LSU
Faculty Senate

Ad Hoc Faculty Senate IT Committee Meeting

30 August 2023
8:45 AM, 1008B Center for Computation and Technology

Minutes of the Meeting

I. Call to Order: Singh called meeting to order at 8:45 am

II. Roll Call

Present: Param Singh (Chair), Gerry Knapp (Secretary), Scott Baldridge, Ken Lopata, Juana Moreno, Sam Robison, Larry Smolinsky, Craig Woolley (Ex-officio), Sumit Jain (Ex-officio)

Absent: None

III. Public Comments: None

IV. Ad Hoc FS IT Meeting Minutes Approval from 23 August 2023: No amendments proposed. Moreno moved to approve the minutes. Passed unanimously.

V. New Business

1. PS 122

- Jain: Noted LSU is required by Gramm-Leach-Bliley Act (GLBA) and PM 36 to conduct the risk assessment activity each year. They are aiming to make these standards consistent across LSU System.
- Moreno: Does this cover BYOD?
  Jain: Does not cover BYOD, although if the device is on the campus wired network unauthenticated vulnerability scans will be run (checks for OS and version, open ports). ITS does not currently scan the Wi-Fi network (EDUROAM) or student dorms devices but this may change in the future. In the future, there may be additional "segmenting" (via VLAN, IP range) based on user role (employee, student, guest), and this may influence access to resources (and may require VPN to be used even on-campus, currently not possible). This segmentation is not done currently and likely is a few years out. Any processes decided on will be reviewed with the Ad Hoc FS IT committee.
- No additional discussion. PS-122 document review completed.

PS-122-ST-1:

- Singh: Who gets results of scans, or can ask for results?
  Jain: Scans are performed periodically by ITS. TSPs cannot currently initiate a vulnerable assessment themselves but can initiate a remediation scan for a previously identified vulnerability and can put in a ticket to have scans scheduled for the areas under their responsibility.
  Moreno: scan reports are not always clear.
  Jain: believes the reports are clear for *unauthenticated* scans and are consistent with reports

produced by other commercial tools on the market. TSPs can request authenticated scans; this does require giving permission to an ITS-controlled account on the target machines. Authenticated scans can provide much more information on vulnerabilities. TSPs can also provide an explanation of why flagged vulnerabilities are not real (Linux backporting for example), and ITS can mark so it is not flagged again in future scans.
Moreno: Don't get communication on scans being performed.
Jain: TSPs are informed.

- Section A.1: Timeframe of systems security assessments
  Jain: replaced "its" with "their" to avoid confusion with "ITS".
- Sections A.2, A.3: System security assessments
  Jain: clarified primarily for port exposure through "firewall' to external network.
  Lopata and Baldridge: provide example, and link to where requests for these exceptions through LSU firewall are described (PS-131-ST-2). Jain made changes.
- Section A.4: Internal vulnerability scans
  Jain: clarified "without access to internet" as "systems without access to networks outside of LSUAM" in document.
  Baldridge: Change "system" to "IT Assets" throughout document (Jain will make changes)
  Jain: changed weekly to regular as this may change in the future.
- Section A.5: Internal security assessments and self-phishing exercises
  Smolinsky: Faculty don't like "psychological training" of phishing exercises.
  Jain: Some % of user population tested every month. Noted 30% of students click on the fishing training links, fairly high percentage for faculty too. Links bring you to training page. If you click the fishing exercise you go on the list for the fishing exercise for next month. This training has been effective for faculty, not so much for students. Jain recommends clicking "report fishing" button to report (Math dept is different, have their own email system).
  Singh: Does ITS target a higher percent among users with high level access to systems?
  Jain: No, it’s a safety issue for everyone (for example, personal data being stolen, personal accounts compromised).
- Section A.8: Security assessment and critical university business
  Singh: can we clarify what is being done to coordinate with units?
  Baldridge: clarify that business process includes research, academics, and administrative processes.
  Jain: added language to clarify both issues raised
- Section F.2: Security assessment reports
  Singh/Baldridge: clarify wording. Jain made changes addressing concern.
- Baldridge: The term "system" is unclear. Jain agreed to change to "IT assets" throughout document.
- No additional discussion. PS-122-ST-1 document review completed.

Announcement: Jain indicated that the GROK article draft of the policy statements and standards index had been created. He will get the committee members permission to view the article and send us the link. The committee looks forward to discussing this in the next meeting.

The Meeting was adjourned at 10:19 am.