IT Briefing Agenda

• Exchange/Voice Roadmap
• IM Implementation
• Continuous Security Scan
• General Security News
• Bookstore Announcement

• Jay Flanagan
• Farah Remtulla
• Elliot Kendall
• Brad Judy
• Leah Toy
Jay D. Flanagan
Manager – UTS Messaging
Exchange/Voicemail Roadmap
Archiving Replacement
Voicemail Refresh
Office 365 – Student Email
Exchange/Voicemail Roadmap
Farah Remtulla
ITSM Specialist – UTS PMO
itSMF Project of the Year

Incident Management Implementation
- On-going development and promotion of ITSM (IT Service Management) best practices, standards and qualifications in the United States
37 000 Customers
400+ IT Support Staff
~8 “Tools” (Listservs & Spreadsheets inc)
25 IT Support Organizations
And let’s not forget…
We’re ALL Unique!
Gaps drove functional requirements
Value Creation
Value Creation
Value Creation
Cultural Transformation
Elliot Kendall
Information Security Specialist – OIT Enterprise Security

Continuous Security Scanning
How it works now

Scheduled scans

• Four scanning servers, one per network core: Academic, DMZ, Secure Admin, HIPAA

• Each has a schedule of scans to run each month – on day X, scan network block Y
How it works now

What’s wrong with that approach?

• Inefficient – scans lots of addresses that are unused
• Incomplete – easy to miss systems that aren’t online all the time
• Out of date – scan runs only once a month. Firefox major versions come out more often!
The New Approach

Continuous scans

- Keep a set number of scan jobs running on each scanner server, number TBD

- When a job finishes, intelligently determine next address to scan
The New Approach

Intelligent target selection 1

- ARP (Address Resolution Protocol) maps MAC addresses to IP addresses
- Network switches maintain tables of cached MAC/IP pairs
- We can query the tables with SNMP and aggregate the results
- Result: we know what IP addresses are in use at any given time
The New Approach

Intelligent target selection 2

• When we scan a system, save the time and IP address to the database
• Now we know what’s online and the last time we scanned each address
• Just pick the online address with the last scan time farthest in the past
• Hard limit of one scan per day per IP!
The New Approach

Scanners → Scan Engine

Scan Engine → ARP Database

ARP Database → Switches

Scanners → Scan Time Database

Scan Time Database → ARP Database

Who is online?

I just scanned IP

Who should I scan next?

Results

Scan IP

10/20/11
The Future

Emory Security Portal

• Will offer access to scan data on the web
• Every group can see data for its own devices and networks
• High-level data for managers, and detailed data for technicians
• More info coming soon!
Security Scanning

Questions
Information Security

Brad Judy
Information Security Specialist – OIT Enterprise Security

Information Security
AV Consolidation

• RFI’s were evaluated and four vendors moved forward
• Team attended vendor demos from:
  – Symantec
  – McAfee
  – Kaspersky
  – Trend
• Now selecting two vendors for POC
• AVCONSOLIDATION-L@LISTSERV.CC.EMORY.EDU
Awareness

• Copyright infringement
  – Annual requirement for HEOA

• Smartphone security policy
  – Coming soon to Local-L
  – Maybe Dec awareness topic?
Emory Bookstore Announcement

Leah Toy
Marketing and Sales manager

10/20/11
Emory Bookstore Announcement

• Emory Express

• Original iPad Sale
Thank you for coming!