

General Discussion

Achieving a Resilient Cyber Ecosystem: A Way Ahead

Unidentified: My question is, as IPv4 goes out and IPv6 comes more into the norm, with the spoofing that goes on with IPv6, is that going to change how some of the tools work?

Mr. Fonash: I would think so. That is going to be an evolution. There are all kinds of problems. It is also getting more difficult to do security because everybody is doing tunnels and that is why you have to be very innovative. Innovation is critical here because it is always changing. We are always going to have to be rapidly changing security. If we just do the static model of how you do defense, it is not going to work because the threat actors are innovating quicker right now than we are. Part of the problem is that we do not have the standards. Right now we basically have a security cottage industry, which is being attacked by an automated adversary. We need to move to the Henry Ford model of the assembly line—as the products go down the assembly line, they are all put together and they all work. That is where we need to go with security, but right now the adversary is better equipped to be innovative than we are and that assembly line mentality and that standard set of data interfaces allow for innovation. We talked to a lot of the research organizations, like In-Q-Tel, for example: what we want to do when we come up with a standard is get In-Q-Tel, and other organizations like it, to ask that part of the funding it provides to companies actually be directed to the standard. Now, the other thing I forgot to mention was that the way we are going to get industry to lead this is by forming a CIPAC, a Critical Infrastructure Protection Advisory Committee. DHS has certain privileges under the law in terms of what it is allowed to create, how it partners with industry. The Federal Advisory Committee Act says that normally if government meets with industry, there have to be notes taken, the notes have to be very public and the meetings have to be open. Under CIPAC that is not true, and we can pick who we want as part of that

CIPAC organization. We are going to form a CIPAC to try to get these accommodative models and we got a very, very large IT security company to agree to be the lead chair. We are going to have industry lead this and we are going to ask the banks and healthcare to participate and get consensus on these control plane models, accommodative models and standard APIs. We hope to do standards, but we are not going to do API standards in the traditional manner. We are going to do standards in the sense of doing specifications and getting industry consensus. We are going to try to get to the 20 percent of the industry that controls 80 percent of the market and then the standard will become de facto. We develop the standard, test and prototype those concepts in our lab, show it works and then hopefully industry will adopt that. Eventually, when it is mature, we will make it a standard and go to the standards. We have done this with the STIX and TAXII (Trusted Automated Exchange of Indicator Information) protocols, which are the protocols for threat indicator information sharing. We developed a specification that right now is in the standards organization called OASIS (Organization for the Advancement of Structured Information Standards). So, we are making a standard, and there are 103 commercial companies involved in that standardization process. That is the idea of where we are trying to go and how we are going to have industry facilitate getting there. We are not going to do it; they are, but we are going to help them because CIPAC allows them to get together and come to a consensus.

Mr. Dubbert: So, Peter, could you discuss how you want the industry to lead here? The federal government is going to try to create the right incentives, perhaps the right foundational investment to ensure that the speed with which this can move along is acceptable. I think we can all agree we are behind the curve, we are probably getting increasingly behind the curve and you would probably agree with that. Talk about the financial and non-financial incentives you think will be the key factors that will motivate the industry to collaborate, like how we think about working together collectively as players in the payments system to collaborate and move that forward.

Mr. Fonash: First, we are going to have to form the CIPAC organization, but we are going to use our contractors, MITRE Corp. and Johns Hopkins Applied Physics Lab to do a lot of the leg work in the development of the specifications. Much of the financial cost of developing that will be borne by the government. But we also feel that what we want to do is try to influence future acquisitions. The idea is that once we get these specifications done, they will then become part of the contracting process for both DHS

and DoD. This CIPAC is not just DHS but also NSA. We are covering the whole federal marketplace with this. That is a big market driver, but not the significant gigantic market driver it used to be. If we get the banks as users and customers of that IT industry, along with healthcare, and if the IT industry sees that this is where they want to go, the incentive is either you go this way or you lose market share. But we will bear the large part of that cost of getting there. An example is SWIDs (Software IDs), which is a licensing mechanism—Microsoft and Adobe use it for identification of their software so they can verify if you have paid your license or not. But we are working with the General Services Administration to put that as part of the acquisition process. If you do an acquisition of enterprise licenses for software, you are going to have to use SWIDs. We are going to drive the federal marketplace to doing something like that.

Mr. Cunha: I know you are Homeland Security, and not world security, and not to complicate your job, but how does this connect with the rest of the world? It seems like you are driving all this as a domestic program, but most of these organizations are international and would not want to have a one-off for technology, products and services in the United States versus the rest of the world. Is there an international component to this?

Mr. Fonash: We do partner with other countries, and we also want to take this to an international standards organization so it will be an international standard. This is not going to be a government standard. Initially, it is going to be a U.S. specification, but if you look at the STIX example, that is an international standards organization and it is going to be an international standard. We already have the Europeans participating in the development of that standard, and we would see the same thing being done here. I also think that in today's world, the financial sector and healthcare sector, particularly the financial sector is a worldwide market. You are not just taking care of the U.S. market, you are taking care of the whole world market. You would want to make these tools be across your enterprise because otherwise you do not get the synergy you need because you cannot share information, you cannot get the automation unless you start doing this, and then you cannot get the innovation. I think innovation is really critical because in today's world it is hard to take a new technology and insert it into the large security environment because you have to ensure it all works together and that the information is understood. If you have all these data standards, you just plug it in there. The other example I give is like a motherboard. In the computer PC industry, they have standardized

motherboards, processors and the like. I can buy anyone's video card, anyone's motherboard, anyone's terminal, anyone's hard drive, anyone's SSD, and it all works because there is a set of common data standards, a common control plane and a common set of APIs. That is how they have driven the costs down dramatically, it is very effective. This is going to make analysts much more productive, enable us to respond much more effectively and allow innovation. That is the vision.

Mr. Hamilton: One of the problems we have been wrestling with, and I think you are wrestling with as well, is IP address does not describe a device. Have you thought about how we could have a more permanent IP device ID, and have you thought about using some of the commercial applications that are out there—Iovation, ThreatMetrix, 41st Parameter?

Mr. Fonash: So, that even gets into supply chain too, right? It is not just the device, but the history, where it came from and everything. Right now we are tracking this software through the SWIDs but we recognize that as a problem. We have not gotten to that yet. Hopefully, that would be one of the things we would address with this working group. When we get industry together, we are going to say, OK, what is the low hanging fruit, what are the things we can do easily, and then do those first.

Mr. Carlson: I am curious to know with the Internet of Things (IoT), given that chart in which you showed the growth in the IoT and the potential risks it imposes to multiple industries, if you had a magic wand in terms of requirements that you would like to see multiple industries adopt to mitigate some of the risks of the IoT, what would those be?

Mr. Fonash: I think you would want security built in as opposed to added on to the end. I also think you are going to have to go to security as a service. What I mean is, again I go back to the lowest common denominator—household partners, the power company and things like that—with which you have these power grids, smart grids and things like that. So, everyone is connected to everyone. Small and medium businesses and individuals, all they do today is buy antivirus; it does not work. We are talking about developing a technology at APL, and we are talking to a major ISP to see if we can convert that technology to security as a service. Small and medium businesses and people do not have the resources to run a security operations center nor the knowledge of how to do security, nor do they want to, nor could they afford it. What we want to do is get security much cheaper, and

then I can see, for example, the Internet service providers providing that as a service so all your devices would be covered. There also would be some type of network discovery tool that would discover your refrigerator was smart and your dishwasher was smart, which would then provide security over that. That is my personal view of where things need to go.

Mr. Dubbert: One last question: When should we invite you back to report on the implementation of all of these? Peter, thank you very much for being with us today.

