uberknowledge

Vincent Sritapan, Portfolio Manager, U.S. Department of Homeland Security Science and Technology Directorate

Security on Our Most-Used Device

Vincent discusses the neglected world of mobile security. He shares insights on how to get a government contract and offers sound advice to both vendors and practitioners.

02:06 We need to be able to trust the result that comes out of a security vendor tool.

04:05 Vendors need to be honest upfront, check their facts, and have substantiating evidence because trust and reputation are very important.

06:58 Just how hard is it to become a government vendor?

11:19 Mobile security is 100 percent underrepresented in the industry.

12:26 You have antivirus on your laptop; where is the endpoint protection for your phone?

14:10 BYOD or enterprise owned, how should app downloads be governed?

15:05 Ownership of security in the mobile landscape still belongs to the enterprise. IoT isn't as smart as we think it is … yet.

18:16 Enterprises have got to do the basics: know how many devices they have and know how to protect them.

19:19 For CISOs managing tight budgets look to consolidate, look to leverage existing technologies; that will help save money and mature enterprise security overall.

19:35 Get ahead of the curve. If you're in a regulated industry, those regulations will get updated. Make sure you're protected upfront.

21:55 Vendors must be honest about their strengths and weaknesses because practitioners factcheck.

Ashwin Krishnan: [00:00:41] Welcome to the podcast, Vincent. So, quick intro. A Google search did not reveal too much about you, and I'm not surprised — probably by design — but you are interested in mobile security, particularly DHS, and teaching seems to be a big passion of yours.

[00:01:02] Let's get started right away. So, we were talking just before launching into the podcast itself. In your opinion, just given you're sitting in front of probably one of the most valuable assets inside of government agencies, what are you seeing in terms of what vendors are doing right and areas where they're completely doing the wrong thing? Any input into that?

Vincent Sritapan: [00:01:27] Sure. So, Vincent Sritapan, I'm actually a program manager in Mobile Security Research and Development. I look at taking technology and getting it adopted in government based on doing advanced enhancements to an existing product or new development altogether. Whether it's a commercial solution out there being sold, trying to be sold to the government or we're enhancing a technology doing research and development that's being sold to the government, it's the same thing. What we're finding nowadays, and what you're going to see, and I can tell the vendor community this is be careful on overselling it, overhyping things. So, what I'll say is when you show a capability make sure that yes it can give you a green, yellow, red; it can give you a number score; but what does that actually mean? The government, in this case, and a lot of enterprises now are checking to see well OK, you said it's green, what is green? What is the evidence underneath that actually shows that it passes or fails? We don't want false positives or false negatives. We want to be able to trust the result that comes out of a security vendor tool, as an example.

"We want to be able to trust the result that comes out of a security vendor tool."

[00:02:36] So when we do research and development at DHS Science and Technology Directorate, yes, we're the research arm for the Homeland Security Enterprise, but we're trying to make sure that it is meeting the government's need and the output is actually enough to provide evidence-based results. So if I tell you something is bad or something is good, well can I go all the way back to say, can I get the raw data or can I get the summarized data that shows me in what part of line of code is this going bad? How do I fix and remediate these things? With a lot of the solutions that are out there today, why we in the government may choose something or not choose something is going to be more than just you're nice, it's a great sales pitch, slide deck, and good demo. At the end of the day, it comes down to do you actually have substantial evidence to prove that you can do this or not? You can't just say it's a good or bad or say that there's a vulnerability. You actually have to have evidence to back it.

Ashwin Krishnan: [00:03:33] So let me ask you something, again being situated at

Black Hat, for you to play the game as a vendor, do you have to have the marketing whizzbang jingoism? So it's almost like you're playing two games, one is to play the game in a competitive environment, but once you get in front of, let's say, Vincent of DHS, you've got to become real, right? Is that something you have to deal with?

Vincent Sritapan: [00:04:05] There is that constant struggle of people trying to get PR to get visibility in the competition space, and we see that. The problem you may have with that is what happens if we try to validate that work and find that it's all wrong.

Ashwin Krishnan: [00:04:19] Yeah.

Vincent Sritapan: [00:04:19] You said that there's something being spoofed here, but the truth is someone else was able to forward it, and it can ruin your credibility, right. But at the same time, once you get into the government or any enterprise client, there are also references and recommendation. So if you say X is my reference, I will actually go and check and call. And if they say no, that is not the case, well then guess what? There can be trust issues. Trust is very important in any enterprise, government included. So if you say this functions online without any connectivity in my data center, it better do that. If not, and then we find out you need 30-something connections that may be a challenge because later on if you tell me something else, how do I know I can believe you or not? So I would say be honest upfront with it, make sure you check your facts, and make sure you actually have the evidence to prove whatever you're trying to prove.

Ashwin Krishnan: [00:05:19] If you can walk through your vendor ... do you actually go to vendors' websites and look at the marketing detail, or do you kind of rely on your own community? What's the process?

Vincent Sritapan: [00:05:31] So it's a combination, I would say. On our research and development side, we do research — I happen to just work with the different government stakeholders who actually do adoption in operations — but on our side, we post out different calls for research in different technical areas and say, "Hey, we have a problem in X and it needs to be solved. We don't know the solution." And you know, vendors, researchers, academia they can all apply, and based on that selection process, we will go and review what's there. We don't necessarily look outside, it's not allowed, different procurement processes, right. But I will say that references and those types of things, in the government they do have a ... for example in mobile security, it's very small — cyber in general is very small, mobile's even smaller — and so we know each other. If you have a bad reputation with one or another, say like trust issues because you oversell it too much, you say you did this and it's not true, then we'll know. And those types of things may impact you, influence people's decisions as they go forward. So the reputation is important.

"Reputation is important."

Ashwin Krishnan: [00:06:44] So one of the myths, or reality, I don't know and that's my question to you, is for a new vendor to get into procurement, it's a long process.

Vincent Sritapan: [00:06:55] Very much so.

Ashwin Krishnan: [00:06:56] It is? OK. So, that is reality.

Vincent Sritapan: [00:06:58] Somewhat yes and no. So, if you're familiar with DHS's Silicon Valley innovation program, that is one of the ways that non-traditional tech startups that want to interact with government can. We have a process for that. The procurement time is shorter, you're introduced to the customer, and those types of things are great. But if you're doing traditional IT and you want to get on IT schedule 70 or NASA SEWP, there is a process that goes in because you still have to establish yourself as a business. Whether it's small business or whatever, you still have to establish yourself. You have to go through the process itself.

[00:07:32] In government there are different vehicles I can tell you that I would recommend. So in the case of GSA, there's the GSA FASt Lane program. We were able to get a small business — hadn't really done work with government at all in this case, on the research side, sure, but not on the selling them IT product. We went from working in this program to get them trained, so government actually paid to train them to do paperwork and all this other stuff, from submission to when they were able to be listed on GSA IT Schedule 70. I think it was 45 business days and that was actually during the holiday season, like it was in the wintertime. So it actually went really fast compared to other people who say it takes six to nine months to get in. So it just depends. I would look for those types of programs. Look at do you have a government need, a government customer, different types of sponsorship you can do. I understand government does take a while. In general it's not a myth, it is true. But there are different vehicles and mechanisms so that you can sort of accelerate that path. Like I said, DHS's Silicon Valley innovation program, that's another one. It just depends, we define what we need. If you have a solution to a problem that we don't have, it's not going to work.

Ashwin Krishnan: [00:09:51] Well, that's really good to know: 45 days from initial paperwork to actually getting acceptance. Wow. OK. So have you had projects where after a bunch of spend you end up in a situation where ROI was nonexistent, and if so just anything that you can shed light on?

Vincent Sritapan: [00:09:14] Sure. So on our side luckily we're the research arm, right, so if we do a project it's not going to succeed every time. If it did, it wouldn't be research, to be honest. So, we do have a failure rate that we're allowed to have and expected to have; it's understandable whether it's with a big business, small business, or university, it really doesn't matter. But an example of one area that we did some time back was around physically unhackable functions. This was actually for a high assurance device, high assurance and you think of, what's it called ... root of trust.

[00:09:58] It was a root of trust technology, software based in particular. It's not that the research was a failure all together, we got lessons learned out of it at the worst case scenario, but when we tried to go down the route of physically unvulnerable functions, software based in this case, we were leveraging it in a part of RAM, and I can tell you based on like temperature differences — whether it's hot or whether it's cold — it actually impacted the results. So, it wasn't stable for us. If you're going down that route, I know some people are still doing it, we spent a significant amount — a portion — but it was a lesson learned. Maybe that wasn't something we want to use, maybe we want to use the trusted execution environment, android based, there are other parts. So, it's something that we learn, but something when we're talking about high assurance on a phone, we have to do different paths, right. We have to look at different options and we may find something that works, but we also will find things that don't.

Ashwin Krishnan: [00:10:56] Got it. If you were to look at overall security issues that you've dealt with and what vendors are promoting, what is the most understated security issue that you think doesn't get as much attention as it should?

Vincent Sritapan: [00:11:17] So I'm a little biased ...

Ashwin Krishnan: [00:11:19] Sure!

Vincent Sritapan: [00:11:19] because I'm the mobile security R&D PM. So, I honestly think mobile security is 100 percent under represented here because we've done server-side desktop clients on a laptop, as an example, and we do a great job. We've done it for quite a long time. When it comes to mobile devices, a lot of enterprises are maturing nowadays and it's getting better, but a lot of times, in the past especially, different CIOs have said, oh well I have enterprise mobility management, I have a mobile device manager, essentially something that helps me configure my phone and do policy enforcement. You break a rule, I'll wipe your device or lock your device or something like that. And they'll think that that is the silver bullet. Nowadays they're coming to the reality of if I have known malware that tries to attack my phone, SMS phishing, whatever it is, an EMM is not made to stop that. It's made to, once it's informed by something else like mobile threat defense then it knows something bad occurred, and I need to do a remediation action.

> "I honestly think mobile security is 100 percent underrepresented."

[00:12:26] If you think about, yes, we have endpoint protection on our laptop, antivirus, whatever. On our phones, whether it's civilian or whether it's enterprises, government included, do we actually have some kind of endpoint protection on our mobile phone? We have configuration management and policy enforcement, that's a MDM, EMM solution, but I think that's an area that really we do need to have. It's an easy area, technology exists today, we actually did an enhancement with a company called Lookout for mobile phishing protection. It

just came out a month and a half ago. And so that's an area that, yes, the technology enhanced what we did. We saw the need. And now we're actually helping. We're hoping, I'm pushing for it, whether it's in policy, whether it's in metrics for the government, any enterprise should actually be able to leverage this.

Ashwin Krishnan: [00:13:17] That's actually an interesting point. I want to dig a little deeper into the mobile side with all of the bring-your-own-devices and that whole phenomena. MDM kind of hit a roadblock over there when company-issued devices started going away and then people started bringing their own devices. Is there also a psychological effect, where a mobile device is essentially your digital extension?

Vincent Sritapan: [00:13:41] Yeah!

Ashwin Krishnan: [00:13:42] People feel that oh if I can trust myself, I can trust my phone.

Vincent Sritapan: [00:13:46] Yeah. So, there's a concept called corporately owned, personal enablement, known as COPE, in this case government-owned, personal enablement. So if you gave somebody a phone, you know, end user, unlike your laptop where we control everything — you can't install any software on your laptop unless we say so, you have to have privileges to do that. There is that idea of whether you're bringing your own device, although there's not as many deployments in government, but in the government-issued device, there's still the idea of I want to be able to have my own apps on the phone, not just government-owned apps. And so that does provide a paradigm of are we just going to let you install anything you want? Do we provide a separate marketplace? So that has been a challenge for a couple of years. Some people have determined, hey I'm going to manage my own enterprise app store. Others have said, well I have an enterprise app store plus we will allow you to use the official app store, but we will have different types of mitigation or protection. So a mobile thread defense or mobile application vetting EMM is still on there today. So that is a challenge area, but it is being addressed and could be addressed even further over time.

Ashwin Krishnan: [00:15:05] So if you extend the mobile landscape, not just your mobile phones or smart devices but also IoT increasingly, where does the ownership lie in terms of security? What do you see?

Vincent Sritapan: [00:15:17] So I think that there is a lot of, I don't want to say hype around IoT ...

Ashwin Krishnan: [00:15:22] You can say hype!

Vincent Sritapan: [00:15:24] But there is, there's a lot of hype around IoT and wearables and other things. But the truth is, current day, majority of what we use and whether it's for a homeland security mission purpose, sensors out there in the field, the truth is they're still going to be coming back through some network protocol. In some cases, it may be a wearable that's on a law enforcement. But

think about it, it still goes through some app that's on the phone and that phone goes back to the enterprise. So you still have that control of an application and a mobile device. So all of the EMM that you may think of about device management, application management, and other things, all the piping that goes underneath, all that can actually be leveraged to support today's use of IoT going forward. There is another portion that's still a harder challenge. When you think about attestation of an IoT device and the other consequences that may occur with it, but the truth is it's not that new of a technology. There is IoT out there, but a lot of times they are not as smart as you think they are. They provide different types of sensory information. So until that changes and the 5G and other things come online that help us, and it is around the corner, then you're going to see a paradigm shift and then we're going to have to figure out ... maybe we'll figure out now, maybe we figure out in the future how we address that challenge.

Ashwin Krishnan: [00:16:52] So the concept of whether it's antiphishing or other kinds of spyware-detection or attack-detection mechanisms that you're talking about from a mobile phone perspective, given the fact that these are mostly unifunctional devices with very little processing and software itself, do you see the same MDM vendors we're talking about, Lookout and others, expanding that to say, let's talk about the five most widely used IoT devices, whether it's your connected thermometer or your first responders' connection back and let's address that, or do you see that also will be kind of a long tail where let's solve the smartphone problem first, then worry about the IoT later?

Vincent Sritapan: [00:17:34] Yes. So it's a combination. I do see the vendor community going more towards what they call a UEM, unified endpoint management, side of the house and they want to control everything or manage everything. But the functions and features and reporting, auditing mechanisms that we traditionally will get for hardware-software asset management, identifying things that are on the network, those things today, in my evaluation of technology, haven't actually been one-to-one. I can't just take a UEM and substitute existing technology and expect to get the same type of reporting and output. It's just not there. It's creeping towards there, and they're trying to manage more and more things, IoT included.

"They're trying to manage more and more things, IoT included."

[00:18:16] But that's the vendor side. From an enterprise side, I personally think as we manage this program, we've got to figure out how to do the basics first as an enterprise. Knowing what you have: how many phones do you have; what operating system; are they up to the latest version? How are you doing patch management? Are the applications you have on your phone appropriate or not? Do you have endpoint protection, mobile threat defense? Those types of basics. It goes beyond, in my opinion, cyber hygiene, but it goes towards enterprise capabilities and management of mobile devices.

Ashwin Krishnan: [00:18:52] So that's actually a great lead into my next question. What advice do you have for CISOs of large enterprises? There's a lot of vendors hitting at you, your budget is always questionable, so how do they get through the noise? Any advice you can offer?

Vincent Sritapan: [00:19:09] Yes. So I would say, there's always economies of scale that you can leverage, right, that's a known thing. But I would say look at your existing technologies and technology is advancing more and more every day. Are there things in which you can consolidate? Are there things that you can leverage, existing technologies to cover or mitigate a new challenge or new problem you have? Or is it something where you have to show value? We have all these mobile devices today, and I know that I have this budget. The cost of, say, EMM has shrunk compared to two, three years ago. So is that cost saving now being reinvested into new, different types of technology that's maybe mobile threat defense or mobile threat intelligence? How are you allocating those costs? Think of it that way because if you're in a regulated industry, those types of standards, those types of regulations are getting updated too. And just like you should be maturing as an enterprise, if you're a CSO or CISO of an enterprise organization, you're going to have to watch out for those audits and regulation regulatory issues. So you know, I'd say get ahead of the curve. Make sure you're protected upfront. Definitely make sure you're covering all your bases from a compliance point of view, but do make sure that you're looking at can I reduce costs, can I consolidate, can I leverage existing technologies? Those things will help you save money and mature your enterprise security overall.

"Get ahead of the curve. Make sure you're protected upfront."

Ashwin Krishnan: [00:20:37] That's actually great advice because, like you were saying, your mindset of you might have evaluated an EMM two or three years ago and you had this is going to cost me X, but going back and reevaluating, it's a third of the cost. It's affordable and we have more devices, therefore I need to go back. Sometimes I think it's the people themselves that are the biggest obstacle, your mindset.

[00:20:57] So same thing, now turning to the vendors. If you had three points of advice: start, stop, and continue. What should they start doing that they are not doing; what should they absolutely stop doing, and continue stuff they're doing OK?

Vincent Sritapan: [00:21:13] Yeah. So one thing I'd say is do look up the people you're going to talk to beforehand.

Ashwin Krishnan: [00:21:20] [Laughs]

Vincent Sritapan: [00:21:20] I kid you not, that is very, very important because if you say, I'm here to talk to you about mobile security, but this person does nothing

in mobile, it's probably not a fruitful engagement, right. I know that the different vendors will leverage what's called business development folks to help start that engagement because they want to get in with that organization or agency. You want to make sure you get the right person targeted. Do your homework. If you go in there and you get the wrong person, then that sets a bad first impression and that's the first piece.

[00:21:56] The next thing I'd say is make sure you're honest about things. It's not about selling a quick product and making a quick buck. If you're upfront and honest about your weaknesses and strengths and you say, "We're working to address those and make those enhancements," or whatever it is, that's more valuable than you saying, "I do everything." If I say, "Well, do you do X or do you do Y?" saying, "Yes, I do it all!" because you just want that business, then the chances are we're going to fact check it because it's too good to be true, and you're not going to make the sale. So be upfront and honest about those types of things.

Ashwin Krishnan: [00:22:34] And anything that you see they're doing well that they should continue?

Vincent Sritapan: [00:22:36] Yes! So some businesses do, do that. All the things that I mentioned; they've done that. I would say that it's not always the case. But being able to establish that relationship, being able to actually work through the process — in the government it's a lot longer, and I think that a good chunk of the vendors who work in that space understand that and understand that it does take time to build that connection. Because even if I said, hey I want to buy X technology tomorrow, I'm going to have to wait for FY19 funding, right. So depending on what industry you go into, if you know that space and you know this is a fiscal year thing, or you may have to wait till the end of FY18 because people need to expend budget, that may be a good timing. So people do, do a good job at that. I think it just depends on an informed vendor and experienced vendor or somebody who's just, you know, a little too pushy.

Ashwin Krishnan: [00:23:37] That's great to know, and I could not agree more in terms of just doing your homework before getting in. It's been fascinating. Thanks for coming on the show and hopefully you have a great day to come. All right. Thank you.

Vincent Sritapan: [00:23:52] Thank you.