

## ALERT

THE NEWSLETTER FOR INFORMATION PROTECTION PROFESSIONALS

Number 216  
March 2001COMPUTER  
SECURITY  
INSTITUTE  
600 HARRISON STREET  
SAN FRANCISCO  
CALIFORNIA 94107  
TEL: (415) 947-6320INSIDE  
INFORMATION**In Print**  
Tangled Web snares  
rave reviews

8

**In Case you Missed It**  
Horror stories from  
the dark side of cyber  
space

9

**Calendar of Events**  
New - Hands-on class  
in forensics

11

**Bonus Item**  
Dangers of aggregated  
data

13

**Job Listings**  
Career opportunities

14

**Has network security lost its way?  
Mapping and visualizing will help****Richard Power interviews Bill Cheswick of Lumeta**

*I have attended a lot of information security conferences over the years. And I have spoken at a few of them. I have read a lot of information security publications. And I have generated my share as well. I have listened to those who information security is primarily a people-problem, I have listened to those who say information security is primarily a technical problem. There has always to my mind been a big gaping whole in most approaches to solving the problem or (perhaps more realistically) reducing its scope. Nobody really knows what they're talking about.*

*What is it that you are securing? Where does it begin? Where does it end? What is its structure? Remember the Sufi tale of the townspeople who went to visit the elephant in the dark. Each one came back with a different description of the elephant, because each one had only grasped hold of one part of its massive form. It is analogous to much information security "architecture" and much information security "assessment." How much can you really know if you don't have the big picture? How far can you go if you don't know where you're going or even where you are?*

*I hope you enjoy the following interview with Bill Cheswick, Chief Scientist of Lumeta ( [www.lumeta.com](http://www.lumeta.com) ). Cheswick has worked on operating system security for nearly 30 years. In 1987, he joined Bell Labs (now Lucent Technologies) as a member of the technical staff. There he worked on firewalls, network security, PC viruses, mailers and interactive science exhibits. He co-authored the first full book on Internet security, Firewalls and Internet Security with Steve Bellovin in 1994. (Cheswick's personal Web site has some excellent papers and presentations for your perusal.)*

*Lumeta Corp. is an infrastructure analysis company that has taken Bill Cheswick's technology to support a suite of network intelligence services for risk, change and asset management applications. The company, set to launch at the end of March 2001, already boasts a dozen "Blue Chip" clients including Microsoft. In addition to Lumeta Network Discovery and Perimeter Verification, the company also offers Lumeta Firewall Analysis through an application service provider model.*

*Richard Power, CSI: How did you get into mapping? What was your motivation?*

*Bill Cheswick, Lumeta: There were several motivations. When you're a semi-famous person in Internet security, you get invited to the Washington Marriott. You get invited to the Washington area quite often. You give lots of talks to rooms full of people who will not tell you their names or job titles. I've made a number of trips down there. In 1996, I went to something called the Highlands Forum, which was hosted by the Assistant Secretary of State. There were some fairly famous people there briefing the President's Infrastructure Protection Committee on what we should do about protecting the infrastructure. We played a Rand Corporation game called "The Day After." You pretend that it's ten years in the future and imagine bad things happening. A long list of*

*continued on page 2*

suspicious buzzword-compliant attacks have occurred. For example, a polymorphic computer virus appears in the New York Stock Exchange, a Trojan horse is executed in the Cincinnati power grid control computer. You get the idea. Our job was to sit around chatting for three hours and come up with recommendations for the future President. (Parenthetically, it's interesting to note that none of the attacks in the scenario were on the Internet itself. They were all through the Internet or through modems on various targets that we already know are important. I suspect that a much more devastating attack would be to just take down the whole Internet itself for a week. I actually have a talk I never give at public conferences, entitled "How to Take the Internet Down for a Week," and it contains five ideas for doing it. I usually don't give that talk. You really have to trust the crowd for that one, but I digress.) At the end of this whole scenario, you say, okay, it's back to 1996, what can we do to be prepared? One of the things I thought was, "Gosh, having a map of the Internet, especially if we're under attack, might be a good thing to have of variety of reasons." And I like maps anyway. About the same time, reports of the SYN packet denial of service attacks on Panix published.

*Power:* That was the first significant DoS attack?

*Cheswick:* That was the first one that everyone really noticed, yeah. I worked with the team of people trying to figure out how to solve the problem and came up with a technique for tracing anonymous packets. You do little denial service packs on the link, then prune the tree. It's sort of using a bad tool for a good purpose. Once again, hey, I needed a map. I needed a detailed, link-by-link map of the Net. I gave a paper at USENIX LISA in December 2000 on the work I've done with Hal Birch in this area.

"Gosh now," I thought, "maybe this is starting to tell me something."

The third motivation was the clear knowledge that intranets are out of control. If it's big enough to be called an intranet, it's out of control. The Bell Labs network had 1,330 hosts on it in 1988. It had grown without the corporate headquarters of AT&T knowing or caring what was going on, and of course now it is Lucent and AT&T and NCR and 200 other business customers, and who the heck had any idea who was connected to whom? Gosh, a map might be a way of finding out what's going on. That's how it all links together. So I said okay we're going to try some stuff. Let's see if we can make some tools that can map the Internet, which is a big place so the tools have to be light weight. Let's see if we can go map this place, and also let's start mapping Lucent and see where things go and figure out what's going on.

Of course, security people get called into consult all the time and we're constantly talking to CIOs. Over and over, I'm hear the same things that you've heard, "Where does our network begin and end? How far does it go?" It was clear to me that once again we don't know where this stuff goes. So Hal and I started this mapping in the summer of 1998, and we've been mapping the Internet on a daily basis since then. But it's hard to run a program everyday constantly with a couple of researchers hacking around. In October 2000, we spun this technology out from Bell Labs and I'm now in a little company called Lumeta. What we're doing is mapping corporate intranets and extracting information using the new techniques we have. If we can do the whole Internet, we can do your intranet pretty efficiently. We're doing this as a business, as a start-up.

*Power:* Such a tool would be invaluable during the assimilation or break-up of corporate networks during mergers, and acquisitions, wouldn't it?

*Cheswick:* Certainly—mergers and acquisitions one of our strong points. We've already scanned a number of customers including Lucent. They keep breaking up and reforming in front of us. It's a fine tool for seeing the pieces. We've watched, for example, Lucent split into Avaya and Agere. These two large groups are splitting off from Lucent and we have maps that show the pieces of each one. You can watch them disappearing as the mapping goes on. We're actually thinking about doing movies, though we're not quite sure how to sell them yet. But we have some in the lab here. You can watch the Lucent

intranet for six months and see this giant bump appear one day and disappear the next day. There's some great potential in visualization with this technology.

*Power:* Let's talk about the daily database and the issues that it brings up.

*Cheswick:* Well, we do the Internet daily, or we do about a tenth of the Internet daily. Of course, this means that a machine has to sit there and run for months on end so we try to run a stable operating system (3BSD). You've got to make sure that this space doesn't fill up and that it's robust in the face of network outages and errors and so on. We've had three years of system administration experience trying to make it robust. I do a full scan on the first of the month and about 10% of the Internet everyday. This limitation isn't so much for load as it is because our mapping (which is very lightweight) still annoys some people. So we don't want to bang on your firewall too much, I mean we're very careful. We tip-toe up to your firewall and if the packets disappear or if we get a firewall message we just go away. We don't want to bother people who are watching the network. We just want to map the "center" of the Internet.

*Power:* When you say "tip-toe up," what do you mean? How far are you going? Like going to somebody's front gate?

*Cheswick:* Well yeah. We get a list of all the networks on the Internet. We get that from various databases and many of them are behind firewalls. We go to about 150,000 nets. Essentially, what we do is a trace route to them. Now it isn't running trace route, we have our own software that does it, with great parallelism and gentility. But we go hop by hop, creeping along the network looking for responses. If something doesn't respond, we try to go one beyond it and re-sume. If we get two hops that don't respond, we say, "Right, never mind, we're out of here." It could be any network that's announced on the Internet, it could be somebody's Class C in their basement, but it's more likely to be a Class B network that ends at a firewall. For example, Exxon is probably a single point on our map. MIT might be a single point. We're doing the "center" of the Internet, for some definition of the "center." Obviously, we're not sending packets to every computer in the world.

*Power:* When your full scan the first of every month what change do you see from the month before?

*Cheswick:* Well, that's hard to say. Because the database is 100 megabytes long, it's all passed data, we have turned this over to researchers who have done various studies on branching factors and so on. And we hope others will do it, this database is online. You can go and grab it if you want. We do maps of it but I'll tell you it's so big and complex that's hard to tell the differences and also when I send out a packet from point A to point B, if I do it again two seconds later it may take a different path—simply for load balancing or routing flaps or that sort of thing. So our daily snapshot is I guess I'd say semi-accurate but if you go through a months worth we'll probably accumulate most of the different ways of reaching a particular point. And we have saved this, I have a line of CDs up here on my shelf and we have a pile of giant IBM disks which store these databases for three years now.

*Power:* But if you were to map a corporate intranet on a daily basis, you would be able to see change directly?

*Cheswick:* Yes. If nothing else you want two maps, you'll want one to see what it is, then you'll go fix it and then want to see that you've fixed it. We think people will want subscriptions to this and therefore we have differences maps that show since your last scan this came, this went away, here's what it looks like and here's a list of things that are going on.

*Power:* What are the limitations on the technology?

*Cheswick:* Well, there are several. No Internet tool is going to be completely precise. When we map from a particular area we get the outgoing routes for the packets. Incoming routes might be different. What we like to do for

a customer is map from several points and sort of blend the trees together. On the Internet mapping project itself, I have a variety of volunteers lined up and we're going to do mapping from perhaps dozens or hundreds of points around the Internet to try to get these opposite directions and sew them together into a more coherent description of what the center looks like.

*Power:* So it's like the earth is the center of the universe, it's subjective, it's perspective, it seems to be the center from where I am standing?

*Cheswick:* It is definitively one view of the Internet and we have ways of combining multiple views of the Internet into something that's a bit more objective?

*Power:* To say it's one view, or subjective, doesn't mean it's not real, it's what actually is but from one angle?

*Cheswick:* If UUNet is my local ISP then obviously the center of the map is going to have UUNet in it. But by the time the packets reached Sweden they're probably going through a fairly standard set and if I map them from San Diego, Sweden will probably look pretty much the same. So the idea is that if we can do this from a long way around the world all around the "edge" of the Internet, we can sort of collect all the Swedens together into a more objective view and collect the incoming routes as well as the outgoing routes.

*Power:* In your presentation at the CSI conference, you mentioned that "gentle mapping means missed end points"?

*Cheswick:* That is correct. We are more interested in mapping the past than hitting a final host. But when you run trace route, you have to pick a final destination and we do that sort of randomly. When we find a final host that we like we remember it and keep going to it. Someone watching their logs over a long period of time (and there are people who have) would notice that we're doing a slow random scan of their network. We've had a couple of people comment on that.

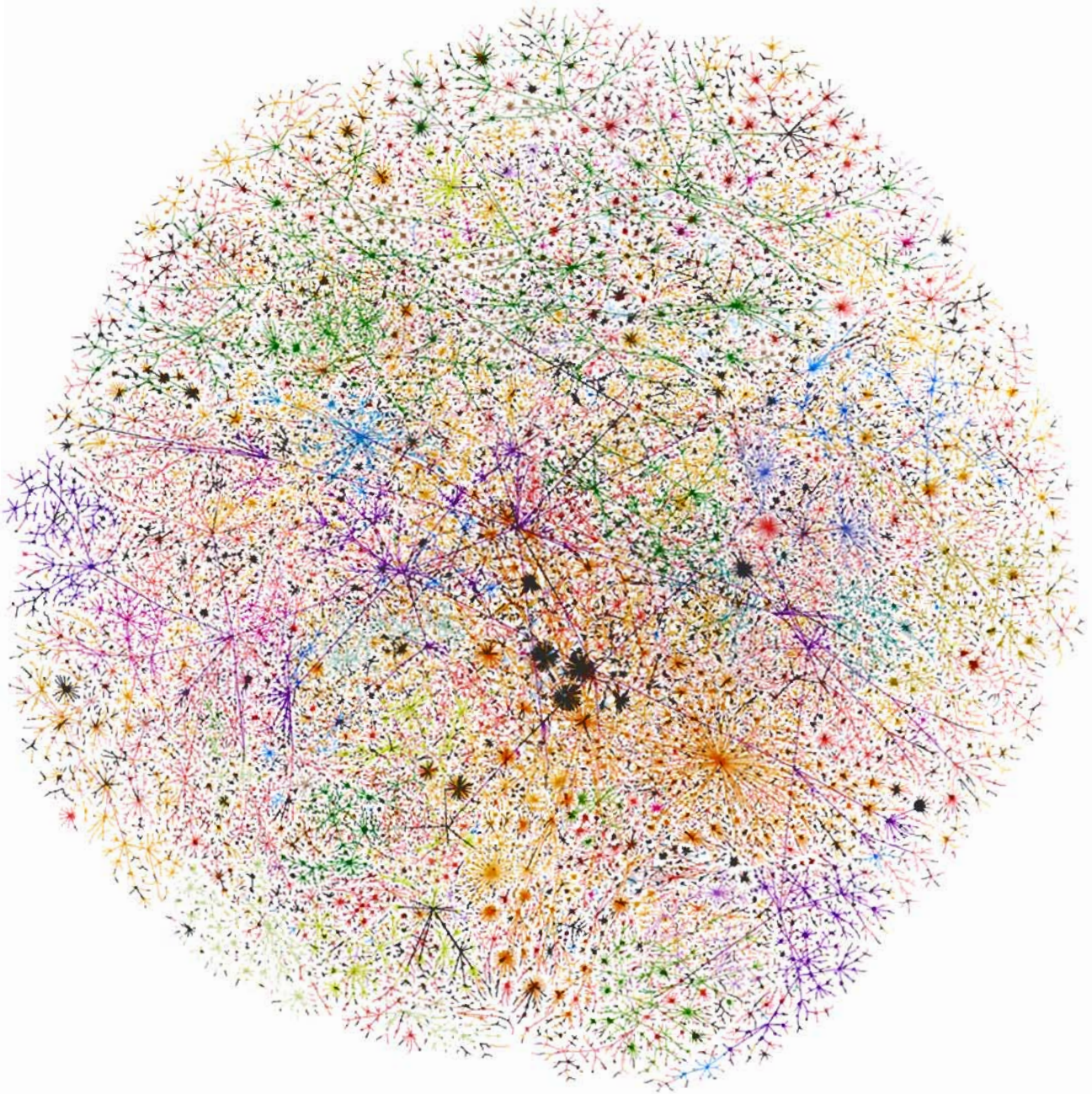
*Power:* Well, that leads into the complaints. Didn't the Australian Parliament protest?

*Cheswick:* Yes, we have had a few complaints.

The Australian Parliament complained the day we started this project. There have been a few others I think there are about 25 networks on our stop list that we don't scan anymore because people have complained. Now you may not think of the Australian Parliament as being a hotbed of technical activity, but it turned out that they had just been hacked, so they were especially sensitive.

I had to make a list of whiners who would not be scanned. Of course, there are probably other people out there who notice and just block our packets. It would be entertaining to try to scan from someplace else and see if we get through when we don't get through from the net

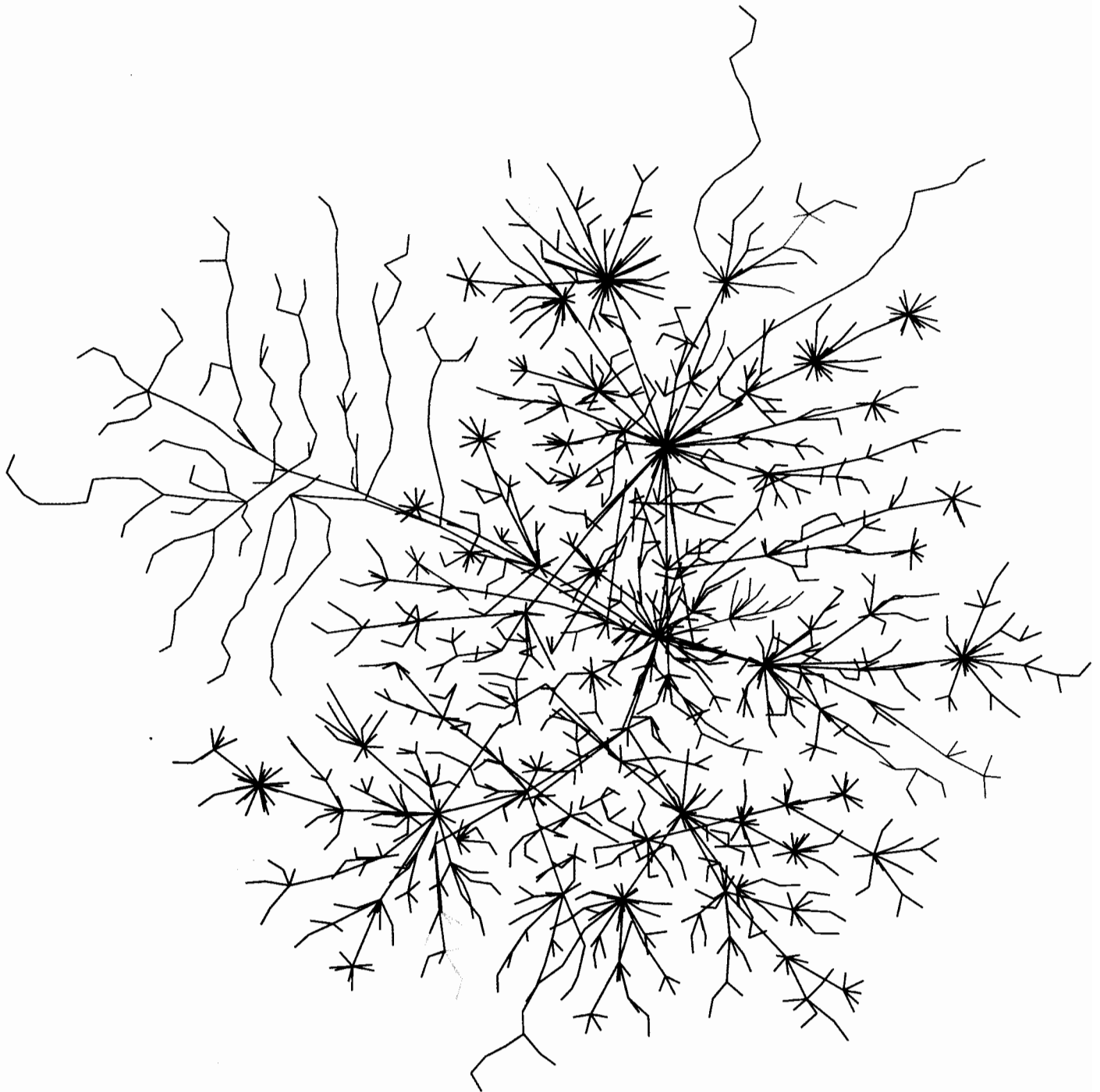
*continued on page 6*



Patent(s) pending & Copyright © Lumeta Corporation 2000. All rights reserved.

***A Lumeta map of ISPs in cyberspace***

*This map depicts the shortest outgoing routes from a test computer at Lumeta headquarters in New Jersey, to each of over 100,000 registered or announced nets on the Internet. End nodes may represent a handful of computers on a small network, or large companies with hundreds of thousands of hosts. Each intermediate node is a router.*



Patent(s) pending & Copyright © Lumeta Corporation 2000. All rights reserved.

***A Lumeta map of a corporate intranet***

*Lumeta Network Discovery provides a compelling representation of the composition of the enterprise network. Spurious networks and backdoors (colored in red) were unknown to the client and may indicate dangerous breaches to this enterprise network. (IP addresses and canonical names have been removed)*

*continued from page 3*

mapping machine, and we're going to do that.

As a matter of fact, if we're only getting the outgoing paths and we do this scanning from different places on the network we can actually fit together the middle and get most of it. We have technology to do that now and in fact I am looking for people who are looking to accept tunnel packets.

*Power: What they send you Email back, they call you up?*

*Cheswick:* They contact us all sorts of different ways. We point them to the Web page showing them what the Internet mapping project is doing. Almost all of them say, "Oh, that's okay, never mind." A few say, "Never the less, stop scanning me," and we cheerfully put them on the list.

*Power: We ask the following question in the CSI/FBI Computer Crime and Security survey every year: "Have you unauthorized use of your computer systems within the last 12 months?" I laugh because the choices are "yes," "no" and "don't know." The only truthful answers, I believe, are "yes" or "don't know." How many of the people you haven't heard from simply didn't notice your activity?*

*Cheswick:* Well, I suspect that almost nobody's noticed.

*Power: Of course, the .mil people noticed.*

*Cheswick:* The military noticed immediately. This fact surprises some people, but it turns out that DISA doesn't have to be good at detecting this sort of stuff because there are people downstream who instantly notice and complain to them. At DISA, they run most of the military connections to the Internet, they noticed quickly because, of course, people inside asked them, "What are these packets?" That second level means that they're fairly well informed. It was interesting. Was I going to be allowed to continue this scan that goes to military sites? I'm just going out there. I told them what I was doing, I told them about the Highlands Conference, and they said, "We'll get back to you." Two days later, I got one bit back. I don't know if it came from the CIA or elsewhere, but it said, "Okay," which is probably all I'm every going to get out of that community. But it was one bit more than I expected and they let me do it.

Well, our database is an open source information pool for

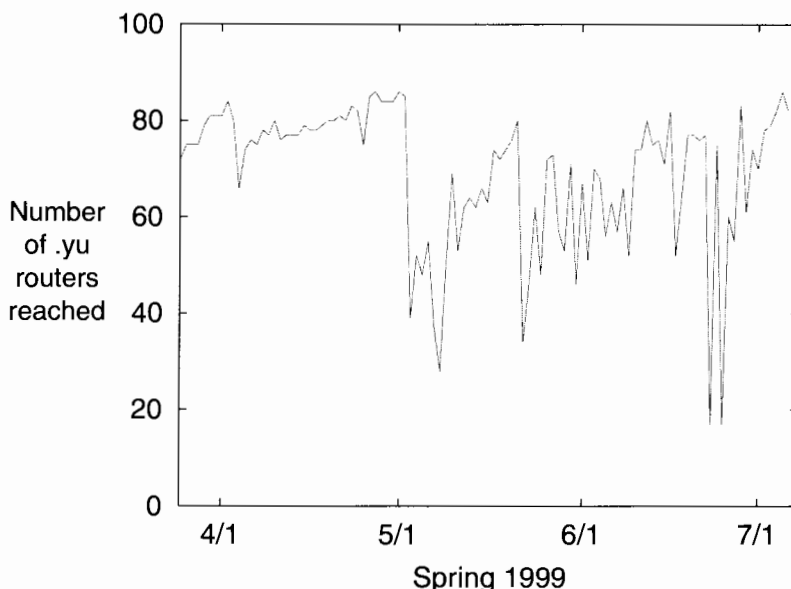
research. I have not checked the logs to see who comes and gets it but I suspect some of them maybe rather *official*. I hope so. I think already the database is useful and when we get multiple points it will be more useful. I've given this talk many times in the Washington area.

Steve Northcutt of the U.S. Navy was working on the Shadow program and he noticed too—because he watches very closely. We only send a couple of packets and it does not match the pattern of a hacking attack. There are a couple of pings and then it goes away.

*Power: You were conjecturing as to who might be access-*

*ing your open source database. It reminded me of an irony about that Microsoft site where you access satellite photos. It's accessible from the Internet. If you're in North Korea or Iraq, for example, you can't get into it. Of course, you could be an Iraqi and get into through Japan. It is laughable. But the point is that there will probably come the day, arguably it is already here, when maps of the Internet and of huge intranets will be as powerful an intelligence source as satellite imagery is today.*

*Cheswick:* Well, we watched the war in the Balkans with our technology. About three days after the bombing started Steve Bellovin



*This graph depicts the number of .yu routers (Serbia/Yugoslavia) that could be reached during a span of days in the NATO action to force an end to Milosevic's "ethnic cleansing" in Kosovo. May 3rd was the time of the first bombing of power plants and power lines.*

and I had lunch and Steve said, "Why don't you watch Yugoslavia?" Now this has actually caused some controversy because there are some people in Europe who think that we Yanks view war as a video game and here I am taking my mapping and watching bombing and killing in Serbia. On the other hand, this is a technology that has been used before. People have seen the results of earthquakes in California from pings and we're going to see a lot more of this. This wasn't really very hard, I just went in and found all the Yugoslavian networks and cranked them up to class C networks and that is a third scanning shade.

The map was interesting. For example, the government is connected through the internet to their universities, not a big surprise. The university would be connected first and the government guys said, "Hey throw us a line." It made it easy to find some of their propaganda pages, and as the war progressed I found one that was all written in Serbian and it had pictures of dying children and lots of Serbian language, and it would say words like Dresden, Hiroshima,

Baghdad, Belgrade. I could have taken this Website out. I ran a strobe on it and it was not very securely run. All of a sudden, the Republic of Cheswick needs a foreign policy.

As a rule I don't ever attack a site. I study hackers, I don't actually go out and do this because I have a life, but it was an amusing thought that I could actually participate in the war and that a civilian could have some activity here. I could knock out a propaganda page and probably keep it out for quite a while. I decided that an open network is probably better than a closed one and so I left it alone, but it's sort of an interesting new thing. Traditionally, the folks at home haven't been able to participate in overseas wars to that extent.

What we did was count the networks that we could reach, it was around 80 networks. Here are the number of reachable networks by day. You can tell that something happened on May 5. Steve Brannigan came up with this map. What happened was the allies started attacking the power grid by dropping carbon fibers on the lines and attacking substations and so on, and that certainly took out a lot of routers. You can see that through the rest of the bombing things never really got better again until later. I should actually run one of those now to see how things are going. Actually, I scanned two countries. I scanned Serbia and Bosnia-Herzegovina. That was sort of my scratch country. Pick one that's under attack and one that isn't and see what happens. It turns out what I learned was that Bosnia gets most of its power from Serbia. So they got cut off too. It was an interesting point to find out while sitting at your computer in your basement. This is called remote assessment of battle damage and this is of considerable interest to the government.

It's very interesting plot and sort of suggestive that we can watch well disasters of any sort. Well, you get into questions of power supplies, etc. but it might be interesting to watch California for the big one for example. I wonder if India's networks are well enough connected that we could have seen the recent earthquake.

*Power: During your presentation, you mentioned that there was a site or a network, as you tracked it in real time, that just never went down during the bombing.*

Cheswick: Well I haven't examined this too closely but we made a map of just Yugoslavian sites in the month of May 1999. If you look at it there's one point that's a little set aside from the general mass of Yugoslavia. It was always reachable. We checked it out. The hop before this site was in Maryland. Now usually a connection to Yugoslavia goes to Brussels then Berlin then maybe Italy and then into Yugoslavia. I don't believe that there were trans-Atlantic connections from Maryland to Yugoslavia though it's possible. Some general said, "Son, you've found their embassy," which might well be true. I actually did a quick scan, it was a little scan, a sort of hacking scan just to count the hosts on that network and that Class C network had 72 hosts that were .yu—which that sort of sounds like an embassy.

*Power: Or big global corporations to find other big global corporations?*

Cheswick: Well yeah of course it's not hard to find them. They're all on the routing data but finding a particular site

like that I suppose could be intensely interesting to some class of people.

*Power: Bringing back to the business world you're saying here Internets are out of control. Ad hoc growth. This plays to the need for this kind of technology for commercial use. You want to talk about that? What people can use this for?*

Cheswick: We have two major products. One of them is this mapping and it isn't just the mapping in fact we go in and examine a large intranet quite quickly and fairly thoroughly with some state of the art tests. We're talking in order of hours or days at the most existing tools can take months crawling through all these routers. We scaled the Internet, we can handle intranets. What we produce are pretty pictures for the CIO to put on his wall, plus a list of things to go check out and see if they're okay. So a map can tell a technical person, "Oh, look we seem to be leaking out into the Internet when we go to Singapore, we do it through the outside." That sort of stuff shows up on the map and people dive right in and check it out immediately. Maybe it's okay, we can't tell as the scanning company whether it's okay, we can just say, "Hey guys take a look here." We also color the maps red for bad, green for good and we use a lot of criteria that come up with ourselves. Other criteria may come from the customer. They may say that this set of networks or domains are bad or good and show us everything that's not there. They may say, "We think our intranet is these routes, show us everything that isn't on these routes."

*Power: So when you said "bad" and "good," you're talking about what you're supposed to find and what you're not supposed to find?*

Cheswick: Right. We even have companies that know which networks go to which business units. We can color the map by business units and this helps with mergers and acquisitions very nicely. That's the mapping part and even the technical people look at the maps cause it does give you some insights. We're working hard on making more insights on that end. But the other thing we do is we find lots anomalies and strangenesses in our scans, things like routing loops, etc. How many internal firewalls do you have? Well, we come up with a list.

*Power: Isn't it funny that now we're talking about how many firewalls do you have?*

Cheswick: That's right. How many firewalls you have inside your network? We are connected to the customer on the inside, we do this after signing a big pile of legal papers. We also run a census which is pretty much your standard ping everything. Following that we can take the list of hosts we found and run them through a patent pending leak detection. We can find hosts that can talk to the inside and the outside which might be DMZs or telecommuters or people running through VPNs or business partners that have firewalls that are broken. And we basically make a list and we have found people who are running businesses in the home on company computers. This is new technology there's nobody doing this right now.

*Power: Just to wrap it up as you were talking the following question occurred to me, "What should be the impact of this on doing a security assessment?" It seems to me that if some-*

*continued on page 8*

continued from page 7

one were to have access to a tool like this it would change or deepen the quality of a security assessment.

Cheswick: That's what we think. It helps you with your security assessment, it helps with network hygiene. You know our marketing people are crawling up and down trying to find the right words to describe what we do. But I know and you know from talking to CIOs for years that all you have to do is show them one of these maps and they say, "I want one!" Now what is going on in his head? What are the magic marketing words: security, management, network hygiene, etc? No, he just wants to know where that stuff is, it's beating back ignorance.

Power: *It's a huge step forward because you try to explain network security architecture to people but the reality is the thing grows organically—out of control, no one knows what it is. Then, as Marcus Ranum says, you're trying to change a hull of a ship at sea—but you don't even have a blueprint of the hull. Mapping and visualizing is something that will be invaluable.*

Cheswick: Well we think so. Not only for security reasons. We had one customer that had a legal request, a discovery demand to list all of the web servers they had in their company. And they ran their own scans and they had 17,000. We ran our stuff, much faster than theirs, and it came up with 31,000. Now it turns out that a number of those were being run by the people who run their network and they were getting charged \$120,000 a piece for these web servers. Obviously, if they can just go through and remove some of those—it's hundreds of millions of dollars.

Power: *It's hard to believe that if you had a technology like this that it would not be considered not only advantageous but "sound practice."*

Cheswick: Well, you know our management leans back and dreams. Wouldn't it be great if the FDIC required banks to run this?



## IN PRINT

### Tangled Web snares rave reviews

*In the September 2000 Alert, I heralded Richard Power's Tangled Web: Tales of Digital Crime (ISBN 0-7897-2443-X) as an important and unique contribution to the field of information security. The following excerpts are culled from just a handful of the many rave reviews of "Tangled Web" across a broad spectrum of publications. — Patrice Rapalus*

#### Security industry publications praise Tangled Web

Niels Bjergstrom, *Information Security Bulletin*: "Richard Power is one of the few people I know who combines excellent journalistic qualities with a solid background in information security. He also knows an awful lot of people in the field and these qualities taken together has enabled him to produce a fascinating and very well written book. The book is a must read. Though it is written to benefit a broad

readership even the most seasoned information security professionals will learn something from it. Richard Power is an excellent writer with a fabulous overview of information security issues."

Ben Rotbke, *Security Management Magazine*: "Whether it be the activities of Vladimir Levin, the Russian cybercriminal who stole millions from Citibank, or Tim Lloyd, a disgruntled network administrator who caused millions in financial losses to his employer; occurrence after occurrence, Power shows how we are indeed in the midst of a cyberwar. Information security is far too important to be neglected, and *Tangled Web* clearly shows what happens when it is."

Graham Roberts, *Network Security Magazine*: "If Power is a cyber-prophet, he is not a doom monger. The final chapter is brilliant, and possibly worth the cost of the book on its own. 'Countermeasures' has more than 30 pages of eponymous guidance. If you are an individual or a company concerned with protecting your information, this book can give some excellent practical guidance."

#### Mainstream, technology media praises Tangled Web

Michael Zuckerman, *USA Today*: "After more than six years of chronicling the insecurities of cyberspace, Power finally decided to put it all together in a book. The result is *Tangled Web*, which explains in everyday terms for non-techie and security pro alike how and why cyberspace has gained a reputation as a bad neighborhood."

Joseph Szadkowski, *Washington Times*: "A riveting chronology of computer crime."

Robert Bruen, *IEEE Cipher*: "*Tangled Web* provides lots of data along with case examples. It is often hard to read books with lots of dry data, but Power has turned volumes of data into a very readable book."

Lewis Z. Koch, *ZDNet Interactive Week*: "A voice of impressive logic and rational perspective, a no-nonsense trek through cyberspace without hyperbole, fear-mongering or undue conjecture."

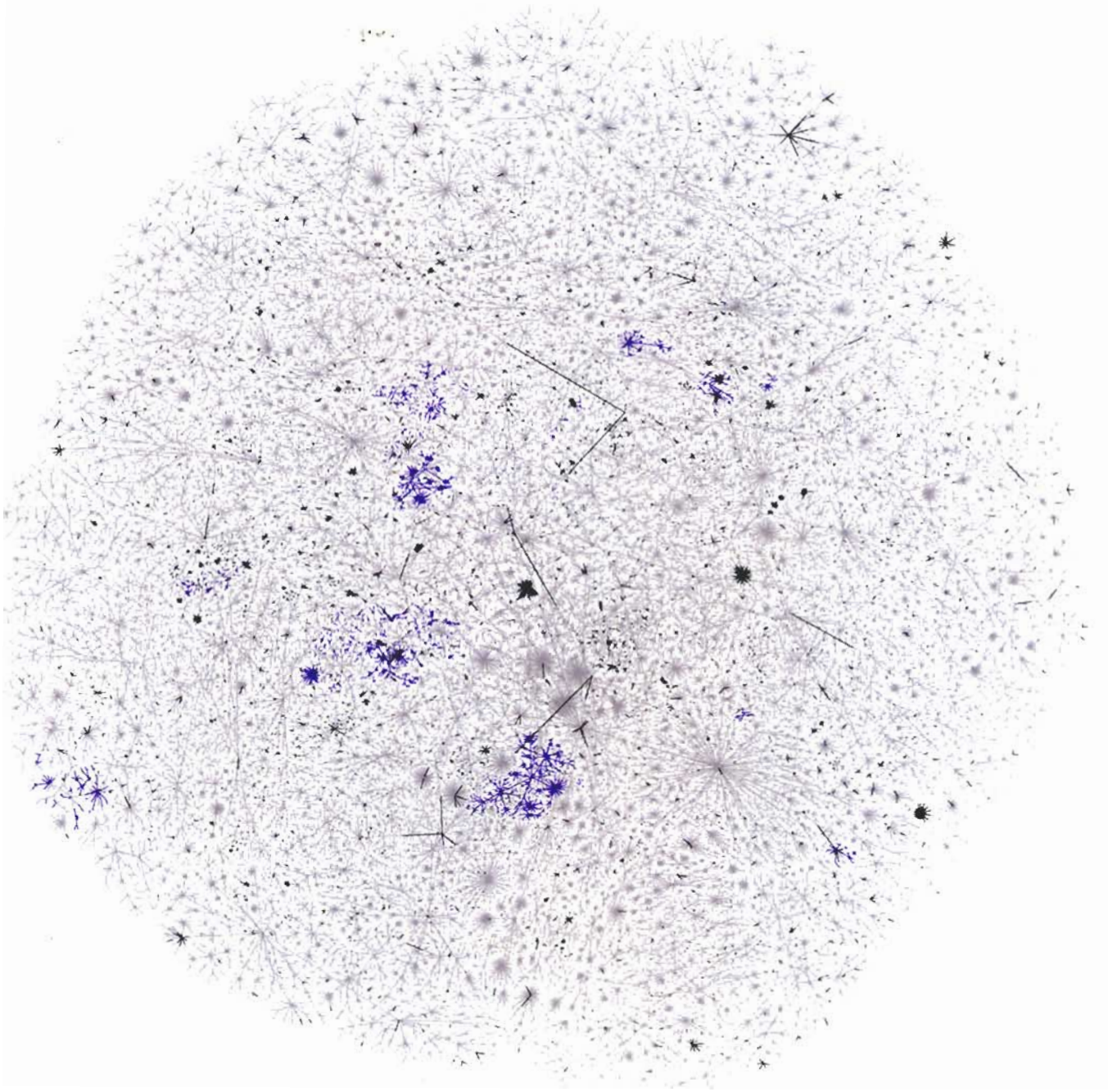
Caryn Mladen, *CanadaComputes.com*: "It's engrossing. It's enticing. And, like hacking itself, it's seductive."

#### Law publications praise Tangled Web

James Christy, *Federal Communications Law Journal*: "The intricacies and nuances of the case studies that *Tangled Web* features were impressive. Power detailed several comprehensive, lesser-known case. *Tangled Web* is a must-read for all cyber cops, prosecutors and information technology heads and policy makers."

*FederalCourts.com*: "After reading through the tales of cybercrimes, 'Chapter 18: Countermeasures' will ensure that your mind somersaults, and your stomach turns, over the risks attack to the assets and operation of your organization. Corporate America and government agencies, especially federal courts, should provide a copy of this book to its entire management team."

*Prosecutor Magazine*: "The strength and the intrigue of the book lie in Power's detailed, often personal accounts of particular cybercrimes and the investigations they triggered. *Tangled Web* is both an enjoyable read and an invaluable introduction to the new frontier of crime."



Patent(s) pending & Copyright © Lumeta Corporation 2000. All rights reserved.

***A Lumeta map of Australia in cyberspace***

This image depicts routes to routers and hosts in the .au domain (Australia) in contrast to the rest of the Internet.