Network Security Stripped
from layered technologies to bare essentials

Jennifer Jabbusch, CISSP, HP MASE, JNCIA-AC

Trends for 2009
CAUTION

This presentation contains technical information not included in the slide presentation. If you did not hear the presentation live... you’re missing all the good stuff. Sorry. 😊
For over 25 years, Carolina Advanced Digital, Inc. has offered the highest level of engineering expertise in support of all enterprise sectors. Serving government, education and commercial customers, CAD focuses on IT infrastructure, security and management. The company helps customers guard their core network, ensuring network security and availability of critical data. Find us at http://cadinc.com.
About Us
About Us

Jennifer has over 15 years experience working in various areas of the technology industry. Most recently, Ms. Jabbusch has focused in specialized areas of infrastructure security, including network access control, 802.1X and wireless security technologies.

Jennifer has consulted for a variety of government agencies, educational institutions and Fortune 100 and 500 corporations. In addition to her regular duties, Jennifer participates in a variety of courseware and exam writings and reviews, including the official (ISC)2 CISSP courseware.
What We’re Doing

What am I telling you?
What I’m telling you

How to **leverage** security features you have and start down a **holistic** security path.
What We’re Doing

Why am I telling you this?
Why I’m telling you

You have goals.
You have bosses.
We want to help.
What We’re Doing

Why hasn’t someone else told you this?
Why they haven’t told you

They want to sell you **stuff**. If you don’t **buy** more stuff, their **bosses** get mad.
Why they haven’t told you

But, we don’t care about their bosses.
What we’ll be covering

1. **The Business of Security**... understanding goals and options
2. **Back to Bare Essentials**... working towards holistic security
3. **Tapping into Technologies**... ways to leverage what you have
4. **Getting Started**... ideas to get you going
The Business of Security
The quest for **goals**, smart use of **resources** and ways to keep your bosses’ boss happy.
Moving toward a goal

- IT Department
- Your Team
- Your Projects

- Regulations
  - Security
  - Compliance

- Customer
  - Serving Public
  - Inter-agency
Moving toward a goal

Agency • IT Department
• Your Team
• Your Projects
Focus on resources

Bigger focus on using resources wisely
Focus on resources

Adapt for the resources available
Focus on resources

**Balance** what’s missing with what’s **abundant**
Current projects

What are you working on now and in the next 12 months?
Ways to meet goals

3 Options

Buy some more stuff

Use what you have

Get someone else to do it
For your projects

Which one are you planning to do?

And why?
What we’re buying

There are plenty of manufacturers and vendors that would like your money.
• NAC
• Endpoint Security
• Enhanced AV
• Guest Solutions
• Wireless Security

• Firewalls/IDS
• Data Leakage
• ID Management
• SIEM
• Encryption

They want us to buy all this
Side effects of new stuff

- **Training**: For staff and end users
- **Budget**: To buy new products
- **Services**: For install, configure & support
- **Resources**: Manage and maintain
Side effects of new stuff

What’s the real TCO involved with new products?
Balancing the real TCO

- TCO
  - Stop Gap
  - New!

+ TCO
  - Training
  - Budget
  - Services
  - Resources
The question

Is buying new stuff the solution?
The answer

Probably NOT
For your projects

Would you ‘use what you have’ if that were an option?
Back to Bare Essentials
The quest for **holistic** network security and the **realization of ignorance**.
Using what you have

- Leveraging built-in features
- Retooling the infrastructure
- Designing for security from the start
Leveraging what you have

Use **features** and **tools** built in to the **products** you have.
Retooling the infrastructure

Reengineer the network for security and availability.
Design for security early

**Architect** security into **solutions** at the **start**.
Holistic security snippets

Access Control
- Using switches instead of NAC

0-Day
- Using sFlow instead of IDS

User Control
- Using directories instead of overlays

Management
- Using effective logging and reporting
A simple concept

It seems so **simple**, so why aren’t **more people** doing it?
Holistic holdbacks

There are several common factors that prevent IT departments from effectively using what they have.
Holistic holdbacks

- Under-staffing and high turnover are problems

- Staff

- May not have necessary skills in-house

- Skill

- Redesign and training is time consuming

- Time
Holistic holdbacks

- Awareness of current environment
- Complicated vendor-specific features
- Pulling pieces together for an integrated solution

Documentation
Complexity
Integration
Holistic holdbacks

- Ignorance
  - Not knowing what products and solutions you have

- Understanding
  - The overall goals and objectives

- Management
  - Getting buy-in from management
Tap Into Technologies
The quest for finding added functionality in your current stuff... so we don’t have to buy new stuff.
Tapping what you have

Switch

Firewall

Encryption

Management

Coming Soon
CAUTION
Here are slide references to the cool stuff you missed, including the new 802.1X-REV overview...
Switches and wireless

VLANs (Virtual LANs)

- Not new
- Protects by segregating network traffic
- Lets you logically segment and secure instead of physically separating
Switches and wireless

802.1X Port Security

• Also not new
• Protects unauthorized users from connecting to a port or wireless SSID
• Uses standard communication to lock ports until the user is authenticated
Switches and wireless

MAC Lockdown (Port Security)

• Protects unauthorized devices from connecting
• Statically set or dynamically ‘learns’ allowed MACs
Switches and wireless

**Dynamic IP Lockdown (IP Source Guard)**

- Protects from statically set IP addresses
- Tracks DHCP results to match IP to MAC-port-VLAN
Switches and wireless

Source Port Filtering (Protected Ports)

- Protects devices from communicating directly
- Similar to wireless communication segregation for endpoints
Switches and wireless

DHCP Snooping

• Protects from rogue DHCP servers
• Maps known servers with its MAC address to an assigned port
Switches and wireless

Dynamic ARP Protection/Inspection

• Protects from ARP cache poisoning
• ARP matches MAC to IP
• Sees spoofed MAC addresses and ARP flood attacks
Switches and wireless

Dynamic Port Mirroring

- Not direct security feature
- Lets you offload traffic for security inspection with low overhead
Switches and wireless

Other monitors

• Monitor for port scanning by watching for packets sent to closed TCP/UDP ports
• Monitor for DoS attacks from IP flooding by watching for a volume of new learned Ips
• Monitor for viruses by watching for sudden increase in ARP requests
• Monitor for other DoS attacks by monitoring system resources
Switches and wireless

Other monitors

• Monitor for management intrusion by watching for failed logins
• Monitor for other attacks by watching for excessive or unexpected events- new or moving MAC addresses and IP addresses, system resources
Switches and wireless

- VLANs
- 802.1X
- MAC Lockdown
- Dynamic IP Lockdown
- Source Port Filtering
- DHCP Snooping
- Dynamic ARP Protection
- Dynamic Port Mirroring
- Other Monitoring
Tapping what you have

Switch
Firewall
Encryption
Management
Coming Soon

[Image of network switch, fire, safe, and 2009]
Firewall, UTM and IDS
Firewall, UTM and IDS

Gateway Security and UTM

• Use built-in anti-virus and anti-spyware for an added layer of protection without a separate appliance
• Use integrated IDS/IPS instead of purchasing an additional solution
Firewall, UTM and IDS

Application Security

• Use a firewall to apply application access control up to layer 7
• Add security by using encrypted VPN connections on the LAN to access sensitive data
Firewall, UTM and IDS

Network Segregation

• Use firewall logical zones and routes for segregation of LAN traffic
Firewall, UTM and IDS

Inspection

- Offload or mirror internal network traffic to your firewall or IDS for further inspection to supplement NBAD
We’re really gettin’ crazy now!
Tapping what you have

Switch  Firewall  Encryption  Management  Coming Soon
Encryption
Encryption

Data Protection

• Use encryption to secure sensitive data on endpoints and storage
Encryption

Key Management

• Used your encryption product for centralized key management
• Map to your user directory for added security and reduced management
• Use single product for FDE, removable media, mail and other applications
Tapping what you have

Switch  Firewall  Encryption  Management  Coming Soon
Management
0-Day Protection

• Use integrated tools for NBAD (network behavior anomaly detection)
• Collect sFlow/NetFlow from switches and wireless to see real-time problems
Management

Inventory

• Use current management systems such as patching and anti-virus servers for asset inventory

• Use inventory reports to identify unpatched and unhealthy devices
Management

Event Correlation

• Use built-in management, search tools or syslogs for event correlation

• Data can be used for compliance reporting and change management
Management

Log Management & Reporting

• Use a central log server or search tool for all your network devices, instead of manufacturer-specific products
Tapping what you have

Switch  Firewall  Encryption  Management  Coming Soon
Coming Soon
Coming Soon

802.1X - REV

- Revision of 802.1X to incorporate 802.1AE, 802.1af and other security features
- Look for the standard release in Q1 2009
Coming Soon

802.1AR

• Device identity...
• Look for the standard release in Q1 2009
Coming Soon

TNC IF-MAP

- Framework for sending endpoint health status to a centralized server
- Offers NAC-like integrity functions without a specific vendor solution
- Look for more adoption in 2009
Getting Started
Embarking on the quest for integrated security...
Learning to leverage

Strategies for getting started with what you have.
Training for staff

- Classroom
- Lab
- Webcasts
- Online
- Conference sessions
Vendor assistance

• From manufacturer
• Pre- or Post-sales SE
• Pro services
• Bundle with product
Consultant or integrator

• Your choice
• Integrated assistance
• Objective 3rd party
• Flexible
Staff and contractors

- Staff may have expertise on a topic
- Find self-motivators with interests in the solutions you need
User groups

- Product user groups
- Peer user groups
- Industry associations
- Conferences
Bang for your buck

ROI

Training
Vendor
Consultant
Staff
User groups
The final frontier. Getting the buy-in from management.
Selling a holistic approach

- Devices, software, licenses, contracts and personnel
- See what’s been purchased and rate effectiveness

Survey
Selling a holistic approach

- Needs, goals and projects
- See where you can leverage what you have
Selling a holistic approach

- Find the ROI for leveraging technologies instead of products
- Factor in TCO of product vs long-term investments in staff
- Put it in terms of dollars & cents
Selling a holistic approach

The **key** is to understand the bottom line...
Selling a holistic approach

What is the bottom line?
A dollar saved is a dollar you can spend on some other super-cool geeky toy.
Recap
A super quick review of the last 100 slides.
Seven steps to remember

1. Understand
2. Survey
3. Identify
4. Strategize
5. Supplement
6. Sell It
7. Succeed
This is where I took a bunch of crap out...
Seven steps to remember

If you **follow** these steps, you **will** reach a state of security Zen...
Disclaimer

*The preceding statements have not been approved by IEEE, TNC, IETF, the FDA, the FAA or the FBI. Please consult your doctor before attempting these, or any other regimens to reach security Zen. Neither CAD, the conference management, or the presenter will assume responsibility, explicit or implied, for the use of this material in reaching security Zen. Please proceed at your own risk.
Thank you.
Carolina Advanced Digital, Inc.
http://cadinc.com