Security, Management & Mobility of Wireless Networks (WLANs)

Issues
Approaches
Solutions

Mike Brockney, Sr. Sales Engineer, Bluesocket
Agenda

- Benefits of Wireless Local Area Networks (WLANs)
- What new problems do WLANs create?
- WLAN pain points
- How do you solve these WLAN customer pain points?
- Bluesocket Wireless Gateway Overview
- Rutgers University Examples
- Questions and Answers
The Benefits of Wireless LANs

- Work where you choose— at home, the airport, as well as your workplace
- Rapidly dropping prices
- Ease of deployment
- Compelling technology:
  - High productivity gains
  - Reduced support and network management costs
- 

STILL, worries remain…
# Wireless Worries Dampen The Dream

<table>
<thead>
<tr>
<th><strong>Network Managers:</strong></th>
<th><strong>Network End-Users:</strong></th>
<th><strong>CIOs:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fear: Is IT safe?</strong></td>
<td><strong>Fear: Is IT safe?</strong></td>
<td><strong>Fear: Is IT Safe?</strong></td>
</tr>
<tr>
<td>Network Vulnerability</td>
<td>Is my privacy ensured?</td>
<td>Threats from the unknown</td>
</tr>
<tr>
<td>Network Unsecurity</td>
<td>Can my information be manipulated?</td>
<td>Are we prepared?</td>
</tr>
<tr>
<td>Virtual break-ins: War Driving</td>
<td>Vulnerability</td>
<td>Cyber Attacks</td>
</tr>
<tr>
<td>Sensitive customer information</td>
<td>Lost intellectual property</td>
<td>Legal ramifications</td>
</tr>
<tr>
<td>Loss of control?</td>
<td>Compromised assets</td>
<td>Compromised assets?</td>
</tr>
<tr>
<td>Will it work today and tomorrow?</td>
<td>Can Crackers Get My Info?</td>
<td>Missed-management</td>
</tr>
<tr>
<td>Which vendors to choose?</td>
<td>Is it worth the possible risk?</td>
<td>What’s the right investment?</td>
</tr>
<tr>
<td>I’ll get the blame!</td>
<td></td>
<td>How do I prevent obsolescence?</td>
</tr>
</tbody>
</table>
Unsecured WLANs Create Problems

Gartner

“By year-end 2002, 30 percent of enterprises will suffer serious security exposures from deploying WLANs.”

META Group

“Deploying LAN based VPNs is not simple or inexpensive. Major problems include…the lack of ubiquitous client support, limited roaming and the loss of management control.”

CERT Coordination Center

“Network security violations on the upswing. Almost 35,000 such incidents in Q1-3 2001.”

Aberdeen Group

“WEP fails to provide for the access control and authorization needs of enterprise wireless networks.”
Wireless LANs: The Unfulfilled Promise

- WLAN benefits are clear: rapid deployment, user convenience, productivity, low TCO but....
- To meet your requirements, key issues must be resolved with wireless LANs:
  - Security
  - Compatibility and Simplicity
  - Quality of Service and Bandwidth Management
  - Cost
  - Mobility
- Your “pain points” must be addressed and removed
WLAN Customer Pain #1
War Driving – The Uninvited Guest

Chip-a-holic?
Or cracker **attacking** your WLAN?
How To Address Pain Point #1
War Driving

- Have a professional wireless site survey performed
  - Access point placement, power output, antenna selection can help prevent “leakage” outside your buildings
- Do not broadcast SSIDs (wireless network names)
- Install a solution that only allows access to the network for authenticated users
- Use some form of encryption if air privacy and protecting your data is important
- At a minimum use WEP
  - There are other more secure options
WLAN Customer Pain #2
Layer 2 Wireless LAN Weaknesses

Weak Security

Stop or Go - Same Access For All Visitor or Employee or Contractor

No Bandwidth Management

“Bandwidth Hog”
How To Address Pain Point #2
Layer 2 Wireless LAN Weaknesses

- Deploy a solution that allows you to control access to your network.
  - Guest, Contractor, Employee/Staff/Student
  - Even registered users may need access control
- Role based access/authorization
  - Control access to network resources
  - Require encryption or no encryption
  - Set policies based on location and time of day
  - Limit bandwidth for visitors, guests, etc.
  - Prioritize data
WLAN Customer Pain #3
WEP ‘Security’ is Fatally Flawed

- A series of academic papers exposed serious flaws in WEP—the security system built into the 802.11b standard.
- Rapid passive attack was first described in July 2001 by Fluhrer, Mantin & Shamir.
- AT&T Labs team successfully implemented the attack and concluded that WEP is "totally insecure".
- In August 2001, the Airsnort program was released as open source code. Airsnort allows users to decode the WEP key.

http://airsnort.sourceforge.net/
How To Address Pain Point #3
WEP ‘Security’ is Fatally Flawed

- 802.1x for keeping unregistered users from associating to access points
  - Many choices, each with pros and cons: TLS, LEAP, etc.
- Use layer 3 encryption to ensure air privacy
  - PPTP, IPSec, AES
  - Same encryption used in most VPNs
- Only require encryption for those users that need air privacy
  - Guests and visitors may not need to run encryption
- Use a combination of encryption and authentication
WLAN Customer Pain #4
Supporting Emerging Standards and Vendor Implementations
How To Address Pain Point #4
Supporting Emerging Standards and Vendor Implementations

- Choose a security and management solution that will work with most or all standards.
- Solution should be agnostic to all air protocols
  - 802.11b, 802.11a, 802.11g
- Your environment will dictate the right solution
  - Can you control all wireless devices and operating systems on the WLAN?
  - Will there be a mix of WLAN devices?
WLAN Customer Pain #5
Supporting A Plethora of Mobile Devices
How To Address WLAN Customer Pain #5
Supporting A Plethora of Mobile Devices

- Choose a security and management solution that will work with all devices
  - PC, Mac, Linux, PDA, scanners, etc.
- End-user experience needs to be simple and secure
  - Logins, encryption
- Support common methods of authentication
  - Windows Domain, Browser based authentication using SSL
- Use VLANs for different device types
  - Ex: WLAN IP phones may need to be on their own VLAN
WLAN Customer Pain #6

Cost and Complexity
Choose an integrated solution – One device that supports multiple security and management functions – Authentication, Encryption, VPN, Firewall, QoS, IP Mobility.

Integrating systems will typically reduce your overall cost system.

The fewer devices you have, the easier it is to maintain the system.

Cost and Complexity

#6

How To Address WLAN Customer Pain
WLAN Customer Pain #7
Inconvenience of Required Client Software
How To Address WLAN Customer Pain
#7
Inconvenience of Required Client Software

- Choose a security and management solution that utilizes common access methods
  - Browser based logins
    - PCs, Macs, Linux, PDAs
  - Window Domain logins
    - To provide “transparent” authentication
  - Eliminates the need to load client software

- Take advantage of native encryption when possible
  - Windows and MACs have built-in PPTP and IPSec
WLAN Customer Pain #8
Lack of Seamless Secure Mobility

- Users cannot roam between IP subnets with encrypted sessions
- Users must receive a new IP address, re-authenticate, and establish a new secure connection
How To Address WLAN Customer Pain #8
Lack of Seamless Secure Mobility

- Choose a solution that allows users to move seamlessly
- Users should not have to worry about:
  - Their IP addresses
  - Moving between subnets
- Users should be able to roam without re-authenticating or re-establishing a secure connection
- You should not have to create a “flat” network just to accommodate your WLAN
Two Approaches For WLAN Security and Management

Current Solutions:
- Admission Control
- QoS
- Mobility
- IPSec

Better Solution:
- All Security and Management in one Wireless Gateway
  - Security
  - Access Control
  - Management
  - QoS

Enterprise Network

Access Point

Wireless Gateway

Enterprise Network

© 2003 Bluesocket, Inc. Proprietary and Confidential. Do not copy.
Network Placement of the Wireless Gateway
Bluesocket Wireless Gateway: Summary of Features

- Easy to use for network manager and network user alike
- Single-component configuration, simple to implement, integrate, manage and update
- Support for major Access Points, NICs, network protocols, authentication/security clients, VPNs
Bluesocket Wireless Gateway: Summary of Features

- Authentication
  - Native, Windows Domain, LDAP, RADIUS, 802.1x, Mac based

- Authorization
  - Role based access control
  - Roles are determined by user attributes in your directory

- Encryption
  - PPTP, IPSec, AES

- Bandwidth Management
  - Set bandwidth thresholds per Role
Bluesocket Wireless Gateway: Summary of Features

- Distributed intelligence
  - All Gateways are independent systems with full functionality

- Mesh Architecture
  - Provides centralized management of entire system of Gateways

- Full logging and reporting of user activity
  - Allows IT staff to monitor WLAN usage
    - Helps with capacity planning
    - Find users who violate your WLAN policy
Warning

Security is only provided for your initial login to the wireless network. It is possible for someone to obtain the information that is being transmitted if additional security measures are not taken after you have connected. Information is available to assist you with securing your connection.

By using RUCS-Newark Wireless LAN (RUCS-N-WLAN) you acknowledge that you are responsible for the security of your personal computer and the data that you are transmitting.
Rutgers – New Brunswick Login

Rutgers University Wireless Local Area Network

A Service of Rutgers University Computing Services

First Time Users Please Begin By Selecting Your Operating System Below For Configuration Info

Select OS Here

Need Help?
Thank you.
Any questions?