Task J: Cooperate on Security Challenges (DRAFT, 4/16/2009)

J. Work with EDUCAUSE, government agencies, and other domestic and international partners to identify and address the security challenges unique to advanced networks and higher education; expand that collaboration to include carriers, standards bodies such as IETF, other corporations and government(s) for the broadest discussion and understanding of solutions to this fundamental challenge.

Environmental Scan

- The cyber underground collaborates well, talking, trading notes, and sharing code and techniques -- at least as long as it is to their advantage to do so. Higher education, private sector/commercial sector security groups, and government/law enforcement agencies also need to work together if we're to have any chance of collectively prevailing against our common cyber adversaries.

- At the same time, sharing sensitive system and network security information requires some care. If you accidentally disclose confidential sources and methods, your ability to continue to get information from those sources and methods will go away. Normally, sensitive security information will only be shared within trusted and vetted information sharing communities. One example of such a community in higher education is the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC).

- Information sharing may be constrained by law, with examples of relevant laws include FERPA (the Family Educational Rights and Privacy Act) and ECPA (the Electronic Communications Privacy Act). Institutional policies may also have an impact. For example, Internet2 only shares anonymized network flow data with authorized researchers to insure that the privacy of Internet2 participants is protected.

- Technical issues may also arise when sharing data. For instance, if we're sharing spam samples, what format should we use? If we're sharing millions of samples each day, there *must* be standardization if we're to have any chance of successfully automating data reduction, analysis and reporting.

- Other times just finding the right point of contact for a security issue can be a challenge. Whois and rwhois, two online distributed contact databases, may nominally have point of contact data for domains or network addresses, but often that information is missing or stale, or the office that's tasked with dealing with security and abuse issues may be understaffed and overwhelmed. Thus, one of the most jealously guarded "professional secrets" of many security professionals is their address book of clueful friends at other sites, and the carefully nurtured trust relationships those contacts represent.

But what if you're a new security person, and because you're new you don't already have those sort of relationships? These days you may face a tough time bootstrapping those critical professional relationships because of budgetary constraints and widespread travel restrictions, but until you become integrated with the community and trust relationships develop, security peers may be reluctant to share sensitive information or to allow new security staff to participate in private vetted security communities such as the REN-ISAC (although the REN-ISAC's new two tiered membership model may help in that regard).

- Many network security issues are transnational. While in an ideal world everyone would speak some common language (such as English, perhaps), you may find yourself in situations where critical international security counterparts only speak a language you never thought to learn.

- Collaboration also involves coordination. The cyber security community is small and there's lots of work that needs to get done, so Internet2 works with Educause, the REN-ISAC, and other groups to insure that we all aren't trying to do the exact same thing, that conferences don't conflict, etc. By coordinating our limited resources, we collectively get "maximum bang" for our "limited bucks."

Current Support

The are many examples of recent and ongoing Internet2 collaborations with Educause, government agencies and other domestic and international security partners:

- Representatives from the Internet2 community and representatives from the Educause community jointly serve on the Internet2/Educause Security Task Force Leadership Team

- Faculty and staff from Internet2 member universities and regional networks routinely attend and present at Educause events (and vice versa), and we happily contribute to each other's committees and working groups.

- Internet2 works closely with the REN-ISAC, sharing data from its Arbor network sensors, providing staff for REN-ISAC advisory bodies, and contributing funding to help underwrite the cost of operating the REN-ISAC. In return, REN-ISAC acts as a security NOC for Internet2 and the higher education community as a whole, brokering incident information and sharing information about emerging threats. Educause also collaborates with and supports the REN-ISAC in a variety of ways. For instance, the Educause Security Professionals meeting staff works with the REN-ISAC so that the REN-ISAC meeting can happen immediately after Security Professionals meeting concludes, thereby minimizing registration hassles and travel expenses for those who are interested in attending both.

- Internet2 security staff have also worked with various federal agencies on their cyber security research and development roadmaps and planning activities. Examples of this sort of engagement from recent years have included participation in:

    - the National Coordination Office's (NCO) Networking and Information Technology Research and Development (NITRD) Workshop on Research Challenges for 2015 Global Networks

    - the Department of Energy's Office of Science Cyber Security Research Needs for Open Science meeting, and

    - the Department of Homeland Security's Cyber Security Research and Development roadmap sessions

InfraGard represents another fora where government and academia can meet and collaborate on cyber matters of mutual concern.

- Examples of collaborations with carriers and corporations can be found in things such as staff engagement with MAAWG (the carrier Messaging Anti-Abuse Working Group) an anti-spam organization representing nearly a billion mailboxes worldwide, APWG (the Anti-Phishing Working Group), and interaction with other private sector security organizations. We also welcome technical presentations from Internet2 corporate partners, and their participation with our community.

- Collaboration with Internet coordination and governance organizations/Internet standards organizations can be seen in Internet2 staff being invited to participate as a subject matter expert on the ICANN GNSO Fast Flux working group, and in ISOC providing a speaker for a Salsa meeting which resulted in ongoing collaboration thereafter. We also appreciate ARIN sending its staff to speak at Internet2 events, thereby keeping the community briefed on IPv4 address exhaust and IPV6 address deployment, and other issues.

Possible Future Work

In addition to continuing existing collaborations, we're also organizing a Department of Justice-funded workshop entitled, "Collaborative Data-Driven Security for High Performance Networks," which will be held May 21-22, 2009 in Baltimore, Maryland. We anticipate having approximately sixty attendees,

split roughly equally between the academic community, the commercial/private sector/non-profit cybersecurity community, and the government/law enforcement communities.

We also look forward to participating in appropriate IETF, IANA, ARIN, NANOG, DICE and TERENA activities if/when travel budgets or other funding permits, as well as more fully engaging with unique communities of interest to higher education such as GENI, the Open Science Grid, GLIF, etc.

We may also want to formally poll Internet2's membership as part of an effort to identify other organizations with which we should be collaborating.

Metrics for Success

We could track total engagement hours with various external organizations, tally leadership roles held, and seek to formally document existing inter-organizational relationships via memoranda of understanding or reciprocal organizational memberships, however those crude indicia can't begin to capture the genuine regard and friendships underlying many of these ongoing and exemplary security collaborations.

Contacts

If you have feedback on this document, please contact Joe St Sauver, Manager, Internet2 Security Programs (joe@internet2.edu or 541-346-1720)

Appendix: Glossary of Acronyms, Entities, and Terms

A glossary of acronyms, entities and terms used in this document can be found in Appendix I: Glossary of Acronyms, Entities, and Terms