

Information Security Committee Minutes – 3/13/08

Present: C. Tianen, Chair, O. Bawa, J. Claudio, R. Duca, T. Ferris, J. Fritz, L. Poirier, H. Kahn, T. Poon, E. Terrazas

Absent: M. Day, A. Dobson, J. Easterbrook, B. Flynn, A. Saggio, H. Schmidt, R. Slaughter, D. Yano-Fong, M. Ye

Guests: Virginia Hodge – Privacy Office

Staff: J. Evind, S. Lau, T. Maxwell, S. Schluntz, R. Trott

The January, 2008 minutes were approved. February's meeting had been cancelled.

MyAccess, the identity and access management system, is piloting wireless access for the conference rooms in the OAAIS suites.

The Perimeter project nears the completion of planning for final implementation and OAAIS business units are now discussing the policy related to what will, and what will not, be tied directly in to the Perimeter equipment (to be differentiated with what will be connected to the Campus Core network). The team expects to have the final proposal to Jeff and Carl for approval in April.

The Pointsec licenses for encryption will be available in April. PGP is awaiting availability of the MyAccess system. The per-computer recharge for the products will be:

- Pointsec - \$100 the first year and \$50 subsequent years.
- PGP - \$200 the first year and \$100 subsequent years

The Intrusion Detection System (IDS) project is in discussions with some UCSF departments and schools with the aim of partnering with them to expand the IDS nodes installed on the Campus network. The current installation of nodes at the border and OAAIS datacenter give a limited picture as to the traffic patterns on the campus network and by partnering with other groups a more complete picture will be formed. This partnership is also beneficial to the joining groups as it will give them view in to what is happening on their existing networks. These new monitoring nodes and the supporting data storage and reporting systems are planned to be in place and operational by the end of the fiscal year.

Amended Assembly Bill 1298 expands the definition of "personal information" to include medical and health insurance information. This will complicate assessments of incidents because such information is more difficult to unearth using present discovery tools.

The committee discussed an incident involving UDAR and a third party vendor which highlighted the concept of ownership of data and BAAs/Partner Agreements. This needs to be reviewed with Procurement.

The SATE program has trained over 200 administrators, managers, and supervisors on Policy 650-16. SATE can provide reports to each control point of who in his/her organization has taken the training. While the tracking of training through a department code list would enable control points to see who is

not being trained, EIS does not have the resources to create, obtain, or administer such a list. Progress on security comprehension is instead measured through security assessments. SATE will inquire with campus HR about whether they have such a tracking device.

Jeff Fritz, Director of Enterprise Network Services, discussed Network Admissions Control in relation to UCSF's varied network. UCSF's network was built in the 1990s. At this age support for it becomes less certain. The NGMAN project to rebuild the *core* of the network is just beginning, but it will not replace any equipment from the network closets out to offices ("the last mile"). That equipment is multi-vendor and not necessarily interoperable with common NAC solutions such as Cisco or Foundry.

The Medical Center is presently applying NAC to their one-vendor network.

Jeff stated:

NAC allows network access only to compliant and trusted endpoint devices (PCs, servers, PDAs) and can restrict the access of noncompliant devices. NAC assesses all endpoints across all access methods, including LAN, wireless connectivity, remote access and WAN. It does not protect against viruses, social engineering, or theft, nor protect USBs or applications. Further, it is not standardized and is an immature technology. It is only one component in layered security in depth.

Therefore, much deliberation is necessary for the ISC to pursue NAC. Issues that must be resolved are an equipment replacement strategy/funding; training; performance issues, bandwidth, bottlenecks; time consumption of putting on network; impact on help desk/support staff; plans for enforcement and remediation.

Draft rules for granting and decommissioning accounts for two OAAIS applications for Identity and Access Management (now called "MyAccess") were shown to the committee. Application owners must draft business rules for their applications and may use these as templates.

The Minimum Security Standards are to be reviewed annually by the committee per policy 650-16. EIS Policy and Programs unit has drafted proposed updates to the standards. The proposal will be emailed to ISC members for review before our April meeting.