Comments on Network Information Security

Center for Global Security Research
9 Dec 1999

Mark Graff, Sun Microsystems

INTRODUCTION

I do work for Sun Microsystems. I want to explain something. This is not a product talk. I'm the guy who's trying to make the network safe and protect all our information. Before that I spent four years trying to ensure that our products had as few security bugs as possible. I have a lot of experiences in the trenches of how hard it is to actually secure stuff.

You can think of this as a report from the field. I thought I'd better get up and give this talk before the stock got any higher, because my options are so valuable now that I'm not sure I'd have the courage to do this talk any time later. I'm going to try to describe for you today--it sounds kind of pessimistic; I think of myself as an optimist--but I'm going to try and describe what I understand as the difficulties today. The main thing I'd like you to walk away with, I'll tell you right now, is that none of the security stuff works very well at all today. And it's not likely to work very well in the near future. That kind of sets the tone of what I want to say. It's not working very well, I'm going to try to explain why, and then I have some ideas on how we might make that better. Let's let it rip.

EVOLUTION OF THE NETWORK

1. Our data is deserting us

To begin with, I saw a slide out there, Gordon Bell's slide, which said SAN. I thought that meant "Solar Area Network" or something. The WANS are really dissolving. I have another talk I'm giving in a couple of months, called "My WAN Went Away, and Yours Will Too." What's basically happening is that our data is deserting us!

We have one of the best firewalls and one of the oldest firewalls in the world. And I was an MIS director when PCs started coming in and you remember how frantic we were trying to say, "No, no you can't have one of those because we control all the data." Well, it's the same kind of thing now. The data is leaving the nest. The data is moving. I don't know if you've heard the initials ASP yet in reference to applications service providers, but you will. I'm going to talk about that. What we used to have was a firewall and our data inside. Now we have thousands of special connections between strategic partners and preferred customers and even our competitors. We have some contracts with our competitors where we're bound not to let this cooperative effort become visible to other parts of the company. It's an incredibly complex setup.

2. The modern network is unknown, and unknowable

Another thing I want you to understand is that our (Sun's) network today is actually larger than the entire Internet was 10 years ago. We have a remarkably homogeneous network, and, by the way, we run our own hardware and software. We are in a better position to manage our worldwide net than practically anybody because we make this stuff. Yet, we don't understand, we don't have a clear idea of what's on our network, in terms of intellectual property, we don't have an understanding of what's connected to our network in terms of what machines have access to it, and we don't have a clear idea of who's using this stuff, either. I would argue that this is true for all connected networks.

I could say we have so many thousands of systems and so many thousands of subnets and this is our product space and this is our other stuff. I'd like to keep in mind the words of the Greek philosopher Heraclitus who said, "No man can set foot in the river twice, because the river changes and so does the man." We can never use the same network twice. People are frantically adding things onto our network and connecting. We bring in whole new countries. I read yesterday that we are now active in 173 countries. I don't know how DoD is, but 173 countries sounds pretty good to me and we're making money in all those countries. We add another one every day. There is no one single mind now, at Sun, that understands our entire network, our entire configuration. It comes and goes and changes so fast that we can't keep track of it and I judge that no one else can either.

3. Denial of Service attacks are irresistible; plan for them

Denial of service is basically a trivial exercise. I've often asked the reason why some massive denial of service has not happened yet. Believe me, it's not because it's hard to do. It's because the economic incentive isn't there yet. The sociopaths are there, the mechanisms are there, it doesn't pay off yet, but it's not because it's hard to do. Just this week and last week, a lot of security organizations that are my friends came out with a cascade of warnings about distributed denial of service attacks where we build up a cascade of distributed systems which we make use of as launching points so that we can coordinate a denial of service attack from around the world, focussing on one particular kind of system or network. Mind you, these denial of service attacks offer a very strong analogy to the telephone network too. If I wanted to deny one of you folks telephone service, I'd just enlist a bunch of my friends and we'd call you all the time until you took the phone off the hook. It's not that it's a new problem. The scale of the problem is new, and I want everybody to see that it's here. (This warning came in December, 1999, about 2 months before the huge denial of service attacks of February, 2000, in the USA.)

4. Current economic factors are not driving towards security quality

Another thing is the economic factors in designing and building secure hosts, secure operating systems, and secure networks. I'm not speaking as a representative of Sun (if you haven't already figured that out). I'm not trying to produce corporate policy. But I am strongly linked to a company that's one of the last places left standing where we make our own stuff, hardware, software, and operating system. I've been involved in trying to make all of it secure when it goes out the door, and I understand why that's hard to do economically. There are lots of reasons. Some are technical problems, but that's not really

it. Some of it is because that's not an appropriate use of a company's resources, to guarantee security and stability to the level that we would anticipate in other platforms. We're used to 99.99% reliability in our telephone system; we don't expect that from our computer systems today. I would argue that the time is coming when we will.

AN ENGINEER'S OBSERVATIONS

Let me give you some observations that I have culled over many years of working on these problems. Some of them may be new to you.

1. The rate of incoming security bugs seems to stay about constant

First of all, I have been tracking for many years the rate of new security bugs that are reported to us and of course, the ones that relate to our product specifically and also most of those are generic UNIXÒ bugs. I've charted them, and tried to balance out things like the growth in our customer base and so forth. My observation is that the rate of incoming security bugs has remained pretty constant. In other words, there is some factor out there that is limiting the reporting of new operating system security bugs.

Now, it's not the number of bugs in the operating system. I've spent years trying to figure out whether the bugs in our operating systems and others' systems should be represented as a lake or an ocean. Is there a finite number of fish, or an infinite number of fish? We finally kill all the bugs and we'll have all the fish out of the lake and I've come to realize that it may not be an ocean, it may be a lake--but there are an awful lot of fish in there and we keep restocking it. (Some bugs are so important, we fix them more than once). I ask myself, what is the limiting factor? It's not an intrinsic limitation to the operating system; it's not a limitation on our ability to record bug reports. Because I have corrected for those things. It is not how we fix them, because that is a different issue. I am talking about recording them, and my view is, having spent years dealing with some of the nut cases that work out these bugs, is the limiting factor is the people who want to find these bugs so they can exploit them require a certain level of access to operating systems and hosts and the things they secure. They want to have a certain ability to get in, maybe it is an hour that they want to spend fooling around to try to break into security, maybe it's a day, but my view is that that is what is held constant. It's the requirement by the hackers, who will find most of these bugs, the requirements of the hackers to have access. And that's an interesting thought I want everybody to kick around.

2. Critical systems are most often the least secure

There is another thing that I have learned in my role of trying to protect tens of thousands of systems and a complex network, and that is that it is the critical systems that are most often the least secure in a network--and not by accident! It's because if we have a mission-critical system we can be very conservative about administering it, and it's the last one to get the patches. I will spare you all of the sordid details, but believe me, trying to convince some vice president that he needs to take his critical system off line on a Sunday night so that I can apply security patches is a very difficult thing to do, so that

(and I think it would apply very widely) the critical systems are the ones that have the oldest technology, have the lowest patch level, and this is another factor that is going to influence trying to secure cyberspace.

3. Firewalls tend to become routers over time

Another fact is that due to the tremendous economic pressures that we have--we are trying to make a buck, we have customers all over the world, the field is expanding, we are having a great time, stock is going through the roof--what happens is that everybody wants to be connected to somebody else, we have sales people, we have VPs, we have our illustrious CEO saying "Yeah, we can do that. We can hook you up." And what happens (and all my buddies in other companies tell me the same thing) is that over time any firewall will become a perfectly fine router, right, because the essence of network computing is connectivity, so we are going to be connected.

4. Information wants to "co-mingle"

I'll tell you something else in that context too. You may have heard the expression by some of the folks that I regard as adversaries, "Information wants to be free." You've heard that? OK, it took me ten years, but I think I figured it out. That's true but incomplete. Information wants to be free so it can reproduce. Because information wants to co-mingle with other information. OK, our information is dying inside out network. It wants to be outside our network so it can be combined in the databases and knowledge warehouses, and people can make products out of it. So the information inside the network is like a plasma that is leaking out, not because we are careless, not because we don't know what to do, because the very economic factors that cause us to build networks in the beginning, the very things that cause these things to exist, are the same forces that drive the information out, to work and be used and shared.

5. The information security of a static system, decays due to external influences

My last observation in this area has to do with what I call security decay. Walk with me on a short thought experiment. Let's take a brand new SparcStationÒ and put on the brand new version of your latest favorite operating system--mine is SolarisÒ. Then, let's put all of the security patches in there, and let's do everything we know how to protect this system as an element of a general-purpose workstation sitting on a network. We've got all the passwords in the world. We've got all the encryption in the world. You can have anything you want. And let's take that workstation and set it right here and shrink-wrap it, turn it off--turn it off!--and come back in a year and a half and turn it back on. How much of its security will have decayed? How secure will that system be, as compared to how secure it was when you turned it on?

Now, a lot of you have been in business a long time, you are probably familiar with the concept of "bit rot." This is an extension of the idea of "bit rot," that security decays and, for what it is worth, it does seem to be 50 percent in 18 months. (I like that figure, an inverse Moore's Law rate.) Security decays even if you don't change anything, because

the outside world moves on. There are new attacks developed, new classes of bugs found, new ways of mounting attacks and so forth. And so, even if we do nothing, even if we turn the thing off, it is much less secure than it was a year and a half ago, and you can imagine when we factor in how quickly we are changing things and how quick the mission of the computer changes and how fast we are putting in bugs and patches and other things. You can imagine that it must decay.

6. Technology sprawl makes networks harder to secure

I'd also point out that there is a factor I call "technology sprawl." We see a lot of it, and I think we have an unusual environment because it is homogeneous, so you guys must see more of it. Technology sprawl is what I use to denote the mix of technology levels. At Sun it is pretty simple; we have old Sun boxes and really old Sun boxes and more and more Sun boxes, and then we have a few of those little Intel things. But we have lots and lots of Sun boxes, and they run Solaris 2.0 (two-zero), and Solaris 2.1 (two-one), and Solaris 2.5 (two-five), and Solaris 2.7 (two-seven) and so forth, and in any technologically rich environment what you are going to find is that for economic reasons and for reasons of mission criticality and conservatism, you are going to find that over the years, the mix of platforms that you need to support sprawls out over and over and over

Now today we can see it. We get ready for the Y2K stuff and everybody has been thinking about this. You know we have programs that are running COBOL, programs that are still running FORTRAN, machines all over the world that are running the kinds of operating systems they don't make anymore, including our beloved TOPS-20Ò. There is this incredible sprawl of systems, and if you combine that with what I was talking about before, which is the security decay, then a network, even if you don't try to change the network, just as you are adding things and not changing the other stuff, the mere fact that you've got dozens and dozens of different kinds of things means that your network in totality is much harder to secure. And if the information is spread across all those different technologies, how much of it is secured as well as you can secure it? Very little.

There was an incident at SunÑnot the kind of incident you think. We have software that goes out on the network and tries to probe our system; we wrote it ourselves. It is like the ISS stuff. It tries to probe it and it checks it for a couple of hundred vulnerabilities. It is not a product; we just use it ourselves. And it tried to connect the system in various network ports and it checks for various thingsÑcan you mail it something bogus and all that kind of stuffÑand we have reports that we sent to management. And the reports said we checked 50,000 systems and the security level was here, and then we run it next month and it said, good news, we checked even more systems and the security level is even higher. And you know we started out with corporate goals, and it's at 12 percent, and now its at 14 percent, and now it's at 80 percent, and oh my [Gosh], I charted this wonderful rise in the reported security of our systems, and I was getting to forward this to the VP. I had this awful feeling; and I went back, and it took me a couple of days, but I got the information on (remember I said we had a homogeneous network) the move through the network, where we were moving from Solaris 2.5.1 to Solaris 2.6. In other words, we rolled out the latest version of our operating system across our entire network,

naturally enough. Well, the tool that was designed to probe for vulnerabilities was written with the 2.5.1 vulnerabilities in mind; it didn't know anything about 2.6, because it hadn't been updated for 2.6, so when I took the curve for the 2.6 updates and laid them on top of the improvements we thought we had been charting, there was a perfect match, and all I was showing was, that our ability to perceive the vulnerabilities had diminished because the tool we were using was getting duller and duller and duller over the months.

7. For many people, the Internet is their first experience with anarchy

Another point is that in this new Internet environment, this is the first experience that most of us will have had with anarchyÑthe very first experience. You all know the story of the woman who called and said, "Let me talk to the head of the Internet help desk." You know, that kind of thingÑIt happens to us all the time. And it is very unusual for us in this highly organized, strongly technological society to be confronted with a system that has no leader. It is beautiful technologically and I bow down to the people who did it, but it is an anomaly in our society and the fact that there is no one in charge and the fact that there is no one you can complain to about things that happen is hard for people to get through their heads, because it is not part of our usual idea. Therefore, the problems of slander, the problems of sociopaths attacking.

8. The Internet multiplies the power of an individual to affect others

I had a terrible summer several years ago; there was a professor at a Serbo-Croatian university who was laid off, and he single-handedly produced more security exploits from his apartment, wherever it was, and then mailed them all over the world, all the other bad guys combined for the summer, actually, while he was out of work. He was mad at Sun for some reason, so he affected tens of thousands of our customers by developing these exploits.

The effect of the power of the individual has been dramatically multiplied. Until we come to grips with that we won't be able to understand security at all.

IMPLICATIONS FOR THE FUTURE

What does this mean for the near future? Well, first of all I am going to assume that everything is pretty much connected to everything else. As a friend of mine says, "Now that everything is connected to everything else, all the interesting problems that are left are security problems." He is a security person, too; maybe he is present.

1. Ubiquitous encryption is the only means of controlling information access

What all these things mean to me is the following: That in this near future, you will be able not to control your information, but rather to exert influence on its distribution. You will be able to trade money and liberty and convenience for time, but you are not going to be able to see who gets to it and who doesn't get to it because everything is connected to everything else! And you need to understand that. an encrypted worldÑubiquitous

encryption, freely available, finely tuned is the sine qua non; there is no security in the future without encryption, and without constant honing of the encryption tools. In fact, everything ought to be encrypted everywhere. When we go to use information, it should be decrypted at the last possible moment.

We are working on a lot of this stuff in the research labs. There is some good stuff on the way in that area, enterprise to enterprise. But I think ultimately we are going to find that encryption in order to be really reliable has to be brain to brain, decrypted at the last possible moment. That was I was alluding to earlier, is I would be really surprised if there isn't somebody in this room who was actually involved in a project to devise encryption devices that can decrypt the information based on the pattern of the brain waves, you know, that your key is based on the way your brain is fixed or something because you want get it the last possible moment. If you decrypt it on your workstation it is useless.

2. A Von Neumann machine makes a lousy network computer

The other idea that I am sure is going to be a little controversial. I think the idea of a general-purpose workstation (a Von Neumann machine) connected to a network is an anachronism. It is impossible to secure. I don't understand why we give people who want to read email a computer that has ten thousand programs on it, three quarters of which were written by a bunch of undergraduate students 15 or 20 years ago. You don't need that. We are moving away from it as best as we can, although (remember what I said about technology sprawl) it will be decades before all this gets resolved. But there is no reason why the average person, or the average homeowner, or the average user, needs it. If his refrigerator is going to be connected to his shower or something (which must be the "shower cam" I keep hearing about) what does he need a general-purpose computer for on the network? No, we need to get these specialized capabilities down and get it down to five or six things that we really need to do.

3. Individual privacy is about to become a quaint concept

Another thing I want to leave with you is, I talked a little before about what I think can be quaint in a couple of generations. I say that the notion of individual privacy, lamentably, I believe is going to be regarded as something quaint. I believe it is going to be regarded as anti-social. I wouldn't be at all surprised if the current move toward narcissism, and the economic advantages of sharing information, lead us to believe that it somehow wrong to try to withhold personal information from people. That ethos, I suggest, might change.

4. Perfected communication is the antithesis of privacy

Moreover, there is a wonderful short story by Isaac Asimov, called "The Dead Past," published many years ago--fabulous story In that story, somebody discovers that a time machine has been invented but the federal government has suppressed it; and he goes on a great crusade to find a way to rediscover the invention, and liberate it from the suppressing government. At the end of the story, we find that this whole scenario is only a vehicle for Asimov giving us one idea, which is to say, as one of the characters does,

"When do you think the past begins, anyway? It begins a second ago? And by making this time machine available to everyone, you have completely compromised individual privacy because we can now watch each other all the time." Great idea, and I would point out that this is also the destination you reach on a parallel path with perfected communication. We get to very much the same place.

5. Communication and transportation are not as different as they seem

Another idea that is going to be quaint is to our great grandchildren--if we are still calling them children by then, don't know what we are going to do--another concept that is going to be quaint is that we made a distinction--they'll laugh at us--we made a distinction between communication and transportation. Isn't that quaint. "You mean, Grandpa, that there used to be a difference between getting a copy of something and getting that thing? I don't understand. If you live in Des Moines, why would you have to move it to Des Moines, why can't you just get it downloaded?" These are fundamental concepts that are going to change.

6. It's premature to put critical-to-life applications on the Internet

The thing that bothers me a lot (I have done some radio talks on this), critical-to-life applications that are making use of some of these innovations are already being deployed today. I have talked a lot about operations being performed over the Internet. I read in the Presidential Commission's report, "Critical Foundations", about 40 percent if not more of the country's 911 systems are migrating on to the Internet as we speak. A lot of them already have. In fact, if you look up 911.com, it is some place in South Carolina, some county's 911 system. There are a lot of critical-to-life applications that are being moved onto the network and it's very immature for that. It is dangerously immature. My view is that society doesn't understand how risky this is because the new world we have created, what we have created, is not in line with our risk instincts. We can't evaluate the risks because we can't understand how powerful this ego multiplication factor is, we can't tune in to what really can happen. Therefore it is vastly premature; and I argue--I am sorry to be pessimistic--but I believe people are going to die before we understand how fragile this is.

I'll give you just one example. When they do we are going to feel the rage of all the people who think we should have fixed it, but here is an example. I had an MRI at Stanford Medical Hospital the other day, and it was kind of an uneasy experience. I know a lot of you have probably had this. I am lying under there and I'm the guy who is responsible for the security of the operating system they are using to guide the gizmo. They were running Solaris 2.4, you know, and it turns out Seimens-Nixdorf makes them, and there is some deal where they use our operating system. I remember talking four years ago to the guys at Seimens-Nixdorf, and the people at Stanford and I said, you really out to be installing our security patches, and they say, no, no, it is a direct ship from Germany. We just take the Solaris and put it on it, and so forth, and the upshot is I am lying there with the ultra high-intensity beams, hoping that there are not paper clips in my mouth, or whatever, and realizing that somebody in another part of the world

(because this thing is on the network, MRI is on the network) could be giving it little tweaks. Now forget the security and privacy of the records. I don't care about that. If somebody really wants to see what I look like inside---I guess for celebrities, there maybe is a market in it. But they could be making little tweaks here, and I think it is vastly premature.

RECOMMENDATIONS

So what are we going to do about that? I've got four possibilities. I've got some attitudinal changes you can make. I've got some technological changes. I've got some process changes, and I've got some legal changes. And I'll give it to you broken down that way.

1. We good guys need to pool our knowledge

First, the most important. We need to pool the knowledge of all the good guys. I'm going to automatically give everybody here the title of "Good Guy." We've got to pool our knowledge. We've got to break down whatever barriers there are, because the bad guys pool their knowledge all the time, and we got to break down those barriers and figure out that we really, really need to work on this. It is very important, we have to get it beyond any hindrances Ñ economic, legal, personal, anything that gets in the way of sharing and improving.

2. We need to recognize the primacy of information

We need to recognize the primacy of information on our networks; the network is not the big deal, it is the information that's the big deal. When I was an MIS director in Orange County, California, I was the first one to tot up his disk drives one day and realize we had a gigabyte of storage. With the new disk drives coming in, we had a gigabyte of storage; they were all DigitalÔ disk drives. Huge farm, five or six times the size of this room, every one of them humming, RP60 or whatever it was, and we had a gigabyte of it. We made the papers. But I realized looking at the disk farm that it was the data that was my product and the computers were the peripherals, not the other way around.

Well, the information is what's important. So even if we can't secure the hosts-- we give that up, believe me; even if we can't secure the hosts, even if we can't secure the network, worry about the data.

Consider: How do you know when you go home tonight that somebody hasn't been in your house? You don't know. It kind of gives you a queasy feeling, but you don't really care as long as they haven't changed anything, I think. And so it doesn't really matter necessarily whether your host has been invaded; it's the information. Is it safe? Does it do what you want it to do? Is it still secure in a way that is meaningful to you?

3. Perfected authentication is essential to future network security

Technically, what we can do is to perfect means of authentication. I think what we see in the future, the thing that stops some of these disasters I've been talking about is to have perfect, perfect authentication so that we know who's doing what. When you solve the authentication problem you begin to achieve personal accountability. Accountability is the foundation of responsibility, which is in turn essential for an ordered society. We need to understand who is doing what. At least you need to be able to stop people impersonating one another. If we can't sustain the changes that would require enforcing authentication--and of course, universal PKI would be an approach--if you can't do that, at least make sure we have some recourse. If somebody goes on the network tonight and says, "That person is a pedophile. I've known him. He did something horrible, x, v, z and so forth." I could blacken the reputation of anybody in this room tonight in the eyes of hundreds of millions of people, and you wouldn't be able to discredit me because I could claim to be somebody that could plausibly have been injured. We need to solve these problems, and authentication is a way to remove the anonymity. We need to get as much encryption as possible and make it as easy as possible so that nobody ever has to think about it, and you decrypt at the last possible moment.

4. We need a way to know when intellectual property has been compromised

In terms of process, one of my jobs is trying to minimize the loss of intellectual property at Sun, and people look at me like I've got a hole in my head when I say, "What is that?" "What is it?" Then they give me a definition, and I say, "OK, fine, I think I understand it. Now how much of it do we have now, so I know when some of it is gone?" I'm perfectly fine. I'll go all night long. I'm a veteran. I'll stay there with my gun and I'll make sure nobody takes it. Just tell me how much we have now, and, oh, how do I tell if it leaves the room? Just tell me. I'll be glad to take whatever measures, and of course nobody can tell me! How do I measure my IP? How do I know if it shows up over there? How would I ever know? Because we don't track the provenance of data, we can't tell where it came from. I can't prove it came from my network. Someone mentioned steganography. I am very interested in steganography as a way of signing documents, but it still doesn't help us measure how the stuff is leaving the company.

5. We need a way to measure the security of a system

The other thing I think we could really, really use is a way of comparing the relative security of one system to the other. If I could just know that I've got a Solaris workstation here, or Windows 98Ò workstation here, and after I finishing patching it I could measure it and find out that I had improved it somehow. You know, if I could just do that. I'm not talking about some complicated orange book, forgive me. I just want to be able to compare two systems and say which one is stronger, even if it is the same one, just with some patches. If I could do that I could make it. And I think an approach would beÑthere are actual physicists in this room who could do it far better than I canÑthink about the security half-life that I was talking about, and imagine that you are trying to measure how long the system could withstand certain grades of attacks and how that declines over time, and I think the intrinsic security strength in its architecture is related to how long it can withstand certain classes of attacks before it degrades completely.

6. We need to facilitate inter-vendor communication

Just as important, we need to facilitate inter-vendor communication and cooperation (need to talk to the Justice Department about this). A lot of the time when we get together with other vendors we have to worry about restraint-of-trade issues and the fact that we invited these people, didn't invite those folks, or they couldn't make it or something. I've talked to the Justice Department many times. I'm hoping that they will, and they have told me there is legislation they are working on, to make it easier for the vendors to collaborate, just as I say we all ought to be collaborating.

7. We need to resolve standards of security liability

Secondly we need to address and resolve the legal standards of liability. You know there haven't been any big liability lawsuits of the kind I expect. But when e-Bay is taken off line by a bunch of teen-agers, which I understand happened not long ago, they're going to turn to people and try to figure out who's responsible that had the deep pockets. We need to understand what the chain of liability really is before we can get into things like Underwriters' Laboratory listings and actuarial tables. You know somebody some day is going to kill somebody with a laptop. It is going to happen. Yeah, maybe just hit them on the head, but you could kill somebody 1,000 miles away with this thing, and the only thing in that laptop that is rated for safety now is the electrical cord, or maybe the battery--you shouldn't throw it in the fire. But that's got to come to the end.

So we need security standards. I think industry and I think government has to stand up together to their responsibilities. I think we need security standards. I think we need to remove the economic barriers for individual companies to achieve sound security. We need to remove that competitive element out of it by mandating that certain fields and certain applications will be required by law to achieve a certain level of security, and vendors who want to be in that market must raise their products to that level. I think it is going to happen. I hope it happens before we are forced to do it. I think if we work together and we all realize rationally, with open eyes, our responsibilities we can work together and get that done.

Fin