

Network Committee

March 12, 2007

Minutes

Attendees: Heidi Schmidt, Jose Claudio, Enrique Terrazas, Carl Tianen, Tim Greer, Chris Orsine, Mike Strizich, Sean Schluntz

Daylight Saving Time: Most network devices not updated, so device logs may be one hour off for the three-week period March 11 to April 1. Any issues with this will be handled manually.

ENS Updates: No updates this month.

Enterprise Information Security (EIS) Updates:

1. *Recording industry copyright violations:* The recording industry has stepped up enforcement and prosecution efforts around illegal copyright infringement activities. The UCSF Security Officer is being ordered to "protect and preserve" all information on IP addresses used by individuals in alleged activities that violate industry copyrights. Subpoenas for information on IP address assignment and network users may be forthcoming. Individuals found to be violating industry copyrights may be offered the opportunity to "settle up" before being prosecuted in a court of law. UCSF network providers should review policies and procedures around IP address assignments and log retention.
2. *Perimeter Security:* Initial testing has been completed. Remaining issues with ACL performance expected to be resolved in next phase of testing. EIS working with ENS on physical placement of Perimeter Security gear. Go-live and further testing expected by July 1. Cutover from existing equipment is expected late in 2007.
3. *Intrusion Detection Systems (IDS):* Network taps are in place. Servers have been built and installed with "burn in" commencing. EIS and ENS have identified space and tap locations at Mission Bay. Further wiring/fiber work needed to connect MB taps to servers. System to provide monitoring and attack information in the first year, with EIS looking to implement "Reactive Firewall" measures sometime next year. More as the project matures.

Identity Management Standards: To be discussed next time.

UCSF Medical Center Updates: Med Center network team is testing an alternative solution for authentication from campus networks. Initial tests of the Identity Engines product are promising. More testing is needed. The Med Center is also testing Network Access Control products by several vendors, with implementation expected after vendor selection. More on this in future meetings. Wireless network access for patients to be rolled out soon. Patient network traffic and IP address space to be kept separate from Medical Center production networks.

Wireless: There was general discussion on the state of wireless networking across the campus. Standardization of access points key in leveraging AuthN/AuthZ when it become available. See UCSF Wireless Guidelines.

Meeting then adjourned.