A Publication of the Georgia Tech Alumni Association

Georgia Tech Alumni Magazine Online

alumni magazine home
photo gallery
archived issues
feedback
search

Tech Notes
Interview
Pacesetters
In Focus
Faculty Profile
Photo Finish

Interview: John Copeland

Communications technology sometimes develops in curious ways, says John A. Copeland, who notes with amusement that television moved from a wireless to a wired — i.e. cable — environment, "while computer networks and Internet access are moving in the opposite direction, from wired to wireless."

The John H. Weitnauer Jr. technology transfer chair at Georgia Tech's School of Electrical and Computer Engineering and a Georgia Research Alliance eminent scholar, Copeland's research embraces the area of wireless computer networks, particularly their associated security issues. Much of his work is done through the Georgia Tech Information Security Center.

Copeland is director of Tech's Communications Systems Center, which performs research on high-speed optical fiber networks using asynchronous transfer mode switches to carry Internet protocol data, video conferencing and other high-bandwidth applications. He also serves on the Governor's Information Technology Policy

More Stories

High-Tech Triumph

The Best in the World

Winning Bid

Council, charged with planning Georgia's next digital communications network.

Copeland earned his undergraduate, master's and PhD degrees in physics from Georgia Tech in 1962, 1963 and 1965, respectively. He joined the campus faculty in 1993 with his appointment to the Weitnauer chair and began a three-year term as director of the Georgia Center for Advanced Telecommunications Technology.

The growth of wireless devices has been remarkable over the past few years. Where do you see the technology heading?
People like anything that increases their mobility and that's the advantage wireless provides. With the way the technology is developing, it has become very inexpensive to add wireless capability to something that in the past was wired. We're already seeing a rapid convergence of home computer networks to wireless, just as many people are using cell phones instead of land lines. Wireless isn't going to replace wire completely. Cable and telephone companies offer very high, fixed bandwidth to homes and offices through optical fiber and that trend is going to continue.

One sees the term "Wi-Fi" in connection with wireless. Are they the same thing?
Wi-Fi just means the protocols that were used on the initial wireless computer networks. Wi-Fi had an encryption algorithm called wired equivalency privacy, which wasn't very good, and hackers immediately started distributing programs to break it. Newer protocols have replaced the Wi-Fi protocols. One of those technologies is called WiMax. It is for long-distance, point-to-point communications. Some cell phone companies are using it because they can cover a much wider area. For instance, you might be a mile or a mile and a half away from the base station and still get a high bit-rate connection though WiMax.

Is wireless inherently less secure?
I don't think you want to depend on the things that come with your wireless router and wireless card to

protect your data. You want to run higher-level programs that encrypt the data and keep it private. But if you don't set the rather weak security features that wireless has, and you're not encrypting your data, then you are broadcasting it for anybody who wants to listen to it.

Why don't some people at least enable the security features that come with the hardware?
They're just too difficult to set up. Security devices, like what you'd find with a wireless local area network card for instance, aren't on by default because they have to be configured based on a number of conditions that vary from person to person and machine to machine. If the configuration isn't done properly, the card won't work. The whole process might take an hour or two going through the manual and a call to customer support to get all the settings right. Computers should serve people, not vice versa —that's something of a mantra at the Georgia Tech Information Security Center. Not only do we develop secure algorithms and encryption techniques to protect data, but we want to find ways of making those measures transparent to the user.

What are some of the concerns related to wireless access to corporate networks?
The new danger to the corporate network is that somebody can hook into the network behind the firewall, which is between the internal network and the outside world, to prevent packets coming through that might be used to set up a connection with your industrial servers. Even without wireless, someone inside the company, inside the building, can use the local area network to access those servers that are not blocked out by the firewall. Somebody down in a closet somewhere could tap into your ethernet line just like they'd tap into a phone line and they could read all your data there. But if somebody buys a wireless access point and plugs it into the wall, he can go to an empty room and use his laptop to connect to the network.

The Georgia Tech wireless network is set up so that when you log on, the only way your packets can get off is to go through a firewall. That keeps people from doing bad things from within Georgia Tech. One of the things my research group in the Information Security Center is doing is monitoring network traffic in certain ways to see if we can tell when an unauthorized wireless hub has been installed on it.

What are some of your other research areas?
Generally we work in the areas of networks and network security. Some of our projects are specific to wireless, like the location of rogue access points I just mentioned. Another project involves fingerprinting wireless computers, that is, being able to tell remotely what type of wireless card someone is using. This would be helpful when an intruder uses a wireless link to break into a network. We're looking at other methods of fingerprinting as well — other attributes that could help identify a specific computer. We're also interested in ways to enable wireless network users to move from one kind of network to another without opening up security gaps.

Securing your computer is another important way of avoiding unauthorized network access.
It is. And that's why people are exploring so many different approaches such as biological identification — automatic fingerprint identification and retinal pattern identification. One of the most secure techniques so far involves a little fob that has a six- or eight-digit password that changes every second. When you want to log on to the computer, you look at the fob and type in whatever number is there. The computer has a similar, synchronized clock that's encrypting the digital representation of time the way the fob is. If the numbers match, or come within a second or two of matching, you can log on. Even if someone is watching you on the keyboard, they can type the same number a few seconds later and it won't work.

Staying ahead of the bad guys is a never-ending challenge, isn't it?
Whether you're using wireless or wired connections, I think you have to assume that somebody somewhere is listening — unless you use the right security protocols to protect your communications.