July 16, 2009

Agenda

- Internet2 & TippingPoint
- Back to School
- Apple@Emory
- Research & Health Sciences IT
- Service Catalog & ITSM Evaluation
- Document Imaging
- Webmail High Availability
- Alan White
- Dawn Francis-Chewning & Daniel Palmer
- Alan R. Cattier
- Marc Overcash
- Karen Jenkins
- Felicia Bianchi
- David Gottschalk
Internet2 and TippingPoint

Alan White
TippingPoint IPS

What is TippingPoint?

TippingPoint sits inline on the network and inspects traffic for known exploits and policy violations.

<table>
<thead>
<tr>
<th>Time</th>
<th>Severity</th>
<th>Name +</th>
<th>Category</th>
<th>Action</th>
<th>Hit Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>4463</td>
<td>SYMANTEC: AntiVirus Client Buffer Overflow</td>
<td>(461)</td>
<td></td>
<td></td>
<td>3703</td>
</tr>
<tr>
<td>3888</td>
<td>HTTP: PHP File Include Exploit</td>
<td>(398)</td>
<td></td>
<td></td>
<td>720</td>
</tr>
<tr>
<td>1456</td>
<td>MS-SQL: Slammer-Sapphire-Virom</td>
<td>(61)</td>
<td></td>
<td></td>
<td>51</td>
</tr>
<tr>
<td>5121</td>
<td>Telnet: Login Bypass (General)</td>
<td>(22)</td>
<td></td>
<td></td>
<td>26</td>
</tr>
<tr>
<td>4276</td>
<td>HTTP: PHP Code Injection</td>
<td>(5)</td>
<td></td>
<td></td>
<td>20</td>
</tr>
<tr>
<td>4212</td>
<td>HTTP: PHP File Include Vulnerability</td>
<td>(13)</td>
<td></td>
<td></td>
<td>20</td>
</tr>
<tr>
<td>5291</td>
<td>MS-RPC: Microsoft DNS Service Buffer Overflow</td>
<td>(2)</td>
<td></td>
<td></td>
<td>12</td>
</tr>
<tr>
<td>3601</td>
<td>HTTP: PHP File Include Vulnerability</td>
<td>(6)</td>
<td></td>
<td></td>
<td>10</td>
</tr>
<tr>
<td>1585</td>
<td>HTTP: Jat Command Execution</td>
<td>(2)</td>
<td></td>
<td></td>
<td>8</td>
</tr>
<tr>
<td>4810</td>
<td>HTTP: PHP File Include Exploit</td>
<td>(5)</td>
<td></td>
<td></td>
<td>8</td>
</tr>
</tbody>
</table>
TippingPoint IPS

Quarantine

TippingPoint is also used to quarantine IP addresses

Your Computer Has Been Quarantined

Your Network Access Is Limited

The TippingPoint Intrusion Prevention System has quarantined your computer. Typical reasons for this include

- Virus Infection
- Spyware
- Network Policy Violations

The offending traffic has been automatically blocked to protect you and other users. While quarantined, your network traffic will be limited.

Emory Healthcare users receiving this message Please contact the Call Center at:

- 404-778-4357 (8-HELP)

Emory University users receiving this message Please call the help desk at:

- Atlanta Campus - 404-727-7777
- Oxford Campus - 404-784-4685
TippingPoint IPS

Current Deployment

Internet

TippingPoint IPS

Internet

TippingPoint IPS

Internet

TippingPoint IPS

Emory

Internet2
TippingPoint IPS

Coverage for Internet2
TippingPoint IPS

Coverage for Internet2

- Internet2 is 10 Gbps
- Our current TippingPoint boxes are 1.2 Gbps
- Emory has not exceeded 1.2 Gbps in the past year
TippingPoint IPS

Coverage for Internet2

- Insert TippingPoint IPS unit between Emory and Internet2

- Gather information and let management decide if we should invest in a solution that can cover 10 Gbps
TippingPoint IPS

Coverage for Internet2

- Proposed implementation:
  - July 29th between 9pm and 10pm

- Waiting on CRB approval
Questions
Back to School

Dawn Francis-Chewning & Daniel Palmer
Back to School

On Your Mark

ResNet
2009

EMORY
Back to School

Already?

• When does it happen?
• Who is it for?
• Why do we do this?
• What’s different?
• How do we do it?
Get Set!

Emory On Line (EOL)
- 64 bit support
- Symantec Endpoint Protection
- Skype Supernode
- Adobe Flash
- FirstClass

*Fewer Windows Updates
*MalwareBytes in manual install
Back to School

It’s a Go!

BTS Now & Then Review: July 23
Account Master/Coordinator Trg 8/3
Tech Training: August 20

Anticipated Arrivals
August 19 – International Students & Student Athletes
August 22 – Saturday, Freshmen
August 23 – Sunday, Upperclass
Questions
Apple@Emory

Alan R. Cattier
Apple@Emory

SAVE THE DATE!

October 12th, 2009
• Focuses
  – Snow Leopard
    • Apple Mail and Exchange 2007
    • Entourage and Exchange 2007
  – Citrix, VDT, and the Mac
  – Parallels and VMware Fusion
  – iPhone and Ipod Touch
    • Apps in the Medical Arena
    • Securing your Device
Apple@Emory

October 12th, 2009

• Other Highlights
  – Emory Genius Bar
  – Favorite Emory MacTips
  – TechTrack with Emory MacExperts

• Save the Date
• Look for Online Registration
• Tell Your MacUsers and Apple Curious
Thank You to:

- Megan Levitt: SOM
- Tiffany Kady: SPH
- Eric Logan: OIT
- Shea Jarman: UTS
- Jim Brown: Oxford
- Damon Lynch: ECCS
- Marcus Rodriguez: Library
- Alex Kyrychenko: Library
Questions
Briefing On

- Division of Research & Health Sciences IT
- Key Projects/Platforms
R&HS

Boxes Aside

• 28 FTE positions
• Bifurcated missions of:
  – Supporting Research through IT
  – Coordinating WHSC IT
• Key Areas:
  – HPC
  – Web Design
  – Data Management
  – Project Management
  – Programming
  – Research Areas (Research LIMS, Data Capture)
Platforms/Key Services

- eBIRT
- Data Capture
  - Surveys
  - Electronic Case Reports
- Virtual BioRepository
- High Performance Computer Cluster
- Web Design Group
eBIRT

Electronic Biomedical Interactive Resource Tool
Investigators find resources
- Cores

Emory University & Morehouse School of Medicine

National Efforts
### Electronic Data Capture

**Features:**
- Skip Patterns/ Data validation
- Longitudinal Study Support
- Export to analysis tools (SAS, SPSS)

**Types:**
- Surveys (a la WebMonkey)
- Clinical Research

---

<table>
<thead>
<tr>
<th>Demographics</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Editing existing Study ID “1”</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Study ID</strong></td>
<td>1</td>
</tr>
<tr>
<td><strong>Demographic Characteristics</strong></td>
<td></td>
</tr>
<tr>
<td>Data subject signed consent</td>
<td>YYY-MM-DD</td>
</tr>
<tr>
<td><strong>First Name</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Last Name</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Contact Information</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Street, City, State, ZIP</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Phone number</strong></td>
<td>Include Area Code</td>
</tr>
<tr>
<td><strong>Second phone number</strong></td>
<td>Include Area Code</td>
</tr>
<tr>
<td><strong>E-mail</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Gender</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Race</strong></td>
<td>Caucasian, African American, Hispanic, Asian, Other</td>
</tr>
<tr>
<td><strong>Date of birth</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Height (cm)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Weight (kilograms)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Dry weight (kilograms)</strong></td>
<td></td>
</tr>
</tbody>
</table>
Virtual BioRepository

Laboratory Information Management Systems

- Research Labs to manage data, specimens, quality control
- Connecting Research Labs together
- Searching across Multiple Repositories for Specimens
- 1024 node cluster
- Operation over 2 yrs
- Average 50% utilization last month
- Augmented with a Large Scale Memory Machine
- Latest addition
- Content migrations onto Cascade
- Web site development
- Flash and interactive applications
Electronic Conflict of Interest

- Manage conflict of interests and conflict of commitments across University
- Annual certification process
Questions
Service Catalog

Karen Jenkins
Within Service Design

- Service Strategy
- Service Design
- Service Transition
- Service Operation
- Continual Service Improvement

Service Design
Service Catalog

Terminology

• Service Catalog (Phase I)
  – Defines the services that are in production or readily available
  – Defines the scope, conditions, options and service levels

• Service Request Catalog (Phase II)
  – List of available service requests
  – Value is measured in turn-around time, backlog, cost, customer satisfaction
Restaurant Analogy

Do you order ingredients?

Eggs, butter, salt, pepper, garlic, bread crumbs, olive oil, oregano, mozzarella cheese, parmesan cheese, tomatoes, pasta, chicken

... or the entree?

Chicken Parmesan - *Breaded chicken breasts topped with Marinara sauce, roasted Bruschetta, Mozzarella and Parmesan cheese, and herbs. Served with linguini.*
Service Catalog

Email Example

Service

Features / Options

HW Platform

Exchange S/W

Zantaz (EAS)

.Server 1

Server n

Email

OWA

BlackBerry
Service Catalog

Guidelines

**Do’s**
- Present in customer friendly terms
- Group according to business drivers
- Create a “menu” of Service Offerings
- Set initial customer expectations
- Create an Actionable catalog*

**Don’ts**
- List tasks organized by UTS departments
- List the functions of a team
- Identify the features of a service
- Write in technical jargon
- Provide all the gory technical details

*Service Request Catalog in Phase II*
Approach

• Workshops with service owners to provide overview of services
• Customer oriented names & groupings
  – Eighteen open card sorting exercises with faculty/staff/students
  – 4 closed sorting exercises
• Developed in Cascade using Emory template
• Workshops with UTS, Local Support, and customers to obtain UI feedback
https://secure.web.emory.edu/it/staging/catalog
Service Catalog

Local Support Workshops

• Still scrubbing content ... for now concerned with layout and usability
• Please attend a workshop
  – Friday July 17th 10:30 -5:00, North Decatur Building, Kennesaw 225
  – Monday July 20th 9:00 – 5:00, Woodruff Memorial Library, ECIT 217
Questions
IT Service Management Evaluation
Incident Management Summary

Open Incidents - Aging Report

<table>
<thead>
<tr>
<th>Aging</th>
<th>Local Support</th>
<th>UTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 Days</td>
<td>35</td>
<td>42</td>
</tr>
<tr>
<td>3 Weeks</td>
<td>120</td>
<td>59</td>
</tr>
<tr>
<td>3 Months</td>
<td>159</td>
<td>50</td>
</tr>
<tr>
<td>3+ Months</td>
<td>251</td>
<td>36</td>
</tr>
<tr>
<td>Total</td>
<td>187</td>
<td></td>
</tr>
</tbody>
</table>

Change Management

- 8 RFCs submitted (wk)
- 7 RFCs approved (wk)
- 7 Changes implemented (wk)
- 50% Successful Emergency Changes to date
- 93% YTD Changes successful

Service Management - Annual

<table>
<thead>
<tr>
<th>Priority</th>
<th>Met</th>
<th>Missed</th>
<th>Actual</th>
<th>Goal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>65</td>
<td>19</td>
<td>77.38%</td>
<td>90.00%</td>
</tr>
<tr>
<td>High</td>
<td>408</td>
<td>31</td>
<td>92.94%</td>
<td>85.00%</td>
</tr>
<tr>
<td>Medium</td>
<td>4559</td>
<td>449</td>
<td>91.03%</td>
<td>85.00%</td>
</tr>
<tr>
<td>Low</td>
<td>17826</td>
<td>64</td>
<td>99.64%</td>
<td>85.00%</td>
</tr>
</tbody>
</table>

Today

- 8 RFCs submitted (wk)
- 7 RFCs approved (wk)
- 7 Changes implemented (wk)
- 50% Successful Emergency Changes to date
- 93% YTD Changes successful
ITIL v3

26 Processes

SERVICE STRATEGY
- Service Strategy
- Service Portfolio Management
- IT Financial Management
- Demand Management

SERVICE DESIGN
- Service Catalog Management
- Service Level Management
- Supplier Management
- Capacity Management
- Availability Management
- Continuity Management
- Information Security Management

SERVICE OPERATION
- Event Management
- Incident Management
- Request Fulfillment
- Problem Management
- Access Management

SERVICE TRANSITION
- Transition Planning and Support
- Change Management
- Service Asset & Configuration Management
- Release & Deployment Management
- Service Validation & Testing
- Evaluation
- Knowledge Management

CONTINUOUS SERVICE IMPROVEMENT
- Service Measurement
- Service Reporting
- Service Improvement
1. We could do more than Incident
2. We could actually find Services
3. Reporting wasn’t based on Excel
4. Self service was real
   a) For requests
   b) For self-help
   c) For status updates
5. We had a better interface
6. We could save money
Service Management

Your Alternative

Emory University - IT Service Management Suite

My ITIL Homepage

News
- Home)mopation: We have a new office
- Sales Force Automation is DOWN
- Reminder: Email Interruption Tonight at 11:00 PM Eastern
- New Corporate Travel Policy
- Reminder: PC Refresh starts next week
- SAP Outage - We are aware of the SAP outage. Service will be restored soon

All Incidents By Assignment

Open Items by Escalation

My Open Incidents

ITIL Summary Counts
- Critical Items
- Overdue Items

Done
Service Management

Today - How many clicks?
Service Management

Today - self-service

NEW REQUEST

Step 1: Verify contact information
You may change your contact information here if needed.

First Name: brett
Last Name: cornell
Phone: 404-727-6147
Email: brett.cornell@emory.edu

Step 2: Select a summary
Please select the subject of your request by selecting a summary from the drop-down list

Summary:
- Application
- CampusLife Division
- Clean Room
- Compromise / Virus
- Departmental Application
- Development Alumni Relations Support
- General Services
- Network
- New Account
- Other
- Paging & Radios
- Procurement and Payment Services
- Research
- Research IT
- UTS Security
- Web Hosting
- eResearch

Optional: Routing
Your request will be automatically routed to the appropriate support team.
To override this automatic routing, please select a support group from the list:

Assign to Support Group: [Dropdown]

Submit
Cancel
Service Management

Alternative

Catalog Item - Development Laptop

Laptop preconfigured for developers

- 2.0 GHz Intel Core Duo Processor
- 1 GB of memory
- 15.4" 1680 X 1050 screen

Developers have the option of ordering a larger hard drive and can specify what operating system they need installed.

What size hard drive do you want?
- 80 GB [subtract ($20.00)]
- 90 GB
- 100 GB [add $110.00]

Please specify an operating system
- Windows XP [subtract ($50.00)]
- Windows Vista

Order Status

Summary
Your request number is REQ10008, which you can use to refer to this request in future interactions with the service desk.

You may also bookmark the following link to get back to REQ10008.

Note that clicking on the bookmark link (above) will simply take you back to this screen.
Service Management

Why now?

1. We are all frustrated with Remedy
2. We have divergent practices ... now we know better
3. All IT groups are facing cost pressure  
   a) Remedy is expensive as is  
   b) Maybe something else costs less
4. Good practices save money ... we need additional modules
5. BMC’s licensing model is broken  
   a) $87k to buy the car (new modules)  
   b) $258k to buy the keys (licenses)
Objectives

1. Usability
   - Improve self-service
   - Simplified support interface
   - Current technology

2. Deployment Speed
   - Easier administration
   - Rapid deployment of modules
   - Faster deployment of enhancements

3. Cost
   - Reduce annual spend
   - Reduce cost for new capabilities/modules
Service Management

Our best hope

1. Other vendors (HP, CA) are similar to BMC
   a) Expensive
   b) Complex

2. SaaS model is attractive
   a) Reduces software cost
   b) Eliminates hardware refresh, OS support

3. Service-now looks viable
   a) Fully featured with simple UI
   b) Highly configurable
   c) In business since 2004, profitable, quarterly revenue growth, 2x revenue last fiscal year
   d) Significant number of large customers (Hyatt, TIAA CREF, CBS, Facebook, Cisco, MetLife)
Service Management

Simplified administration

Fact Sheet

282 Customers
3,770,850 End Users
6,188 Successful Upgrades*
16 Releases since founded

Product Integration

- **Single Sign On**
- **Business Applications**
- **Events/ Alert / Alarm**
- **Discovery Data**

- **PGP**
- **Oracle Financials**
- **Tivoli (TEC)**
- **IBM CCMDB**

- **SAML**
- **Oracle PeopleSoft**
- **SPECTRUM**
- **Altiris**

- **Digest**
- **Salesforce.com**
- **HP OpenView**
- **HP OpenView**

- **Site Minder**
- **Right Answers**
- **JMS**
- **LanDesk**

- **Site Minder**
- **Right Answers**
- **JMS**
- **LanDesk**

- **SAP**
- **LDAP**
- **Nimsoft**
- **EMC Smarts: ADM**

- **EMC nLayers**

*Upgraded 1,000 instances in 2 hours
Service Management

Evaluation Approach

• Define campus-wide working group
  – Solicited volunteers through ITPC and DeskNet
• Identify functional requirements
• Identify evaluation scenarios
• Create PoC environment for evaluation
• Recommendation by July 31st
Service Management

Working Group

Todd Burroughs  UTS, ITSMO
Paul Corigliano  University Relations
Tina Crum  UTS, ITSMO
April Dunson  Emory College
Karla Fields  Oxford College
Tiffany Kady  School of Public Health
Andrew Kincaid  UTS, Enterprise Apps
Meggan Levitt  Department of Medicine
Eric Logan  Research & Health Sciences
Jean Robert Mathador  School of Medicine
Farah Remtulla  UTS, ITSMO
Al Shelton  UTS, Enterprise Apps
Joel Thomas  School of Medicine
Luciano Dalla Venezia  UTS, ITSMO
John Wilson  UTS, Enterprise Apps
Service Management

Status

• 8 demonstrations and Q&A sessions completed
• Team has worked through
  – 25 functional requirements and evaluations scenarios
  – Over 40 questions answered to team’s satisfaction
  – 90% of Change process configured in one-day
• All working members involved in evaluation and own one or more functional requirements
Reactions

• Favorables:
  – Team impressed with the usability of the tool
  – Very flexible
  – Customizations not lost with upgrades
  – Survey, Knowledge, and Reporting superior to Remedy

• Concerns:
  – Training for administrators
  – Campus involvement with the rollout
  – Quote, contract, references
Questions
Document Imaging

Felicia Bianchi
Requirements

- Enrollment Services has a pressing need for Imaging
- Integration with PeopleSoft
- Current Imaging solution does not scale well
- Need for centralized scanning on campus
Document Imaging

Current project Status

• RFI/RFP process complete
• Campus vendor presentations
• Three finalists chosen
• Proof of Concept process refinement
• Onsite visits to vendor finalists
• Reference checks for the finalists
Next steps

- Sign a Statement of Work for a POC
- Schedule the POC on campus
- Several groups involved in the POC
  - Admissions
  - Purchasing
  - Human Resources
  - Department of Medicine
- Communications to all other interested parties
Questions
Webmail High Availability

David Gottschalk
Old Architecture

- 2 Apache Web servers running Solaris on old Sun 480.
- 1 Database server running Solaris on a Sun 480.

Problems
- Old hardware out of maintenance needed to be replaced.
- Software was significantly out of date and had multiple security vulnerabilities.
- Overall system performance was poor, and system was not redundant.
Webmail

Old Architecture

Old Webmail Architecture

HTTP/HTTPS Traffic

Front-end Web Servers

MySQL Connection

MySQL Database Server

HTTP/HTTPS Traffic

Load Balancer

webmail.service.emory.edu
170.140.52.143

Client Web Browser

Webmail Servers

Alkmene - 170.140.202.42
Sun 480R; 16GB

Aglaja - 170.140.202.46
Sun 480R; 16GB

IMAP Connection

Daphne - 170.140.202.44
Sun V240; 2GB

IMAP Connection

pop.service.emory.edu
170.140.52.105

imap.service.emory.edu

Webmail

New Architecture

- 2 Web servers running Linux on a VM
- 1 Database server running Linux on a VM

Software

- Latest version of Apache/Horde/IMP.
- Updated version of MySQL on database server

Problems

- Oracle did not work properly with Horde/IMP
- Switched to MySQL on Linux VM.
- Vacation application had to be replaced.
Questions