IDESG

SECURITY COMMITTEE MEETING NOTES
October 29, 2015

Attendees:
Mary Ellen Condon
Adam Madlin
Martin Smith
Adam Migus
Christine Abruzzi
Paul Knight
Jim Kragh
Bob Pinheiro
Christopher Spottiswoode
Hans Vargas
Martin Smith
Barry Hieb
Judy Fincher
Rebecca Nielsen
Bryan Russell
Robin Ore
Sal D'Agostino

Linda Braun, Global Inventures

Meeting Notes:

Mary Ellen led the call. Notes taken by Linda Braun.

Agenda Review: Distributed by Mary Ellen in advance of the call (approved)

Roll call; quorum determination. Quorum was met.

IPR policy reminder:
http://www.idesg.org/portals/0/documents/governance/IDESG%20IPR-Policy.pdf

Approval of minutes: October 22 and October 29 minutes to be approved at November 5 meeting.

Minutes:

- Healthcare discussion
  - The Healthcare Committee joined the call. They have ten documents they want to share with the Security Committee regarding interoperability. Timekeeping is a big area in cybersecurity/medical devices. People being remotely monitored. Reporting from the center networks and location awareness and remote operation of medical devices – function of cell phone networks in many cases. Analog cell phone for the most part. This is area where they have difficulties. They need end to end reporting. What is happening at the patient and hospital level is important and how to incorporate into HIPAA rules. Question they put forward is how to incorporate medical devices into the future network of the functional model and how do we work together?

- Supplemental Guidance – authenticating a device and people to a service? Both have an identity. LOA3 is important for the device, but also important to the practioner trying to access the device. There is a need to bind identity together in one profile so you can associate the device with the person who it is embedded in. Engineers at VA are already doing this with C++ binding. System being developed for interoperability is going to have to include information about machine, device and person who is wearing the device. It also means that if you travel, you need to make sure you know where the person is so they are legitimate. Practice is moving ahead of policy in this regard. You have to be able to associate the device with the person.
- Person authenticating to a device is understood (phone or computer), but authenticating to a pacemaker is what they are talking about. Censor information has to be correct. Censor might detect an irregular heartbeat. Information is going over cell phone network to a server and servers are managed by various groups; doctor's office or hospital. Information goes to an authentication level where doctor is alerted where they have built in authentication to the device (that something is wrong with the patient). They can send remotely shock the person's heart to put it back into rhythm. All information end to end has to be secure and with precise timekeeping to correct the problem with the patient. Interoperability and timestamping is crucial in all elements. Hackers have been found to hack into pace makers and killed people. Robin has a paper on this, but not for public distribution. We need to diagram a safety network for the cybersecurity of cyberphysical systems as they relate to healthcare devices as they relate to diagrams you are working on in the Security Committee. This is the IOT – Cyberphysical networks as NIST refers to it. No one has sat down and looked at this from a standards perspective, except for NIST. There has been some work within the FDA. How does the device relate to the clock and how does the clock relate to the network?
- What is crucial is integrity of data when it involves a medical device that is embedded in a person. Network needs to be secure and data needs to be secure as it transitions through the network (encrypted). Person accessing the device on behalf of the patient needs to have correct permissions.
- The Heathcare Committee is working on the properties of the identifiers; mostly for individuals. Identifiers for devices are important as well. Also, how to take people's identity and make them anonymous. Error recovery and timing are also areas that our groups should be able to interact. We are not just talking about just digital aspect of the network. We are also talking about option and analog as well. Think digital optical and digital analog.
- Purpose of today's meeting was to share with the Security Committee (and Privacy Committee) some of the work they have been doing and issues they face.
- Discussion was focused on implantable devices. Patient does not authenticate himself. But there are many cases where patient is refilling their containers, so we need to have all actors involved to make sure the overall system works properly.
- Patients' records are always accessed before action takes place. There is no way to separate out cellphone functions – we need to know what device the system is taking to. IOT is going to be the electronic health record of the person involved. Need correct record of patient. Patients are authenticating themselves to a patient portal.
- Geolocation, device location, censor data, dashboards, and some way to override push notifications to the device are necessary.
- The Security Committee needs to determine how best to help the Healthcare Committee…a phased approach. It might be worthwhile to make a couple of general observations – today's conversation is much broader than just the identity architecture.
- Where is network system architecture in cyberphysical systems taking place? NIST? No control over private sector; they influence, but don't control.
- How can our two groups work best together? A lot of concerns are IOT. Has there been any effort in Healthcare to isolate the parts of the problems that are specific to them? Healthcare needs an extension of those domains. Healthcare of highly regulated as Dr. Tom has pointed this out many times. But not from an IT perspective. FDA is pushing manufacturers who develop the devices. Need to recognize the force and who you need to influence.

- Where is the regulation for the IOT located? There is no oversight. There are people who are working on standards so HC should do some research to find out where this is being done.
- Adam Madlin volunteered some colleagues at Symantec to bring forth their expertise – authentication of medical devices, Axel Worth was named. NIST – has a center that focuses on medical device security and is another avenue to touch base with. Robin has contacted them and is familiar with their use case and agrees that Heathcare should be speaking with them as well.
- Healthcare folks left the call at this point.
- Mary Ellen suggested we break into what we can handle and in what timeframe, then go back to Dr. Barry with our recommendation. HC is finalizing their patient ID requirements and circulating to other committees for feedback. This is a good basis for what they want for patient authentication. They should be finishing up their requirements soon. Document is specific to "identifier" requirements. Good to sync-up with those documents is a good thing to do earlier, rather than later. Supplemental guidance is part of the patient ID requirements document.
- IDESG has done a good job of leaning on existing material. We need to make sure that is the case here. We need to focus on problem solving that isn't being solved by other organizations.
- Security Committee believes they should initially focus on people authentication (people to people). Include authorization as well. Brings in UMA.
- Action: Mary Ellen to get back to Dr. Barry Hieb and let him know that people to people authentication including authorization will be Security's initial focus.
- FIDO Issue: Paul Grassi wants it endorsed. Being added to the Standard Committee's prioritized list. Paul has to put the application together. Security would like input early in the process.
- Ryan Galluzzo has completed forms for 80063 and 27015 and in queue for the Standards Committee. There is a backlog in the Standards Committee for reviewing.
- FMO: Dashboard updates – functionality model maintenance is listed as a Security Committee upcoming task. Recommendation to move into a cross-organizational committee.
- IDEF V2.0 work plan is being worked by Management Council. Draft plan right now is to meet requirements for federal funding, includes Gantt. Gantt for org will be more interesting to Security Committee.
- Rewrite of ROA: Queued up as Q4 work. Steve Mednick working on this. Commonality of charters is also something IDESG needs to do. Speak to Kim if interested. Security to leave charter as is until ROA work is further along.
- Action: Christine to contact Tim McKay to make sure Security gets a standard notification that a certain standard is under consideration.
- Steve Orrin will lead next week's Security Committee meeting in Mary Ellen's absence.

- New Business
  - None.

- Wrap up and actions for next week:
  See above.

- Next meeting: November 5, 2015

- Adjourn: Meeting was adjourned at 2:19 p.m. EDT.