INFORMATION TECHNOLOGIES COMMITTEE
MINUTES OF MEETING
DECEMBER 7, 2004

[In these minutes:
SCIT Meeting Time for Spring Semester 2005, SPAM/Antivirus Update, Network Upgrade Update, Network S
Update]

[These minutes reflect discussion and debate at a meeting of a committee of the University of Minnesota Senate
Cities Assembly; none of the comments, conclusions or actions reported in these minutes represent the views o
binding on, the Senate or Assembly, the Administration or the Board of Regents.]

PRESENT:
Andy Lopez, chair, Nancy Herther, Mark Sanders, John See, Dale Swanson, Jeff Johnson, Linda Jorn, David D
Lynda Ellis, Douglas Ernie, Stuart Speedie, Jim Waddell, Tun Jie, Mahmoud Sadrai

REGRETS: Stephen Cawley, Eric Celeste, Alan Ek, Pushkar Ojha

ABSENT: Greg Laden

OTHERS: Bernard Gulachek, Ken Hanna, John H. Miller, Shih-Pau Yen

I). Professor Lopez called the meeting to order.

II). Announcements:
Professor Lopez announced that the SCIT meeting schedule will maintain the same for spring semester 2005, th
Tuesday of each month from 2:30 – 4:00.

III). Bernard Gulachek provided members with a spam/anti-virus update. He noted that the Office of Informat
Technology (OIT) is working diligently to block spam and viruses from entering the University, at the same tin
striving to not block messages intended to enter the University.

Mr. Gulachek distributed a handout, which highlighted the following information:

- The University has approximately 155,000 central e-mail accounts.
- During 2004, the University received roughly 300 million incoming email messages of which 171.5 millio
  blocked because of spam or viruses.
- OIT uses a multi-faceted approach to manage spam. Examples include:
  - Understanding spam sources and subscribing to a service, which publishes them.
  - Blocking certain dynamic IP addresses that are serving as mail servers. Legitimate mail managemen
    have mail management practices in place with dedicated IP addresses that have specific host names t
    validated and verified.
  - Investigating insecure servers by bouncing messages back to see if the servers are secure or not. If a
    server is identified as insecure, OIT will send a message back to the server telling it how it needs to b
    in order for the University to accept its mail.
    OIT does not want to block mail intended to be received by members of the University community.
  - Blocking particular originators of spam and viruses at the Universityπs border. Blocking spam is OI
    defense from receiving viruses.
  - The use of SpamAssassin to deal with spam that has entered the University community. SpamAssas
    open-source product.
    Users can elect to earmark mail messages from a particular host as spam, and then OIT will manage
    messages.

- In terms of blocking viruses, OIT scans all inbound and outbound messages to ensure viruses are not detec messages with viruses, are set aside and users can go to their blocked list to view these messages. Therefc messages are not necessarily turned away but rather quarantined. OIT also uses a vendor solution, McAfe viruses after they have been filtered for spam.
  Outbound messages that go through the central servers with a virus are reported to OIT Security who follc the user to let him/her know that a virus has been detected.
- Mr. Gulachek referenced a couple web sites with various management tools to assist individuals using one Universityπs central servers to help manage their email.
  Additionally, he distributed a flowchart, which depicts how email is handled once it comes into the Univer central servers.

Comments/questions from members:

- Despite the fact OIT blocks a significant amount of spam, additional spam continues to enter the Universit spam be reduced even further? Vendors continue to develop products to reduce spam count and/or virus c Gulachek added that the University collaborates with other Big 10 universities in terms of developing spar strategies.
  The University is also a member of the åCommon Solutions Groupπ (CSG – for more information visit the URL: http://www.stonesoup.org/).
  The CSG is comprised of a group of universities who are seen as leaders in dealing with solutions to IT ch higher education.
- Are faculty and students, for example, targeted differently in terms of the type of spam they receive? Whi Gulachek is unaware if this is occurring, another member stated that spammers are targeting different Uni community members differently.
- Is there any legislation pending around spam and virus issues? Mr. Gulachek noted the CAN-SPAM Act
- Please comment on the recent system failures to block spam/viruses. Mr. Gulachk reported that OIT has b with EMC to gradually implement storage area network technology as a way to manage the Universityπs e data e.g. email, PeopleSoft, Portfolio, etc.
  Within the last few weeks, OIT experienced a hardware problem followed by a software problem with this Since this time, OIT has replaced some hardware and continues to work with the vendor, EMC, on the sof problem.
  To lessen the impact of a similar problem in the future, in-boxes and previously read messages have been different places on the storage area network.
- It appears that the University is moving away from a client-based approach to a mail service and moving t web-based approach. If this is so, how will todayπs email system be impacted? Would the University be offer one mail service for the entire University community?
  According to Mr. Gulachek, OIT is not necessarily moving in this direction, but wants to be able to facilita for those that are interested in doing so.
  OIT believes as faculty, staff and students become more mobile; a central repository is increasingly necess storage area network is being rolled out, the University is experiencing some growing pains. However, o have been worked out of the system, the University will have a very robust and scalable centralized storag will be able to multi-purpose itself for other applications and purposes.
- More needs to be done to improve web mail.
  A member suggested SCIT actively recommending policy to promote a better web-based email service, w be available to the entire University community.
  An OIT representative cautioned members to be careful what they request and to think the matter through There is a lot to think about in terms of liability issues, financial issues, etc. when it comes to one central e for all faculty, students and staff.
- The University should look into outsourcing its email service. Mr. Gulachek acknowledged that some uni this.

IV). John Miller provided a brief network upgrade update. He highlighted the following:

- In mid August, the new networking core was cut into place.
- There are 65 buildings now connected to the new Edge equipment, out of a total of approximately 195 bui of these 65 building, roughly 9700 active connections have been moved, representing 565 ether switches, been cut over.
- The project is expected to be completed during first quarter 2005.
- LAN administrators have been assisting NTS with this project.
- On average, the trouble rate per building is approximately 5%.
- Currently, NTS is installing and cutting over the new network in the AHC and the some of the residence h campus e.g. Pioneer, etc.
- In conjunction with the new network, NTS purchased a firewall blade. This is a piece of hardware that co software, which allows 255 virtual firewalls to be programmed within the routers. The AHC with its HIP Insurance Portability and Accountability Act of 1996) concerns is very interested in this feature.
- A Quality of Service draft has been completed and presented to Steve Cawley and Shih-Pau Yen for revie Miller noted that the Quality of Service Guidelines treats different types of traffic differently as it travels a network. The document prioritizes traffic using these guidelines:
    1. Management traffic
    2. Special applications (to be defined)
    3. Voice Over IP
    4. Video
    5. Other special applications
- The management system within the network is capable of telling NTS about troubles on the network in ad providing statistical information.
- In conjunction with the service delivery department within NTS, a Service Authorization Matrix will be r service authorization matrix is defined, at this moment and for this purpose, as an informative tool that tel has responsibility/authority for network connections in rooms, floors and/or campus buildings. This matri used for self-service delivery purposes.
- Next steps for NTS:
    - Implement Quality of Service (QOS) Guidelines.
    - Turn on multi-cast across campus.
    - Develop the Service Authorization Matrix, which internally is called åslice and diceπ.

Questions/comments from members included:

- Once the Service Authorization Matrix is put in place will it be possible to find out who is the owner of a jack? Yes, jack owners will know if they are responsible for a jack or jacks. The goal is to localize jack(s wherever possible rather than having users go to NTS for support.
- Once the Service Authorization Matrix draft is completed it would be a good idea to bring it before SCIT
- Will end-users be expected to do any kind of traffic shaping? This remains under evaluation. Scalability management tools and ånetwork policyπ implications have not been sufficiently evaluated, and, need to be moving too quickly on this and other services.
- Are there a lot of people converting from private LANs to the Universityπs etherjack service? Yes, severa indicated an interest in working with NTS to use the Universityπs etherjack service.
- How does the wireless network tie into the new network? No changes have been made to the wireless ser
- A member complimented and thanked NTS for all its hard work related to the network upgrade.

V). Ken Hanna provided a network security update. He highlighted the following:

- Malware is short for malicious software. This software is designed specifically to damage or disrupt a sys Examples of Malware include:
    - Viruses, trojans and worms, which are high security risks for the University.
    - Botnets are a major security headache and often a hidden problem. Botnets are compromised compu controlled by cybercriminals to send spam, etc.
      There are hundred of thousands of computers, which are controlled by other people across the world.

- Phishing or scam emails often pose as 'security check' emails from well-known businesses. These en computer users to send private information such as passwords, social security numbers, which can th for identify theft, etc.
- Infected web sites.
- Spyware is Internet jargon for Advertising Supported software (Adware). It is a way for shareware a make money from a product, other than by selling it to the users. MarketScore is a Spyware, or, in o proxy service, which claims to increase the speed of you Internet connection. It runs at start-up to en web connections are routed through its proxies.
  Users do not observe any significant speed increase from using the service. Every web connection a including åsecureπ connections, goes through the proxies and is logged and analyzed on behalf of M customer companies.
- Root kits for Windows.
- Password cracking.

- Examples computer defenses to address security issues include:
  - Installation of anti-virus software, which is centrally funded available at the mail server and host leve
  - Use of firewalls and filtering products e.g. MircroSoft Service Pack 2.
  - Automated patching using the SUS (Software Update Services) server.
  - Use of security configuration services, which OIT will have available within the next three months.
  - Follow configuration standards and guidelines.
  - Conduct vulnerability scans as needed on servers.
  - Promote user awareness and education.

- Examples of network defenses to address security issues include:
  - Use of border filters.
  - Investigate top talkers or computers that are doing a lot of email traffic.
  - Watch router flows for sources and destinations of traffic and investigate certain ports as needed.
  - Provide intrusion detection services.
  - Investigate DNS anomalies.
  - Installation of Resnet, an access scanning system.
    ResNet provides those living in the residence halls with access to the Universityπs network and the I

- Mr. Hanna shared his thoughts on trends related to security issues. He noted the following:
  - Vendors are producing somewhat more secure software.
  - There continues to be an increased amount of computer criminal activity by organized crime with a p
  - Increased propagation of Malware.
  - More legal requirements by the government in terms of security.
  - An increased amount of information sharing amongst institutions of higher education and beyond rel security.

- In terms of the future, Mr. Hanna foresees:
  - Use of the new features and capabilities in the new network, which is currently being installed.
  - An increased use of firewall and filter products.
  - A concerted effort to promote user education and aware around security issues.
  - The University becoming involved with the use of automated response capabilities.
  - The University continuing to fight the åarms raceπ just to maintain the status quo in terms of security

Questions/comments from members included:

- Were any University passwords stolen through the use of MarketScore? There was no evidence of this sta Hanna.
- Has OIT received feedback from students regarding Resnet? No systematic survey has been conducted, b

be a good question to ask students.

- Has OIT considered registering all ≥Mac≤ (i.e. hardware) addresses? OIT has raised this issue, and, in the good idea, but in practice it would be very difficult to implement due to the size and complexity of the net new network has the capability of locking Mac addresses to switch plates. Mr. Hanna stated that OIT wou proceed cautiously should it decide to move forward with this idea.

VI). Professor Lopez stated that the next Committee meeting is Tuesday, February 1, 2005. Members decided like the following items on the February agenda:

- Technology fees – Mr. Gulachek will arrange for someone to address this topic.
- VOIP - Professor Lopez agreed to contact Linda Deneen to address this topic.
- Classroom Technology Upgrade – Renee Dempsey, Senate staff, was charged with inviting OCM Director Fitzgerald.

VII). Hearing no further business, Professor Lopez adjourned the meeting.

Renee Dempsey
University Senate