Visitor Access: Analysis of a Worldwide Survey

Mark Linton, The Pennsylvania State University
Philippe Hanset, The University of Tennessee

April 24, 2007
Internet2 Member Meeting, Arlington, Virginia
Why did we do this?

• FWNA (http://security.internet2.edu/fwna) is exploring many possible solutions and we want to be sure we know what the problems are

• Disclaimer
  • This is not a scientific survey (self selecting)
About the response

- Thank you
  - 108 responses from
  - 95 institutions in
  - 10 countries on
  - 3 continents

- Within US: responses from 30 states and Puerto Rico

Pie chart showing:
- Yes: 84%
- Considering: 10%
- No: 6%
Visitor Access: Wired or/and Wireless?

- Wireless Only: 49%
- Wired + Wireless: 51%
- No Wired Only: 0%
Visitor Access: Wireless Network Size

- <10: 5
- 10 to 99: 18
- 100 to 499: 43
- 500 to 1499: 19
- ≥1500: 7
What is a visitor?

- General Public
- Not members of the broadly defined University community
- No University Credentials
- Affiliated but non-credentialed (not public)
What is a Visitor? (cont.)

• Examples of affiliation:
  • Prospective students
  • Parents of current or prospective students
  • Patients at a University medical facility
  • Library patrons
  • Employees of on-campus but non-University institutions (bookstore, credit union, post office)
What is a Visitor? (cont.)

• More examples of casual affiliation:
  • Anyone visiting the institution
    • personal, social, academic, recreational, business
      – contractor, vendor, someone using the University airport,
        someone attending an event at the Alumni Center,
        someone attending a sports event, someone waiting for
        their child to finish a skating lesson on the University ice
        rink
    • Invited guests of the institution (professor, lecturer,
      researcher, athlete, performer, artist, press)
  • Workshop and Conference attendees
What is access?

• Possibly with restrictions
  • Application
  • Port
  • Destination
  • Rate (only 256 kbps, up and down, is common)
  • Time (absolute and relative)
    • Short/Long Term?
    • With defined active/inactive times
    • Long term must apply for account
      – Generally about a month
      – Adds access to additional resources
  • Location
What is Access? (cont.)

• At least as much internal access as available externally
  • Possibly no more internal access than they would have externally
• Might add printer access
• May have access to University or licensed resources
• Could be wired or wireless
What is Access? (cont.)

- Access through federated authentication
- Unregistered users that are domain guests
- Any connected device that is not owned by the University
- May be sponsored by institution personnel
- Might actually provide a computer (eg: lab)
Why Not Visitor Access?

• General Security Issues
  • CALEA
  • Liability for Illegal Activity
  • Accountability
  • Compromised Machines
• Lack of Resources, Cost
• Do Not Know How
• Community already provides free wireless
Why Visitor Access?

• People expect/ask for it
• Reduce password sharing
• Community Outreach/Relations
• Convenience
• Added value
• Competition
• Marketing
• Public Relations
• To be a good host
Why Visitor Access? (cont.)

- State law requires access to library e-materials
- Institution mission mandates it
- “Obligation”
- Mechanism to request account/reset password
- Test behavior of Web apps from Internet
- Mobility between institutions
- Reduced support for visiting scholars
- Difficulty of supporting authenticated access for short term visitors
- Serving the needs of the community
Access: Individuals?

- Open Network
- Captive portal
  - Self register
  - ToS/AUP
- NAC
- Separate Network
- Sponsored accounts (fac/staff/student or helpdesk)

- Open Terminals
- EduRoam
- Commercial Hotspot Provider
- Shared account w/rotating password
- Credit card as identity
Access: Groups?

- Turn off Authentication
- Batch account creation
  - by central IT
  - by authorized administrator of the system
- Differentiate this as “Guests” while individual is “Visitor”
- Single ID for all group members
  - Printed on conference materials w/instructions
  - Count MAC addresses
- Self-register based on mag-stripe on drivers license or credit card
Authenticated vs. Unauthenticated

- Different solutions for different community members
- Mechanism to request a real account

Require Authentication

- Yes: 71%
- No: 29%

Allow Unauthenticated

- No: 54%
- Allow Unauthenticated: 46%
How Visitor AuthN?

- EduRoam
- Captive Portal
- 802.1X/WPA/WPA2
- NAC
- MAC Registration
- VPN
- Sponsor
AuthN: Sponsored

• Having an authorized user take responsibility for a temporary account created for a visitor
• Authorized Faculty/Staff/Students requests
  • On paper
  • By phone
  • In person
  • By e-mail
  • By web form
• Visitor specifies sponsor when self-registering/sponsor e-mailed with link to approve
AuthN: Sponsored

- Yes: 33%
- No: 67%
AuthN: Federation

• Using enterprise identity and attributes outside the enterprise
• Examples (federations and enabling tech):
  • Eduroam
  • FWNA
  • Shibboleth
  • InCommon
  • Allowing VPN access between schools
  • Providing common IdM
AuthN: Federation

No: 69%
Yes: 31%
Visitor Issues?

- Yes: 15%
- No: 85%
Visitor Issues?

- File sharing
- Excessive printing
- Infected machines
- Excessive traffic
- Spam sourcing
- DMCA
- Inappropriate sites
Separate Visitor Traffic?

- Yes: 55%
- No: 45%
Separate Visitor Traffic?

- Separate VLAN
- Separate IP space
- Separate infrastructure
  - 3rd party hot-spot provider
  - Outside campus firewall/border router
  - Campus machines patched - don't know status of visitors
- Separate Wireless SSID
Separate Visitor SSID?

- Yes: 42%
- No: 58%
Unauthenticated Restrictions?

- Yes: 58%
- No: 42%
Unauthenticated Restrictions?

- No restrictions
- No internal resources/Internet only
- Web, E-mail, IM, VPN
- Time limited
- Bandwidth limited
- Through a firewall

- P2P restrictions
- No SMTP
- Separate VLAN/IP space treated like global Internet
- Only internal access
- Account request page only
Authenticated Restrictions?

No 46%

Yes 54%
Authenticated Restrictions?

- No restrictions
- Restrict access to certain internal resources
- Firewall
- IPS
- Limit/Block P2P
- Limit student bandwidth
- Packet shaping based on enterprise priorities
- Globally blocked ports
  - SMTP
  - Windows RPC
- BW restrictions at gateway
Visitor Bandwidth Restrictions?

Yes: 27%
No: 73%
Visitor Bandwidth Restrictions?

• Reserve most BW for Fac/Staff/Students
• Don’t want to create “beautiful nuisance”
• Make visitor network unattractive to:
  • institution members
  • potential malicious users
• Limit all users anyway
Visitor Port/Protocol Restrictions?

No: 53%
Yes: 47%
Visitor Port/Protocol Restrictions?

- Stateful firewall
  - Only transactions initiated from inside
- No SMTP
- No P2P
- Limit risk from infected machines
- HTTP/HTTPS Only
  - Some add SSH/VPN, IM, email, specific internal applications, local printing
Extra Visitor Monitoring?

- Yes: 8%
- No: 92%
Infrastructure Issues
Which solution?

- A: Outsourced Infrastructure
- B: Outsourced IP
- C: Account creation + AUP
- D: MAC reg + AUP
- E: Federation
- F: Sponsored
- G: Pool of accounts + AUP
- H: Open + MAC logging
- I: Open Access
What’s CALEA?

• Communications Assistance for Law Enforcement Agencies (USDOJ/FCC)

• CALEA Effect on Visitor Access?
  • Haven’t decided
  • It didn’t
  • Policy already requires CALEA-like
  • Incidental public access/network remains private

• Slight modification
  • Policy
  • Coverage area
  • Stopped public access
  • Switched to sponsored access
Require CALEA Capabilities?

- Yes: 17%
- No: 83%
Wireless Architecture Affected by Addition of Visitor Access?

- Yes: 38%
- No: 62%
Comments on How Wireless Architecture Was Affected

- Multiple SSID/VLAN
  - VLAN assigned from authentication
  - Ability to route Visitor Traffic differently
- Multiple User Roles
- Built-in portal with temp accounts
- Controller-based architecture for central user management
- Separate IP space
- NAC Appliance
- Firewall
Visitor Access uses Wireless Vendor Feature?

- Yes: 41%
- No: 59%
Unanswered Questions?

• How would you give access to a non-person?
  • Sensor network?
  • Surveillance Camera?

• How do you terminate an account for issues?
Questions?
Thank You!

Everybody That Responded
Steve Olshansky
The Rest of FWNA
University of Michigan
www.internet2.edu