RINGS
Registration & Security

Dustin Brown
Software Engineer
ResNet - The University of Kansas
03.14.2006
Outline

• I. Introduction
  • 1. About KU
  • 2. What is RINGS
  • 2. What is !(RINGS)
  • 3. A History

• II. Registration
  • 1. DHCP
  • 2. Activation (RINGS SA – Host Based Security)
  • 3. Network Based Security

• III. Management
  • 1. Tools
  • 2. Deactivations & Reactivations

• IV. Network & Hardware Requirements
• V. Open Source
• VI. Resources
• VII. Questions
About KU

- ~25,000 Students
- ~4500 Students in campus housing
What is RINGS?

- Lots of things...
  - Registration
  - Security
  - System Management
  - Staff Management
What is !(RINGS)?

- Trouble Ticket System (Remedy)
- Billing System
- For Sale
RINGS – A History

• Spring 2004 Virus Outbreak
• Developed Summer 2004
  • 6 Developers
  • 3 Months
• Ongoing Development
• RINGS: ResNet Integrated Next Generation System
Registration

- DHCP (Based on ANSR DHCP)
- Web Process
- Activation (RINGS Security Analyzer)
- Network Based Security Measures
ANSR DHCP

• Developed by NTS Software Engineering Team
• LDAP Based
• Java Core
• Very Flexible
• LDAP Browsing
• LDAP Browsing Continued...
• Sys Admin Magazine

![Sys Admin Magazine](image)

**SECURITY**

*Next Generation DHCP Deployments*

*Dave Hull and George F. Willard III*

As device mobility has transformed a novelty into a user expectation, the need for managed dynamic network configuration in campus and wireless environments has grown exponentially. User mobility and ease of end-user device network configuration have become key requirements when designing multi-user accessible networks. Additional challenges in this environment include maintaining security access controls, usage tracking, billing, and end-user support.

**Operating System Fingerprinting**

Increasingly, security and network administrators are relying on device registration systems for access control as well as intrusion detection and prevention systems to maintain network integrity. Additionally, administrators are actively scanning hosts looking for

• ANSR OS Detection

![ANSR OS Detection](image)
ResNet Spring 2005 OS Distribution

- Microsoft Windows XP: 86%
- Microsoft Windows 2000: 3%
- Microsoft Windows ME: 1%
- Microsoft Windows 98: 2%
- Mac OS X: 6%
- Linux: 0%
- Unknown: 2%

- Microsoft Windows XP
- Microsoft Windows 2000
- Microsoft Windows ME
- Microsoft Windows 98
- Mac OS X
- Linux
- Unknown
RINGS Web

• Authentication
• Activation
• Policy Information & Quiz
• Receipt
Welcome to KU ResNet.
We provide network connectivity, voice service, and cable TV to
The University of Kansas’ student residence halls, Stouffer Place
Apartments, and Scholarship Halls.

Now Available
RINGS Security Analyzer
Version 3.0.2
Click Here to Start the
Registration Process

Downloads
2006 Spring Semester

Online Gaming
Register your
XBox or PS2 now!

Alerts!
Still Not Able to Surf the Web After Registering Your Computer? Haven’t Registered?
› Login to the RINGS System to verify you have a registered computer listed.
› Restart Windows

General Info
› Spring 2006 Registration
› Reactivation Fee Information
› Ethernet Card Information
› System Security
› Virus Info and Alerts
› Sophos Help

News
› RINGS goes Open Source
› Spring 2006 Registration Now Available
› RINGS Service Interruption
› RINGS 1.5 Upgrade
› XBox 360 Registration
› XBox and PS2 Come to ResNet
› Jayhawker Towers and Lewis Hall Network Outage
RINGS Account Management Login

Log in with your KU Online Id and password to:

- Register a computer on the Data Network
- Update a registration after hardware changes
- Purchase optional network hardware
- View details about your ResNet account

KU Online Id: ebrmusic
Password: ********

Click here to return to the ResNet homepage.
### Manage Your Account

**Dustin Brown**

- **Email Address:** ebrmusic@ku.edu
- **KUID:**
- **Campus Phone:** 864 9300
- **Home Campus Building:** unknown

Logged in: ebrmusic [logout]

- Shop ResNet's Online Store
- Long Distance PIN Lookup
- Game Console Registration

---

### KU Data Network Registration

**Your current computer:**

![Use This Computer on the ResNet Network]

- **IP Address:** 10.10.152.251
- **MAC Address:** 00:10:a4:7c:c9:04

You have not yet registered any computers with ResNet

---

### Purchase History

<table>
<thead>
<tr>
<th>Name</th>
<th>Qty</th>
<th>Price</th>
<th>Billed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summer 2005 Data Service, Billed Once</td>
<td>1</td>
<td>$48.00</td>
<td>Yes</td>
</tr>
<tr>
<td>Summer 2005 Data Service, Billed Once</td>
<td>1</td>
<td>$48.00</td>
<td>Yes</td>
</tr>
<tr>
<td>Summer 2005 Data Service, Billed Once</td>
<td>1</td>
<td>$48.00</td>
<td>Yes</td>
</tr>
<tr>
<td>Summer 2005 Data Service, Billed Once</td>
<td>1</td>
<td>$48.00</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Preparation for Account Activation

In preparation of gaining internet connectivity through the University of Kansas ResNet services, every user must verify the security of their computer by passing a series of tests. Below, there is an icon that will allow you to download an application that will run these tests. This application will generate an Activation Code that will be used to continue the activation process.

Currently, our system does NOT see that you have successfully generated an activation code. You may need to either download and run the application for the first time or re-run the application. If you somehow have an activation code already, continuing will not present a problem.

Security Analysis:

All students must pass a security analysis to use the ResNet network. This check is done by downloading and running a small application. This Application will verify the prerequisites of Network Activation. Those prerequisites include:

- Proper configuration of Auto-Updates
- Necessary operating system updates
- Use of a firewall on applicable operating systems.
- Proper Local Network Configuration
- The proper installation and configuration of Sophos Anti-Virus software

If your system passes these tests, an activation code is generated and should be entered on the next page. If your system fails these tests, instructions are provided to help secure your system, once your system is secured you can finish the registration process.
Instructions:
1. Remove all antivirus (other than sophos). (It can harm your computer to do otherwise) For instructions click here.
2. Click the download icon to the right.
3. Your browser will prompt you to save or open the file.
4. Choose the option to open the file, you do not have to save it.
5. Once the download is complete, the application should install itself.
6. Once the installation is complete, double-click the icon on your desktop for the RINGS Security Analyzer.
7. When your system passes the security check, the application will generate an activation code that will be entered in a page to come.

Click here to exit and return to account management
Responsible Use Agreement

- There will be a short quiz over the following information in the next step of the registration process.
- View the ResNet Security Breach Port Reactivation Fee Policy (PDF)

**Scope:** This agreement is applies to all residents of student housing and other on-campus housing of the KU-Lawrence campus who access and use University electronic information resources.

**Definitions:** Electronic Information resources include, any hardware or software for the storage, transmission and use of information. This definition includes electronic mail, voice systems, local databases, externally accessed databases, CD-ROM, motion picture film, recorded magnetic media, photographs, or digitized information. This also includes any wire, radio, electromagnetic, photo optical, photo electronic or other facility used in transmitting electronic communications, and any computer facilities or related electronic equipment that electronically stores such communications.

---

**General Provisions**

The University of Kansas provides electronic information resources to residence hall occupants as part of their living arrangements and by agreement. These resources may be used only in support of the education, research, and public service mission of the University and may not be used for commercial or other for-profit purposes. Incidental personal use of electronic information resources is permitted within certain parameters, outlined under Responsibilities of Users. In addition to course-related and incidental personal purposes, such as email, residents of student housing and other on-campus housing may use electronic information resources for recreational computing as long as such use doesn't infringe on the rights of other users.
Responsible Use Agreement Quiz

1. Downloading copyrighted music and movies without permission is illegal.
   - a. This is false. Everyone does it.
   - b. This is silly to worry about because the artists earn TONS of money.
   - c. This is true and I may be sued or prosecuted as a criminal if I do it.

2. Which of the following statements best describes KU's procedure for responding to copyright violation complaints?
   - a. For a first offense, I must respond within 24 hours to the University email I receive confirming that I have deleted the materials named in the complaint. I will also have to retake the quiz I am taking right now.
   - b. For a second offense, I will be required to attend an educational session to learn about copyright laws and KU's student disciplinary process.
   - c. For a third offense, I will immediately lose the privilege of having a network connection in my residence for the remainder of the time I choose to live in KU's residential housing facilities. I will also be referred to an administrative disciplinary hearing that may result in a misconduct record and jeopardize my student status for violating the Code of Student Rights and Responsibilities.
   - d. All of the above accurately describe KU's procedure.

3. Just as I might lend my car to my roommate, it is OK to let my friends borrow my computer account information and my passwords, or PIN so they can access the network.
   - a. This statement is true. It is my access information.
   - b. This statement is false. My passwords, PIN and computer accounts are for my use ONLY.
   - c. This statement is true if my friend and I are taking the same class.
   - d. This statement is false, but it is OK to share them with my little brother.

4. If I am found guilty of violating policies for the appropriate use of the campus network
   - a. I may lose my privilege to use the campus network.
   - b. I may be subject to other sanctions from the Dean of Students Office.
   - c. I may be suspended or expelled from the University.
   - d. I may be liable to prosecution under federal, state or local ordinances.
   - e. I may be subject to any or all of the sanctions listed in items A to D, above.
Registration Confirmation

Logged in: bbrmusic [logout]

Is this information accurate?
If yes, your registration will be complete and you will be billed the appropriate amount

[Yes] [No]

Registration Info:

Name: Dustin Brown
Email: bbrmusic@ku.edu
Bldg: McCollum Residence Hall
Room: 101
Campus Phone: +1 785 812 0000
Term: Summer 2005 Data Service, Billed Once
MAC: 00:10:a4:7c:c9:04
FEE: $48.00

Click here to exit and return to account management
Congratulations! You have finished the ResNet Registration Process. Your connection should come to life within 20 minutes. You should also receive an email with your registration information. You may want to print this page or the email for your records.

Please wait several minutes for the registration to take effect. If you are still having a problem accessing the internet after 10 minutes then try rebooting your computer.

Registration Info:

Name: Dustin Brown
Email: ebrmusic@ku.edu
Bldg: McCollum Residence Hall
Room: 101
Phone: +1 785 812 0000
Term: Summer 2005 Data Service, Billed Once
MAC: 00:10:a4:7c:c9:04
FEE: $48.00
Activation
The RINGS Security Analyzer

- Stand Alone Application
- C# Based for Windows Version
- Java Based for Non-Windows Version
For Windows

• Fully Customizable
• Updates on each use
• Generates User Activation Code
• OS Detection

• Window’s Update Configuration

• Window’s Patch Level
• Non conforming software check (i.e. Norton...)

• Anti-Virus software installation

• Virus free scan
• IP Address Detection (Router Detection)

• Configure and Enable Windows’ Firewall
Welcome to RINGS

Please Evaluate Your System Security

© 2004-2006 The University of Kansas

Need Help? Call 812-0000
Security Analysis Complete

Enter your username and password below then click continue to begin your RINGS Registration.

Username: [Blank]
Password: [Blank]
Activation Code: [Blank]

[□] Just generate my activation code (Do not proceed to RINGS Registration)
Everyone Else
(Non-Windows)

- OS Check
- Anti-Virus Software Check
- IP Address Detection
Welcome to RINGS

Please Evaluate Your System Security

RINGS Security Analyzer

Start  Exit
Security Analysis Results

IP Address
Click here for support information
Determines if your network interface is ready to join the ResNet Network.

Sophos Installation
Click here for support information
Sophos must be installed and updated to use the ResNet network.

Virus Free Check
Click here for support information
Checks to see if a Sophos virus scan was ran today without finding any viruses.
Network Based Security Measures

- Nessus Scans
- IDS
- IPS
- RINGS Security Event Processor
RINGS Security Event Processor

- Java
- XML Messages
- MySQL Database Server
- Server and Client Applications
RINGS Management

• Admin Tools
• Deactivation & Reactivations
• Cable Television and Voice Services
• Emulation
• Lookup By
• IP Address
• MAC Address
• Online ID
• ID Number
• RINGS ID
• Location

Name: [Name]
KU Online ID: [ID]
IP Address: [IP Address]
Mac Address: 00:0f:1f:20:d7:dc
00:0f:20:d7:dc
Rings ID: 3442
KU Student ID: [ID]
Building Name: 104A Jayhawker Towers E
Campus Phone: +1 785 812 [Phone]
Permanent Address: [Address]
Permanent Phone: [Phone]
Network Device Address: 10.10.93.110
Port: 22
Slot: 0
Vlan Id: 335
Create Date: 2004-08-20
Last Update: 2005-05-24 17:17:29.0
• Activation Code Generator
• Server Status
• User Info Manager
- Equipment Manager

<table>
<thead>
<tr>
<th>Serial Number</th>
<th>Type</th>
<th>Subscription ID</th>
<th>Last Updated</th>
</tr>
</thead>
<tbody>
<tr>
<td>0001381071</td>
<td>VDSL Modem</td>
<td>8784</td>
<td>2006-02-10 14:42:28</td>
</tr>
<tr>
<td>8801432021</td>
<td>VDSL Modem</td>
<td>8783</td>
<td>2006-02-10 14:42:57</td>
</tr>
<tr>
<td>0001381023</td>
<td>VDSL Modem</td>
<td>8978</td>
<td>2006-02-10 14:42:29</td>
</tr>
<tr>
<td>0001381024</td>
<td>VDSL Modem</td>
<td>9178</td>
<td>2006-02-10 14:42:29</td>
</tr>
<tr>
<td>0001381025</td>
<td>VDSL Modem</td>
<td>9247</td>
<td>2006-02-10 14:42:29</td>
</tr>
<tr>
<td>0001381028</td>
<td>VDSL Modem</td>
<td>9106</td>
<td>2006-02-10 14:42:29</td>
</tr>
<tr>
<td>0001381030</td>
<td>VDSL Modem</td>
<td>8800</td>
<td>2006-02-10 14:42:30</td>
</tr>
<tr>
<td>8801432034</td>
<td>VDSL Modem</td>
<td>9108</td>
<td>2006-02-10 14:42:58</td>
</tr>
<tr>
<td>0001381036</td>
<td>VDSL Modem</td>
<td>8826</td>
<td>2006-02-10 14:42:31</td>
</tr>
<tr>
<td>8801432037</td>
<td>VDSL Modem</td>
<td>14062</td>
<td>2006-02-10 14:42:58</td>
</tr>
<tr>
<td>0001381045</td>
<td>VDSL Modem</td>
<td>9180</td>
<td>2006-02-10 14:42:32</td>
</tr>
<tr>
<td>8801432046</td>
<td>VDSL Modem</td>
<td>9073</td>
<td>2006-02-10 14:42:58</td>
</tr>
</tbody>
</table>

Lockup: Serial Number

Manage

Insert
Modify
- Work Request Center

### Do Requests

**Equipment Rental**

| Service Request Id  | 1288  
|---------------------|-------
| New Service         | VDSL Modem Rental  
| Address             | 12-4 Stouffer Place Apartments  
| Action Requested    | Deactivate  
| Service Date         | (mm/dd/yyyy)  

| Service Request Id  | 1342  
|---------------------|-------
| New Service         | VDSL Modem Rental  
| Address             | 5-3 Stouffer Place Apartments  
| Action Requested    | Deactivate  
| Service Date         | (mm/dd/yyyy)  

| Service Request Id  | 1354  
|---------------------|-------
| New Service         | VDSL Modem Rental  
| Address             | 5-3 Stouffer Place Apartments  
| Action Requested    | Activate  
| Service Date         | (mm/dd/yyyy)  

Logged in: ebrmusic [logout]
• News Admin
• Services Manager
• Staff Manager
• Student Scheduling System
• Blacklisting a User
• Bug Tracking

NTS Bugzilla

Search existing bug reports
Enter a new bug report
Summary reports and charts
Log in to an existing account
Open a new Bugzilla account
Add to Sidebar (Requires Mozilla or Netscape 6)

Enter a bug # or some search terms:

Actions: Home | New | Search | Find | bug # | Reports | Requests | New Account | Log In

The University of Kansas
Lawrence, KS 66045
785/864-2700

Contact Us: Copyright © 2005 by the University of Kansas: DMCA: Text Only
This file was updated 08/26/03 04:29 PM
Deactivations & Reactivations

- Automated (Triggered)
- Partially Automated (Requested)
- Non Registered Devices (Requested)
- Notifications
Triggered Deactivations

- Triggered after a set number of security alerts from the Security Event Processor
- Currently set for no more than 1 alert of the same type per day. User is deactivated after 3 alerts of the same type
- Notification Email is sent to user.
- User is added to deactivated circuits page
Requested Deactivations

- Any member of ResNet, ITSO, or other authorized organization can request a deactivation
- Notification Email is sent to user
- User is added to deactivated circuits page
Other Deactivations

• In the event a device is not registered there is also a manual deactivation process that allows non registered devices to be blocked.

• Since the user is unknown their system is locked out of the RINGS system.
Reactivating

• Deactivated users are listed on the Deactivated Circuits Admin Page
• Reactivate options are listed there
## Deactivated Circuits Page

### Device Deactivations

[return to Account Management] | [return to Administrative Tools]
[View Device Reactivations]

#### Manual Deactivation

Indicates only DHCP is Disabled
Indicates only Mac Address is Blocked
Indicates DHCP is Disabled and Mac Address is Blocked
* indicates manually-entered entry

<table>
<thead>
<tr>
<th>Customer/Circuit</th>
<th>Location</th>
<th>Device</th>
<th>Info</th>
<th>Net Device port/slot/vlan</th>
<th>Deactivator</th>
<th>Deactivated Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Robert</td>
<td>820 McCollum Residence Hall</td>
<td>129.237.152.00:0c:f1:e5:7c:6c</td>
<td>Host is infected w/ probable Korgo.P varient. See MS040111 patch</td>
<td>10.10.155.15/0/336</td>
<td>perry</td>
<td>2005-02-01 15:50:31</td>
</tr>
<tr>
<td>Kathryn</td>
<td>716 McCollum Residence Hall</td>
<td>129.237.155.00:10:7a:69:51:97</td>
<td>COPYRIGHT VIOLATION. MUST REPLY TO EMAIL FROM <a href="mailto:copyright@ku.edu">copyright@ku.edu</a>, SENT TO STUDENTS KU ACCOUNT.</td>
<td>10.10.155.12/0/336</td>
<td>sorrels</td>
<td>2005-05-16 08:41:18</td>
</tr>
<tr>
<td>Lindsey</td>
<td>1005 Ellsworth Residence Hall</td>
<td>129.237.156.00:07:e9:86:2b:61</td>
<td>COPYRIGHT VIOLATION. MUST REPLY TO EMAIL FROM <a href="mailto:copyright@ku.edu">copyright@ku.edu</a>, SENT TO STUDENTS KU ACCOUNT.</td>
<td>10.10.157.14/0/313</td>
<td>sorrels</td>
<td>2005-03-10 13:18:13</td>
</tr>
<tr>
<td>Jacqueline</td>
<td>721 Lewis Residence Hall</td>
<td>129.237.49.00:0f:20:21:26:14</td>
<td>COPYRIGHT VIOLATION. MUST REPLY TO EMAIL FROM <a href="mailto:copyright@ku.edu">copyright@ku.edu</a>, SENT TO STUDENTS KU ACCOUNT.</td>
<td>10.10.49.31/0/342</td>
<td>sorrels</td>
<td>2005-04-20 15:50:18</td>
</tr>
<tr>
<td>Tom</td>
<td>345 Oliver Residence Hall</td>
<td>129.237.52.00:07:e9:c7:5f:51</td>
<td>Computer has an IRC based bot installed on it and is actively infecting hosts on campus via an LSASS exploit. System has been infected on and off for almost two months. May not be cleaned right</td>
<td>10.10.55.30/0/1</td>
<td>perry</td>
<td>2005-04-04 10:04:58</td>
</tr>
</tbody>
</table>
Network Setup

- Network Topology
- Nessus Scanning Cluster
- IDS
- IPS
- Cisco Option 82 Enabled Gear
Hardware Requirements

• 4500 Users
• 2 – Dell 1750’s (Dual 3 GHz Xeon, 2GB Ram)
• Minimal load on servers at full capacity
• Server 1:
  • Tomcat Web Server
  • RINGS
  • ResNet Website
  • MySQL Database
  • Server Status
  • Security Event Processor (Event Collector)

• Server 2:
  • ANSR DHCP
  • iPlanet Directory Server
Open Source

- Approval granted (06/23/05)
- RINGS 1.5.6 available from Source Forge
- [http://www.sf.net/projects/rings](http://www.sf.net/projects/rings)
- Looking for University partners
What’s Next?

• Integration into our next generation wireless deployment
• 802.1X Integration
• Deployment to other departments on campus
Resources

- ResNet website: www.resnet.ku.edu
- NTS website: www.nts.ku.edu
- RINGS Source Forge: www.sf.net/projects/rings
- ANSR Source Forge: www.sf.net/projects/ansr
- Bugzilla: www.bugzilla.org
- LDAP Administrator: www.ldapadministrator.com
- This and other RINGS presentations: www.resnet.ku.edu/opensource
For More Information

Dustin Brown
Software Engineer
ResNet – A Division of Information Services
785–864–9300
ebrmusic@ku.edu
RINGS–opensource@ku.edu
Questions???