Event ID: 1905416
Event Started: 2/16/2012 11:48:39 AM ET

"Please stand by for realtime captions." 0001 "

Operator:" Welcome and thank you for standing by. At this time all participants will be in a listen-only mode. During the question and answer session, please press star one on your touch-tone phone, and please record your name clearly when prompted, when recording your name please make sure your phone is off mute. Today's conference is being recorded. If you have any objections at this time, you may disconnect. And now I would like turn the meeting over to your host, Mr. Sam Weber, Mr. Westbound are you may begin, sir.

Thank you. I'd like welcome everybody so the ninth in our monthly series of watch talks which are currently being held every third Thursday, and in room 110 in the National Science Foundation. If you're able to come in person and tell advised. And just to start, when I was a young grad student I remember someone coming up to me saying, okay all these old security folks are really grumpy because they've spent their entire life telling people how to make systems secure to be absolutely no art. You really wanting to into this area? And it is true that there is this big gap between academia and practice. And it seems even GRART in security than other field but there are actually people who have managed to pass over that gap, and in our program the secure and trust worthy cyberspace program, we're now actually making a specific effort to do transitions practice with [INDISCERNIBLE] Thompson to try to help and assist academic work to make that transition to practice. And I'd like to introduce Paul Barford, who actually is professor of [INDISCERNIBLE] Computer science of University of Wisconsin. He was the founder and former CEO of Neiman network, which of network security start-up company, which was acquired by, how do you pronounce it? [INDISCERNIBLE] And therefore has, has a lot of experience in taking academic work and put it out into the real world and getting results. Therefore I'd like turn it over to him.

Thank you. Sam. Well, it's a pleasure to be able to come and speak to this group today. I'm going to pass along some thoughts and ideas that are not deeply technical in nature, but hopefully a little bit challenging, and also that inspire conversation about how we might better facilitate transition of technology in the security domain from research into actual practice. So feel free to interrupt and I think it's okay, if that's right. From the local audience, I guess the telephone audience might have to wait until the even. So please jump right in. Solets let me start out by offering a little bit of, of a history of the threat space, something that I think everybody is probably familiar with at some level. You may or may not know that the fossil records show that roughly 5 hundred million years ago most of the [INDISCERNIBLE] that actually existed on earth today came into existence, and I think we're going to see something similar in the security domain, that in this time of the early 2000s that most of the basic threats that we're actually experiencing in the Internet today have come into existence, and while there will of course, continue to be lots of innovation in terms of how threats actually are imposed on systems and capabilities in the inter vet. I think that you can boil down, boil things down into a basic set of models that we have today, so if you look back historically, most people point to the Morris worm in the late '80s being the sort of major instance of Internet line of attack. Then we had this kind of strange period in the 1990s, where, yes, there were viruses, but which were not too major we all felt about the Internet then all of a sudden in 2001 we had a real explosion of [INDISCERNIBLE] there's been a gigantic [INDISCERNIBLE] since there of a long series of worms of pfishing activity that a lots of that came into about the 2004 time frame, and now we have the super Botts out there that are really causing a lot of problems. I would characterize today's environment as one in which we, we're seeing evolving cyber ecosystems, the folks at Berkeley and San Diego did some really interesting work that was published in security last year on the paper install activities that's going on, which is just fascinating when you think about the fact that there's a recognition of different strengths and capabilities of different individuals, whether it's to compromise systems, or to actually place capabilities on systems to garner intellectual property or financial gain. And to recognize that separation and then to create an infrastructure to leverage that separation in terms of paper and stall was really even sight full and really interesting, and I think we're going to see more of that as time goes by. The point is what this highlights is the fact that the threat landscape and the corresponding security domain are highly complex. Diverse, dynamic, and are going to continue to change over time. But because of the fact that we have really what I would say is the 5 to 7-year difference between what's going on in the threat domain, and what's going on in the security domain, meaning the defenders are 5 to 7 years behind the people who are actually out there conducting malicious activity in the Internet, the only way that we're going to make gains, I had contend is through innovation. In other words, step function increments and capability to defend against attacks verus incremental capabilities, which we're really seeing coming out of industry today. Okay. So to sort of further those thoughts, the way that I characterize the security activities in the Internet today is that we're, we're winning battles, but we're really losing the war and unfortunately the black hats are quite a ways out in front of us. So the defenders of Internet infrastructure typically are often think about this notion of defense in-depth, and we have capabilities that offer a certain measure of security. We have parameter defenses, we have host defenses, we are paying more attention to physical security of infrastructures. We have some nice KRIP tow capabilities. I think people are paying more attention to strong passwords and the more ubiquitous use of encryption. We are also Roying that policies, procedures, and education play an important role in defending our infrastructures. And I will, I will also concede, I guess at some level, that best practices do, in fact, provide a measure of security. We don't hear mention of script kidries that often anymore. Okay. So really what we're looking at is the, a raising of the bar, right, in terms of best practices, but the problem is that the sew fist indication and capabilities of attackers continues to evolve, and the most malicious actors are acting, continue to act with Impunty. Sadly these people are moving up the food chain in terms of targets for their efforts. Already there's been a great deal, or a large number of reports of the financial and data related cybercrime. Much of this of course, I'm sure you know is coming from state actors, so there is a recent report of a group that is called from folks in the US, Byzantine foothold group out of China have XRIE Meijer'sed data and financial information from over 760 companies over the last ten-year. You know that is just really a STRAGerring number for one group, one group of act ors to have accomplished. We have really game changers when you look at Stuxnet and duqu. We can't think for a minute that just because those pieces of code were possibly developed by state actors that PRIEF the a -- private actors aren't going to pick up on the capabilities and techniques of those tools. Probably some of you have read the forensic analysis that have been published in places like wired, I found those fascinating. But nevertheless, the point is that these tools are insidious, they're highly capable. They're expertly designed and developed and they represent a threat that I think we all have to be very concerned with as a possible model for what we're going to be facing at a broad scale over the foreseeable future. What they also point to very directly is the fact that while we have been predicting attacks on infrastructure, of course, Stuxnet is the example of a piece of software that targets infrastructure. Even though it targeted in a very focused way semen center fudges in Iran and was not used as far as we know broadly behind that, Duqu is something that has a broader focus. Even though reports of its use are limited to attacks in Iran and the Sudan at least stars the literature that I've read, it is an amazing piece of software, and something that is based on Stuxnet but also has enhanced capabilities. When we talk about infrastructure what a lot of us are really KOERPD about of course, are the control systems. The SCADA systems that are used to operate machinery, manufacturing, the power grid and other major infrastructures. There was a report that appeared in wired recently about a private group that that did a broad analysis of the SCADA systems, over a expected period of time looking for vulnerabilities in those system. Perhaps some of have seen this report, it was actually appeared at the S-four conference before appeared in wired. The news was very bad, in fact, most of PLCs that are available for major vendors today, not only have identifiedville innerabilities but this group has further identify, or developed exploits for those vulnerabilities that are now available in [INDISCERNIBLE] so is doesn't take very much imagination to come to the conclusion that people are going to begin what meta slight an openably available piece of free wear to potential target SKAD a systems and that is what was respected on the last slide with respect to the water systems in Springfield Illinois. The point is this group looked at these PLCs quite broadly and the news is not good. Unfortunately some of the references from Wired from the vendor are saying, we don't have the ability to include security on some of these systems because they're old. So what are we going to do? Well, that's a great question. Well let me takes even down a little bit further. Make things even a little bit more negative. Which is to really take a kind of cynical view of the whole environment here. Which is if you're a company that provides security solutions, you want bad things to happen. You're very happy when new bad things happen because it gives you a broader way to potentially bring value it your customers, and to that end, why would you ever really want these things to go away? You don't really want to solve security problems. Again, this might -- this is my totally cynical view. It's not the way things are necessarily in reality at all. You want to sort of solve them okay to continue to be very relevant and to add value broadly. I would ask on the heels of that, we hear about the bad things that are going on all the time. What are the big security success stories? In other words, do we have major successes where we say we've entirely shutdown this avenue of attack and it will never happen again? I don't know of these. Actually, I think that the security success sore -- stories that I've heard of recently are actually these forensic activities to decompose some of the more insidious threats that we've seen recently and some of the things coming out of the research community in terms of digging into for example the paper install or some of the value chain issues that, that people are looked at, at recently. Further cynicism on my part. There's been this amazing kind of explosion in government contractors, all this sort of usual suspects having large security groups. I've not really seen research publications from these groups. I've not interacted with these groups in, let's say, in the early 2000, why are they all suddenly having a big presence in security? Well, I think the answer is pretty obvious, because there's money to be made through through normal government channels which tend to be very complex. Very hard to figure out, but these guys have really dialled in. And of course, the danger there is that, in fact, best practices, new research, and the innovative ideas are not going to be brought to the forebecause these companies are ill equipped to actually bring that technology into the mainstream.

So I'm going to present a series of challenges here, which build from this sort of somewhat dire state of affairs that I've just presented over the last several slides. And the first challenge is this issue of technology versus innovation. And I pose the simple question in the security context, what is the next big thing? And from a threat perspective well I can think of a lot of things right. Think we all can. And most of them are kind of scarey right. They're large scale events that make us frightened as opposed to small scale events, where, you know, it's somebody else, or some, you know, over seas financial institution which doesn't have anything to do with me. It's the large scale events which are real, which are really quite frightening right now. But from the other side, from the defenders side of things, and things that NFS has been a big supporter of, I think that the real counter measure opportunities are in very different ways of doing things not pursuing and incremental electric and standard best practices. It's actually changing the playing field through new security architectures that offer us the best opportunity to address the SMEK trump of threats that we're faced with today and in the future. So the question then is, though, if new architectures are sort of one possibility. Where will that next big thing come from in terms of, you know, what group is going to develop it? And what I would submit is that companies in general and security companies in particular are good at developing new technology. Okay? They have something, some tool, some infrastructure some capability, some service that they've already developed, and they're very good at making an incremental improvement on that potentially to address some broader set of threats, all right? We don't really entirely know what's going on in the government mill space because there's this sort of tend EPScy to immediately classify something as soon as is might possibly be something of interest. So what I would say is, that entrepreneur are the true innovators and the people where we can have high hopes that we might come up with the next big thing, the solutions that are really going to provide these [INDISCERNIBLE] improvements in security.

Well let me not limit my finger pointing. I'll point some fingers at academia too, which is of course, is the beneficiary of all a lot of research funding that comes from NSF, and what I would say is that in my experiences, many of the processes in academia actually stifle innovation. We have this tenure con none drum, which I've talked about with many people here at NSF, which you have to get as many papers published as possible. You have to get a career award. You have to get funding from NSF and other important agencies in order to get tenure and what I would say is that all of these incentives (are not oriented necessarily around innovation. And definitely not oriented around technology transfer.

Well, that's unfortunate, okay. There is I think a recognition at some point that true innovation often happens when people are young, and if we impose these set of processes at universities that, in fact, drive people away from innovation, then that's a real disservice to the broader community, which I think we're all really interested in having a positive impact on. I would also add that unfortunately, at many institutions, and I'll single out Wisconsin as an example, we to have a rather uneven lightened IP management process. Intellectual property management process. A lot of this is height evened by the fact is that we're in a time of tight budgets and intellectual property and patents are seen as a potential stream of revenue, so we must monetize those as quickly as possible. Right and we have to patent everything that comes along because there is then ultimately the possibility of driving revenue, but the problem is, that sometimes patenting something and sometime trying to license something on a non-exclusive basis is not the way to actually introduce technology into the mainstream. And ultimately our goal is to move innovation into the mainstream, especially in the security domain in a way that enables it to have the, the broadest possible impact.

So one possible direction that I think people have been paying a lot more attention to recently is this direction of trying to foster companies, right, trying to actually incubate companies within universities, and we have that activity going on within University of Wisconsin right now, we have a program whereby professors can make proposals, and give a little bit of money to start a company.

Well, as I was discussing with some colleagues earlier today, I would submit that professors are not the best target for Inc. base, there's some people who are very successful entrepreneur's who come out of academia, no question about it. And they've done great and we know who they are. And you know, we can go down a rather short list of them. But in general, professors are very concerned with their research program, very concerned with their students, very concerned with their teaching, very concerned with their service, and when you have that many activities on your plate, you don't have the ability to throw yourself into a company on a 24/7 basis for a period of a couple years, which is what it takes to get a good company off the ground. So perhaps some of our incubation efforts at least from universities are a little unfocused right now and maybe there are ways to re-focus those to be more successful in the future. Finally let me say that why aren't we teaching entrepreneurship in computer science? At University of Wisconsin we teach entrepreneurship in the business school, but if look at the major success stories, at least from the perspective of technology over the last ten years, you look at companies like Google, you look at companies like Facebook, Facebook can be argued as being the most important development in the last ten years, right? 5 hundred million users log into Facebook every day. It is a new mode atty for communication we haven't seen before. Zuck. In business school. Was a computer science student much maybe me need to embrace entrepreneurship as an element of XOOUPT computer science going forward.

I put this slide in the deck because it's something that on my sabbatical I took, last year I took some time thinking about. Which is, very related to all of the incentives in academia, which are where we publish papers, and I took some time going through the site seer archive, maybe some of you are familiar with that, it tracks computer science publica. And you can quibble about the [INDISCERNIBLE] versus Google scholar, versus Mike owe soft, versus whatever index of papers you happen to look at. The nice thing about site seer they do provide a most top 100 most kited papers on an annual basis. I took a selection of top three papers, ashably against [INDISCERNIBLE] the conference in networking and I plotted the instances of top, of occurrence in the top 100 most cited over a period of 15 years, and what you can see from this graph is that Sigcomm has a very prominent role right, a lot of top 100 cited papers over a period of about ten years, kind of fallen off in the last couple year. Not quite sure why that's there. I have some conjectures about that. But one of the nice thing that you see is that there is an up swing in innovation from the security conferences. Probably on the heels of all that growth of malicious activity that we've seen starting in and around about the 2001 time frame, with the, the big worm out breaks. So the point is that there are good ideas that are capturing the computer science computer at least at some level in security and now what our task is, is to see if we can bridge that gap between the development of these ideas and the actual deployment into practice.

So how do we do that? Well, starting companies is FROJ with difficulty. And I'm sure that I'm preaching to the crowd at some level in terms of this, but having gone through it in my company, [INDISCERNIBLE] Which I founded in 2007, and transitions to QALAS in 2010 I can tell that you gap in hindsight is way way bigger than it is when you're standi front of it to begin with. It looks like a short jump when you first get the company started. No problem we're going to start revenue streams we're going to start getting customers we're going to start being profitable. You know in the next 2 or 3 years and then once you have cross the gap you can look back and say oh, my God I can't believe I thought I was going to get over that. So the point is that there are standard issues when starting any company that face network security start-ups, but then there are additional issues which really complicate the process. So one is the fact that there are of course, huge concerns with privacy, when it comes to actual deployments in companies. So a standard first step for a young company is to look very carefully for a company that's willing to deploy your technology as a proto type deployment. But depending upon the product that you're actually bringing to them, that can be HUMGly, hugely fraught with difficulty. Right. What traffic are you going to actually, you're not going to look at our live traffic, are you? Well, that, I mean, it's those kinds of questions and those kinds of issues which, which really complicate this process of bringing a company into revenue positive state.

Another compounding issue is that there are many complexities with respect to regulations and especially governmental processes, if you ever want to deploy your capabilities in governmental networks. I will not forget a conversation that I had with [INDISCERNIBLE] when my company was very early, when I had just finished making a presentation to the NSA and I called FARN um and said, you know they had a positive response. Do you think I should continue to pursue this in he said absolutely not. He said, you will, you will encounter huge difficulties when it comes to actually getting your system deployed in those network. Getting any information about from them about how it's working, and effectively operating your system in the way that you want it to operate. If you want to throw it over the wall to them, if they want to take it, then, you know, maybe that's something you can consider, but don't look at it as a revenue stream anytime soon. And of course, lastly we're in a very Fick will XUNTy when it comes to things -- community when it comes to things that are hot. Targets move all the time. Something is in, something is important, two years later, it's not important. There's no solving this last bullet point. It's just something that we have to recognize (that the boot strapping process in the security domain really can't take a long time because if you go to a conference like RSA, year after year you can see that the buzz words change very frequently, and if you're doing something that's considered pass&é;, then it's just, it's really not deemed important anymore. Even though it might be important and it makes the sales process and the transfer process much more difficult.

Okay. So this is going to be, motherhood and apple pie to this audience, there are always challenges with resources. And I spent some time trying to come up with an actual number for the annual investment in cyber security research, basic cyber security research from the U.S. Government on an annual basis and in the even I gave up, because it's just too, there are too many sort of avenues and ways that this number can consider. I just use the word tiny I'm not exactly sure maybe somebody in the audience know what's that number is on an annual basis.

But the fact is if you look at NSF budget or if you look at DARPA's budget or you look at any other standard funding agency for cyber security research development and then you try to sort of parcel out what percentage that basic security research might be in that, you can see that in the end just given the raw numbers that the total investment must be small. But if we're thinking about threats, that have the possibility of having an impact on the country, and remember the president mentioned kinder security in his recent state of the union address, then why are we investing such a small amount of money in basic research on something that's that big a threat? There should be a corresponding recognition, especially if you believe my arguments that innovation are the way in which these threats are going to be addressed. There needs to be a much larger investment in basic research. And again, I'm sure that I'm not going to get a lot of push back there. Another piece of good news is we have strong advocates. I'm very bullish on the advocates we have in National Science Foundation, in Homeland Security, and DARPA and so forth. The cyber security bell is being running by many of those people and I'm confident that we will see an uptick in funding for basic research over time. But I will say and I think we all know, and, and respect Doug [INDISCERNIBLE] leadership in this space, it's been a long time coming. So hopefully the fruits of those efforts will, will be able to be Harvested in the not too distance future. But one thing I will say, when it comes to basic research, is that it's not just about writing papers. It really is about putting technology into practice. Okay. So it's nice to write a paper but to actually develop an algorithm or a tech near or -- technique or capability that can be scaled. That takes a lot of extra effort not a little extra effort, but a lot of extra effort. What I wonder from NSF 23 we need to put more emphasis on that. I understand that with there is this tension between intellectual merit and broader impacts I get that, maybe we can do things like I don't know, linking the ability to, let's say, fast track NSTTR or SBIR award based on an existing award. I don't know. I think that you guys have probably talked about these, this problem a lot, and I look forward to engaging in that conversation as with well, because I think it's an incredibly important conversation.

Well, let's consider the issue of resources from the industry perspective. So this is a graph that I copied without permission from The Wall Street Journal. That lists the total amount of venture funds raised and allocated over the last several years. And the news is not good. All right. So remember, this is all venture funding. This is not just funding in IT securities. Cyber security, which by the way makes up a relatively small component. If you go to the top tier venture firms. The is he Coy I can't and SKELZ of the world and you look at the list of the technologies they're most interested in what you're going to see is you're going see the word green, green shows up a lot. You're going to see the word social, social is very popular these days. What you're not going to see a lot of is security. Okay. So what you should do, again, is sort of back out what percentage of venture funds are going into cyber security start-ups from this community and, again, don't know the exact number, but I'm going to say it's tiny. All right. So we have these big problems. Government has this tiny investment, private industry has a tiny development, we need innovation in order to get past these problems. Where's it going to come from? Well, one piece, 1 possibility is that we really are seeing a shift in the private funding model. Maybe some of you have heard of the company Y COMBAN Nate or, Y COMBIN Nate or is a interesting venture spun off in Boston around 2005 by a couple of people who had just successfully spun out their company to Yahoo. And what they said is, hey, you know, we like hanging out at around universities, and we want to foster innovation, you know, maybe we'll be venture capitalists and they really lappeded on a cool model, and they're model is, that if you have an idea, you can make a proposal to Y COMBIN Nate or and if they like your idea, they will incubate you in an interesting way. They'll give you about 20, $25,000. You can read their website, they take a small percent age of your company, but importantly they will give you hands on guidance to move your, your piece of software, their purely software oriented, to a proto type demonstratable form. So that you can take the next step and hopefully get funding for the company and grow it, and these guys have been wildly suck full. Look at the companies on their website that they list that they have incubated to at least a A round of funding. I love this incubation idea. This is springing up everywhere. If you just do, type in incubate or into Google you're going to find hundreds of they companies. There are Y COMBIN flate or clones everywhere. I think this is great. This is really important, what it recognizes is that there has been a shift in the funding model. We are no longer in a situation where we follow the traditional A round, B round, C round. Mezzanine round and then exit. We're in a situation where we have a lot of money in the angle domain and an increasing amount of money to incubate, much less money for A round funding, but once you get past that, that, what is typically considered success in early days, meaning that you're, you know, have a nice revenue growth stream, and have the, a situation in which you need a alarmer amount of money, let's say, 5 to $8 million to really scale your company, well, there's money in that, in that area as well. So we've seen this shrinkage in traditional A round in growth Inc. base in angle and still money to roll out companies down the line and I think Y COMBIN Nate or is a great example of what can be done in terms of incubation, and I've just learned about this great new incubation program that NSF is spinning up. I think it's wonderful and I think it will be widely successful. Assuming you have the right amount of mentor ship in the pr.

So I think this is about my last challenge. I think we all need to recognize that, that there is a huge amount of competition out there. And the competition really is, is coming in my mild from a couple different places. Number one, India and China of course, are very focused on growing their research capability, right. Starting new universities, keeping their best and brightest at home, good for them, but what we have to do is we have to react to that, right. We can't count on getting all of the top IIT students in our universities in the future. We have to do things that keep our talent at home, and, I'm sorry, foster our own talent at home so that we can track the best people into research at least those people who have a pension for doing that kind of work. I think we also have to recognize that domestic talent has lots of options. And I will highlight a, what I think of as a real dramatic shift in hiring that Facebook is undertaking. This is actually slash dotted about 3 or 4 months ago. I can give you the link to that if you'd like. But Facebook is coming to campuses. They have a target set of 20 campuses. They're holding hack a-thons on campus, which are just programming contest that they run for under grads typically the programming contest runs all night long, for the winner they get fun prizes and it's generally seen as a, an image building activity on campus. But what's happened recently is that the people who run these hack a-thons have the authority and the ability, if they identify people who are outstanding to make them job offers on the spot. And the nature of the job offers are dramatic. Okay. Much different than anything we've ever seen in the past. Salaries are incredible high starting at six figures. Okay. Huge bonuses. If students have companies. They will buy the companies on the spot, okay. What's most dramatic about these offers is that they do not require the students to finish their degree. They offer them the ability to come and start working and actually encourage them to come and start working immediately if they want to. Okay. I don't blame Facebook one bit for this. They recognize that attracting the top talent and the top creative talent is the life blood of that company and the way that they're going to continue to be competitive, and have new offerings and new innovation down the road. They're doing the right thing for them. Okay. And I think what we have to do as, we, the academic community needs to offer students options so I don't to counsel these students to say, yeah, you know what you should take that offer. You THO should go work for them right now. That's a great things for you to do. And I mean, this is not making this up. I mean, we actually had a counseling exercise, my colleague and I this fall this fall who was made this offer. Twice as much his dad ever made. It's hard to counsel a student not to take that offer. And we didn't.

Yes. Another challenge. One that will resonate of course, with people who operate in the security domain. Which is that when it comes to producing a new technology, there have to be means for actually assessing that technology in a in objective fashion. Unfortunately in security, we don't have and an log for FLOPS Orbits for second. Security is good when nothing happens. We all feel good about that. But that's not a good message right. The number zero is typically not seen as being something that's positive. What zero things happened. Nothing happened, it's not, can't be negative. Can it? No. It's either zero or bad. We need better metrics, and this is something that a friend of mine, Roy [INDISCERNIBLE] at CMU has harped on for years and years, and the fact is that this is a very hard question, but maybe it's not the right question, right. Maybe me need to change the conversation. Maybe me need to orient this conversation around about being proactive. What you can do in your infrastructure to make it more secure, right? Maybe me need to orient the conversation about adding robustness so that if things do fail, robustness take over and we can continue to operate. All right? And then of course, there is this ongoing very attractive notion of somehow linking security as, of two products as a value add for products, I don't know how to do that, but if we can do that, then maybe this is a metric that's meaningful and that will resonate in, in the commercial domain. This is a big problem, though.

Yeah I already mentioned this issue of deployment, so math my surprise when I was talking to a major bank about my technology, an intrusion detection, you know, knew intrusion detection company, and I naively thought well if you want, they indicated they wanted to test our technology and I thought, well, they will deploy it in their network, which is what you do with, with I know truce DEB detection system right? And then when I said, well, how can, we'll help you deploy it in your network. They said, we would never deploy it in our network, what are you kid, that's where our actual money is made. You can't deploy something in a network. I'm not making that up. While the security people were extremely enthusiastic about our product the decision makers in the company were the people who made money, okay, and under no circumstance were we going to be allow to actually deploy an unproven brand new product, a proto type product into an operational network to test it. And sadly that's where that conversation just kind of ended. Yeah, that bank had problems subsequent to that in 2008, so maybe this was sort of an institutional issue and not just an issue with our product, but the point is, that deployment of security systems, when it comes to this issue of technology transfer is non-trivial. It's very easy to give someone data. If your value proposition is about data, and I'll come to this in another slide or two, then that's something that is very easy for people. Oh, you want to give us intelligence, we'll consume something, that's fine but when this comes to actually deploying something in a security infrastructure in a live way, this can't be under estimated, and this is a significant challenge.

Yes, my last, this is not a challenge I call it a chall-atunity. Most security research has been focused on defense. Right. And, and really driven by threats and threat models and what this has lead to is April infrastructure that has robust capabilities but is of course, very, very fragile, right. If there's a new threat, something that the infrastructure. Designed for, then it's, it immediately breaks. And that's not the kind of infrastructure we want. So there is this possibility of the other side of the playing field, which is the offensive side of the playing field, right. Attackers always have the advantage. They only have to find one entry point into an infrastructure, defense has to coverall possible entry points much it's an inherently unbalanced situation. It's just like sports. How often do you see zero zero ties. Well you don't. Offense is always able to score at some point on defense. Furthermore in our situation, right, we always have humans in the loop so even if the infrastructure is perfect. Humans are not perfect, right, we always have that entry point into an infrastructure. Well, it's pretty clear that offense in this cyber security domain can have an impact and, in fact, you're probably aware that in December of last year, congress actually authorized offensive military operations in cyberspace, that was, that's a big deal. It's on the congressional record. So the question is, how does the research community react to that. Now, I'm pretty sure NSF has regulations against these kinds of proposals, right. If I came in and said I'm going to develop the next Stuxnet, plus plus, that that would the no be embraced let's say in the cyber technology directorate or cyber security technology directorate. However, this is, it's been authorized by congress. So how do we, how do we bring technology to bear in that area in a way that can have an impact in this domain, but one which satisfies the regulations and constraints of NSF and other agencies. The answer is, I don't know, but this is a conversation that I think we need to have.

Well, now we'll get more positive. I think there are lots and lots of opportunities and ways in which we can facilitate the transition of cyber security technology. So one, which is directly, a direct result of sort of this deployment con none drum is that there are opportunities to have an impact in terms of data (, right. And I will, I will offer a couple examples of those aggregates and signatures, what I mean, by aggregates, it's actually putting together intelligence from disparate sources that give people the opportunity to orient their security infrastructure in a way that minimizes attacks surface. So a great example of this are the data services on attack that are offered by is a man tick and other security companies for different vertical domains, right. So what are my competitors seeing in terms of attacks? They gather that information for vert cams and they produce it in a report, and these are very popular in the, in the IT security operations domain. Obviously signatures. I know we don't like signatures, but signatures are reality, right, for deployed IT security infrastructure, when it comes to antivirus or it comes to in network defenses, having updated and tuned signatures are the key to stopping the majority of threats, okay. So maybe that's a success story that, that we can point to if we can do in a way that we can demonstrate again, reduces the attack surface to a minimal standpoint. We have all of these opportunities in cloud's now. We have software storage, security as a service. And there are a lot of reasons to be positive about the opportunities and capabilities that clouds give us, right. Simply FOOIDZ deployment. Sort of lower costs I don't know whether anybody's actually work with S three or EC two, but it can actually be pretty darn expense I have. But anyway, they want to sell you value on lowering costs and at some level maybe it does from an operations perspective. But the point is, it does change the playing field, and we should you know, potentially, I think we need to embrace this, and think about it in terms of what might be offered in terms of broader set of security services going forward that are coming from the cloud and that are also offered within the cloud, because remember, it's a totally controlled environment in the cloud, right?

Well, this is somewhat motherhood and apple pie, another opportunity to secure software. Probably most of you are familiar with the fact that on the heels of the worm out breaks, Bill gates wrote a trust worthy computing memo to the entire Microsoft corporation, which really high lighted the need for software assurance. And I'm, I'm totally in agreement there, and I think that there are indeed continued opportunities to develop tools and capabilities and we have seen a growth in commercial offerings of tools and capabilities to make software more secure. Of course, the difficulty is that software is incredibly complex and you always have humans in the loop, but really starting with programming languages and moving into software development and software engineering techniques can lead to software that is inherently less vulnerable than what we've seen in the past. Right. So it's not just development methods and languages that we need, but we also need to recognize the entire development process, and to pay attention to where and how bugs are introduced and how they might be fared out and addressed.

Additional opportunity is to more broadly education on issues related to cyber security, and I'll point out three constituencies that I think will benefit greatly. First of all, consumers, these are private users, developers, and in, industry entities, that can, I think benefit very importantly from understanding how and when to recognize where threats might be introduced and how they can take advantage of certain simple ideas that will ultimately improve the security of network infrastructure. Another important con state KWENSy are -- constituency are the policy makers. There was the 2003 White House memo on a strategy for national cyber security, which is a very nice memo. Maybe some of you have read it, and there has been a growth in those kinds of documents over the last several years. The point is that policy makers, especially now that we've actually had presidential recognition are going to become more involved in cyber policies, and we need to educate them often, and with details on, so that these policies can be formulated in a what that can -- in a way that can actually have an impact. And then finally the next generation innovators not only need to be educated on how they might create technology to enhance security, but also how they can develop systems that don't have anything to do with security that are inherently more secure.

So to that end, we have a new activity, which I'm excited about at the University of Wisconsin, which we call the Wisconsin innovation in software center. Kind of play on our abbreviated name for the state. Cute, and the whole idea here is to recognize two things, one, is that students are not typically trained in computer science programs with the skills that actually enable them to build Internet deployable software. We're very good at teaching standard topic. Right. Simple programming languages, compilers, systems, databases, theory, AL go rim THEJ -- AL go rim THEJs, you name it, we're very good at teaching those things but most of the time students have to go through training once they exit our program to create software. The first component of the center seeks to actually provide students with the training to actually development develop. Internet deployable software and to couple that with an entrepreneurial experience to teach them about what it takes to start companies and to give them the perspective and even fuse them with enthusiasm about creating a company. How do you that? How do you build a piece of software that can be deployed, that's scalable, that's robust and that's expensable. To actually get users to start using it?

The second component of this center recognizes that, hey, we could have the next Zook at University of Wisconsin so what we should do is not let that value go to Y COMBIN Nate or or go to Silicon Valley immediately we should foster that through an incubation process on campus, leveraging our incredible alumni and other partners to move that product into a demonstrating prototype much like Y COMBIN Nate or. This is a company that operates in a way this other incubators operate, that leverage the students and the innovation that's happening on campus all the time. So we have this WUND wonderful idea, the Wisconsin idea that was articulated in 1916 by the university president Charles van HIES which is the idea that the boundaries of the university expected the boundaries of the state. It's a term that we use frequently at University of Wisconsin it's been used at other university we should have an impact beyond our campus and we think this kind of center, which has the opportunity to start companies and create jobs have an economic impact on our state is an embodiment of this idea in the 21st Century.

So partnership, the idea of partnerships are bantered around a lot. Public private partnerships. I agree those are the real opportunity for success, but what I would say is that if you look at the call for partnerships in the cyber security policy statements from the early 2000, what you'll see is that they may be haven't had quite the impact open things that we'd like. I think this is because we have some lack of alignment on go forward strategies between the government and between some of the private entities. And what this means is that we need to more broadly engage, I believe, with academia as a trusted third party to perhaps give a perspective that isn't currently there in some of these conversations. And even though I'll mention it in a litter slide, I'll tell you the story right now, I participated in a meeting at NATO in about a year ago, early 2011 on the heels of the NATO summit that was held in the fall of 2010, where cyber security was identified at NATO's number two responsibility. Number two objective, right. Right behind missile defenses and I sat with the supreme commander. James [INDISCERNIBLE] very articulate guy. Very, very impressive guy. And an assistant secretary of defense, and he just said, guys, I was the only academic there. Thank God I wore a tie. I did have jeans on, but at least I decided to wear a tie that day, he said we don't know how to do this. We need your help. Okay. Supreme commander of NATO saying that to a group of, of private companies, and one academic, and what I would say is that was a very interesting conversation that unfortunately hasn't gone anywhere. So maybe it's because I don't have a contract number that I can begin billing to. I don't know.

All right. So I'm almost done with my talk and I know I'm almost out of time, to facilitate the, the technology transition, I think we've built some very good infrastructure, which I'll point out here at the bottom here in terms of DHS, the DETER and the GENI project. That gives us the ability to do basic testing of cyber security capability. We need to escalate that, we need much more capability to routinely robustly and in a metrics base way assess new and innovative technologies so that you don't have the problems that I face where I only could point to my deployment at the University of University of Wisconsin say, here's how my system verus [INDISCERNIBLE] versus you a couple other systems in this one deployment. We need the ability to actually test new systems, new tools, new AL go rim themes and capabilities so the word can see, hey, there's the underwriter's lab version for cyber security and this is really what I'm appealing to here. I think we have basic infrastructure and basic capability in place, and now what we need to do is take that to the next level so that we can truly assess and evaluate new technologies. I mentioned policy a little bit earlier. This is basically saying, this slide is all about the idea that policy is going to become more prevalent in the conversation, and we need to play a prominent role in educating the community about what technologies are, where the pit falls are, and how we can form policy that, that actually has the opportunity to have an impact. I will point to a very interesting workshop that took place that was organized by freed Snyder last year. Some of you were familiar with that. SMFS all oriented around training academics to participate in scientific policy. Totally school SDERS, exercise. I also participated in an activity at the Senate foreign relations staffers which was organized by a Tobin group, based in Boston. People are eager for cyber security policy. I think we as a community really haven't had much discussion about how we might inform and guide that conversation.

All right. Second to last slide. The real opportunities are in innovation. This is the whole theme of my talk, is that we have to foster innovation and I just offer a couple of ideas, so number one, whenever you talk to anybody in cyber operations about situational awareness, they would tell you I will love to have that of anything that you can give me to enhance situational awareness would be great, okay. Unfortunately, there aren't that many tools, there aren't, isn't that much KAPT to provide situational awareness. Secondly, I think we have to recognize that cloud mobile is here. So developing capabilities to provide solutions in the cloud mobile environment are going to be eagerly embraced if we can do that. I decided to put something controversial on here, which is regulation and enforcement. But again I think we all, we have to recognize that for example the FBI is very, very focused on cyber security right now, and it's important for us as a community to understand what their needs are, and to see if some of the technologies that we're developing can actually play a role in enhancing their activities.

Okay. So in conclusion, right on my hour almost, if I looked at where we started. We have a really scarey threat landscape right now today and going forward, and I believe the OERNL way that we're going to effectively address these threats is through innovation not through incremental change. We have a huge number of challenges that we have to face in terms of bridging the gap between basic research and actual deployment and I've offered a couple suggestions on how we might begin to bridge this gap. But I'm very positive actually about this space. I think we have a huge number of opportunities to have impact. I think that we can have an impact in terms of, of creating metrics, of creating, of developing enhanced capabilities in terms of software assurance, and more generally looking at how we can use partnerships to be able to address some of the end RANSs that we face today for deployment. I will point to my last bullet point which is changing the playing field. I don't know how to do this, but I really love some of the (, some of the ideas that people are having in terms of new security architectures, that just cast communication in a different light. And yes, those changes are very hard to make from a broad scalable sense, but from a more controlled, more confined perspective, I really do think that they have the opportunity to have an impact. So thank you very much for your attention. I'll be happy to take some questions at whatever time we have remaining. "

Operator:" Thank you, sir, and for those listening on the phone if you would like to ask an audio question or make and comment at the time please press star one on your touch-tone phone. And record your name clearly. Again that was star one, and please record your name clearly when prompted. One moment while we wait for our first questions.

.

[INDISCERNIBLE, VOLUME TOO LOW.]

So I just learned about ICOR today. And I put these slides together last night, so that's why it wasn't reflected, but I think ICOR sound like I great program and I'm very enthusiastic about it. "

Operator:" And we do have a question from the phone, would you like to take the question at this time? It does come from SAVA [INDISCERNIBLE] your line is open.

Thank you. Great talk. I'd like to ask the following question. So what we're discovering is that, not just the adversity but the technology we're trying to secure is also moving at an astonishing rapid pace, so can you point to some specific ideas on Newark tech TURZ that allows us to LeapFrog the technologies that we're trying to secure so we arrive on time rather than, you know, trying to secure yesterday?

It's a great question, and unfortunately I can't give you sort of a list of the top three. Where I think we have the best opportunities are, as I say, in the, in the, opportunities are in the area of software assurance. Where we're actually developing software where it's provably or testably secure, and in, when we control the entire system. In other words, when we're not trying to extend basic IP infrastructure some in way so that we can detect attacks at a, you know, more precisely, more accurately and more timely fashion, but rather when we have an entirely enclosed system that we can control from the top to the bottom of the stack. I can't point to specific projects that are addressing that question, but I know that there are some underway, and I think that, that that self-contained approach, you know, it does not lend itself necessarily to broad interactions on the Internet, are ways in which certain verticals or constrained deployments will have the opportunity to be more secure.

Okay. Thank you. "

Operator:" And at this time we have no questions in the queue.

Please.

[INDISCERNIBLE, VOLUME TOO LOW.]

So I haven't talked to Bill, but I have certainly talked to others, you know, as I've mentioned, [INDISCERNIBLE] was an advisor of mine throughout the process. And you know obviously a very successful entrepreneur in his own right, and you know, I've probably talked to, I don't know, maybe a dozen other people who have had varying levels of success, and there are, you know, many similar THEECHLZ -- themes in terms of some of the issues, challenges, and opportunities that, that we've even count he understood. I would say that the single most important element for my modest success was the guidance that I received from my board. I was very, very fortunate to have a, a board of directors that was composed of a lumpney from the University of Wisconsin who invested in my company and who were willing to spend the time to take an academic who had never started the company and to really sort of open my eyes to what I needed to pay tension to, and without those people involved in my company, I'm absolutely certain that I would have failed, so that to me was the single most important element of my success and that kind of mentorship guidance, experience, perspective is a theme that's resonated across all the other people that I've talked to. Please. [INDISCERNIBLE, SPEAKER'S VOLUME TOO LOW]

Sure. A lot of great thoughts in that statement. Let me see if I can tick them off one by one. First of all, I actually, I don't think academics by and large make good entrepreneurs. So I think that, and unfortunately a lot of the infrastructure, especially at universities is oriented toward trying to make academics entrepreneurs. And the main reason I say it is just that I've been fortunate to be around, really, really successful entrepreneurs and they just bring a different element to the table than most academics that I've been around. I don't know exactly how to articulate it. It's, it's a charismatic element it's a strategic thinking element. It's a very kind of on the ground, how do I make this happen by hook or by kind of element, [INDISCERNIBLE] for academics those ideas do come but it's really a different mind set. It's a different embodiment of success and how you make things happen, so where I really think the opportunities are in terms of entrepreneurship as we're trying to stay in this AKdy that we're trying get off the ground at University of Wisconsin I think youth is highly under estimated in the United States. Remember the [INDISCERNIBLE] would we have ever, you know, that young an average age in a major project today? Probably not, right. So, so what I think is embracing youth in terms of creativity, innovation and entrepreneurship is where we should focus some effort and that's exactly what this center is about. I totally think that this issue of external corporate funding for research is separate from the idea of entrepreneurships that I talked about. In other words, I think that, that accepting outside money always comes along with the recognition that you need to, or should come along with the recognition that you need to be careful about your research, right? Full disclosure. Everything need to be completely oriented toward, eliminating bias from the work, otherwise, well, you know what the, what the result is. What I don't think is that necessarily getting outside money is something that, that leads to innovation. It's simply another modality to funding research. What I think is we need new modalities for fostering innovation. I think the ICOR program is one. We have one with our WISC activity and there are probably others.

I think we're done. All right. Thank you. [EVENT CONCLUDED] . "

Operator:" And for those on the phone, your call has been concluded and you may disconnect at this time. Once, again, your call has ended and you may disconnect at this time. Thank you and have a great day. [EVENT CONCLUDED]

Actions