### Inside this issue:

<table>
<thead>
<tr>
<th>The Rise of Snoopware</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justice Department’s Proposal threatens Your Privacy</td>
<td>4</td>
</tr>
<tr>
<td>Privacy Groups, Microsoft, NSA</td>
<td>6</td>
</tr>
<tr>
<td>Editorial – “Trust”</td>
<td>6</td>
</tr>
<tr>
<td>how important is it to the Enterprise?</td>
<td></td>
</tr>
<tr>
<td>A Message from Our Faculty Advisor</td>
<td>8</td>
</tr>
<tr>
<td>SSG News &amp; Events</td>
<td>9</td>
</tr>
</tbody>
</table>

---

## Net Phone Rings At NetWorld

*By Loring Wirbel, EE Times*

**THE COMMUNICATIONS INDUSTRY** heard the call of the Internet telephone at NetWorld+Interop, in Atlanta, as Cisco Systems set the tone by rolling out a converged systems architecture powering 35 new product lines that support voice-over-IP services.

Companies at the chip, board and systems levels scrambled to respond to Cisco's gambit, which put packetized voice at the core of everything from back-end servers to a line of Internet Protocol (IP) telephones.

The arrival of Net phones from both Cisco and Lucent Technologies may assure users that packet-based telephony is ready for prime time. But at least one significant technical issue remains to be resolved: How will packet data-based gateways link up with circuit-switched Private Branch Exchange (PBX) systems?

Packet and circuit networks have not yet converged at this key interchange. Some players advocate optimized packet networks for IP that would leverage the Megaco gateway protocol and Sigtran signaling protocol developed by the Internet Engineering Task Force (IETF). Others want to leverage the extensive middleware for Signaling System 7 (SS7), a circuit-oriented stack that already is capable of handling many of the features for IP traffic.

Some companies at N+I voted with their feet. Embedded computer specialist RadiSys, in Hillsboro, Ore., showed the first implementation of voice gateway functions using the pre-standard Megaco protocol stack, the IETF’s enhanced version of the earlier Media Gateway Control Protocol (MGCP).

DSP chip set specialist Audio Codes, in Yehud, Israel, offered early firmware-level support for MGCP, demonstrating the interoperability of call agents over IP using its own chip set and Clarent’s call-agent software.

Clarent itself tested MGCP software at the show with Tut Systems Pleasant Hill, Calif., a manufacturer of DSL access units for apartment buildings. Greg Ioffe, senior director of market management at Tut, said the company would likely add voice Digital Signal Processor (DSP) hardware to its DSL units in the future so one unit could be a voice gateway for an apartment complex.

On the SS7 side, Harris & Jeffries announced its intention to move into signaling stacks for the circuit-oriented protocol, augmenting its work in protocol stacks for ATM and multiprotocol label switching. And SBE, while showing off a combined router, firewall, and packet monitor for enterprise customers at N+I, also quietly shopped around a PCI board that offers full SS7 support in a multichannel environment. The board taps T.Square’s network processor and is slated to debut at the Embedded Systems Conference.

Underlying signaling stacks can make a big difference in the development plans for chip ven-

---

*Where is the wisdom we have lost in knowledge? Where is the knowledge we have lost in information.*

~ T. S. Eliot ~
dors, real-time Operating Systems developers, middleware companies, and OEMs alike. Virtually all models of future networking architectures now assume the bulk of voice traffic will be carried in the packet networks, which have moved from being the data-overlay nets of the past to the predominant transport networks of today. In such models, the semiconductor switches at the heart of both circuit and packet networks are soft-programmable, capable of being retargeted on the fly for different mixes of services.

Use of Megaco and MGCP can ease development tasks and yield hybrid packet and circuit switches that look more like the packet switches familiar to the data community. But if SS7 functions such as the service control point and service switching point are retained, a richer feature set, developed for the circuit-based Advanced Intelligent Network (AIN), can be leveraged for packet services.

**Strategic Edge**

Deepak Shahane, president of Harris & Jeffries, in Dedham, Mass., said his company elected to develop SS7 code as a strategic edge against such public network specialists as Trillium Digital Systems and Ulticom. Megaco protocols are important as a rapid-gateway approach for IP systems, Shahane said. But H&J, rather than develop its own native SS7, will partner with Hughes Software Systems to offer Megaco protocol stacks.

Dean Hamilton, chief executive of CoSine Communications, in Redwood City, Calif., heads a company with an IP-centric service-switching hardware platform, but even he said he believes many of his packet-switching brethren may be too quick to dismiss the power of SS7. Hamilton said IP-oriented developers frequently seek to shoehorn circuit services into a world optimized for packets, without taking into account the years of research that went into SS7.

"A lot of data efforts in voice are based on a poor understanding of voice characteristics. If developers were smart, they'd leverage on top of the SCP framework already developed for the AIN functions in SS7," Hamilton said. "AIN is not going away. We need to move to a more seamless interface with existing AIN circuit standards, or the voice-signaling end products for IP could end up being little more than toys."

But whether toys or industrial-strength applications, there was no end to new ideas arriving at the N+I show for efficient transport of low-latency voice.

Cisco Systems' five-phased strategy to integrate packetized voice into data networks made a leap into the enterprise Monday, when the company introduced a variety of switches, small routers, and call gateways under its Avvid initiative. Using VoIP technology from earlier WAN efforts, as well as client phones acquired from Selsius, Cisco fielded its first voice-integration products applicable to enterprise customers.

Mario Mazzola, senior vice president of the enterprise line of business at Cisco, said the company now has more than 1,000 developers in various divisions working on voice processing. The enterprise work leverages earlier "jukebox DSP" concepts for voice packetization as well as advances in the Internetworking OS for call-processing services, dubbed Symphony. This is the first time, however, that the technology has been ported to such enterprise switches as the Catalyst 2900, 4000, 5000, 6000, and 8500 series.

Jayshree Ullal, vice president of marketing in the enterprise group, said there was more to the Avvid (architecture for voice, video and integrated data) effort than the 35 new product lines with voice-packetization capabilities. Cisco also has launched a dedicated mission-critical call server platform, the Media Convergence Server 7830, that's intended as a high-availability Pentium III-based platform for call-manager software. Multiple server platforms can be linked via H.323 interfaces.

Enterprise voice product manager Dave Buster said the work doesn't end with H.323 gateway functions. "We have been working on the different functionality available under H.323, MGCP, and Megaco definitions of a gateway, and we'll have full call agent software available for all environments," he said.

**Program Completed**

Avvid essentially completes the five-phase program for voice integration that Cisco announced two years ago, although the Phase V policy-management functions still require some fleshing out in software capabilities for quality-of-service features. Having brought Selsius IP phones into the enterprise product suite, Cisco said it plans to offer a PC-based SoftPhone function as client software by year's end.
Cisco launched Avvid with kick-off parties at the World of Coca Cola Museum and a Webcast by CEO John Chambers. The high visibility sparked complaints from vendors such as Lucent, which claims already to have in place most of the pieces that Cisco touted this past week.

Doug Ruby, chief technology officer of Lucent's enterprise internetworks systems unit, pointed to such products as its IP Phone and IP ExchangeComm. "Everything Cisco touts as revolutionary, was things we announced six months ago," he said. "Unlike Cisco, we're not forcing our customers to do swap outs and upgrades to add voice to enterprise networks."

Start-ups took more radical steps. Lara Technology in San Jose, Calif., known for its SuperCAM content-addressable memories, turned full-bore into systems sales this week with the rollout of the Unified Services Exchange 1000. The VoIP service switch uses an advanced MediaExpress ASIC design based on large look-up tables to achieve claimed circuit-to-packet conversion latencies of less than a millisecond.

Ajit Medhekar, president and CEO of Lara, said the company's switch would not rely merely on Megaco. The MediaExpress architecture used in Lara's switch can use Q.2931 signaling, ISUP or SIP+ protocols from the ISDN environment and such IP-native QoS methods as DiffServ and MPLS. The architecture sets up multiple real-time protocol channels, called the RTP Multiplexer, to establish the lowest possible latency for packetized voice traffic.

Merlot Communications, in Bethel, Conn., meanwhile, used a deterministic Ethernet method in its Magnum enterprise architectures to aim at higher voice-stream speeds than traditional packetization methods. Lara's architecture bears some similarity to Merlot's in that the RTP multiplexed channels of the USX1000 rely on Ethernet, not ATM or TDM, as a transport backbone.

IPCell Technologies, in Richardson, Texas, a new company formed by NEC and DSC Communications executives, demonstrated an ATM switch based on Sun embedded servers. The offering aims at direct Megaco interfaces to the InstantOffice platform from Vertical Networks, but it also targets a mix of SS7 and ISDN call control on the circuit side, with H.323, SIP and MGCP/Megaco control on the packet side.

Early customer interest in packetized desk-set phones has bordered on the fanatical, causing Cisco to warn users that some call-feature applications are still in the beta phase. The key to bringing in legacy circuit services and coexisting with PBXs, executives said, is to give customers a choice in where the call-processing function is carried out. Cisco will sell voice-enabled routers, voice-enabled switches, traditional digital gateways and the MCS-7830 server, with circuit-call aggregation and packetization capable of being performed at any point in the network.

Martin deBeer, director of multiservice solutions, said the ability to choose codecs for scaled voice quality should convince customers to replace circuit PBXs. A PBX is limited to carrying voice over 64-kbit channels with a G.711 codec, he said, while a packet phone can range over codecs that support rates from 6.3 to 256 kbits per second.

The point in the breadth of Avvid hardware, Ullal said, is to make sure "the packetized infrastructure absorbs the existing traffic over time."

---

**The Rise Of Snoopware**

By Fred Langa

**Snoopware**—software that monitors user actions on a PC or LAN—is everywhere. There's application-metering software that tracks who's using what application on a LAN. There's nannyware: Web-use monitoring software that can block employee access to specified "forbidden" sites, chat rooms, and such. There are proxy-level URL and IP loggers that track (and can enable or block) access to any online resource. There are E-mail monitors that track and parse messages, looking for "bad" words that might indicate that corporate E-mail is being used for sexual purposes or to disclose confidential company information. And then there are keystroke loggers that can track user activity down to each individual keystroke.

All this software has some legitimate purposes. For example, application-metering software can help a company buy only the number of licenses it really needs (usually less than the number of seats). It can inform a help desk about which applications they
The Rise Of Snoopware – Continued...

should concentrate on. It can help an IT department know which centralized applications need the most bandwidth, and which ones can be placed on slower servers, or stored offline or near-line.

There are similar legitimate uses for the other classes of snoopware, too, even down to keystroke loggers: For instance, they can help a company determine exactly how much time is really being spent on various tasks, projects, or assignments.

But the downsides are enormous. Things like nannyware and keystroke loggers prejudge employees and assume the worst about them. When you install this kind of software, you are sending the message: "We don't trust you to behave. We will monitor your every move, and--like Big Brother--we can catch you if you do something naughty. Be on guard and stay on task, not because it's the right thing to do, but because you'll be caught and punished if you don't."

This approach treats all employees as bad apples, and prejudicially lumps everyone together in the category of "untrustworthy." It strips away individuality and treats employees as children who can't or won't distinguish between right and wrong.

Applications like nannyware and keystroke loggers often are used as a substitute for good management practices. The need for this kind of intrusive, Big Brotherish monitoring could be avoided with a few preemptive steps: If you hire good employees, keep them informed and clear about their goals and missions, and cultivate in them a sense of personal responsibility and trustworthiness. They'll usually respond well. No, not all employees will respond in the way you want --there are always some who are lazy, some who abuse what trust is given them, and some who lack self-discipline. These are the personal failings of the individual employees, and management should deal with them as such rather than prejudging all employees as untrustworthy and in need of constant monitoring.

If I'm interviewing a prospective employee and get a bad feeling that maybe this person can't be trusted, I just won't hire them. On the other side of the desk, if I were in a company that indicated (by installing this kind of software) that it didn't trust me as an employee, I'd start polishing my resumé.

Snoopware's damage to trust and morale is bad enough, but this type of software has other failings, not the least of which is imprecision. If I'm running, say, a word processor and working on a document related to Project A, but I'm called away to a meeting on Project B and don't close my document, the keystroke logger will think I've been working on Project A that whole time.

Or, imagine you're counseling a valued subordinate who's depressed and obsessing about a failed project. The failure is painful, but not the sort of actionable issue you want put in the subordinate's personnel file; you do not want to officially involve the HR department. You write in E-mail: "I know you're sorry. The thing to do is to learn from the errors and move on. Spending your time in mea-culpa breast-beating won't do any good." Do you want a sexual-harassment E-mail filter to intercept your message and send it to the company's HR department anyway because it contains the oh-so-terrible word "breast?"

The era of downsizing has produced many departments where too few managers are trying to supervise too many employees. Snoopware is an attempt to solve the problem with technology. But I think it's a mistake, and one that can backfire. If you can't trust your employees, then you have a larger issue than can be solved by logging their keystrokes. Likewise, if your company doesn't trust you and wants to monitor your every move in the office, what does that say about the company? What does it say about you, to accept that level of distrust?

I can see some legitimate uses for snoopware. But not many. And snoopware's limitations, to me, far outweigh the benefits. As both an employer and as an employee, when it comes to snoopware, I just say no.

Justice Department's Proposal Threatens Your Privacy

InternetWeek
Wayne Rash

The U.S. Department of Justice couches its proposal as something minimal, something that will just clear up a few details. But it may hold more danger for your company than anything that's been proposed for years.

The deceptively named Cyberspace Electronic Security Act would, if passed by Congress, give government agents unprece-
tended power to obtain warrants, break into your computer systems (including your premises if they so desire), alter your soft-
ware and install new software. Worse, they could do all of this in secret. You'd never know until something failed or your con-
didential business information turned up in the hands of others.

The Cyberspace Electronic Security Act is an effort by the Clinton administration to deal with its fear of encryption. The admi-
istration has already tried and failed to require that public encryption keys be filed with the government. It's tried and failed to
mandate other types of "back doors" into computer systems and communications equipment. And it's tried and failed to outlaw
encryption completely. So far, the only result has been to hamstring U.S. software companies trying to compete with companies
abroad.

Now, however, the administration's efforts are taking a sinister turn. The Justice Department is talking about secret warrants,
covert operations, tampering with secure systems and break-ins reminiscent of Watergate.

It would work like this: The Justice Department (or another agency) decides that it wants to investigate a possible crime being
conducted with the use of a computer. That agency will go to a judge for a warrant to search any computer or network device the
suspect may be using in the commission of this alleged crime. The warrant will be sealed, which means that the details of the
search--and the very existence of the warrant--are a secret.

Armed with that warrant, the police or another investigative agency could break into the home or office used by the suspected
bad guy and search his computer or network server for records of nefarious activity. The operatives could also install software
that would defeat any effort at encryption, but in a way that would be transparent to the computer user. Your security software
would appear to work but wouldn't actually do anything. The investigative agency would then siphon off whatever it wants with-
out the need to crack any encryption.

If the target computer happened to be your enterprise server farm, the government could break into that as well, and if your nor-
mal corporate encryption standards got in the way, the agency doing the investigation would break that, too. Material you
thought was being encrypted wouldn't be. Your security would be compromised, and you'd be prevented from doing anything
about it.

That means if you're running a bank or a brokerage, your financial records would be open for all to see. Your customers wouldn't
get the privacy they're paying for.

It could get even worse. Suppose the government operatives don't know what they're doing and end up scrambling the data your
encryption software is supposed to protect? Suppose they bring down your computer system completely? Of course, the Justice
Department will say that such things will never happen, but do they understand your computer installation well enough to know?

For its part, the Justice Department says it's unable to gather evidence of criminal wrongdoing if people and companies are al-
lowed to encrypt their information. Brushing aside the alarm of civil libertarians and business groups, the Justice Department
says it's planning to go ahead with its request for new legislation.

If passed, the black bag jobs we read about in paperback spy novels will become a routine means of investigation in much the
same way that the Soviet Union's KGB routinely broke into homes and businesses to flush out enemies of the state.

At this point, there's little likelihood that the initial version of the Justice Department bill will pass. There's bipartisan opposition
in the House of Representatives, for one thing, and chairs of the responsible committees have promised that this Clinton admini-
stration initiative will never see the light of day.

You can be sure, though, that the administration will keep trying to fix its incoherent policy by compromising your rights and
your business.
Microsoft moved swiftly on Friday to deny allegations that it included an NSA (U.S. National Security Agency) back door into the Windows operating system.

"The report is inaccurate and unfounded. The key in question is a Microsoft key. It is maintained and safeguarded by Microsoft, and we have not shared this key with the NSA or any other party," the company said in a statement.

The key, which works with the Microsoft Cryptographic API (MS-CAPI) is labelled as "NSA key".

Andrew Fernandes, chief scientist with Cryptonym of Morrisville, North Carolina, was quoted last week as saying the inclusion of the key made it easier for the NSA to compromise a Windows user's security, without their knowledge.

"Microsoft takes security very seriously. This speculation is ironic since Microsoft has consistently opposed the various key escrow proposals suggested by the government because we don't believe they are good for consumers, the industry or national security," said Microsoft.

Microsoft added the key had not, and would not be made available to any third party.

The software company said the key was labeled NSA because the NSA acted as the review body for the restricted export of encryption technology from the U.S., and that key was designed to be compliant with U.S. export laws. Microsoft said the NSA-labeled key was simply a "back-up" for the one used by Microsoft to allow it to update cryptography components (labeled "KEY").

But director of the London-based Foundation for Information Policy Research (FIPR), Caspar Bowden said: "Building in a 'back up' key makes no sense unless there is a revocation method for the primary (key). There is no revocation method."

Microsoft said the back-up key was there should the original ever be lost due to a natural disaster. The company also acknowledged the name of the key was "unfortunate".

"I don't believe them -- what kind of natural disaster are they talking about? A meteor destroying all the earth's structures?" said Privacy International director general, Simon Davies. "Microsoft's argument is inconsistent with its operating procedure -- it could hold a single key in multiple locations, that is a standard security procedure." He added that to compromise user security, "it's not necessary to share access with the NSA -- simply complying with their requirements will do that."

"It goes right to the heart of the deal between (software companies) and global operators. Ultimately we need to be more open about how these systems are developed. Microsoft should have taken this opportunity to talk to us about the requirements of the U.S. government," said Davies.

**Editorial – “Trust” how important is it to the Enterprise**

(09/16/99; 05:00 p.m. PT)

OPINION

By Marty Cortinas, TechWeb contributor

Just when you think Apple is humming along and can do no wrong, somehow the company everyone loves to love -- and hate -- finds a way to throw a monkey wrench in the works.

Is it your "given" right as a computer user to be able to upgrade your existing system? Tell us in threads.

Mere days after Apple rolled out the shiny new G4 desktop models at the Seybold publishing show in San Francisco, G3 owners across the land were up in arms.
Back in May, Apple released the Power Macintosh G3 Firmware Update 1.1. According to the documentation that accompanied it, the update was designed to improve the PCI performance on all blue-and-white G3 desktop machines. By most accounts, the update does exactly that, and if that's all it did, everyone would be happy and still madly in love with Apple. But recently, users discovered it does more, and that's what's got everyone hopping mad.

The update also effectively blocks a G3 Mac from running on a G4 processor -- something it could do before the update. So if you had a G4 upgrade card (theoretical, for now) running in your old G3, then ran the firmware update, you would have a dead Mac on your hands. There are several reasons for users to be peeved about this, but I think only one is truly legitimate.

Many are mad because they are stuck with a machine that cannot be upgraded. In one of the few statements coming out of Apple over this brouhaha, officials have been very careful to point out that no upgrade path was promised for the blue-and-white G3s. You can trace the roots of this policy back to the Performa upgrade fiasco, in which Apple lost a class-action suit.

It's become an expectation in the computer industry that when you buy a machine, you will be able to upgrade it. But that's all it is -- an expectation. Sure, it's close to de rigueur, but an upgrade path is not the computer consumer's equivalent of manifest destiny.

Is there a technical reason why the blue-and-white G3 machines can't run the G4? At first blush, it seems that the answer is no, since the low-end G4 Apple is selling uses the same motherboard as the G3 boxes. But it's possible that Apple had to jump through all sorts of tricky technical hoops to make that work. Unfortunately, we don't know. Apple isn't talking. Ah, now there's the problem. You can carp all you want about not being able to upgrade your machine, and not many people aside from those in the same boat are going to lend a sympathetic ear. But let's say a company gives you a piece of software that improves performance while at the same time removes a capability of your machine -- without telling you? Now you have the real seeds of good group gripe.

"The issue here is trust. Apple didn't tell us the firmware update blocked upgrades."

The issue here is trust. Apple didn't tell us the firmware update blocked upgrades -- but was more than happy to tell us PCI performance would be enhanced. Maybe there is a damn good reason why G3 machines should be blocked from running G4 processors, but we don't know because Apple won't tell us.

This is a big problem for Apple and its customers. Like it or not, if you want to work on a Mac, you have to deal with Apple. You don't have a choice. For this relationship to work, you must place your trust in Apple. The way I see it, this firmware bait-and-switch and Apple's silence is making the company something less than trustworthy.
WHY SSG (or any other student organization)?

Some Thoughts from An Advisor
by Dr. Stephen Lunce, C.C.P.

During a student’s life at the university there will be many opportunities that may not be offered at any other time or place. Friendships pass, jobs change, careers evolve, but there are some very special things about the university and the campus life. It is obvious that for most students, your academic career will be dominated by your program of study and your course work; but during those classes you will associate with more well educated people than perhaps at any time in your life. The intellectual challenge is pervasive; however, there are some other facets to your time at the university. This essay will briefly address one facet: student activities.

All students are expected to attend classes, pass examinations, write papers, and make presentations. As an undergraduate student, you will develop the skills to become a life-long learner, and you will learn the basics of your major field of study. The graduate student will master the knowledge components of field, and will learn how to do research in order to continue to explore the field of interest. The challenges of earning a university degree are significant, and you will be deservedly proud of your accomplishments upon completion of your program. However, there is more to an education than just attending class and completing assignments.

Four almost six centuries the university has been a community of scholars. A place where students come together to learn from the faculty and from one another. One of the major ways that students learn from one another is to find groups of students who have similar interests. Those interests could be athletic, academic, intellectual or simply enjoyment. Student organizations exist to facilitate the interaction of students with one another, and many exist to provide some educational and service activities, as well.

Even on a small campus, in a relatively new university, there are many student organizations to choose to join. How does a student make a choice? Ask yourself, “what am I looking for? What do I expect from the organization? What will the organization expect from me?” Let’s look at each of these questions. Are you looking for a social group, or a collection of inquiring scholars, or a congregation of aspiring athletes? Or are you simply looking for new friends? Most groups will tell you, usually in their name, what they are about. For example, the Student Systems Group (SSG) is an aggregation that is interested in the development, implementation, deployment and management of all types of systems, but concentrating on computer based information systems.

Will the organization provide more than just companionship? Most do, but will the organization provide insights and impetus into a chosen career? Will being a student member of the group provide post-graduation benefits. In the field of information systems (and remember that we are currently living in “the information age”), the premier professional organization is the Association of Information Technology Professionals (AITP). Student members of are entitled to membership in AITP, and discounts on professional dues after graduation.

What does an organization expect of membership? Well, the members should participate in the activities, learn from the events, mature in the process, and have fun with people with similar interests. SSG provides students with professional training, leadership opportunities, and the chance to travel and compete with other information systems students from across the U.S. If nothing else, SSG provides a line on a resume that will allow a potential employee (you, the student) to discuss your interests and accomplishments with an interviewer.

Does participation in student activities enhance the collegiate experience? There is no doubt that it does. Are there organizations with more to offer than others? Probably. Will any specific organization provide an entry into a chosen profession? Well, SSG members are already AITP members, and through AITP the student can meet a potential employer at any time. Just ask the SSG members who traveled to the University of Texas @ Arlington and heard H. Ross Perot...
SSG – Mission
The Student Systems Group's (SSG) purpose is to act as a link between the academic and business world through an affiliation with a professional information resource management association.

Newsletter – Mission
To disseminate information on current events and issues concerning the Information Technology field.

SSG attending Competition in Oklahoma!

Our next student conference will be held on Oct. 8 & 9, 1999 in Lawton, Oklahoma. It will be hosted by Cameron University Student Chapter & Oklahoma City Professional Chapter. The hosting motel will be the Howard Johnson's Hotel & Convention Center.

Student Programming Competitions to include:
- Visual Basic 6.0
- Linux Based C++

The exact version of COBOL and C++ will be identified at a later date.
Practices for these competitions are being held every Mon. & Wed. at TAMIU in the C-labs room 113, from 3pm - 4pm. Prof. Carmona will be holding the practice sessions. Come and join the practice sessions to prepare for Oklahoma!