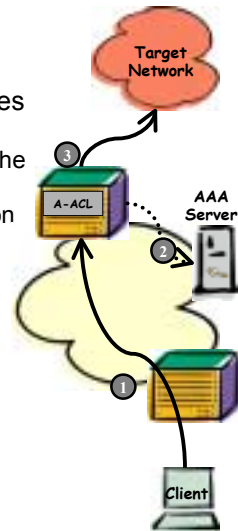


ACSAC 12.01 – slides 8



Authenticated Layer 3 Access Subnet or Host

- Dynamically create access rule when the source address is not pre-configured in the router/switch
- Dynamic access rule (ACL) created after user goes through an authentication process
 - Client initiates request with the adjacent switch to the network to which is being protected/desired
 - Works like real firewalls with dynamic authentication
- Leverage most common AAA servers
 - RADIUS, DIAMETER, LDAP
 - Could be extended with 2-factor authentication
- Can be extended to a network / directory-based implementation
 - Not on a device basis
- Potentially easy to use
 - If based on HTTP/Java-based client-to-switch dialogue



ACSAC 12.01 – slides 9



Strong Authentication

- Proper identification and authentication is the basis for computer and network security
- Passwords – most used and most abused
 - clear vs encrypted / transmitted vs stored
 - easy to guess/attack vs frequency of change
 - Bruce Schneier stated in May 2001
 - “You can’t memorize good enough passwords any more, so don’t bother
 - Create long random passwords, and write them down
 - Store them in your wallet, or in a program like Password Safe. Guard them as you would your cash
 - Don’t let Web browsers store passwords for you
 - Don’t transmit passwords (or PINs) in unencrypted e-mail and Web forms
 - Assume that all PINs can be easily broken, and plan accordingly”
- Stronger methods exist and should be used
 - Most based on two of the three: something you know (PIN), something you possess (card), something you are (biometric)
 - Tokens and proximity cards
 - Smart cards
 - Biometrics
 - Single sign-on? Yea, right



ACSAC 12.01 – slides 10



Smart cards

- Authentication based on something you know and something you possess
 - Card and PIN
- Smarts vary technically
 - Simple magnetic stripe to embedded CPU with on-board encryption
 - Many tied to PKI – using certificates
 - Multiple systems - physical facilities and network
- Usage varies by country / region
 - Very common in Europe
 - Getting common in Asia/Pac
 - On the verge in North America
- Deployment obstacles
 - Cost
 - Reader deployment
 - Lost cards



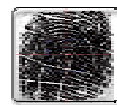
<http://www.scia.org/>

ACSAC 12.01 – slides 11



Biometrics

- Authentication based on something you are
 - Often tied to user ID / PIN
- Lots of products
 - Last count over 300 companies, not a lot of revenue
- Technology
 - Crossover issues - false acceptance and false rejections
 - Strength and weaknesses of technologies (strong to weak)
 - Palm & Hand
 - Iris & Retina
 - Fingerprint
 - Voice
 - Face
 - Keystrokes
- Deployment obstacles
 - Cost
 - Confidentiality
 - User willingness



<http://www.biometrics.org/html/sites.html>

ACSAC 12.01 – slides 12



Tokens

- Authentication based on something you know and something you possess
 - Hard or soft token and a PIN
 - Often referred to as one-time password systems
- Widely accepted
 - At least 5 leading companies
 - Established technology
 - Easy to use
- Technology
 - Challenge/Response
 - Time Synchronization
- Deployment obstacles
 - Battery life
 - Costly in large deployments
 - Lost hard tokens
 - Soft tokens hackable

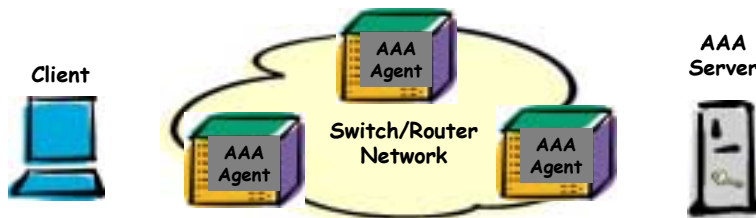


ACSAC 12.01 – slides 13



Tying It All Together

- Target desired element of network
 - Port, VLAN, IP network / host
- User two-factor authentication to identify user
 - Smart card, biometric, token
- Switch leverages the AAA server to provide disposition for user
 - Authorization to desired target
- Accounting logs record actions

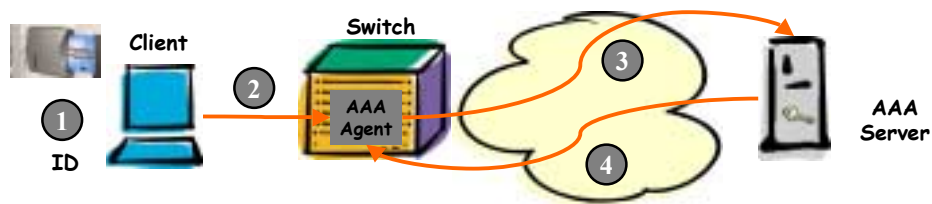


ACSAC 12.01 – slides 14



Authenticated VLANs and Smart card – Case 1

- University medical facility
- Require physical access to parking/buildings as well as network
- Each card has a certificate for authentication
- Client application obtains authorization from AAA
- User gets access to VLAN based on pre-defined privileges/access rules

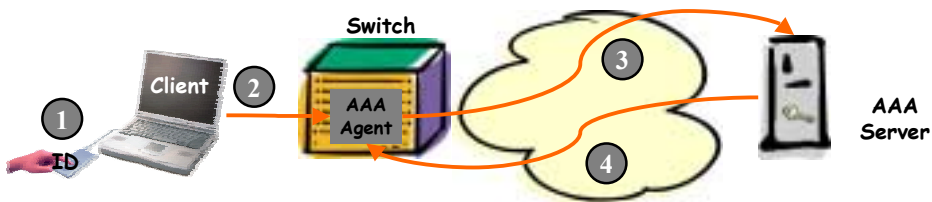


ACSAC 12.01 – slides 15



Authenticated VLANs and Biometrics – Case 2

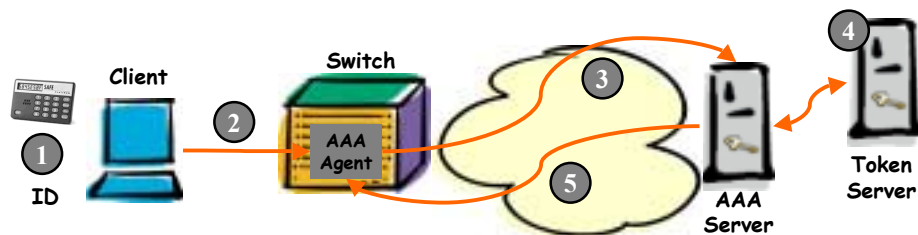
- International manufacturer
- Requires biometric to gain access to VLAN without entering ID/pswd
- Fingerprint ID unit pre-programmed with userID and password; stored locally on unit
- User IDs to FIU which is connected to USB port which activates client script which logs user into VLAN



ACSAC 12.01 – slides 16



- Local government
- Requires one-time password access to VLAN for high-security workers
- RADIUS AAA server facilitates challenge/response authentication
- RADIUS AAA server authorizes user to access VLAN and accounts for activity



ACSAC 12.01 – slides 17



- LAN Access Issues and Requirements
- Authentication vs Authorization
- Strong Authentication
 - Tokens
 - Smart cards
 - Biometrics
- Tying it all together
- Case Studies

Layered networks require layered security. It starts at the switch port. It secures port access, VLAN access, and access between VLANs and subnets

ACSAC 12.01 – slides 18