

2006 ResNet Security Practices and Policies Survey

Introduction

As part of an on-going assessment of computer and network security practices and readiness specific to residential computer networks (ResNets) at higher education institutions, the ResNet Applied Research Group (RARG) has developed this 2006 ResNet Security Practices and Policies Survey. This survey is built upon topical security concerns and data and analysis from previous surveys, particularly the ResNet Vulnerability Survey conducted in 2004 and the comprehensive 2005 ResNet Survey. Notably, respondents to the 2005 ResNet Survey indicated security as their number one short- and long-term concern, consistent with results from other recent computing surveys such as the EDUCAUSE Current Issues Survey and the Campus Computing Project. Continued assessment and publication of security practices and challenges provides value to the ResNet and higher education communities.

To ensure validity of the survey and enable members of the RARG to contact respondents should questions arise regarding a response, respondents of this survey will be required to provide their name, e-mail address, and institution. However, names and e-mail addresses will not be released or in any way linked to survey data in public presentations or publications; we respect and will protect your individual anonymity as you provide information about security related to your institution. A list of participating institutions will be published but survey results will not be linked in any way to an individual institution or respondent in publications and presentations.

The RARG wishes to acknowledge and thank the Effective Practices Working Group within the EDUCAUSE/Internet2 Computer and Network Security Task Force and the Internet2 SALSA-NetAuth Working Group for assisting with question refinement and suggested survey topics.

GENERAL SURVEY INFORMATION

Print Copy of Survey:

To assist you with completing the online version of the survey, a printable copy of the entire survey is available at <http://resnetsymposium.org/surveys/security/>.

Time to complete the survey:

There are a total of 35 questions in this survey. However, the number of questions you may be asked to answer may be less depending on your responses. Based on pilot tests, it is estimated that it will take 20-25 minutes to complete the survey.

Completion deadline:

We ask that you complete the survey by April 7, 2006.

Stopping and restarting the survey:

You can stop at any point and return to the survey at a later time. To do this you must, however, complete the entire survey using the same computer (the survey tool uses cookies to track your progress through the survey).

To return for any reason:

- Visit the URL that was included in the e-mail you received. You will return to the page of the survey where you left off.
- You can go back and forward through the survey to answer any questions you did not complete previously or to change your responses.
- You can return to the survey to edit your responses even after clicking on the "Done" button as long as you use the same computer.
- Survey responses are saved on a page-by-page basis.

Results:

Results will be presented at the ResNet 2006 Symposium at Bowling Green State University in June and will be placed on the ResNet Symposium web site in July. In addition, we may seek to publish or present results elsewhere (EDUCAUSE, ACUTA, etc.). Results will be presented only in aggregate form and responses will not be identifiable by institution or survey respondent. We will notify you when results are initially published or presented if you request such notification in question 35.

Still have questions?:

Questions regarding the survey can be addressed to resnetresearch@lists.uncg.edu.

The RARG greatly appreciates your participation in the 2006 ResNet Security Practices and Policies Survey.

2006 ResNet Security Practices and Policies Survey

Demographics (Section 2 of 7)

* 1. What is your name?

* 2. What is your title?

* 3. What is your e-mail address?

* 4. What is the name of your institution?

5. In what department(s) do you work?

2006 ResNet Security Practices and Policies Survey

Governance Information (Section 3 of 7)

6. Who is primarily responsible for setting policies governing the residential computer network? (Choose one)

- Central IT
- Housing
- IT Security
- Legal affairs
- Networking
- IT advisory committee
- Other - Please explain:

7. Who is primarily responsible for enforcing policies governing the residential computer network? (Choose one)

- Central IT
- Housing
- IT Security
- Legal affairs
- Networking
- IT advisory committee
- Other – Please explain:

*** 8. Does your institution ever block, filter, or otherwise restrict any services for security purposes, in any manner or situation? (Choose one)**

- No (Response will force respondent to skip to Question 17)
- Yes
- Other – Please explain:

2006 ResNet Security Practices and Policies Survey

Network Services Practices & Policies Information (Section 4 of 7)

Questions 9-11 ask about specific services your institution blocks, filters or otherwise restricts for security purposes, in any manner or situation, externally to, externally from, or within the residential computer network.

9. Please indicate when you block, filter, or otherwise restrict the following services when they originate *external to* (i.e coming into) the residential computer network (choose all that apply):

	Never	Sometimes	Always or continually	Do not know
We block all non-established traffic	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
VoIP	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
P2P networking	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Remote access (Windows Remote Access, PCAnywhere, etc)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
FTP	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
E-mail (incoming SMTP)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Unauthorized resident-managed web servers	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
IRC	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Instant messaging	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Online computer gaming	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Console gaming (X-Box Live, PS2, etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
IPSec (IP Security)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Windows file and print sharing	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
DNS	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

9a. Are there any other services your institution blocks, filters, or otherwise restricts when they originate *external to* (i.e coming into) the residential computer network? (Choose one)

- No
- Yes - Please specify:

10. Please indicate when you block, filter, or otherwise restrict the following services when they originate *from* but with destinations *external to* (i.e. going out of) the residential computer network (choose all that apply):

	Never	Sometimes	Always or continually	Do not know
VoIP	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
P2P networking	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Any non-institutional web sites	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Remote access (Windows Remote Access, PCAnywhere, etc)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
FTP	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
E-mail (outgoing SMTP to non-institutionally-controlled mail server(s))	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
IRC	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Instant messaging	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Online computer gaming	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Console gaming (X-Box Live, PS2, etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
IPSec (IP Security)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Windows file and print sharing	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Off campus DNS	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

10a. Are there any other services your institution blocks, filters, or otherwise restricts when they originate *from* but with destinations *external to* (i.e. going out of) the residential computer network? (Choose one)

- No
- Yes - Please specify:

11. Please indicate when you block, filter, or otherwise restrict the following services *completely within* (i.e they never leave) the residential computer network (choose all that apply):

	Never	Sometimes	Always or continually	Do not know
VoIP	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
P2P networking	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Remote access (Windows Remote Access, PCAnywhere, etc)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
FTP	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
E-mail (SMTP)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Unauthorized resident-managed web servers	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
IRC	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Instant messaging	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Online computer gaming	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Console gaming (X-Box Live, PS2, etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
IPSec (IP Security)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Windows file and print sharing	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

11a. Are there any other services your institution blocks, filters, or otherwise restricts *completely within* (i.e they never leave) the residential computer network? (Choose one)

- No
- Yes - Please specify:

12. Who primarily determines which network services, ports, or protocols are filtered, blocked, or otherwise restricted on the residential computer network? (Choose one)

- Central IT
- Housing
- IT Security
- Networking
- Institution IT advisory committee or group
- Other – Please explain:

13. In the event of an unexpected security incident, who has the primary authority to request the immediate filtering, blocking, or restricting of network services, ports, or protocols on the residential computer network? (Choose one)

- Central IT
- Housing
- IT Security
- Networking
- Institution IT advisory committee or group
- Other – Please explain:

*** 14. Does your institution base its decision to block, filter, or restrict network services, ports, or protocols based on published best practices from professional security groups such as the EDUCAUSE/Internet2 Computer and Network Security Task Force? (Choose one)**

- No, we base our decision entirely on other factors (Response will add a follow-up question asking about those other factors)
- Yes, we base our decision **in part** on published best practices (Response will add a follow-up question asking about factors other than published best practices)
- Yes, we base our decision **entirely** on published best practices
- Other – Please explain: (Response will add a follow-up question asking about factors other than published best practices)

15. What does your institution use to block, filter, or restrict network services, ports, or protocols? (Choose all that apply)

- Bandwidth shaper
- Access Control Lists (ACLs) on network devices (routers, switches, etc.)
- Network-based or Server-based firewall
- Client-side Software Firewall(s)
- Intrusion Prevention System
- E-mail filtering (spam)
- Other – Please explain:

16. How are users of the residential computer network made aware of network services, ports, or protocols that are filtered, blocked, or otherwise restricted on the residential network? (Choose one)

- Users are not made aware
- Users are indirectly made aware through mass communications (webpage, flyers, etc.)
- Users are directly made aware on an ongoing basis through direct or personal communications (e.g. email sent directly to them as changes occur)
- Users are made aware both directly and indirectly
- Other – Please explain:

17. What method is used to isolate or separate the residential computer network from other networks at your institution? (Choose all that apply)

- No method is used to isolate or separate the residential computer network from other networks at our institution
- The residential computer network is physically separate from other networks at our institution
- VPNs
- ACLs
- IP subnets
- IP subnetting (DHCP)
- Other - Please explain:

2006 ResNet Security Practices and Policies Survey

Client Machine Practices & Policies Information (Section 5 of 7)

18. In general, are residents permitted to operate servers on the residential computer network? (Choose one)

- No, residents are not allowed to operate servers
- Yes, residents are allowed to operate servers with access **internal** to the residential computer network **without approval** or permission but are not allowed to operate servers with external access
- Yes, residents are allowed to operate servers with access **internal** to the residential computer network **with prior approval** or permission but are not allowed to operate servers with external access
- Yes, residents are allowed to operate servers with access **internal and external** to the residential computer network **with prior approval** or permission
- Yes, residents are allowed to operate servers with access **internal** to the residential computer network **without approval** or permission but are required to **seek approval** or permission to operate a server with access **external** to the residential computer network
- Yes, residents are allowed to operate servers with access **internal and external** to the residential computer network **without prior approval** or permission
- Other – Please explain:

19. Do you provide VPN or other remote access to allow users not physically in the residence halls to securely connect to your residential computer network? (Choose one)

- Yes
- No
- Other - Please explain:

*** 20. Do users of the residential computer network have an individual bandwidth usage quota? (Choose one)**

- No, we do not set usage quotas for users, but we monitor bandwidth usage
- No, we do not monitor bandwidth usage on a user level and thus do not have a usage quota
- Yes, we have a non-published quota for each user (Response will add one follow-up question asking the technologies used to enforce the quota)
- Yes, we have a published quota for each user (Response will add three follow-up questions asking how residents are informed of the quota, how residents are able to monitor their bandwidth usage, and the technologies used to enforce the quota)
- Other - Please explain: (Response will add three follow-up questions asking how residents are informed of the quota, how residents are able to monitor their bandwidth usage, and the technologies used to enforce the quota)

21. Does your institution recommend or require a minimum operating system standard to successfully access the residential computer network? (Choose one)

- We have neither a standard nor a recommendation
- Yes, we have a standard and computers are required to meet the standard before successfully accessing the network
- Yes, we have a recommended standard but computers are not required to abide by it to successfully access the network
- Other - Please explain:

*** 22. Does your institution require users of the residential computer network to install anti-virus software? (Choose one)**

- We do not require that anti-virus software be installed on computers connecting to the residential computer network
- We require the users of the residential computer network to use institutionally-supported anti-virus software (Response will add one follow-up question asking how the requirement is enforced)
- We do not require users of the residential computer network to use the institutionally-supported anti-virus software but they must have anti-virus software installed (Response will add one follow-up question asking how the requirement is enforced)
- Other - Please explain: (Response will add one follow-up question asking how the requirement is enforced)

*** 23. Does your institution require that anti-spyware or anti-adware software be installed on computers that connect to the residential computer network? (Choose one)**

- We do not require anti-spyware or anti-adware software to be installed on computers connecting to the residential computer network
- We require users of the residential computer network to use the institutionally-supported anti-spyware or anti-adware software (Response will add one follow-up question asking how the requirement is enforced)
- We do not require users of the residential computer network to use the institutionally-supported anti-spyware or anti-adware software but they must have anti-spyware or anti-adware software installed (Response will add one follow-up question asking how the requirement is enforced)
- Other - Please explain: (Response will add one follow-up question asking how the requirement is enforced)

2006 ResNet Security Practices and Policies Survey

Infrastructure Practices & Policies Information (Section 6 of 7)

24. Which bandwidth shaping or Quality of Service (QoS) product or tool does your institution primarily use? (Choose one)

- We do not use a bandwidth shaping or QoS product or tool
- Allot NetEnforcer
- Checkpoint Floodgate-1
- Converged Networks (Sitara) QoSWorks
- Emerging Technologies (ETinc) Appliance
- Packeteer Packetshaper
- "Home grown" (i.e. developed in-house at your institution)
- Other - Please explain:

25. What online network registration product does your institution primarily use? (Choose one)

- We do not use an online network registration product
- Bradford Campus Manager
- Cisco switches with VMPS
- NetReg (www.netreg.org - Southwestern University)
- NetReg (www.net.cmu.edu/netreg/-Carnegie Mellon)
- Cisco Clean Access (formerly Perfigo)
- "Home grown" (i.e. developed in-house at your institution)
- Other - Please explain:

26. Does your institution conduct passive scans on the residential computer network by using an intruder detection system or other monitoring tool(s) to assess network vulnerabilities or detect devices that violate your policies and requirements? (Choose one)

- Yes, we passively scan both to assess network vulnerabilities and detect devices that violate our policies and requirements
- Yes, we passively scan primarily to assess network vulnerabilities
- Yes, we passively scan primarily to detect devices that violate our policies and requirements
- No, we do not conduct passive scans for these purposes
- No, we do not conduct passive scans at all
- Other - Please explain:

27. Does your institution conduct active scans of the residential computer network by directly evaluating hosts on the network to detect vulnerabilities or devices in violation of your policies and requirements? (Choose one)

- Yes, we actively scan to detect both host vulnerabilities and violations of our policies and requirements
- Yes, we actively scan primarily to detect host vulnerabilities
- Yes, we actively scan primarily to detect devices in violation of our policies and requirements
- No, we do not conduct active scans for these purposes
- No, we do not conduct active scans at all
- Other - Please explain:

28. What technologies does your institution use to monitor your residential computer network? (Choose all that apply)

- Intrusion Detection System / Intrusion Prevention System
- Bandwidth shaper (i.e Packeteer Packetshaper)
- Network Access Control (i.e. Bradford Campus Manager)
- Other - Please explain:

*** 29. Does your institution use a patch management technology that provides OS or security application updates after a computer is connected to your residential computer network? (Choose one)**

- No, my institution does not have a patch management strategy
- Yes, my institution employs patch management technology mandatory for all computers connected to the residential computer network (Response will add one follow-up question asking about the patch management technology)
- Yes, my institution employs patch management technology but it is optional for computers connected to the residential computer network (Response will add one follow-up question asking about the patch management technology)
- Other - Please explain: (Response will add one follow-up question asking about the patch management technology)

30. What security methods on the following list are employed or required for wireless Access Points (APs) managed by residents or managed by the institution on the residential computer network? (Choose all that apply)

Resident Managed APs: Institution Managed APs:

We do not allow / we do not have	<input type="checkbox"/>	<input type="checkbox"/>
No security is required	<input type="checkbox"/>	<input type="checkbox"/>
Wi-Fi Protected Access (WPA)	<input type="checkbox"/>	<input type="checkbox"/>
Wired Equivalent Privacy (WEP)	<input type="checkbox"/>	<input type="checkbox"/>
VPN	<input type="checkbox"/>	<input type="checkbox"/>
802.1x	<input type="checkbox"/>	<input type="checkbox"/>
AP is required to be in bridging mode	<input type="checkbox"/>	<input type="checkbox"/>
Naming convention for SSID	<input type="checkbox"/>	<input type="checkbox"/>
Non-broadcast ("hidden") SSID	<input type="checkbox"/>	<input type="checkbox"/>
MAC Address Authentication	<input type="checkbox"/>	<input type="checkbox"/>
Must be an AdHoc network device	<input type="checkbox"/>	<input type="checkbox"/>
Generic inline security appliance (i.e Cisco Clean Access)	<input type="checkbox"/>	<input type="checkbox"/>

30a. Are other security methods employed or required for wireless APs managed by residents or managed by the institution on the residential computer network? (Choose one)

- No
- Yes - Please explain:

*** 31. What type of oversight does your institution exert over APs installed by residents? (Choose one)**

- Our institution does not allow residents to install personally-owned APs
- Residents must acquire APs from the institution which are configured by the institution's IT or ResNet staff (Response will add one follow-up question asking how the security requirements is enforced post-installation)
- A representative of the institution's IT or ResNet staff configures the resident's personally-owned AP before installation (Response will add one follow-up question asking how the security requirements is enforced post-installation)
- Residents must configure APs in compliance with institutional guidelines (Response will add one follow-up question asking how the security requirements is enforced post-installation)
- The institution does not exert any type of oversight on the installation of personally-owned APs
- Other - Please explain: (Response will add one follow-up question asking how the security requirements is enforced post-installation)

32. If your institution employs wireless technology in residential areas, is the residential wireless network a part of the institution's overall wireless network or is it separate from the institutional wireless network? (Choose one)

- Wireless technology is not provided in residential areas
- Wireless technology provided to residential areas is part of the institution's wireless network
- Wireless technology provided in residential areas is separate from the rest of the institution's wireless network
- Other - Please explain:

2006 ResNet Security Practices and Policies Survey

Final Questions (Section 7 of 7)

33. In addition to data collected from the previous questions, the ResNet Applied Research Group (RARG) is interested in compiling narrative descriptions of security practices applied to residential computer networks. These descriptions may be used to provide a summary of practices to assist others with security implementations for their respective residential computer networks. If you are willing to provide a written description of the ResNet security implementation in use at your institution, please do so here or e-mail your documentation to us at resnetresearch-l@lists.uncg.edu. You may also be contacted by a member of the RARG for follow up on your narrative if further detail is needed.

34. May the researchers contact you for additional information or to clarify or follow-up on your responses to this survey? (Choose one)

- Yes
- No
- Other - Please explain:

35. Would you like to be notified when results of this survey and related research are initially published? (Choose one)

- Yes
- No
- Other - Please explain:

2006 ResNet Security Practices and Policies Survey

Thank You

The ResNet Applied Research Group and the ResNet Steering Committee thank you for the time you spent completing this survey. Please feel free to contact us at resnetresearch-l@lists.uncg.edu if you have any questions. In addition, please contact us if you are interested in assisting with this survey, other surveys, or other research concerning residential computer networks.

The ResNet Applied Research Group would like to thank Azusa Pacific University for their generous support in developing and administering this survey.

CONFIDENTIALITY STATEMENT:

Results of this survey will only be published in aggregate form. Individual and institution names will not be associated with the data in any presentations, publications or published reports. A list of participating institutions will be presented with survey results.
