Herbert Baines III
Director of Information Security
Office of Information Technology, Georgia Tech

Interviewer: Grace Agnew, Georgia Tech Library

Q: You're the security director for a large multi-site educational network What problems would you say present the greatest challenge for you?

A: When we look at educational networks, usually they fall in two categories. You have the institutes that are geared toward research; you have the institutes that are geared toward the arts and probably the business processes, more than anything else. Georgia Tech is very unique. There's a great deal of entrepreneurship that we have with GTRI, our research arm, and then we allow a lot of autonomy within the college and the administrative units. And then there's the residential network, where each student has a full two-megabit connection [on which] they're allowed to host services for the full four years that they're here . Each of these services are on multi-user machines, so we have a large population of servers here Most institutions have a centralized management approach. Georgia Tech is very decentralized. So with that autonomy and decentralization, establishing policies, standards and procedures that can enhance the educational process and yet provide security is definitely a challenge.

Q: I've personally visited several hacker and phreaker sites. They're rather scary. You can download software and create a virus without really having to be a programmer. There's also a lot of software piracy…That software piracy is done by just about everyone these days. With the MP3 files for music, there are commercial sites that are basically guilty of software policy. What can we do to teach students that that sort of behavior is wrong and insure they're not performing that behavior?

A: Well, this is a new directorate, and as part of our program initiative we're going to have some education and awareness for the campus. Part of that will be not only attending Psych 1010 courses here, but also going out and hosting seminars and perhaps adding some policy and procedure for identifying the necessary constraints that we must place on our computer systems at Georgia Tech. In the past, we discussed perhaps having a waiver that you sign, any Georgia Tech employee, student or faculty member, stating that you must adhere to our computer usage policy. Part of that computer usage policy is identification of copyright issues, and within those issues, any violations could terminate your usage here at Georgia Tech. Beyond the policy and the awareness, I think that we could more proactively scan our systems to prevent this type of activity. However, that's a political football, because if your mission is to enhance the educational process, entrepreneurship, and research, on the other hand you are scanning for a particular type of protocol or piece of software. That's a political football that we will be debating here at Georgia Tech in the near future.

Q: That's an interesting thing you brought up, because it's not just are you stifling education but how do you see a person's right to privacy? I know in high schools, where the high school is *in loco parentis*, they can search your locker if they need

to. By the time students come here, they're legally adults. Do we take an *in loco parentis* attitude and say we can search your computer? Do students come here assuming a certain amount of privacy on the computer that may or may not be true?

A: …Currently, we don't search, scan, confiscate any computers or files… However, with the advent of a lot of the viruses we have here, to protect the Institute and the legitimate data repositories, we have to take some steps at our gateways and our borders with our Internet-2 connection and our normal Internet connection to prevent viruses from impacting the campus. On the legal side of things, with the advent of MP3 files, as long as they're not copyrighted MP3s, we're safe. However, as you've seen on the news, there have been plenty of universities that have been embroiled in legal battles because of this and judging those cases, I think the artists will probably win those cases. We have to show due diligence here at Georgia Tech. So there will be change on the near horizon. I cannot make a full prediction weighing the right to privacy and the needs of the institution, what that final solution will be, but I think we are heading in that direction.

Q: So we will start tightening up?

A: Definitely.

Q: Do you have children?

A: Oh, yes.

Q: How old are they?

A: 13 and 14

Q: How do you teach computer ethics to your kids?

A: I try the education and awareness approach. I give them guidelines. And they have their limits. As long as you stay within the limits, there's a great deal of latitude for you. Sometimes a generic search will pull up a pornographic site. My daughter went out to look for Barbie dolls, and you can imagine the type of Barbie dolls that came up on the screen. Every now and then, I'll do a random search through the cache files, and I have a firewall running also, so some of those sites kind of caught my attention. We had a discussion, this was a family discussion about some of the searches that are out there. I was really hesitant to put a filter, a web filter, on our computer because there are some legitimate sites out there, and they are teenagers, they talk about it in school. They need to use their own judgment in a lot of cases, and just like Georgia Tech, we want to empower people as much as possible and allow them use their judgment as necessary to maintain computer usage policies here at Georgia Tech, and our policies at home.

Q: Do you have policies at home? Do they understand about software piracy and MP3 files?…A lot of parents haven't thought about that aspect of it. They worry about the pornographic sites; they don't worry so much about the fact that their child may be downloading and keeping files that don't belong to them.

A: My son and I had a debate about this. MTV advertises their web site all the time, and there happened to be a link to a site, I think in South Africa or Australia, a Mariah Carey site. And he says, "I'm not violating U.S. laws because I'm retrieving this information from a foreign country." We had to revisit that issue.

A copyright violation is copyright violation. I think they have a good understanding of the issues involved.

Q: He's a handful isn't he. He's a smart kid. I don't think at his age I would have said, "I'm not violating U.S. law." That wouldn't occur to me.

A: They talk about these issues in school quite a bit. Another issue that also comes up within the school system, is plagiarism. With all the information and resources available on the Internet, homework can become point and click where the child doesn't obtain any new knowledge; they're just rehashing information that's currently available. So we have quite a few conversations about that. Because of my schedule, I try to check homework at least two times per week. My wife checks it in the interim. That's a task. Because the encyclopedias…of the old days, left a lot up to your interpretation. However, there are plenty of opinion papers on any subject out there. It only takes twenty minutes or so and you have a complete homework assignment, and that aspect, more so than copyright for the children of today, I think that's a very negative thing.

Q: You mentioned a personal firewall. That's a fairly new technology. How does a personal firewall work?

A: Most of the personal firewalls that are available actually shut off a variety of common services. It allows the user, the owner of the machine, to establish connections to any site. However, during that connection, if there's a service that needs a response from your system, it will prompt you if you want to allow that service to come through. Simple things like pinging systems. A ping is where you go out and establish just a "hello" to a particular system from your system, even those type of communications are denied. It's up to the user, the owner of that computer, to allow the services that are necessary to do the job. Common services, such as web services, as long as you initiate them, they are allowed through; email, unencrypted, is allowed through. Any encryption mechanisms must be authenticated by you. I think that's a really good thing. [It's software based]. There are several companies out there that really do a good job. The larger companies, particularly the virus companies, are starting to pay attention because they are buying out the smaller companies. My only fear is that the smaller companies went to great lengths to incorporate features, such as logging and auditing mechanisms, a lot of which could be really useful in the corporate environment to protect some of the resources there because they have centralized reporting mechanisms. As the larger companies obtain the smaller companies, you run the risk of not being responsive to customer needs. And I think this technology adds a lot of value and I would like to see it flourish in the future.

Q: It's interesting when this distributed denial of service happened against eBay, Amazon.com and other companies, one article I read mentioned that as these companies get more sophisticated in setting up firewalls that prevent them being used as zombie sites, that people wanting to do zombie attacks may very well turn to home computers that are on cable modems or DSL where they can aggregate enough bandwidth to make it worthwhile. I presume they'd have to ping those computers to identify them, so a personal firewall would protect you being used in that matter.

A: …There are plenty of programs that are out on the web that will scan your computer and [identify] vulnerabilities that are available on your machine A personal firewall shuts at least 99.9 percent of those services off, so for the common user or hacker that's out there, the computer would appear as if it's not on the Internet at all.

Q: A cybercriminal that's frequently singled out in the literature as being particularly dangerous for private networks is the disgruntled insider, particularly the insider who is fired from his job or doesn't get the promotion he expects, so re-enters the network through a hidden back door. How serious is this problem, and what can you do to neutralize the threat of the disgruntled insider?

A: The disgruntled insider, that threat is very, very significant, however the occurrence is very, very low. Anytime that you have an employee, particularly in the network environment or a systems environment, who has numerous accounts, unless you have a centralized accounting mechanism, they will have access for a period of time as each incident is discovered, and during that interim period, if they're disgruntled and they have the know how, they could wreak havoc upon that organization. Sometimes it's not even discovered, and that's very, very unfortunate. The risk is low, but the impact is high. More importantly, the thing I see with cybercriminals is the intellectual property that's out there. Most folks will [say], "you need to sign this waiver if you come to work for us, you cannot use this technology in your new position with another corporation." However, unless you're going to have a 24 x 7 bodyguard on that person, that information is disseminated, and that has potential impact on the corporation also--lost funding, research activities, those types of things. I think that area of cybercriminal activity is much more significant than the disgruntled employee.

Q: Encryption, particularly the standard private key/public key methodology, is a means of insuring privacy of files and privacy of communication. However, it does require really careful management to be successful. Problems that can occur are when individuals fail to safeguard their private keys or lose their private keys, or they leave the institution without removing their encrypted files or sharing their private key. How do you deal with that kind of bleed out that can happen with an encryption system?

A: That's a very touchy subject. Much like the personal firewalls, personal encryption mechanisms are readily available, and there is a great deal of value in that, but it's a shared secret that should be within the organizational structure. Especially when you are encrypting hard drives or you're signing legal documents, there should be a repository that escrows signatures so that you can decrypt those files later on. However, policy bodies at most educational institutions don't understand the methodologies behind these types of systems, so there has to be an educational process that happens here. And here at Georgia Tech, we have an information security policy group, and what we're going to do is bring in some experts, outside opinions, to brief that group. Anytime you have OHR [Office of Human Resources], vice presidents, CIOs and CFOs all in the same room, there has to be some level setting. To establish good policy so that you can manage effectively, is really a challenge. The management of these systems from the technical point of view is almost a fairly trivial thing. It's

implementing a policy that can be adhered to that is the real challenge of management of these technologies. I think that as we go down this continuum, the vendors will start to recognize that and start to facilitate this process more. Because the average user, even though they can easily download a demo copy of PGP and encrypt a hard drive, they don't understand the technology, and to try to extract data from a drive that's been encrypted, especially after you do something simple like forget your password, can be an arduous task. I think education and awareness is part of the management process, but more importantly I think the policies and what you can and cannot do with these technologies is really very important.

Q: That's been a topic of controversy is the government as well. The government has been very interested in having a key management system, where private keys could be escrowed and the government could get at them with a court order. Some of the concerns that have been expressed about that is you're then setting yourself up, with this key management system, a single point of failure, where if you are a determined hacker, you're going to break that first because that's going to unlock a lot of doors for you. The question is: who will guard the guardian, basically. If you have a key management system where you're storing keys in a central location, even if you're splitting the keys, can you really be secure with that? Would that not be the one place where all the hackers would tend to go?

A: That would be a single point of failure in respect to potential threat. However, most folks who are dealing with the Internet in any type of volume will have multiple keys, so that scenario does not exactly fit. You could have a key that's trusted for say, normal commercial use, then another key that you would use for some higher level activity--it depends on your job, your position. I think certificates will pay a higher role in this, because getting away from the personal, asymmetric type of key where I encrypt a file, I send it to you, you use a public key to decrypt it, I think the certificate based authentication and access will probably be the way to go, more so than digital signatures for these type of activities.

Q: The personal certificate includes an encryption key in it. It includes an encrypted signature that says that you are who you say you are, so you are still getting a certain level of encryption. Why is that more manageable with a digital certificate than it is just having your private key?

A: Because you have assurance levels with certificate authorities and certificates and you have general use and specific use certificates where you can manage the lifecycle of those certificates much more effectively without really impacting the owner of that information. You can have access automated to a certain extent where even though you could penetrate the certificate authority, those keys would be of no value to an intruder.

Q: The only thing that's encrypted is the CA [certificate authority] itself and your signature, so you're not encrypting the files. You're saying that given the fact that my digital signature says that I am who I say that I am, you are able to decrypt it and I am able to encrypt it and vice versa. [We can trust each other.] Here are my files, because I now trust you, and they're not encrypted. Once the digital certificate discarded, the files would be open to any determined hacker, but

hopefully if you have a strong certificate program, those files would not be accessible or the certificate would be renewed or whatever. I think you're right. That sounds like a better strategy than encrypting a lot of files and then forgetting about them.

A: Any time that you can consolidate your encryption activities, that's a very good thing. However, in the case of signing checks and distributing funds throughout the Institute, that digital signature should be a personal certificate that you present via PGP, probably. The official data repository for the Institute would have to escrow those keys, and a lot of times you have to escrow not only the keys but the machines that were comparable during their generation, because as machines and technologies evolve, you may not be able to decrypt. Backward compatibility is not something most of the vendors are looking at right now.

Q: That is a really good point, and I'm really glad you brought that up. I do a lot of work with digital video, and I run into that issue all the time. A company will not even be backward compatible with their own files, and so you are absolutely right, that's a very critical issue.

Q: Passwords are common security problems in a network. Users tape their passwords to keyboards or use common words. Pet names are very common, birth dates. They share their passwords with unauthorized users, and it's very difficult to get users to change their passwords frequently. What role does a password policy play [within a digital certificate structure?]

A: Passwords will always have a use as I foresee in the near future because that's the mechanism that generates a lot of the certificates that we have that are currently available, but physical security is always an issue when it comes to passwords. However, with a good password policy, and I think we've moved in that direction at Georgia Tech…The expiration of passwords in ninety days, which is on the central side, on our main campus servers, was an excellent idea and I think has caused the user some discomfort because they are used to checking their email and never changing their password or not even knowing their password. It's been set up by their customer support representative or one of their local field service representatives, and that's information that they should not have. The user should be responsible for their own unique password. As we move toward certificate-based applications, that's going to become increasingly important. A 90-day password has caused some initial pain, but now that we are almost beyond that initial pain threshold, I think that as the need grows, we can shorten that lifecycle, so that it becomes second [nature] for the campus to change their passwords. And not only changing passwords is important, but insuring that easily guessable passwords are not allowed, redundant passwords, where you just add a character at the end of the current password, those activities are not allowed. Most institutions have eight-character passwords. We have gone to 40 allowable and the longer the password, the better the hash so it's less guessable. An additional thing that we have that's very, very important is a strong Kerberos base here, and with Kerberos, as we move to a public key infrastructure, that's a very, very good foundation. And as we will see in the future, some of the policies we are implementing will help us succeed.

Q: One of the issues I've got with the long passwords. I have a few passwords that are really long, with letters and numbers mixed, and I have a great deal of difficulty remembering them. Because I don't want to tape them to my computer, I have to have a password file on my computer, and I have to go there and look up the password. It's really painful. A 40-letter password can be virtually uncrackable, but it can also be virtually unrememberable

A: The way that most end users should balance that is to come up with passwords that are phrases…You can remember a phrase reasonably up to about twenty characters or so. If you have a favorite poem or something, just type in the first [phrase] of that and substitute, as appropriate, with some uppercase and numeric symbols. I've found that to be useful. However, from the corporate or institute standpoint, we're looking at some vendor packages where as long as you can authenticate yourself with a single password, you'll have access to multiple systems at different levels, you'll still only have to retain that single password. So we're tying to consolidate that as much as possible. It's not a single sign-on because a single sign-on, one password gets you direct access to all of the systems. This is an interim approach. You will have to know the passwords for the other systems, but only once. As long as you retain the password you can change the other passwords. So single sign-on is a scary thing because physical security is very, very important. If you write down the password and somebody happens to walk by that, you have access to your financial records, your personal records and all of the systems you have access to.

Q: One thing that is interesting with the Internet is that we are practically living on computers these days, and the things we used to do physically, we're not doing physically any more. A lot of people no longer sit down at the start of each month and write checks. A lot of people never go to the store. I see advertisements on television to do your grocery shopping online. I know the secure socket layer is used, and they establish a session key and encrypt that session, but balanced against that, you do hear of large-scale thefts of stored credit card numbers. How safe is it to do a transaction on the web these days?

A: I think that the American public as a whole has been somewhat duped by online shopping. All the emphasis is on the transport between your connection, inputting your information to a server, and as long as that connection is safe, which ninety percent of them are, then with some assurance you can say that your transaction is legitimate. However the data repository that it's stored on, that is the key issue, and that's the issue that's hardly ever addressed until you read that 400,000 accounts were stolen. The government will eventually move toward establishing standards on the online repositories. If you're going to be an online repository, you'll have to meet some standards. Because currently with DSL, with general modem connections, you can establish your own company in your basement and there are no laws preventing you from sharing that, and if you have poor security, you can be as duped as easily as someone else…There has to be some type of legislation that occurs within the next two years, not to stem the tide of e-commerce, but to really enhance the reliability of e-commerce. When you get e-commerce and government together and try to establish a law, that can be a challenge. However I think that it's long overdue

Q: What do you think about biometric authentication devices? They're [starting to be] heavily used in airports. Once you've been authenticated by the ticket agent and you have been identified physically to be who you are, then they use your palm print or your finger print to let you into your gate. I think that's probably a useful thing for preventing someone for substituting for you before you get to the gate. Do they have a use beyond airport security?

A: Biometric devices will be proliferated in the very near future, because anytime a major vendor such as Dell or Compaq announces that they are going to be incorporating that device, then it's easily proliferated. I think that the PCs for better or worse-- there have been arguments on the Mac side, on the Unix side-- but the PC really drives the functionality in our society…And the PC vendors are moving into biometrics. That's a good thing; it adds another level of security. But the fallacy behind it is once your biometric is encoded, to go back to the data repository, it's just a hash. Some systems have strong hashes, encryption for that particular thumbprint, or fingerprint, even the iris. Once it's there, it's there. You attack the repository and you get access [to that fingerprint]. It's pretty difficult to go to the airport and substitute a fingerprint. You can't be backward compatible. However, the use of a biometric, if it's going to be beyond a physical presence, and give you access to other devices, other systems, I think that the repository becomes very, very important.

Q: ...So it could actually get very dangerous if I put everything behind a fingerprint, then anybody stealing my fingerprint would go way beyond one single failure with a credit card to just about everything I own. It could be very dangerous.

Q: How do we balance our firewall use against the free access to the world wide web We allow a wide range of services [at Georgia Tech]. We have numerous chat lines available on campus, and they're extremely useful. In fact, we use it at the library for real-time reference. We have tons of email, lots of web servers. Can we put all that behind a firewall?

A: Firewalling the campus from the general Internet is possible. It comes with a very, very high cost. However, we have a great deal of modem access here on campus, and that really defeats the purpose of a firewall. Because with a firewall, you are basically establishing the position that you trust anyone inside the firewall. With this campus, that is not doable. That is one of the predominant reasons for not using a firewall on this campus. The other issue here is Georgia Tech is probably the largest user of Internet bandwidth, even more so than e-commerce companies. E-commerce must support web access, and that bandwidth is manageable. However, when we have ResNet, several thousand students, many [hosting] their own services. We are an ISP, there's no two ways about it. We have the Internet at large wanting services from Georgia Tech. We have students that carry more bandwidth across the Internet than some of our centralized servers, so a [centralized] firewall on the campus will not happen any times soon. However, eliminating certain ports, for instance [all] file sharing on and off campus would be a very, very bad thing to do because it gives access, even though Napster sort of circumvents that to a great extent. Giving access to data repositories off campus is not the right thing to do, so we've taken steps to

prevent that. A firewall could be strategically placed to prevent access to some of our business units, our enterprise systems, and to a certain extent on ResNet, because with a firewall we could do some more auditing there. Many of the agencies that contact us whether they are dot coms or law enforcement agencies, ninety percent of the requests that we get for information are concerning violations coming off of ResNet [on-campus student residential network]. With the residential network here on campus, I think educational awareness will go a long way, but to some extent we're have to take steps to firewall that, either through a commercial firewall or through a system of restricting ports…

Q: Can you tell me briefly how a sniffer works? A sniffer is a tool that hackers use heavily.

A: **…**Once you get attached to a certain segment of the network, usually on a LAN, you have the wide area network and the local area network, but usually in the local network environment, there's two types of local network environments, the switched environment, where basically your traffic is sent directly to a router or switch and no one else on that segment can see your traffic, or a shared environment, which a lot of networks are these days, where everyone on a network sees everyone else's traffic going to a hub or router or switch. That's where a sniffer really comes in, because currently a lot of applications are clear text, so if I'm able to establish a connection to a LAN and put my network device in promiscuous mode, this allows me to absorb information, then I can log it or put it through a series of programs, analyze that, check for passwords, check for certain types of data files, I think hackers have used that very successfully, however as technology evolves then the use of the sniffer, [whether hardware or software-based] should be decreasing. We're taking steps toward that at Georgia Tech.

Q: What is spoofing? How do you spoof an address?

A: The spoof attack. That's an attack where I make my machine, whether it's on a local site or a remote site, appear to be your machine. Each machine has an IP address, that's a series of numbers, eight octets, that's assigned to a specific machine. There's also a network card that gives you access to the network that's installed in the machine, which has a MAC address, Those two addresses are sent to the network device, usually a router or switch. At that router or switch, if you are not checking for the correct combination to make that that traffic is in fact coming from your network or if you are only checking for IP addresses, then that information is available to source through your router or switch to be used in denial of service attacks. Here at Georgia Tech, we've taken steps [against spoofing]. To a great extent, ResNet has played a part in that, because [it has] some of the older network equipment out there, and we're finding [ways] to enhance that Internet security.

Q: You can spoof an IP address. There's no way to spoof a MAC address here it's hard wired, or is there?

A: Yes, there is. When you look at PDAs, or some of the wireless technologies that are out there, you can change the MAC address. You can steal someone's MAC address these days. As soon as you have a piece of the puzzle solved, there's a

new technology that shifts the gray line and you are back at square zero. It's a never-ending battle.

Q: Technology evolves daily. Because of that, the only way any of us are going to find solutions is with a great deal of cooperation among the commercial sites, among the government, among education. What is your thought about this cooperation and the role that education plays in it? …Is that something you see as a key role for academia?

A: Definitely. I think Georgia Tech is in a very unique position here. We do a lot of collaboration with law enforcement, especially, and that collaboration comes by way of grants through the National Security Agency, the NSF, we have the Southeast Regional Association of Colleges, those type of activities…And with the dot coms, they contribute funding to Georgia Tech, primarily for our research capabilities. They want some assistance in finding ways to enhance their current technologies and finding ways to deploy that readily. I think Georgia Tech is an excellent testbed, because on the one hand we do everything we can to facilitate entrepreneurship and research, that's a great thing, but we're back to the paradigm of the liability that's associated with that. Because we're in a unique position, there's a lot of opportunity there. We usually take every chance we can to contribute either through research or through some actual project development GTRI has done some excellent things with PKI. And we continue to get offers to develop some kind of think tank capabilities for some of these agencies there.

Q: What are the three or four key things that someone ought to have in a network security policy--the broad pieces of a network security policy?

A: In the broad sense, I think that anytime you look at a network security policy, which is actually an information security policy, because the network and information have collapsed. I used to say it's on the verge of collapsing, now it's there. I think the policy in general needs to be implementable-- the pieces of that are the awareness programs, policies that address the key enterprise systems. You have the technical architecture, those policies associated with standards, you can have the incident response policies and procedures that should be associated there. And you also have--which is very, very key--the responsibilities of each of the players. Those issues all need to be addressed from the user perspective, the departmental or college perspective, and then centralized. We each play a part in information security, and identifying those roles and establishing the security policies associated with those roles is very, very key. That's where we get into the collaborative process. If we continue down that track, we'll be headed in the right direction

Q: At the start of the 21st century, life is getting kind of scary. It seems every day a new virus like the love bug shows up. What I find particularly scary is that the people who are perpetrating this are just kids, average Joes, not the mastermind criminal whose intent I could understand… I'd feel more secure the attacks would go away if they fell within the standard law enforcement paradigm—there are bad people who do bad things--but because the world has gotten so gray…it seems like we're headed for very scary times. If you could look ahead five years, where do you think we will be? Are our growing pains going to be really terrible at the start of the information age or are we going to do all right?

A: Five years out from now, I think we're going to go in some radical directions here. I think we're going to have trusted systems that will have some heavy legislation and regulation behind them, and we're going to have general use Internet. If you look at Internet-2 right now, it's a pilot project, but if you look at VPNs [virtual private networks] that corporations have established, I think we'll have isolationism more than anything else to prevent those activities. The Internet will evolve into segmented pieces. Anyone who wants to participate in the general use Internet will have a high risk associated with that. I don't think anybody in the world can legislate that piece. However, ISPs have agreements that they don't even share with themselves. An ISP that Georgia Tech is affiliated with and that Duke is affiliated with, if we have some commonality between Georgia Tech and Duke, we're going to have to share that policy, because the ISP doesn't share that policy information among its constituents. However, because of that the ISPs with some government mandates could actually stem the tide. In fact, they are taking some steps on denial of service attacks and potentially some virus protection. The capability has been developed by CISCO as we speak where their routers and main core switches will have cards that you can insert in the switch that does the scanning for you for denial of service type of attacks and other attacks. However, that requires some type of waiver to be signed that will authorize the monitoring of content. The ISPs will have that capability, and they actually have the power to do that. But the Internet as a whole in the short term… five years from now…I think that we are moving toward isolationism in a big way.

Q: We're moving toward isolationism and I agree with you in the context of Internet-2 and vBNS, and things like that. What about the growing reliance on wireless, though? I think that is really going to explode. We're going to see every car with a GPS system, probably in the next few years. We're going to see Internet-aware appliances, particularly those that regulate when your heat is turned on. Most of those are going to be wireless, and wireless is inherently less secure, is it not?

Q: Wireless is inherently very insecure. In fact for most wireless networks that are in place now, as long as you are in proximity, and you have a wireless device, you can actually join that network, even though you may not have access to any of the points that are currently contained in that, but you can gain access to some extent. The hacker could potentially inflict some damage on your network. There are some encryption mechanisms associated with wireless, but there are no standards associated with that, so that the wireless platforms that need to communicate in an encrypted fashion can't really do that. PCs, PDAs, they have their own different way of doing it. I think some standards are on the way, but it's going to be two or three years before the industry really gets there. Wireless is going to be a challenge. I think that will put us closer to that VPN solution that I talked about earlier, because with the wireless networks, you want to contain the traffic, and the technologies that that will be involved in the next two years to support that will move more and more toward VPN technology.

Q: So do you think we're going to get a handle on wireless or do you think we're going to evolve into two societies? We're going to see the Internet-2 users doing the research, and the commercials joining in that, and they're going to be segmented and protected while the rest of the world will be lawless and open?

A: We're pretty much there now. We have commodities. Any wireless product is just going to be a commodity. They will shrink in size. You're going to have three or four of those commodities on your person and have everyday uses for them. However, if you really want to get to the core of research, I think the larger more intimidating computers will always be around. When I say larger, they may shrink in size, but not to the size of PDA. I just don't think they have enough power to facilitate research in that fashion. So the hard wire will be there and the computer will always be there, but the disposables, PDAs, personal computing devices will definitely explode in use.

Q: And they're going to be pretty insecure?

A: In the short term, but two or three years out they should be more secure.

Q: Blaine Burnham[Director (1998-2000) Georgia Tech Information Security Center] talked about the possible use of somebody's refrigerator for a denial of service attack, if the refrigerator is now an Internet-aware device that's communicating expiration dates to your local grocery store.

A: You'll find some users out there, and I use users in a very loosely defined way, actually developers, who have put their homes up on the 'net. You can view inside their homes, turn on lights, view fish tanks, do wide variety of activities in their home, and you're contributing to their research as you access their homes, refocusing cameras and all these type of things. Personally, I don't think I would expose my personal life on the Internet, but there are some individuals out there who are really on the cutting edge, they have wireless devices hemmed inside their clothes…We were in California on a vendor trip, and we talked to one of the developers at Sun Microsystems. When I say a developer for Sun Microsystems, it actually means a freelance type person there, they pay him an enormous salary. He came in, had on a jacket, it was pretty chilly that day, he had an LED display and he was able to access all the electronic devices within the room. He had his presentation on his computer, and he also had another computer in another facility there, and he accessed all the devices in his home and they were visible, we were able to see that, even ping his cats, if necessary. We have individuals who are really out there in the forefront being innovators. I think anything is possible and the really good thing about PDAs these days, we are moving more and more toward technology that is disposable, which is a great thing, which reduces the cost, the speed is getting close to light speed. Imagination and the technology will be there, so I don't think there's any limits to technology in the future.