DePhormed Politics

Description: Steve and Leo conclude their coverage of the serious privacy invasion threat from the Phorm system with a discussion with Alexander Hanff, a technologist and activist located in the United Kingdom, who has been at the center of the public outcry against this invasive technology.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-153.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-153-lq.mp3

INTRO: Netcasts you love, from people you trust. This is TWiT.

Leo Laporte: Bandwidth for Security Now! is provided by AOL Radio at AOL.com/podcasting.

This is Security Now! with Steve Gibson, Episode 153 for July 17, 2008: Bad Phorm. This show and the entire TWiT broadcast network is brought to you by donations from listeners like you. Thanks.

It's time for Security Now!, the program that helps you protect yourself online with all the tips you need to know. Not just, by the way, your security, but your privacy as well. The host of Security Now! is here, Mr. Steve Gibson. Hey, Steve.

Steve Gibson: Hey, Leo. Great to be back with you.

Leo: Good to have you. And we are going to talk about privacy today, aren't we.

Steve: Yeah. Actually we've got one of our rare guest appearances, someone named Alexander Hanff, who's in the U.K. and is pretty much leading the anti-Phorm charge in online newsgroups and in privacy circles. We've talked for the last two non-Q&A episodes about this real problem of sort of this new, growing - unfortunately - tendency towards ISPs to sell access to their customers' bandwidth in return for revenue. And we talked in detail two weeks ago about this Phorm system, about the technology that they have installed.

Alex is going to talk to us today about sort of like the human side, the political side, the

history of this in the U.K., which is where Phorm began experimenting in '06, secretly, and in '07. And there's been a huge outcry. I heard you mention, oh, it was in the last couple of hours on TWiT Live, that over in the U.K. there seems to be a stronger resistance and concern for privacy rights.

Leo: That's ironic because the U.K. has more cameras per square foot than any other country in the world. I mean, they already in many ways have lost privacy rights. So maybe that's why they're more sensitive about it.

Steve: Well, anyway, so Alex is going to tell us all about that. We've got some security news. And I've got a really fun SpinRite anecdote to share.

Leo: Very good. Let's get to security news before we go to Phorm. What's up?

Steve: Well, the galactically huge, mind-blowing security issue...

Leo: Oh, yeah. I know where you're going here, yeah.

Steve: Of course you do, is that it was revealed - let's see, what is this? This is Tuesday. Was it yesterday, or I guess it was...

Leo: No, it was a week ago. And, unfortunately, it was just after we finished recording.

Steve: Right. What the computer industry learned is that very, very quietly, all of this year, and especially during the last few months, a well-known security researcher named Dan Kaminsky has been working with every major vendor of DNS servers - Cisco, the open source BIND folks, Microsoft, and others - to very silently fix a big problem that he found at the beginning of the year in DNS. So what happened is there was a synchronized - I mean, this has never been done before in the history of the Internet. First of all, this absolutely didn't leak. There was no leakage of the information at all. And all at once, all of the DNSes were updated in a big sort of synchronized patch, the idea being to deliberately minimize the exploit window from the time that news of this would leak out to the time that systems actually got patched and rebooted.

Leo: You know what I really liked is that they also said the patch was not reverse-engineerable.

Steve: Well, okay. So this is about DNS spoofing. And it is our topic for next week. Dan is not talking about specifically what he found until he reveals it himself on August 6th at the Black Hat conference in Las Vegas. So I've shot a note off to Dan to see if he's interested in joining us in our recording the week after that, where he'll be able - we could get it, you know, if he's available, if his schedule permits. I mean, you can imagine he's way busy right now. But it'd be fun to hear from him directly what it is he found.

But two weeks before that, which is to say next week, we're going to talk about something we have never covered. We've never talked about DNS spoofing. And that will lay all the foundation for what Dan has found because the topic of DNS spoofing is well understood and well known. There are things you can do to harden your DNS servers. What's going on is that many of them didn't implement some simple-to-do things. And it sounds to me, from reading between the lines, as though Dan discovered that the things they were doing to thwart spoofing ended up not being good enough. And I think that's what he'll probably tell us.

So I just wanted to let all of our listeners know that we absolutely know about this big DNS news, and we're going to give it probably two episodes and complete coverage because this is really interesting from a theoretical standpoint. I know that our listeners that have enjoyed our more propellerhead podcasts are going to get a kick out of this because I'm going to explain in detail how the DNS protocol works between DNS servers and how spoofing works in general. And then two weeks later, after Dan has been able to go public with the details, either he or I will explain what it was specifically that he found.

Leo: Yeah, it's a really interesting story. What's really sad is that the patch went out on Patch Tuesday, went out to Cisco and Microsoft and many Linux, you know, BIND, which is commonly used in Linux. However, many Internet service providers didn't apply it. So Dan made a great site, DoxPara.com, that you can test your Internet service provider's DNS. And I was shocked to learn, you know, I have three different Internet service providers here. DSL Extreme had done it, OpenDNS did it, but my local Comcast hadn't done it yet. I was surprised.

Steve: Yeah, actually OpenDNS has always been running strong DNS servers, which were doing something called UDP port randomization.

Leo: Oh, so they were doing it from day one. That's...

Steve: They were always, yeah, or query port randomization, depending upon who you talk to, the idea being that some servers always issue their queries from the same port, from a fixed port.

Leo: Or sequential ports, or guessable ports.

Steve: Exactly. And so the more random that is, that's one of the things servers can do to thwart this. Anyway, the takeaway, if anyone is concerned about this right now, and we've talked about OpenDNS before, anyone could switch their DNS over to OpenDNS in order to sidestep the possibility that their own ISP's DNS servers might be spoofed. Now, I mean, again, I don't want to get ahead of ourselves. We're going to completely cover this next week. My sense is it's a really good thing that this is being fixed. DNS has been known to be vulnerable for a long time. This is forcing, for example, Yahoo! to give up BIND v8, which everyone has been saying they ought to get rid of for a long time. They're finally going to switch to 9, which is just stronger and better. So this is going to end up being a good thing. And we'll talk about it in detail, the nature of the kind of problem that this represents. It's not like end-of-the-world. But it's really good that this is being fixed because there's no doubt the bad guys would have had a lot of fun spoofing DNS servers wherever they chose to.

Leo: Right. Okay...

Steve: The other news in security world is that there are two new zero-day exploits. They just came out after Patch Tuesday. These are Windows exploits. And of course they were timed, typically, to come out, like, on Patch Tuesday so Microsoft doesn't have time to respond. One of them only affects users of Word 2002 Service Pack 3. So it's a bad problem because the idea would be if something was - if something sent you a document that was maliciously designed, which you opened in Word 2002 Service Pack 3, it can perform a remote code execution exploit on your machine. Microsoft offers no workaround for this except says, uh, maybe upgrade to Word 2003 or XP or something else. Don't use Word 2002, it's vulnerable. I'm sure by next Patch Tuesday in August that this will be one of their fixes that they'll be offering.

Okay. The second one, the second zero-day exploit - and by the way, just to remind people, zero-day means that it was found in the wild, that is, exploits of unknown vulnerabilities were found in the wild. Oh, I ought to mention, however, that virus updates, virus signature updates have been updated and are being updated by the various virus-scanning companies to detect this particular type of maliciously formed document. So even if you had Word 2002 Service Pack 3, and you were a person who likes to open documents that you receive in spam or unsolicited...

Leo: What kind of person is that?

Steve: Good luck to you. But it does mean that if you've got a good antiviral scanner that has been updated, it'll probably stop you from hurting yourself by doing that in any event. Okay. So the second zero-day exploit is once again an ActiveX control which Internet Explorer can invoke if you visit a malicious website. You know, we've talked often and repeatedly, unfortunately, about ActiveX and the problem it represents because these are essentially DLLs which normally exist on your system and which, because Internet Explorer is all powerful, you're able to visit a site which runs a script that invokes an ActiveX control that was really never intended to be used by Internet Explorer. You probably don't want to ever use it with Internet Explorer. But the site found that there was a mistake in some sort of the parsing of data in that control which it is able then to leverage to execute code on your machine.

Well, this is the Access Snapshot Viewer, which affects Access 2000, 2002, 2003, and the standalone viewer. It does not affect the Access that ships with Office 2007 because it doesn't include an ActiveX control for that. On our notes page, on the show notes for this episode 153, I've got two links. I've got a link to Microsoft's Security Advisory about this because there is a workaround. We've talked before about the so-called "kill bits." Kill bits is a bit you can set in an ActiveX control's registry entry that prohibits it from being instantiated - as is the jargon in object-oriented land - that prohibits it from being instantiated into Internet Explorer. So the second link on our show notes page is a reg file which anyone who wants to can just click on it, and they can either save it or they can just run it. And that will set the three kill bits for the three different variations of this control. If you then shut down and restart Internet Explorer, what's happened is, even if you've got Access 2000, 2002, or 2003, or even the standalone Access viewer, IE won't be able to load it, and you'll be safe. And again, I'm virtually certain that, by next Patch Tuesday in August, this will be one of the things that Microsoft is fixing. But in the meantime, both of these things, this Word document exploit and this ActiveX exploit, are in the wild, and they appeared before anyone knew that there was a problem. Thus,

those are zero-day exploits.

Leo: Very interesting. I have a story for you, I don't know if you saw it in the San Francisco Chronicle. It just broke today. A disgruntled computer engineer in the city has commandeered San Francisco's multimillion-dollar computer network and prevented access to anybody. He's a computer administrator, and he has changed the passwords at this new FiberWAN network. It's their Wide Area Network over fiber. It's a $5 million, or a multimillion-dollar system. I think they spent hundreds of millions of dollars on it. And nobody can get in. They threw him in jail on Sunday, and he won't tell anybody the password.

Steve: Oh, goodness.

Leo: The whole thing is down. Apparently he's been having trouble, and they've been trying to fire him, and so he did this, started this on June 20th. He basically modified the system so that only he would have, you know, he could pull a cord, and only he would have access to this system. He did, and now they're stuck.

Steve: So he built some sort of like trapdoor that would allow him to get in and change the master password in a way that nobody else could deal with. Wow.

Leo: And they're saying right now that undoing this denial of access could cost them millions of dollars. They're also worried that he may have told somebody, a third party, how to set off a bomb in the system, a logic bomb in the system that would destroy data. And they're trying to find that quickly. He has no access to the outside world. He's in jail. But it's a little scary, if you think about it.

Steve: Wow, that's crazy.

Leo: It just shows you that the guy who knows how to run the computers wields a lot of power.

Steve: Yes, more so every day.

Leo: Yes. It's very interesting.

Steve: The jocks in high school are no longer laughing at us, Leo.

Leo: No more wedgies, huh? No more super atomic wedgies for us.

Steve: Okay, so my really fun SpinRite story for the week came to me with the subject line "SpinRite Got Me a TC1100 Tablet PC."

Leo: Oh, I like that.

Steve: Well, actually, you like the Tablet PC or you like the subject line?

Leo: I like the subject line and like the fact that it got him one.

Steve: Yeah. He says, "Steve, my wife's laptop was in the trash for three days after dying a slow and relatively painless death." Okay, he calls this painless. I would call this painful. But he says, "It had been having problems for a while now, and so I was only using it as a TV display in my office. One day it finally died completely. And without hesitation I tossed it in the trash. I normally hate parting with legacy technology, as my wife can attest. But I resisted retaining it on this occasion. So there it sat for three days in our trash can, collecting coffee grounds, mayonnaise, leaking ketchup, and all manner of other exotic sauces. On the third day" - poor laptop.

Leo: Oh, my.

Steve: "On the third day it dawned on me to give SpinRite a whirl. So I pulled the laptop, docking station, and cables out of the trash, cleaned it up, and placed the SpinRite CD into its half-broken CD drive. Sure enough, SpinRite booted, worked its magic, and completely recovered the drive. SpinRite brought my computer back from the grave, only this time with a 'For Sale' sign attached. I sold that laptop to a friend and used the money to purchase an HP TC1100 Tablet PC on eBay. It still runs great for my friend, and I was able to purchase a legendary TC1100 on eBay with the proceeds from the sale. Thank you, Steve; and thank you, SpinRite."

Leo: Wow. That's a great story. I love it.

Steve: And by the way, I mentioned before we were recording that I have two of the HP TC1100s.

Leo: Why is that?

Steve: Well, do you remember the gal who used to come on the show when we were recording Call For Help in Toronto? She had one.

Leo: Oh, Jenn, yeah, Jenn Cutter. You fell in love with it, that's right.

Steve: I did. Every time I saw that wacky thing I thought, oh. I was lusting after it. It's like, okay, I don't have one of these. So I have to fix that problem.

Leo: She loved it, yeah.

Steve: Oh, and I've got to say, I mean, for, like, used to be when I was involved in my homeowner's association I would be jotting notes in the meetings. It's perfect for jotting notes. And Microsoft has that very cool application, that organizer. I can't remember the name of it.

Leo: OneNote. I love OneNote.

Steve: OneNote, yes, which works perfectly with a Tablet PC. Anyway, it's interesting to me that Tablet PCs never really caught on. But I have to say, anytime I want to, like, really use a laptop, it's just easier to use it with a traditional pointing device and a keyboard, especially when you really want to put text in. But the handwriting recognition is very good. I installed Vista on one of them, and I've got XP on the other. And they're just kind of funky machines. But I do like them.

Leo: Love it, too. Let's get our guest on, Alexander Hanff. And he's calling from England. Am I correct? Is that right?

ALEXANDER HANFF: I'm from England.

Leo: Ah, wonderful. It's nice to have you. Thank you for joining us.

ALEXANDER: You're a bit quiet, then. You could turn yours up a little bit.

Leo: I'll just talk louder.

ALEXANDER: Okay.

Steve: Okay, so Alexander, tell us the story from the beginning. Like what happened with Phorm, how did it come to people's attention, how did you get involved, and what's going on?

ALEXANDER: Well, on February 14th, earlier this year, Phorm gave out a press release stating that it had signed deals with Carphone Warehouse through their Talk Talk company, BT, and Virgin Media regarding this deep packet inspection technology for the purpose of behavioral advertising. Obviously that made the news fairly quickly on a technology news site called The Register. They've been - they've covered this issue extensively from the beginning. And the outrage started.

I read about it first on The Register. Being somebody who's, A, from a technology background for 17 years; and, B, a sociologist, a lot of my work during my studies over the past three years have been based on privacy issues and issues surrounding technology. So it was something that I was interested in both from an academic

standpoint and from a professional standpoint of having worked in the technology field for such a long time.

Steve: Okay. So go ahead.

ALEXANDER: Okay, yeah. So I got involved in looking at some of the different laws which I felt may have been violated by this technology. The news continued to flow on The Register, with a whole bunch of articles over the period of about six weeks. And more and more information came through about what was happening, how the technology worked, so on and so forth. And then we found out about the covert trials in 2006 and 2007. And at the time I was working on my dissertation, which at that point was a dissertation on the validity of Microsoft within the public sector, so the effect that has on the economy, et cetera, as opposed to using open source solutions. However, I started to write a paper on Phorm purely out of my own interest. And that ended up taking on the role of my dissertation. With six weeks to go before the deadline, completely changed my topic and ended up writing this legal analysis of the covert trials in 2006 and 2007.

Then in April I was invited by Simon Davies, who's the CEO of 80/20 Thinking, who were doing the privacy impact assessment for the Phorm system, to appear as a guest speaker at what they call a "town hall meeting" or a public meeting, where Phorm and their executives addressed the press and the general public to discuss the technology and discuss their concerns. There was me there; there was Dr. Richard Clayton from Cambridge University; there was Phorm's CEO Kent; and Phorm's technical director I believe was there. So we all did our own little speeches. I was asked to give a speech based on the perspective from the general public. So I gave a speech about the privacy concerns, the issues under Human Rights Act that this causes, and the fact that people just find the entire system offensive, that it's an anathema to society to be profiled in this way.

So that's where it all started. And then a week later I was called in to do an interview on a BBC News show called "Click," which is a technology news show, where I had a head-to-head debate with the CEO of Phorm for that show. Then I published my dissertation shortly after that, which has now been downloaded over 70,000 times since May the 1st. So that's been particularly successful. And I continued my interest from there. As a result of the attention I was getting, obviously I kind of became a natural leader for the campaign. Then we announced the protest event, which takes place tomorrow. And everything's stemmed from that point. So that's where my involvement came from and how I'm moving forward with the campaign at the moment.

Steve: Well, so I would imagine, with the confrontation that you've had with the CEO of Phorm, I mean, where you guys have literally been head to head on this, he's justifying or defending what they're doing on the grounds that it's anonymous. And they've, like, gone to great measures to anonymize, they don't know anyone's identity, they assign random 256-bit tokens to people. Given that - and I don't mean to play devil's advocate because obviously I'm way in your court on this, but I want to sort of expand our understanding. Given that, from your perspective, how is that not a useful counterargument?

ALEXANDER: Well, basically, in the U.K., and Europe as a wider area, we have a number of laws which protect us from this type of interception. And purely the act of processing data in the first place is covered by these data protection laws. So in order to anonymize this data that they claim that they're doing so effectively, obviously they need to process that data. So there was an issue there. There was an issue with regards to the interception of communications under a piece of legislation we have in the U.K. called Regulation of Investigatory Powers Act, which is basically entrenching certain aspects of

the European Convention of Human Rights into the British statute and makes it a criminal offense for any party to intercept the communications of another without the consent of that person. Or, in the cases of national security and the prevention of a crime, the police can obtain a warrant to intercept those communications. Then there's other situations with regards to secret trials such as the Computer Misuse Act, based on the fact that they were, certainly in the covert trials, they were altering the content of the data stream, or the "click stream," as people like to call it now, to insert their JavaScript. So that's forcing the CPU of the computer to run extra cycles to use resources within that computer without the consent of the person who owns the machine. So the Computer Misuse Act came into play there.

The Privacy and Electronic Communications regulations here in the U.K., which is a European directive, also prevents intercepting and dealing with communications data without consent of the people who are engaged in that particular communication. So we have a whole host of laws here in the U.K. - and certainly that's not all of them, that's just a short summary of some of them - which protect us from this type of behavior. And when you have laws in place, it's pretty difficult to offer a counterargument to say, well, it's illegal, but we're anonymizing it. So do you get my point?

Steve: Yeah, I mean, that makes absolute sense. So it must be that the ISPs just sort of ignored the fact that anyone could argue persuasively that what they were allowing a third party to do in return for monetary gain was a violation of a bunch of laws.

ALEXANDER: Yeah. Of course the ISPs involved were claiming that they've had legal advice, and they're perfectly happy with the legal situation. They believe it's legal. But a number of technical experts, a number of legal experts, peers in the House of Lords, people at the European Commission, MPs in our own government, all believe that this technology is currently, and certainly was during the covert trials, illegal without the informed, and it has to be the expressed informed, consent of the individuals involved. So it isn't a case of they can bury the terms in some end-user license agreement or the terms and conditions. These must be explicit informed consent because it's dealing with communications and issues around privacy.

Steve: So, for example, I know that you've listened to the last couple of podcasts where we've been talking about this. And Leo and I have both been saying that, if this were an opt-in system, which would be easy for the ISP to do, where when the system is being deployed somebody tries to go to any random website, the ISP intercepts their page request and says, hold on a second, we want to just talk to you for a second, we want to get your permission to do the following. If it were opt-in in that fashion, then they would have a position to argue, wait a minute, you know, it is something that people are doing only through informed consent. And of course they know that a huge percentage of people would say, uh, no thank you, I don't want to be watched while I'm surfing the Internet by my own ISP or my own ISP's agents.

ALEXANDER: Exactly. And that's the point. Certainly, if it was an opt-in situation, I would have fewer arguments. There would still be issues regarding the consents of content providers, people who are providing these web pages which are being basically stolen for the purpose of commercial gain. They're being copied, which certainly infringes on copyright. So whereas I may not be the biggest fan of modern copyright, certainly in this situation it could turn around and bite them. But yes, if it was opt-in, then there would be far fewer arguments against technology.

Steve: So when you say that they're stealing the web pages, you mean that it's the keyword-searching algorithm which is parsing all the pages that are being retrieved by the user in order to categorize their interests and build a profile of them.

ALEXANDER: Yeah, I mean, essentially they do a little more than that. They actually take a copy of the page and process it offline so it doesn't interfere with the routing hardware that they have in there. Obviously they need to keep as much resource available for routing all these people through this Layer 7 technology, this DPI kit, as we've come to know it. So in order to lower the overhead on that piece of equipment, the page is actually copied to another piece of equipment, which does the analysis offline.

Steve: I see. So unlike their earlier work, where they were inserting JavaScript - which as I understand NebuAd is still doing in their current technology, but Phorm no longer is - instead they're doing, as we've talked about two weeks ago, the detailed technology, this redirection dance in order to push their cookies out in a first-party context across all the domains that anyone visits and using that to track people.

ALEXANDER: Yes, certainly this whole 307 cookie dance, as you put it last week, which I found quite amusing, is a big issue and infringes on a piece of legislation we have here called the Fraud Act. Basically by their equipment claiming to be a third party, when they really aren't, is an issue of fraud, especially in a commercial transaction between an end-user and a website. Say for example they were purchasing some goods on Amazon, for example.

Steve: That's really interesting. So the user puts the URL in for a domain they've never visited before while Phorm has been in place, thus they don't already have a Phorm cookie. The Phorm system sees that and fraudulently intercepts their clear and explicit request to be connected to whatever website they were trying to get to and pretends to be them, redirecting their browser instead over to Phorm's domain.

ALEXANDER: Exactly, yes. It's not new technology. It's basically a cache, a proxy cache, in respect to the way that it works. So it's not new technology, and this sort of technology has been used with positive results in the past for the purpose of network, alleviating network resources and overheads. But certainly for the purpose of advertising it puts it in a much more sinister light.

Steve: Right. So what's been traditionally done is, for example, and we talked about this recently in fact on Security Now!, an ISP's caching proxy where their customers are - the ISP's customer's query goes to the proxy server. It reissues the query for the web page, which it caches based on the caching rules which are provided on the page. And then the customer receives that copy, the benefit being that another customer, another of the ISP's customers, might request that page or components of the page, images and so forth, which could then be served by the caching proxy and minimize the ISP's bandwidth out onto the Internet and give the ISP's customers faster response time, potentially.

ALEXANDER: Yes, exactly. So it has had very positive uses in the past. But this is the first time - perhaps not with Phorm. NebuAd have been doing this for some time now in the U.S. But certainly this type of application of this technology for behavioral profiling is new and is very sinister and something that we find very offensive.

Steve: So where does this go from here? What do you think happens? Do you have, like, a sense for the strength of both sides of the argument and how it's going to evolve?

ALEXANDER: Well, I am traditionally a technologist, so I am in some respects in the unique position to be able to see this from both a technical understanding and also from many other viewpoints, such as being a father, such as being a social scientist, such as being somebody with, I like to think, reasonably high-quality morals and ethics. I'm not

anti-advertising per se. Obviously we use advertising every day in our lives. But there's ways of doing it which are acceptable and don't intrude on people's rights and don't infringe on their privacy the way that this technology is going to do.

And obviously we have issues with mission creep, or function creep, as well. Certainly as a technologist you'll be aware that DPI technology has the ability to do pretty much anything it wants to do to that network stream. And in that situation we've only got the word of an anti, you know, an ex-spyware company that they're not going to add new functionality to this technology, which for an experienced admin wouldn't even take a great deal of time because basically we're just looking at regular expressions or parsing text.

So whereas it's complex for a nontechnical person to understand, certainly for an experienced technician making changes to the system to change the way that it's looking at these pages or this data can be done very quickly and almost be completely undetectable. Because there's no oversight of these systems. There's no way that they're using open source. Everything is proprietary. Certainly in the previous trials they used Squid, but they were running other technology on top of that. So if there's no oversight, and there's no measures in place to monitor what they're doing and keep an eye on any updates they make or any access they have to the systems, then how can we trust the company that were responsible for what was pretty much regarded as the worst rootkit ever to be deployed on the Internet with all our communication data?

Steve: Yeah, I think you're exactly right. One of the concerns that we've talked about while we've been discussing Phorm in the past couple weeks is this idea that this already makes people feel uncomfortable and really upsets users who discover or learn that this may be going on. And that's only this much of it. But you can imagine that if these kinds of companies, these third parties get a foothold in ISPs with the technology, that just as you said, it's not a huge stretch to imagine them saying, oh, well, look at how much better job of profiling we'll be able to do if we also parse people's email. Because email between the user's client and the ISP's SMTP server is typically not encrypted in any fashion. It's like, well, yeah, we could do a better job, make a better set of decisions about who this person is and what sort of information they're interested in.

The other thing that I find really interesting is that there's even been a question raised about how effective this profiling would be. I mean, even if it weren't being done the way it was, the question is, has it even been shown in anything I've been able to find or read that you get a demonstratably better result after doing all this?

ALEXANDER: Well, certainly we haven't been able to find any information that suggests you can. NebuAd are pretty much claiming that they're still in trials, and they're not going to be willing to disclose that information to the public. Phorm haven't done so, either. So, no, I mean, there's no evidence. It's an untested system in reality, and it's entering into an incredibly competitive marketplace.

Steve: Well, so tomorrow there's a big demonstration.

ALEXANDER: Yeah, we've got the protest in London outside BT's AGM tomorrow.

Steve: And so that'll be just the idea being to raise additional awareness and get it, like, bring it to a head with BT where they're saying okay, we're going to move forward with this or we're going to abandon it.

ALEXANDER: Certainly, yes. And one of the other functions of the protest will be to

deliver a case file to the police with a complaint regarding the covert trials of 2006 and 2007, with the intent that they're going to investigate that and hopefully lead on to a prosecution.

Steve: So you do have attorneys, then, involved over on the anti-Phorm side of this.

ALEXANDER: Sorry?

Steve: So you do have legal counsel involved on the anti-Phorm side, and so there's some legal pushback, not just outrage among users.

ALEXANDER: Oh, there have been some very influential legal experts who've been involved on our side of the debate, yes. Nicholas Bohm, who's general counsel for Foundation of Information Policy Research here, which is the U.K. government think-tank on technology issues, he's a retired solicitor. He also is quite heavily involved in Cambridge University technology law as a guest lecturer there. And certainly he's made comments as regards to his position within FIPR - Foundation for Information Policy Research - that this technology's illegal. And his legal analysis pretty much paralleled my own, actually. So that was a very positive thing.

Steve: Do you know anything about, or have you looked at where we are in the United States in terms of the laws and issues and interception of our traffic relative to the legal framework that you've got in the U.K.?

ALEXANDER: Well, certainly recently I wrote a paper on the sunset articles within the Patriot Act, which is an academic paper I wrote. And as part of that I touched on information regarding personal data in the U.S. Now, as far as I understand it in the U.S., the Fourth Amendment, which is what would normally cover privacy issues, doesn't afford any rights to the individual who volunteers their information to a third party. Excuse me a second [coughing]. So obviously there's an issue there that there isn't sufficient protection within your Constitution. And the Patriot Act, again, takes that even further. So with regards to strong legislation, you're actually in a worse position than we are in the U.K.

That said, however, you've had a lot more success with your politicians there in Congress than we have here in the U.K. I think under the Cable Act your congressmen have stated that the NebuAd technology would fall foul of the law. Now, obviously the Cable Act is an act of legislation, so it is important. But it's not really one of the bigger pieces of legislation you hear talked about in the U.S. So it was interesting to see that a single section of a relatively unknown piece of legislation in the U.S. can stop NebuAd and Front Porch dead in their tracks as regards to Congress. Whereas over here we have multiple pieces of legislation, I think seven or eight different pieces of legislation, which this technology falls under. And we haven't been able to get a positive response from our own government. So whereas you may not be as protected, it's unusual for us to see a country that is normally seen as being less secure with regards to privacy than the U.K., certainly receiving much stronger support from your government than we are here. And that's a great thing to see, obviously.

Steve: Well, and it may also be aided by the fact that, thanks to the Patriot Act and what this country has been going through for the last seven years, ever since the events of September 11, that there's an awareness and a concern about the issue of privacy. So we just may be more primed and ready for addressing these things.

ALEXANDER: I had a meeting with the Earl of Northesk here in the U.K. He's a peer in

the House of Lords, which is one of our houses of Parliament. And he's been covering the Phorm issue from an official perspective in his position. And he believes - he actually lives in the U.S. for half of the year. And he believes that your Congress are actually much more knowledgeable about technology issues than our politicians are here in the U.K. Maybe there's younger blood in your political system, or maybe simply because of the massive tech industry that's there, it's something that's unavoidable. But certainly his belief is there's a huge lack of knowledge of these issues and a huge lack of understanding of these issues within the British government.

Leo: It's funny, we've been saying that about American government for some time. But I guess it could be worse.

ALEXANDER: In this case, yes.

Steve: Leo, can you think of anything else that...

Leo: No, I'm just - Alexander, I'm just really glad that you've brought this to light and that others are fighting so hard. I think in a way, by leading the way on this, you've kind of protected us here in the states against it. I mean, you've raised awareness to the degree that by the time it came to our shores there were people prepared and ready to fight it. So thank you.

ALEXANDER: But we owe you some gratitude, as well, because obviously the storm that's raised in the U.S., Phorm are very much interested in expanding their markets into the U.S. And certainly this was one of the arguments they were using to try and attract investors over the past couple of months. Now with companies like NebuAd and Front Porch effectively being frozen out of the market by Congress, this obviously affects Phorm's financial interests. And as a result we've seen a stunning fall in their share price over the past five months. And that's partly been down to the action that's been going on in the U.S.

Leo: Well, great. Thank you so much for your time. I really appreciate it, Alexander. I know it's late there, and we're glad you could speak to us.

ALEXANDER: Thank you very much for having me on, and thanks for other two shows you've done on this and the continued coverage. I look forward to listening to the rest of the show.

Leo: Thank you, Alexander. Take care.

ALEXANDER: Thank you, bye bye.

Leo: I'm sure we will do - you're planning, I'm sure, doing more about this in time.

Steve: Well, absolutely. I mean, we've got a communications link established with

Alexander. He and I have been exchanging email. He's been participating over in the newsgroups at GRC.

Leo: Oh, great.

Steve: So I'm sure he'll be able to keep us appraised of what's going on. And I will let our listeners know as things develop.

Leo: Steve Gibson, what happened to your Kindle, my friend? What happened?

Steve: Well, okay. The good news - this has a happy ending, and I'm very impressed with Amazon. I was sitting in a restaurant on, like, a bench seat. So only, like, two feet off the ground. I had my legs crossed, and the Kindle was in my lap. And I was, you know, eating or drinking some wine or something. And it slipped out from between my legs.

Leo: Oh, no.

Steve: Now, I knew it was slipping, and the floor was carpeted, and it was two feet. And I figured, eh, big deal.

Leo: Let it go.

Steve: And actually about a week before it had done the same thing, exact same position, same bench. I have my, you know, the table that I like in one of my favorite restaurants. And so it was like, eh, you know. So it drops two feet to carpet; right? No problem. Except this second time I pick it up, and the screen image is severely damaged. Like the upper quarter inch across the entire top of the screen and about an inch over from the left vertically streaking down was just dead. Sort of like dead scan lines. So I was like, ooh, ow, no. And so, figuring that it was sort of like the high-density edge connector that a screen like that would use, I sort of squeezed on the top of it? And, sure enough, it changed the nature of the outage on the screen, but didn't improve it, really. It just sort of modified it. So I knew I was, like, in the right area. So I'm thinking, oh, my, you know, now what?

So, okay. No Kindle is more than a year old because they were only selling them since last November when you and I both got ours. And so I went online, looked around in the online groups and saw that several people had had very good experiences when they'd, like, done something bad to theirs, or the Kindle had died or something, as is going to happen with any consumer product when you're pumping out as many as Amazon is. So I contacted Amazon about a week ago. I don't know if it was email. No, I think I phoned them. Oh, yeah, I found a phone number in the online forums. I phoned them, talked to an Amazon person. He said, oh, yeah, no problem, we'll send you a replacement.

Leo: Wow.

Steve: And you have a month to send back your other one. And I'm going to send you email with a link to a UPS prepaid return deal. So I've printed that out.

Leo: That's amazing, Steve.

Steve: I am very, very impressed. In two days I had a brand new Kindle.

Leo: Wow. And the account was transferred over?

Steve: Yup.

Leo: Wow.

Steve: Yup, I was able to move the content over. And I boxed up the old one and sent it back. And, I mean, and I have to say, Leo, speaking of the Kindle, just as that was happening, I was noticing that the battery was already beginning to show some fatigue. That is, it was - normally I could, on a full charge, I only turn the cell radio on for, like, briefly at 5:00 a.m. when I'm at Starbucks in the morning to update my Wall Street Journal and Slate and periodicals; then I turn it off. So it's barely on. And normally I could go for several weeks before I would even notice that the battery gauge came even the first increment down below full. But here, now, what, eight months old, it was clearly not lasting as long.

Leo: Interesting. Of course you're using it very heavily.

Steve: I am using it every day. Although a lithium ion battery should have about two years of useful life. They actually do get old, even if you don't use them at all. There's, like, sort of a freshness factor to them. The good news, of course, is unlike some consumer products made by that company whose name starts with "A"...

Leo: You could change the battery.

Steve: Yes.

Leo: In fact, you know, it's funny, when I ordered my Kindle, I ordered a second battery. They're cheap.

Steve: Yes, they are inexpensive. And so I know that a year from now, assuming that this is the same, that my replacement Kindle's battery begins doing the same, I'll just get a second battery and, you know, and be back...

Leo: I have my second battery, but I haven't ever used it. I got it because I thought, oh, maybe I'll bring it with me in case I go on a longer trip and I can't charge it up, like when I was going to Egypt. But I never needed to use it at all.

Steve: No, I mean, the Kindle's battery life is spectacularly long.

Leo: It goes a long time.

Steve: Anyway, so my story of dropping my Kindle had a happy ending, and I'm very, very impressed with Amazon's customer service. And I thought, I mean, literally, I'm bound to this thing. So I thought maybe they would make me send it back, and I would be without it for a month or something. I was considering buying a second one just so I could have my own overlap. And then I thought, well, what am I going to do with a redundant...

Leo: Two.

Steve: Yeah, exactly. So they just - they solved the problem in a very satisfying way.

Leo: That's truly impressive customer service. I have to say, credit to Amazon for that. Yeah, it may cost them a little bit in the short run. But in the long run, boy, what great word of mouth you get when you start doing stuff like that. I mean, to be honest, you broke it.

Steve: I did.

Leo: They didn't have to fix it.

Steve: Yeah, it wasn't their fault; it was my fault. Even though I have to say, Leo, that should not have broken it.

Leo: It shouldn't break after a two-foot fall to carpet.

Steve: It was a gentle fall. And so it was like, okay. Although up till that point it had been absolutely perfect. So it's not like I had any other complaint. And I've got to say I'm still of two minds about the page turn. It's annoying that it's so easy to do it by mistake, but it is so nice that it is so easy to do it when you want to.

Leo: Yeah, once you learn how to hold it, which is down on the keyboard, counterintuitive though that may be, it's not such a bad thing. And I do a lot of reading on the Kindle. Although in between the audio books, and now I'm reading

Neal Stephenson's book, and the only way I could read it was in paperback because it's a pre-release, and that's a thousand pages. That's kept me pretty busy. So I've actually been reading a paper book.

Steve: Oh, my god.

Leo: They're heavy. You've got to hold them up.

Steve: What's paper?

Leo: I don't know. This thing, it's not going to work. Actually, when I mentioned that to Audible they said, you know, we record these ahead of time. And they said we really ought to talk to the publishers about the readers copies, offering - because we know many reviewers like to use audio books, maybe doing audio versions for the reviewers. And actually I think that's a great idea.

Steve: I'll bet it helps, I bet it would help to get books reviewed.

Leo: Yeah. I know I'm looking, yeah. Hey, thank you for covering this. I think you've done the best job of anyone covering Phorm and NebuAd and all of these creepy little ISP things. We do have a victory already under our belt because Time Warner decided not to use NebuAd. I think that this is so important to get the word out about this. And I think we might have stemmed the tide. And I think a lot of credit goes to you for that.

Steve: This is something we had to nip in the bud.

Leo: Yeah, no kidding.

Steve: And next week I want to tell all of our listeners to wind up their propeller hats because we've got a terrific episode planned on explaining exactly how DNS can be spoofed. What happens when you do that is you stick the wrong IP address for a website into a DNS server, such that anybody who then queries for the IP address of that site gets the wrong IP address, and they are then directed to a potentially malicious server instead of the right one, even though everything looks just fine from their browser. So we'll talk about how that happens next week.

Leo: Yeah, that's a creepy one, and I'm glad we're going to be talking about that. And that'll lay the foundation for our interview with Dan Kaminsky, we hope, after Black Hat. Once he's told the world, he'll come on and give us some greater detail.

Steve: Yup.

Leo: Steve, always a pleasure. Make sure you go to GRC.com. That's where you'll find Steve's great SpinRite, the bestest repair utility and maintenance utility money can buy, a must-have if you've got hard drives. Also you'll find his great free programs including ShieldsUP! to test your router and a whole bunch of useful little tools like Wizmo, and 16KB versions of the show, and transcripts for those who like to read along as they listen. It's all at GRC.com, the Gibson Research Corporation.

Steve: And this week I will remind our listeners that the show notes for this episode has the links for people who are concerned about the ActiveX exploit of Access that allows them to easily set the kill bits for the three variations of that control in order to just shut that down until Microsoft patches it. Certainly I'm virtually certain they will during next Patch Tuesday, which will be the second Tuesday in August.

Leo: Thank you, Steve. We'll see you next week.

Steve: Talk to you then, Leo.

Leo: On Security Now!. Bye bye.