Phracking Phorm

Description: Steve and Leo continue their discussion of "ISP Betrayal" with a careful explanation of the intrusive technology created by Phorm and currently threatening to be deployed by ISPs, for profit, against their own customers.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-151.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-151-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 151 for July 3, 2008: Phracking 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!, our sesquicentennial episode. Steve Gibson is here from Irvine, California.

Steve Gibson: Aren't we sesquicentennial plus one?

Leo: Is this 151? You're right.

Steve: Sesquicentennial was last week.

Leo: You're right. What was I thinking? Well, but, you know, it's that old "when does the year 2000 begin" thing; right?

Steve: I hate that, that zero or one. Are we counting from zero, or are we counting from one?

Leo: Well, we counted from one. So I guess we can say this is our second...

Steve: Go ahead, I'm sorry.

Leo: It's our second sesquicentennial of - I don't know.

Steve: Well, this is a big one, too. There's been a huge amount of interest about our promise this week to discuss the technology, the horrifying technology which is being used by the Phorm system essentially to spy on ISP customers without their knowledge, unless they're clued in to what's going on. So we opened the topic two weeks ago, discussing this whole notion of the betrayal of ISP trust which is beginning to happen. And so this week our main topic is to talk about all of the specific details of what Phorm is doing in order to achieve long-term profiling of ISP customers.

Leo: These are advertising platforms. Or at least they bill themselves as advertising platforms, not as spy platforms. We should mention that. Actually I got an email, and I sent it along to you, from the folks at Front Porch, who said we'd like to, you know, talk about what we do. Do you - at some point I guess we could give them a chance to explain it, I don't know...

Steve: Oh, I'd like to very much. In fact, you also sent one, and another guy contacted me through GRC and on the newsgroups who's been very active in the U.K. in anti-Phorm stuff. And so we're going to have him on the podcast in two weeks to talk about sort of the political and regulatory and, I mean, he's really been in the fray. And of course Phorm is the - one of the sites that we'll talk about is registered in New York, and they have corporate offices in New York. So despite the fact that they've also got a presence in the U.K., they're very much planning to attack the U.S., much as they have already been very active - too active, everyone would believe - over in the U.K.

Leo: Well, and an update on our conversation here, and some really good news, at least I think so, Charter has announced that they're not going to go forward with the NebuAd program that they were talking about.

Steve: Yup. And NebuAd is a different approach to achieving the same sort of concept, you know, it's the same sort of ISP-installed equipment. And NebuAd, well, it's hard to say one is worse than the other from a technology standpoint. They do inject JavaScript into the pages that ISP customers download, which is what Phorm was trying to do a couple years ago, in '06 and '07. That was the early approach that Phorm was taking. They messed that up so badly that they backed off from that approach. So anyway, we'll go over all that today.

Leo: So I'm glad you've kind of lifted, pried this rock up, and you're shining some light in here. Because clearly the spiders are moving.

Steve: Well, and you know, it's the sort of feeling like when I download software now, or

go to a website, often now I'm confronted with an interception page that is showing me something full screen. And then up at the top it says, "If you'd like to bypass this ad, click here." And it's like...

Leo: I hate that.

Steve: ...yes, I want to bypass this ad.

Leo: It's so funny that they give you that option. I mean, of course you don't want to watch it.

Steve: And so my point is that we began with less annoying ads. Then we went to Flash, where they've got dancing fish prancing around the screen. And now we've got interception pages. And so my concern is that if we allow ISPs to give third parties a foothold in their facility, if they have the ability to start intercepting our traffic, and that becomes acceptable, then what's next? I mean, you could easily imagine email filtering follows on. It's like, oh, well, we're just doing - we're not reading your email, we're just doing a keyword scan to determine kind of what kind of categories you fall into. And then when you go on the web we'll be able to deliver more targeted advertising. So my point is, I guess, that I think the sense is this ought to be nipped in the bud and stopped immediately, before it goes any further.

Leo: Yeah. I mean...

Steve: [Indiscernible] got a whole bunch of other stuff to talk about.

Leo: Yes, we are. Okay. Let's - I tell you what. I know, there's so many things I want to say. Let's get to some of the top security stories. And we also have some updates, I'm sure, from the week past.

Steve: Yup.

Leo: And then we can get to the main topic, which is Phorm. And then at that point maybe I'll talk a little bit more because I want to say, you know, we're advertising supported. I don't think advertising is necessarily bad. But I think that there are ways to do it that are acceptable. And I think there are some philosophical issues here as well as some security and privacy issues.

Steve: And here I am wanting to follow up and continue talking about this. For example, websites are just not that expensive to put up.

Leo: Right.

Steve: I mean, so there was all this early nonsense about, oh, well, if it weren't for the ads, we wouldn't have the web. It's like, yes, we would. We had the web before we had advertising. So it's not...

Leo: Well, not only that. There are, like, a million Web 2.0 sites that are fairly expensive that aren't doing any advertising. So you don't - obviously the ads aren't necessary. Yeah, I don't diss anybody's right to make a living doing what they're doing. And, look, the ads are necessary for what we do. We spend more than a quarter million dollars a year now on producing content, so we have to have some revenue come back for TWiT.

Steve: Right. And so, for example, I think what's happened is popular websites have said, oh, let's just do a little experiment here and see what kind of revenue we can generate. And when they actually start generating cash from visitors who are encountering their ads, then they think, wow, this doesn't just have to be a black hole that our money all goes into. It can support itself. I mean, which is a good thing. Although, again, this notion of going to a blocking page presenting you with not the URL you clicked on...

Leo: That drives me crazy.

Steve: ...and then you have to do something or to bypass it, that's, again, it's becoming...

Leo: I'll tell you what I think about all that in a second. But let's talk right now about what's been going on in the world of security because there are a few important security bulletins I'm sure people want to hear.

Steve: Yes. I noted that a copy of Acrobat that I had installed on one of my machines updated itself since we last spoke.

Leo: How could you tell? It's updating itself every five seconds, it seems like.

Steve: Yeah, well, I mean, Adobe's really in the middle of security nightmare land, at this point. They've got another JavaScript parsing vulnerability which is being exploited in the wild. There are some situations where, without any user interaction, a PDF document will display itself. If that were a malicious PDF document, which...

Leo: Is there such a thing?

Steve: Oh, yeah, which this vulnerability now is again closing. I mean, there are a continuing series of these JavaScript parsing bugs in Acrobat that are being uncovered and are quickly being exploited. So I did want to let people know, if they've got Acrobat and they use it a lot, they may want to - and they don't have, like, automatic updates and checks and so forth verified, it's worth going into the toolbar and saying check for

update and make sure that you have updated yourself recently because there is - this is in the wild. It's being exploited. Again, it's not like it's going to be a huge problem. But people listen to Security Now! because they want to know about this stuff. So there is one. Also the Safari version, the Safari for Windows has a number of vulnerabilities that Apple has just recently patched. Two of them are remote code execution vulnerabilities. So that's definitely worth updating also for any people who, for some reason, are running Safari under Windows.

Leo: There's a - Apple updated its own operating system, OS X, with a fairly major update. At least that's judging by the way they number these. 10.5.4 came out yesterday. But of course I haven't seen exactly what they patched. But I'm sure there's some security patches on there.

Steve: No doubt a lot. And you know how we were talking sort of anecdotally a week or two ago, wondering about Microsoft, the effectiveness and value of Microsoft's software removal tool, which they're constantly updating, as we said. Certainly every second Tuesday of the month we get a new version of the Malicious Software Removal Tool. There was an interesting statistic that was revealed by Microsoft. 330 million copies of the Malicious Software Removal Tool were downloaded in June, and it was updated to remove a particularly pernicious game-password-stealing malware, and it encountered and removed two million copies of this game-password-stealing software on Windows machines.

Leo: This is a big business in Asia in particular. These online games are big business. And I've seen, there have been a lot of security flaws or viruses trying to take advantage of this fact and stealing game passwords. You'd think who cares; right?

Steve: Well, of course the reason is that now games have become such a big deal that, if someone gets your username and password and logs on as you, they're able to steal the resources and sell them for cash. I mean, they can turn them into money. So, and as a matter of fact, you mentioned Asia, it is the case that more than half of these instances of malware were found at Chinese IP addresses. So there dose seem to be a real concentration of that over in China.

Leo: I think they're worth more in China, I guess.

Steve: I updated Wizmo, my little wacky Windows gizmo, with two new commands. I don't know, I was just in the mood late last week. I got another piece of email that my tech support guy Greg forwarded to me with a Wizmo person saying please, please, please could you just give me a command for locking my computer. I mean, locking the computer, a Windows machine, is not hard. You do Control-Alt-Delete, and then you choose Lock. But it's the most requested new feature in Wizmo. So it's like, okay, fine, I give up, I'm putting "lock" in. And then I tried combining it with "monoff," which turns off the monitor. And that sort of - you can do it that way, say "wizmo lock monoff." And you set that up as a shortcut on, for example, down in your toolbar. And you just do a one-click. And so anyway, but it doesn't work as well as it could. So I did a second command called "blindlock." And, you know, Wizmo you can find at GRC.com just under our main menu in freeware, or also GRC.com/freeware. And "blindlock" locks the system and then powers off all the monitors and keeps them off. So it looks like the system, you know,

you're not getting any clues, you can't see the username which you otherwise can see if you just use the "lock" command or if you just lock the system. So you can't see that. And of course it's dangerous if you fumble around with the keyboard. So you want to practice first just using the lock command. And also Alt-U and Alt-P are shortcuts to the username and password fields. So you can use those, you know, to recover from a typo when you're not able to see what you're doing. But anyway, I know that it is the most requested feature. And so I said, okay, what the hell, we'll just - I'll add that. And so now Wizmo has it.

Leo: Lot of people love Wizmo. It's free. You get it from GRC.com. I didn't realize you were still getting so many feature requests. How long has - Wizmo's been around for years.

Steve: Yeah, it has been.

Leo: It's really neat.

Steve: I got my first SGI monitors. And they had the ability to power down. And I thought, hey, that's cool, I want to - I didn't use a screensaver. But I always know when I'm getting up from my machine for some length of time. I'm not someone who continually power cycles his computer. So the machine was going to stay on; but I wanted the monitors to, like, turn off when I wanted them to turn off. And so I just - that was the genesis for Wizmo.

Leo: Is it a BIOS call that it makes, or is it a bunch of different stuff you're doing, or...

Steve: It's in the Windows API. There's the whole power control API that allows you to manipulate Windows power...

Leo: But you've expanded it much beyond power. I mean, it does other stuff, too; right?

Steve: Oh, it's got the graviton screensaver that's got, you know, where all the equally gravitationally mutually attracted little white balls do all kinds of cool things.

Leo: And it's got that new zero, wireless zero config fix, which is good.

Steve: Right, for turning off the wireless zero config, which is - it's amazing to me that Windows will install on a machine that has never seen a WiFi adapter...

Leo: Isn't that silly.

Steve: It'll have that service running.

Leo: Yeah, just in case, I guess, suddenly you get a WiFi adapter.

Steve: Yeah.

Leo: So how could people send you suggestions? Because already I'm seeing in the Stickam chatroom, like, four different things they want you to make Wizmo do.

Steve: GRC.com/feedback is the all-purpose feedback catchall for Security Now! input. GRC.com/feedback. Also a new version of Jungle Disk was released.

Leo: I saw that. I just downloaded it. What's new in there?

Steve: Oh, I mean, it's got so many new things, I can't even enumerate them. And frankly, I haven't gone yet to take the trouble to download it. It is a free upgrade for everybody who has v1.whatever it is. This is v2.0. And there is also a new groupware version of Jungle Disk which is specifically designed for allowing multiple Jungle Disks to be logged into the same remote Amazon-located bucket and be able to share files. So he's solved, basically created the ability to have a shared directory, essentially, through Jungle Disk. One of the features that I know that it has is you're able to simultaneously access multiple buckets, which is the term he and Amazon use for, like, the equivalent of a directory, essentially.

Leo: Right, right.

Steve: So but it's got a ton of new features, a whole bunch of backup. He increased the number of things that the built-in backup facility could do because basically he's been listening to users and doing what they wanted to.

Leo: Yeah, I like it. The backup now has an interface right on the window so that it's very easy to start the backup, pause the backup. You have much more control over it now.

Steve: Right.

Leo: That's Jungle Disk, by the way, which we've talked about before. But if you don't know about it, it's an interface to Amazon's S3 storage. And it's not free, but it really adds to the - it enhances the value of S3 immensely, and it's cheap. It's JungleDisk.com, I think it is.

Steve: Yeah, and it's very inexpensive. I mean, it's...

Leo: Oh, it's great. 20 bucks?

Steve: 20 bucks, I think, yeah.

Leo: What else?

Steve: Oh. Also your big TWiT episode on Sunday...

Leo: You know, first of all, I want to apologize. What was I thinking? You know, we're getting old-timers on. And we tried very hard to get David Bunnell, who would have been great. What it ended up being is old-timers in the computer magazine industry who had known Bill Gates. Because we were talking about Bill Gates. His last day was last Friday. And why I didn't think of getting you on, Steve, is just beyond me. I'm sure you have many stories to tell about Bill Gates.

Steve: Well, yeah.

Leo: I apologize. I apologize.

Steve: I would recommend to all Security Now! listeners, if there are any who are not listening to TWiT, it was a great podcast.

Leo: It's so funny because I never know. I was so nervous about doing it because it isn't, you know, TWiT's normally a news podcast. Sure, that's the big story of the day, but we didn't cover any other stories. It was a bunch of old guys, you know, people your age and my age, Steve. And I thought, oh, you know, this is not going to be - and I received nothing but positive.

Steve: Oh, no kidding. I'm really glad to hear that. I thought - I was just - it was fun. I mean, Gates is a, well, he's the richest man in the world. But for all of the people listening to this who are involved in PCs and computers, obviously, I mean, you know, he matters. He's...

Leo: Yeah. He matters more than almost any - I can't think of anybody who matters more.

Steve: Well, okay. My problem with Bill is that when we get together, we tend to argue. And...

Leo: Why am I not - why am I not in the least bit surprised?

Steve: I have the utmost respect for him. And but I recognize that he is fundamentally a brilliant businessman. And while he once created a company called TrafOData to process traffic - the punch tape that the old traffic measuring equipment produced...

Leo: When he was 15, I might add, or 14, yeah.

Steve: And then, you know, no one's really clear what involvement in coding Bill had. But I recognize that his genius, his brilliance is that of a businessman.

Leo: Oh, yeah.

Steve: And so what happens is, the trouble I get into with him is he says something which he wants to be true because it's important to Microsoft's interests that it be true, but it's not. And most people, you know, aren't sure if it's true or not. But I am. And so I call him on it.

Leo: You stand up to him, yeah.

Steve: Well, okay. So the one most memorable event, and it's funny, too, because as I was listening to the podcast I was thinking, oh, shoot, I mean, I'm sure that Dvorak and...

Leo: Bill Machrone? Jerry Pournelle?

Steve: Yep, Machrone and Pournelle were all present for this because this was very public.

Leo: Oh, boy.

Steve: This was the announcement of the Pentium. And there was one - the big annual conference for the computer industry is Comdex, that I was always going to. At the time, I was in the middle of - somewhere along my eight years of writing my weekly column in InfoWorld magazine called "Tech Talk." Which, because I really gave it a lot of time and attention, ended up being a very, very strong component of InfoWorld. There was the Cringely column. And Cringely and I were vying for first place among all the different assets in that news weekly. And sometimes he would be - he would pull out in first, and sometimes I would. But so what I said mattered. And in fact I was largely credited with launching Visual Basic because the gal from Microsoft, Nevet Basker, who was the original product manager for Visual Basic, came down, paid me a visit, and showed me VB 1.0. And I was like, oh my god, everything - this changes everything. And it's funny because one of my programmers said this is really a bad idea. And I said why? And he says, this makes it too easy to program.

Leo: He might have been right. That might be the real problem.

Steve: But anyway, so I'd established my creds. And this was the year that the Las Vegas Convention Center was being remodeled. So Comdex was at McCormick Place in Chicago that year.

Leo: Oh, I remember that. I was at that Comdex, yeah.

Steve: Yeah. And so the big deal at the time was Intel's release of the Pentium. You know, we had the 286, the 386, the 486. And it was like, okay, at Comdex Intel is announcing this new processor. So the entire industry, the entire press community - that's why I'm sure that John and Bill Machrone and Pournelle were all there. In fact, I remember partying with Jerry. He's got a neat wife. Roberta is a great hugger. So...

Leo: I've never met Roberta.

Steve: ...we always hug whenever we're together. Jerry just sort of looks at me thinking, okay. Anyway...

Leo: Here comes that Gibson again.

Steve: Tighten your string tie. So the whole press community is there. We start off - and this is in the large auditorium at McCormick Place. And we start off with Intel's presentation of the new, radically different and improved Pentium architecture. And there are a number, you know, I'm glued to this because I want to be writing, I'm thinking this'll be good for three or four columns. I want to explain what Intel is doing with this new architecture. So one of the things they explained is that this thing has - and this was the first chip, I believe, with on-chip cache. No prior processors had major on-chip cache. But what was happening was the clock speeds of the processors were - it was moving ahead of the speed of dynamic RAM. So there was a greater and greater disparity, so that the Pentium - there must have been some little, like, Level 1 cache; but no big, like, Level 2 cache. So that was a big deal. And Intel - the buzzword at the time also was still RISC.

Leo: Oh, what a - yeah.

Steve: Reduced Instruction Set...

Leo: That was the battle because Macs were running on a, quote, "RISC" chip. And everybody was saying, well, can you get more complex with CISC? Who's going to win, RISC or CISC? Yeah.

Steve: Right. And of course MIPS was the big RISC producer at the time. And so Intel, of

course, I mean, as an Assembly language programmer, I'd been programming the Intel chips for years, and I knew just how complex the instruction set was. I mean, I'm still sometimes picking up my little reference book and going, okay, wait a minute, is carry set on this kind of instruction or not? I mean, it's incredibly complicated, as opposed to being a long instruction word which is much simpler and flatter. But Intel wanted to have RISC because, oh, that's - it was a buzzword.

So they said, oh, we've reengineered our processor from scratch. This is a RISC core with an emulation wrapper which runs at very high speed. So it still runs the relatively horrible Intel instruction set, but it does it much faster. And we've profiled all this code out there. And for the first time, thanks to this RISC core, many of the instructions which are used more often now execute in a single cycle. And that was new. The idea of one-cycle instructions, back in the 286, 386, 486, these things were so heavily microcoded, meaning that there was actually a ROM on the chip, and the chip was basically emulating the Intel instruction set, which is called "microcode," because the instruction set was so complicated you just couldn't do this in hardware. You had to sort of make a computer within a computer in order to execute this instruction set.

So, okay, so we got - a whole bunch of instructions are now able to execute in a single cycle. We've got a big on-chip cache for the first time. So as long as all of the data for the instruction is in the cache, that's part of the requirement for a single-cycle execution. So it meant that the benefit of executing from the cache would be much better. And the penalty for so-called "cache miss," where you had to go out and pull that data from the increasingly slow-seeming dynamic RAM, that penalty was much greater. So, I mean, so okay, I absorb all this. And so...

Leo: I just want to say something real quickly before you get to your point. This was the beginning of a very bad road for Intel which ultimately bit them. But go ahead.

Steve: Okay.

Leo: I mean, no, seriously, this was kind of some of the problems that they ended up having was this penalty for backing up.

Steve: Oh, right, exactly. Well, and the problem is that the instruction set that they were moving forward over time for the sake of upward compatibility, it was really hard to make it faster. They had parallel execution pipelines and speculative processing where instead of - in computer jargon, you come to a branch. And you either take it or you don't. So they would do both. They would take it and not take it and, like, split the execution stream. And they were trying to execute ahead of the code so that by the time the code got there, then they would know what path to take. I mean, it's just - it's bizarre how, I mean, like what effort they had to go to to continue making this system faster and faster. So after the presentation, the hall lights come up in the auditorium. And we're going to have a panel. Now, the panel members were Philippe Kahn, Bill Gates, Fred Gibbons, and Jim Manzi.

Leo: Now, we should probably, because there's a lot of people too young to know any of those names, which were legend in the industry then, of course...

Steve: Yeah, I mean, these were, like, "the" guys in the PC industry. And the moderator was someone I knew, Stewart Alsop. Stew wrote the PC Letter for years. He was - for a while he was the editor-in-chief at InfoWorld, in fact.

Leo: Little side trivia, Stewart Alsop, John C. Dvorak, Fred Davis, Gina Smith, and I did the first pilot TV show for CNET, a show I produced.

Steve: Oh, very true.

Leo: And it was a great roundtable. It was basically the precursor of TWiT and Silicon Spin and a bunch of other shows like that.

Steve: Yeah, and he also was a major industry figure and follower. So he was going to moderate this panel. Now, okay. There was a long, long-existing blood feud essentially between Borland and Microsoft. That is to say, between Philippe Kahn, president and founder of Borland International, and Microsoft. What happened was that when Microsoft began all this, remember they were the language people. And in fact that was the - back in the genesis of the PC, IBM went to DRI for the operating system and went to Microsoft for the languages. This notion that Microsoft was an OS company hadn't been born yet. Microsoft was into languages. They started, of course, with BASIC for the Altair and those machines, and then they did - they had a BASIC for the Z80 and some Pascals. Well, Microsoft's financial model at the time had their languages priced at $499. I remember Microsoft Pascal, I mean, I just was drooling for it. But, you know, $500, it's like, ow.

Leo: This is where Philippe Kahn comes in. I know where you're going.

Steve: Yes. And so out of nowhere, I mean, from a company no one had ever heard of, were these huge, full-page ads for something called Turbo Pascal.

Leo: And I loved it.

Steve: For $49.

Leo: 49 bucks.

Steve: It just blew the crap out of Microsoft's whole pricing model.

Leo: Well, not only that, it was better; it was fast.

Steve: Oh, it was fantastic. I think it was the first place, the first time we saw an integrated development environment, or at least one that size. So you...

Leo: And you could compile and run - write, compile, run, like this, boom boom boom boom boom boom.

Steve: Yes. Yes. So you run in Turbo Pascal, and your editor is there, it executes there. And, I mean, it just ran like a bat out of hell. Okay. So you can imagine how Bill Gates felt about this. It was like, I mean, this was just, you know, talk about twisting the knife in him. Because it, I mean, it destroyed their whole pricing model. So needless to say...

Leo: I can see the steam coming out of his ears.

Steve: Oh, needless to say, I mean, there was just, I mean, it was a feud between those guys. Now, Fred Gibbons was the CEO of Personal Software. And I think this was just...

Leo: They did PFS Write, PFS - all those PFS programs; right?

Steve: Right. And I think this was after the medical trouble that he had, that John referred to on Sunday's podcast. Because he had a stroke. And, I mean, again, he was enough of a figure in the industry that this was just horrifying for those of us who knew Fred. And, I mean, he was a neat guy. But he was back on his feet, and so he was present. And then Jim Manzi was Lotus, the other major factor in the PC industry with spreadsheets. And of course Bill was pissed off at them, too, because he wanted to do Excel and everything. But mostly he was furious with Philippe at Borland.

Okay. So Stew, Stewart Alsop, the moderator, says first, right off the bat, first question - and I remember Philippe was on the far right of this table. It was Philippe, Bill, Fred, and Jim Manzi was over on the left, at the left-hand side of the stage. So Stew was closest to Philippe. And so he says, "So, Philippe, we've just seen this presentation by Intel. You guys, as the preeminent language compiler makers" - and there again Bill is just [growling] - "does this mean you're going to be coming out with a new line of compilers for this new processor?" And Philippe said, "Oh, absolutely. You know, we've been working with Intel," and he gave his Intel, pro-Intel spiel about they've been on the inside, they know all about this stuff, and they'll have immediately Pentium-aware compiler versions for their software.

Okay, now the other thing I forgot to mention was that Microsoft had been suffering under the reputation of being several chips behind for a long time. Remember that, Leo?

Leo: That's the story I've told where Andy Grove was just furious because Microsoft wouldn't keep up with Intel.

Steve: Right. And so Microsoft's OSes - and this was the joke in the industry at Microsoft's expense was, like, the 486 was out, and they were only supporting the 286.

Leo: Just killed them.

Steve: And you could run Windows on the newer processors because Microsoft had made them backward compatible. But Windows wasn't taking advantage of any of those features. And remember that at one point there was Windows 3.0, and then there was a Windows 386 which was sort of this weird, okay, we did something that now uses a 386. So please just shut up about it.

Leo: It doesn't run well, nobody uses it, no software runs on it, but we made it.

Steve: So the worst possible thing for Bill Gates was that another new processor has come out, and they don't have anything for it. And...

Leo: And it was a Pentium - it was 32-bit, too; right?

Steve: Yes, yeah. So they, you know, and they have no language, you know, plans...

Leo: New instruction set, so everything...

[Talking simultaneously]

Steve: So Philippe says, oh, absolutely, we're going to come up with a whole new set of languages. Okay. Bill cuts him off. I mean, he finishes, but Bill interrupts him and says, "That's ridiculous. The Pentium is completely upward compatible." Oh, and by the way, I don't know if he's changed it now or since, but at the time Bill couldn't say "processor." He said "prosser." He was in a big - I don't know if he was in a hurry or what it was. But he said, "The Pentium prosser." We knew what he meant, and we all forgave him because he was Bill. So...

Leo: But I have to say also he is a first among equals at this point. He is not Bill, the Bill Gates of later years where he's really the titan.

Steve: True.

Leo: It wasn't like people were afraid of him at this point. They were kind of - they knew him.

Steve: So anyway, he rails against Philippe, saying that that is ridiculous, there's absolutely no need for new languages or new compilers or new anything, this thing is compatible with the existing "prossers," and that's just a bunch of baloney. And so I'm following this fight and waiting for Philippe to rebut. Which he doesn't do. And so I was, like, in the third row in the auditorium, and I stood up.

Leo: Oh, boy.

Steve: And Stew saw me standing up and said, "Oh, it looks like Steve wants to weigh in..."

Leo: Oh, boy.

Steve: "...on this. And so I turned to Bill, and I said, "Well, Bill, you're wrong." And he stares at me, not happy. And I said, "You know, just off the top of my head, I mean, we just saw Intel's presentation. Now, they explained that with this so-called 'RISC' core, many of the instructions which are used most often now execute in a single cycle. Whereas other instructions are heavily microcoded because they're not used that often. So in order to save silicon they've not tried to implement the things you don't do that often in hardware. They've microcoded that more heavily. But overall, it ends up being better.

"Now, a compiler has several different stages. The back end, the so-called 'code generator,' is what takes sort of a pre-parsed language and turns it in - it emits the absolute final machine language." I said, "That is, an optimizing compiler is all about running the resulting program as fast as possible. So if a compiler were targeted at the Pentium processor" - I think I might have said "pro-ces-sor."

Leo: Pro-ces-sor, three syllables, Bill.

Steve: "So if a compiler were targeted at the Pentium processor, knowing that it was generating code for that particular instance of the universal Intel instruction set, it would definitely choose different instruction mixes for its final product because that would run much faster on a Pentium than it would on a 486, and so on." I mean, and to the tech-savvy audience, everybody knew I was right.

Leo: Of course. Intel, when they make a new chip, the first thing they do is make a reference compiler for that chip, an optimizing compiler for that chip.

Steve: Okay. Then I said, "And another thing. This is the first processor with a large Level 2 cache. All these instructions only execute in a single cycle if all the pieces that they need are available on the cache. Now, again, we know that there's a huge benefit for maximizing cache hits and a huge cost for going off-cache. So again, if the compiler were targeted at a Pentium, it could know" - I think they were 4K caches at the time. I sort of, you know, I'm not sure, but I think that's what it was. "If it were targeted at this Pentium, and it knew that it had a 4K cache, again, it could optimize the instructions so that, like, loops and things would tend to fit in the cache and maximize cache hits in order, again, to increase performance. So it seems very clear to me that it does make sense, as Philippe has said, to have compiler technology that recognizes what chip it's writing to."

Leo: Yeah, but we don't have that yet, Bill.

Steve: And so, I mean, this is like - you could have heard a pin drop in the auditorium. And it was extremely uncomfortable. And then Stew said [clearing throat], "Well, okay.

Moving along, then..."

Leo: So Bill didn't even respond.

Steve: He didn't at that point. But then after, you know, we got through the whole thing, and we were milling around a little bit, he came up to me. And he said, "Steve, you're a technical guy. It's very important that the world not get the wrong impression about the compatibility of the Pentium 'prosser.' And, you know, that's...." And I said, "Bill," I said, "you know me and the care I put into communication." I said, "I absolutely will not give the wrong impression. But I want to be technically accurate." And he kind of glared at me a little bit and then wandered off.

Leo: His big concern was that, well, of course his big concern was that people would continue to buy his products over the better product from Philippe Kahn. But I can see what he was saying is that, you know, well, this could - and by the way, this is what John was saying. The message Bill said, and ultimately was right, is you don't have to worry about optimization because it's all going to be taken care of as these things get faster and better and better.

Steve: Oh, and I have to chime in something...

Leo: He was right on that, though.

Steve: Had I been in the TWiT group, I would have agreed with Jerry wholeheartedly about Pascal. It is - the failure of Pascal to win is one of the great losses in computing science.

Leo: For people who didn't see or hear TWiT.

Steve: It is absolutely, absolutely my favorite language of all time. I could write code in Pascal, and it just worked the first time. And more significantly, if I came back to something a couple years later and looked at my own code, it was still clear to me what it did. It was just - it was a fantastic language. And they were right during that podcast that it was because it was - and originally UCSD Pascal was an interpretive Pascal. You had a little front-end pseudocompiler that compiled the pseudocode, which a Pascal interpreter ran. It allowed you to bootstrap the language environment, the UCSD Pascal environment to, you know, many different processor architectures very quickly.

Leo: Much as Java is today, actually.

Steve: Yes. And in fact one of the things that Turbo Pascal did differently was it emitted native executables, EXEs, and just ran like a bat out of hell, so...

Leo: Yeah, well, and Jerry's point was that it was a strongly typed language. So programmers didn't make - it actually has a security impact. Programmers didn't - weren't allowed to make the same dumb mistakes about typing and casting and so forth. And probably, I don't know, I'm guessing, we'd have fewer of these buffer overruns, as well, because Pascal wouldn't let you do things like that.

Steve: Well, it was - and it was just visually beautiful. I mean, you know, there were...

Leo: See, I was a C guy. I liked C. But that's...

Steve: Well, and there are languages like C where there are contests, like okay, how much can you do in one line?

Leo: Obfuscation, yeah.

Steve: You know. And I'm trying to think, there was, oh, APL was famous for this, too.

Leo: APL didn't even use English. You had to put key caps on your type, on your keyboard, before you used it.

Steve: Yeah, you had bizarro symbols, super powerful, but they were wacky. But anyway, so I wanted to share that anecdote because that was, you know...

Leo: You know, if Pascal lives - I think probably most people don't use it. But if it lives, it would live on in Delphi, right, which is pretty Pascal-like, the database programming language.

Steve: Yes, well, it's basically a heavily object-oriented Pascal is what Microsoft, I mean is what Borland did to it with Delphi.

Leo: But I think that's probably the only place it still does live on except maybe in an academic environment.

Steve: And in my heart, Leo.

Leo: I wish you could still get Turbo Pascal. I think if you could get Turbo Pascal for Windows Vista, you'd see a lot more great shareware and freeware programs out there.

Steve: Yeah, it was a great language. I'm sure it's around. I mean, it probably still runs. I wouldn't be at all surprised.

Leo: It's not native anymore.

Steve: Yeah, that's true. And lastly there were some - several people made a comment about one of Jerry's books. This was relative to Audible and your dialogue...

Leo: Jerry did. Jerry said to Audible, start doing "Mote in God's Eye."

Steve: Well, that's the book. In my opinion it is one of the classic sci-fi books of all time. He and Niven, Larry Niven co-write it. And I've read it maybe three or four times. And it's just - it's just a fantastic read. So I wanted to add my own "hear, hear" to Jerry, and I think also you and John also talked about "The Mote" being a spectacular book classic.

Leo: I've never read it. I'm going to admit it right now, I've never - I've read all of the Ringworld novels.

Steve: As soon as Audible does it in an Audible book format you should jump on it.

Leo: Absolutely. I'm in the middle of Neal Stephenson's new novel right now. It's very, very long, and it's wonderful, but it's taken me a while to get through it.

Steve: My last little point was I'm setting up a new machine. I think I've - I know that I've told our listeners how annoyed I am that I've got a quad core machine as - I'm sitting in front of it, it's my workstation, and that only one core is ever doing anything at any point because there's nothing I'm doing that taxes it in the way, for example, that doing media does. And so I finally got so annoyed, I had to - something I was doing, I can't remember what, I was recompressing something that took a little over 24 hours to do a two-hour video file on the machine that I had. I thought, okay, that's just - I can't tolerate that. So I built up a new really strong machine. It uses the quad core Intel extreme 9675 or 9560, something, I don't know what it is. But it's four cores, 12MB of on-chip cache. It's in two 6MB chunks shared by each pair of cores with a 1333MHz front-side bus, DDR3 RAM. I gave it 8GB...

Leo: I just want to point out you're building essentially the ultimate gaming machine. That's almost exactly the specs that we're doing for the ultimate game. You bought the 9770.

Steve: Yes, that's it. And, oh...

Leo: $1,500, I just want to point out, $1,500 processor.

Steve: Oh, and in fact I used a Supermicro motherboard and case. And Intel, in the documentation that came with the processor, they were talking about how the new and improved fan and heat sink - this thing, I mean, it's huge. It's like a big mushroom cloud.

Leo: But why - you just said you don't use all quad cores. What are you doing with this?

Steve: This is for my media stuff, for my media work. And but the point is that the case did not fit this huge mushroom fan heat sink. I had to literally - I had to modify the holder of the back fan, cut away some of the plastic, and then it worked. Because I guess Intel had just increased the size of the heat sink for this thing. And they even have a blue LED that they've got shining out through this thing, like all those aftermarket wacky...

Leo: People want that, what the hell, costs a penny more.

Steve: Exactly. So anyway, but my point was that this thing now, as a test, I had it recompress the same thing that took 24 hours. And it did it in better than real-time, in 57 minutes.

Leo: You're kidding.

Steve: No.

Leo: Oh, that's a significant jump.

Steve: So, I mean, it was...

Leo: What kind of hard drives did you put in that?

Steve: I did a - I have a 3TB RAID using...

Leo: RAID 5...

Steve: ...a HighPoint caching...

Leo: I'm writing this all down.

Steve: ...SATA II. So four 1TB drives that give me - running RAID 5. So I'm pulling from essentially all of them at once and getting three times the throughput that you would get from just a single one.

Leo: Did you use the VelociRaptors, those new 2.5-inch, 10,000 rpm drives, or...

Steve: No, I don't - 2.5-inch drives scare me.

Leo: Makes you nervous, I know, yeah.

Steve: They just all seem like kind of flaky laptop drives to me. I know that's crazy.

Leo: Well, they're getting the speed because of the increased areal density.

Steve: I used some big 1TB Hitachi drives. Like there's the Hitachi consumer grade, and then there's a server grade. And I went with the server grade. I put four of those in the case. So, I mean, anyway, this is just my...

Leo: How big is the power supply?

Steve: 650 watts, I think.

Leo: That all?

Steve: Think so.

Leo: You need more, man. I think the processors need more than that. That's an amazing box.

Steve: It's got a pair of Panasonic...

Leo: The only thing that's going to be different probably in the ultimate gaming machine, it's very close, DDR3, the 9770, 8GB of RAM, yeah, very likely, maybe less, but probably 8GB. The only thing that's going to be different is the video subsystem. We're probably going to do - we might do four-way SLI. I'm not sure yet what we're going to do.

Steve: Ooh, wow.

Leo: You're getting it; right?

Steve: It's tricky, though, because...

Leo: Got to fit in the case.

Steve: You're going to have to have slots...

Leo: I know.

Steve: ...that are going to fit all those cards.

Leo: I know. And the cards are double width. They're huge. So we may just do dual SLI because we just - for practical purposes. And we're going to liquid cool.

Steve: Anyway, the point of all this was that in reinstalling my favorite software, I encountered one of my programs, it's called DVD-Lab PRO 2. It is my absolute prize-winning choice for DVD authoring. The things you want to do, like just make a DVD where you put it in and it plays a two-hour movie, it does those easily. If you want to do more fancy, like multi-episode DVDs of, like, your favorite shows that you've captured on the air and so forth, it's easy to do menuing. And it even gives you access to the VM in the DVD player. I don't know if our listeners know, but DVDs actually have a virtual machine in them.

Leo: Really.

Steve: And DVD authoring tools hide all that from you so that when you build a menu they're actually writing - they're, like, using canned virtual machine code to basically do all of the work behind the scenes. Well, you don't have to mess with any of that, and I haven't yet. But I know that it's all there. And, for example, the authors, it's a company called MediaChance, they have, for example, a demo of a quiz system written, basically it's a quiz technology that runs on the DVD player itself using their virtual machine code. But all of that is available. They've got an emulator and an editor and a debugger and - anyway.

Leo: Who makes this? Is this Ulead? Who does this?

Steve: It's MediaChance, MediaChance.com. And the program's DVD-Lab PRO 2. Anyway, the point of this is that when I was installing it, maybe I was upgrading or something, I went back to the site because I'm a licensed, registered user. And one of the things that he said was "does not bother you with any online activation."

Leo: Yay.

Steve: And I thought, exactly. Because the other tool that I absolutely love that does this compression, my killer compression favorite tool, we've talked about it before, is TMPGEnc, the Tsunami MPEG encoder by Pegasys, or Pegasys-Inc.[com]. Anyway, that's the one. But what really bothers me about these guys is that every so often it reauthorizes itself. And so, I mean, I've paid them. Over the years I've paid them a lot of money for a bunch of their different stuff. And so I'm worried that this thing, they're going to go away one of these days, their authentication servers are going to be down

when I need them, and this thing will not run unless it "renews your license," unquote, which it's doing autonomously, meaning that you have to have an Internet connection, and that it's, you know, it's not even, like, doing it once, like activating Windows, and then Windows will stay alive for a long time. And then I wanted to - I was looking for a good simultaneous burning tool. The one that I had been using didn't like this new motherboard and SATA interfaces because I've got four DVD burners, four Pioneer...

Leo: I'm not going to ask you what you're using four DVD burners for.

Steve: Well, because if I need four copies of something, I don't want to have to wait and do it four times...

Leo: Of course not, why would you.

Steve: ...on a single burner. But anyway, so I used a very nice program called Gear Pro. But it was through Digital River, who I hate. That's the eCommerce folks. And everything about Digital River just is...

Leo: I have to buy stuff through there from time to time, and I don't like it either.

Steve: And in this case what happened was I activated it once. And then I can't remember now why, but I rebuilt my hard drive, and it deactivated it, and I could not reactivate it.

Leo: So you had to buy it again.

Steve: And, oh, well, no, I mean, I had to send an email and to explain that I, you know, I told them I resized the partition. And I think I was just messing around with the RAID system. And so I knew I was in trouble. But it just bugged me.

So the point of all this is I just wanted to sort of explain my own philosophy and where SpinRite is in this spectrum. When you buy SpinRite you receive a transaction code which is a 13-character and digit token which we email you, you see it on the screen, you can cut and copy, paste, I mean, that's the keys to the kingdom. That's all you ever need to download SpinRite anytime, anywhere. It does no activation, no online nonsense. I mean, I've never done any kind of copy protection. And I've survived. And the last thing I'm going to do is annoy people the way so many of these contemporary software platforms now annoy people, by certainly not periodically activating and certainly not in any way imposing a limit on the number of times you can use something or download something. And it's really come in handy for people who, for example, they're traveling with their laptop, SpinRite's at home, but they're able to, like, call home, get the code from someone else in their family, enter it into GRC's website, it gives them a fresh download link, and they download their copy of SpinRite right from our servers. So...

Leo: Thank you for doing that.

Steve: Anyway, I just - I was thinking about my approach to this relative to all of these crazy approaches that are increasingly annoying.

Leo: I think it's good for people like you to talk about the fact that this works for you because I think there's the general impression that, well, yeah, maybe copy protection is a bad thing; but if you don't do it you're going to lose your shirt. So I think it's really important for people who know, no, in fact, you can, this is a legitimate business practice, and it works, and you're living proof, and I think there are many examples of this. I just wish that people would come forward and say, yeah, no, you don't have to do it.

Steve: And I know that SpinRite is being used illegally.

Leo: Of course.

Steve: But I don't think those are lost sales. Someone who's going to use it illegally, who's going to borrow a copy from his friend or find it somewhere online or somehow do that, they're not someone who's going to buy a copy from me. And so...

Leo: Don't think of them as illegal copies. Think of them as customers who haven't paid you yet.

Steve: Well, and we've heard so many testimonials over the years from people who did loan, and I have no problem. If they loan their friend a copy, it saves their butt, and then their friends - and then they say, look, SpinRite just worked for you, help GRC out, buy it. And they do.

Leo: People want to, I think - I believe in people. I think if they find something of value, they pay for it. They really do. And if they didn't realize the value yet, then they just - they haven't paid you yet. But people are honest, I think, in most cases.

Steve: And if you treat them with respect.

Leo: If you treat them that way. And the minute they feel like you say, oh, you're a criminal, I'm going to copy protect, then they don't mind stealing something.

Steve: Well, as an example, Tsunami has a lock, in my opinion, on compression.

Leo: Yes.

Steve: I mean, it is a fantastic tool. But in the same way that PayPal has a lock at the moment on what PayPal does...

Leo: We can't wait for somebody to come along and replace them.

Steve: Exactly. If there is an alternative to Tsunami that is a better compressor, that doesn't worry me by constantly needing to renew its license, I would much prefer using that. And I'd rather support that than this nightmare of, like, worrying one of these I'm going to lose access to my favorite compressor.

Leo: Let's talk about Phorms. Is it P-h-o-r-m-s?

Steve: No "s," P-h-o-r-m.

Leo: Phorm, okay.

Steve: Okay. So this is a company that we began discussing in overview two weeks ago that pays ISPs to have their equipment installed in the ISP's data center for the purpose of monitoring the actions of the ISP's customers and aggregating profiles for the purpose of understanding what kind of websites the customers visit. It's then an advertising networking company much like DoubleClick and so many others, which then places ads - they sell ad space on websites. And the idea is that, for example, using Google ads as we were saying two weeks ago, when you go to a page, the Google ads you see are relevant to the page you're on.

What's different about the Phorm system, and there's a whole bunch, a collection of next-generation nightmare companies like this, they track the user, not the page. So they figure out, by profiling what pages you look at, they figure out and divide you into categories. And their marketing brochures talk about how they have, like, a thousand different categories that users get check-marked in. And then when you're on any website which is using ads hosted by this advertising network, you're not getting ads relevant or relative to the page, but to you because they're tracking you separately from where you go.

So as I mentioned, a couple years ago Phorm began this work in '06. And they stumbled a bunch because they were trying to inject JavaScript inline into people's web pages so that when you would go to a page, the page you received from the server had actually been altered by this spy technology, for lack of a better term. I don't know, I mean, that's what it is. They would insert code that your browser would execute. The problem is they weren't very good at it. Maybe it can't be done in a robust fashion, you know, nothing I even want to think about. But as a consequence people would find that this - they were pasting this JavaScript into Web 2.0 blog entries and things. It was like, it was leaking out and being seen. IE would hang and go into an infinite loop and had to be shut down by using Task Manager to lock it down because it would use 100 percent of the machine's resources. I mean, there's, like, all these problems.

And what really annoyed people is that this was all being done surreptitiously with, I think it was BT, one of the top three ISPs in the U.K. was, like, allowing Phorm to use their customers unwittingly, causing them all these problems. So and these are also - this Phorm is a renamed company. It used to be Media something, like Media 247 or something...

Leo: I'm thinking of a bad word that I'm just not going to say.

Steve: Anyway, so these are not good people. And back then they were doing rootkit spyware that was installing itself in people's machines, profiling them and hooking the kernel in order to hide from anyone being able to see the randomly named directories that they created. So there's just a history of badness here.

Okay. So come forward to current time. Now we're in today. Phorm somehow has continued to exist and is causing a huge kerfuffle in the U.K. because the main three ISPs have been seduced by the money that they'll be able to make. The idea is, you know, ISPs would like to make some money rather than just selling bandwidth to end-users. And these other companies come along and say, hey, we'll pay you. We're going to anonymize everything we do. We're going to respect your customers' privacy. We're going to put our hardware, insert it into your network flow, and we'll pay you. Doesn't that sound like a win-win-win? And unfortunately ISPs are saying yes. As you mentioned, Charter here in the U.S. has been made gun shy of this in the case of a partnership with NebuAd because this was really upsetting people.

So what I want to talk about, the reason I warned people to bring their propeller hats, beanies, is what it is that Phorm is doing now in order to forcibly track ISP users without any JavaScript injection. JavaScript injection is the easier way to do it. But that can - people are - maybe people who listen to the podcast are disabling JavaScript. Or they've just never found a way to do it safely. Or the idea of modifying the web page that I download from CNET, you know, just really, really crosses the line. The good news is that U.K. apparently has substantially more stringent privacy guidelines than we do in the U.S. And so, I mean, there are all kinds of people getting ready to talk lawsuit here about just the idea that I go to CNET and get a page, and secretly some spy machine in my ISP is injecting code into the page I retrieve for the purpose of tracking me and profiling me over time. So Phorm came up with a solution which is amazing, amazing in how...

Leo: Increasingly awful, yeah.

Steve: Amazingly awful. Okay, so here's how it works. I'm an ISP. I'm a customer of an ISP that has subcontracted this system with Phorm. So Phorm has installed a bunch of hardware in the ISP's facility. When I go to - and we'll just use CNET as an example. I started with that. We go to www.cnet.com. My request - oh, and let me back up a little bit, give a little quick background on cookies. This is a quick refresher. Cookies, as we know, are little tokens which are offered by servers and are then returned by the browser for subsequent queries to the same server. The server is identified by domain. So, for example, if you go to CNET.com, like with a virgin browser, it's got no cookies in it, it's never seen the Internet before, you put in the URL www.cnet.com. The CNET server, in responding to you with a page, will include in the headers that you never see, that's not part of the page content, but it's things like the expiration time of the page, how long the page should live, and how many bytes long the page is. And there's a bunch of sort of metadata that is sent out first that helps the browser display the page. One of those things is a cookie header which is offered by the server. The browser will retain the cookie for varying lengths of time, depending upon how the browser and/or the cookie is formatted. And with subsequent requests to CNET.com the browser will - it'll look at all the cookies it has, and it remembers cookies by domain. So as it's making a request for an asset from CNET.com, it'll check to see if it has any CNET.com cookies. And, if so, it adds them to the requests and sends them back. So that's how they work. So all of that

is called a "first-party cookie." A third-party cookie...

Leo: And I just might add that I don't think there's anything wrong with first-party cookies. This is really how the web works.

Steve: I agree. I agree. And in fact it's because of the fact that there's no enduring relationship with your browser from one page to the next...

Leo: We call it "state."

Steve: A state, right. I put in a URL, and it gives me a page. Well, then, if I put in another URL, it gives me another page. It doesn't know I'm the same person unless I hand back the token it gave me. And then it goes, oh, that's that guy, okay. And in fact that's the way you're able to log into eBay or to PayPal or to, you know, virtually anything that requires you to have some credentials. I went back to the WallStreetJournal.com yesterday to look up an article that was in there, and it said, oh, hi, Steve. And I'm thinking, isn't that nice. I mean, I'm glad it remembers me. If I went there with a different machine, I'd have to give it my username and password again. But I told it remember me on this machine, and it did so by giving my browser a cookie, which I then send back. So for low security sorts of authentication, like staying logged in at WallStreetJournal.com, that makes a lot of sense. It's a convenience.

The thing that originators at Netscape, I don't think they thought about this, I think it just sort of slipped through, is what if a website offered ads by somebody else? That is, the actual ad URL on the web page said www.doubleclick.net? Well, it turns out that the server whose domain you're on, like CNET, that's the first party. We call assets which come from other servers "third parties" because they're not - the server's the first party, I'm the second party, and this random other thing is the third party. Well, it turns out they're able to do cookies, too. In the normal configuration of browsers, third-party cookies are enabled except in the case of Safari.

Leo: I think that's because...

Steve: [Indiscernible].

Leo: But I think that's because they're kind of seen as owning part of that page. So it's, you know, you've gone to a page, and there's - because these banners are coming from another site. It's almost as if there's a little frame on the page, and that's another site you're looking at there.

Steve: Correct.

Leo: That's the thinking, anyway.

Steve: Well, and so here's the problem with that is that the clever marketing guys, I

mean, and these marketing guys are nothing if not clever, they realized that if they gave me a cookie, they DoubleClick, for example, gave me a cookie because an ad was displayed when I went to pull up a CNET page, the cookie that I get is for DoubleClick.net. That's the domain that the cookie's for. Well, that means if I then later go over to the WallStreetJournal.com, and The Wall Street Journal is also buying ad space from DoubleClick and displays a DoubleClick ad, my DoubleClick cookie that I received at CNET goes back to DoubleClick while I'm at the WallStreetJournal.com. And one of the things that is part of the headers in a query, that is, when I'm sending a request to something, like when the ad is being requested from DoubleClick, the URL of the parent page is so-called the "referrer." So DoubleClick knows what I'm looking at. That is, it knows not only who I am anonymously, but from this token it knows that somebody was at CNET who was later at The Wall Street Journal and knows what articles I'm looking at and what pages I'm pulling up. And so you can see that if DoubleClick succeeded significantly so that they had ads spread all over the Internet, over time they would be able to build up a history of all the places I had been that were serving their ads.

Leo: I mean, it's not everywhere you've been. Again, just places that...

Steve: That were serving their ads.

Leo: ...served those ads, right, right.

Steve: Yes. But now...

Leo: Of course sites like DoubleClick, now owned by Google, are in so many places, that can be a pretty bleak picture.

Steve: Okay. So that's the model. Now, notice that, okay, it has to use third-party cookies. Now, people who are privacy aware are turning third-party cookies off. I'm going to be coming out very strong with a facility for allowing people to verify. And I will be autonomously letting people know who come by GRC to, like, run/use ShieldsUP! or for any purpose, I'll just notify them, oh, by the way, you've got third-party cookies turned on. If you're interested in turning them off, click here, and I'll show you how to do that. Because there's just no purpose for them. They should be turned off. They're used for tracking people around the 'Net. The other problem with the profiles generated by DoubleClick is that they only have visibility into me, as you said, Leo, for all the sites who are serving ads. They don't know anything about me for all the sites I go to that are not using DoubleClick ads. Well, except there are variations on that. For example, as we've seen when you go to PayPal, many PayPal links actually redirect you through DoubleClick. So there's another way that DoubleClick is able to access a user by actually using a redirected link.

Leo: Could you block it in other ways than by turning off third-party cookies? For instance, using a hosts file to say block DoubleClick?

Steve: Absolutely. That would null any of the ads which were being served because your

browsers looks in the hosts file first. It would not get the IP address for DoubleClick. The problem is that there are side effects, like none of the PayPal links would work. You couldn't click on a DoubleClick.net PayPal link because...

Leo: And as we know now, some of those links lead to pages you need to get to. They're not just to ads.

Steve: Right. And so it's a way of...

Leo: I think that's why they do that.

Steve: ...enforcing that not being done.

Leo: That's why they do that.

Steve: Okay. So now imagine...

Leo: I bet DoubleClick pays them. Now we understand why that DoubleClick referral is in there.

Steve: Well, there's even something worse. And that's called "cross-context leakage." But I'm going to leave that for the episode where we really get in and talk about first- and third-party cookies because it's possible for browsers that do not block outbound cookies, but only block inbound - and, by the way, that's IE and Safari - it's possible for them to receive a cookie in the first party and then subsequently leak it out through the third party, even when you've got third-party cookies disabled.

Leo: Sounds like a legal document. The party of the first part just leaving cookies that the party of the third part is going to get.

Steve: Okay. So now we understand, we've got some background for cookies. Now listen to what Phorm is doing. The only nice thing about DoubleClick is that they're relatively hands-off. They're not involved with the ISP. They have a relationship with the website that you go to. And they have sort of a forced relationship with your browser because they're putting cookies in there, and you're displaying their ads. But, you know, they're still - they're not nearly as invasive as what we're seeing now with this next new generation of advertisers.

So I'm a customer of an ISP using the Phorm system. I go to www.cnet.com. I put that URL into my browser and send a query out to the Internet. Well, my ISP receives it because that's what my ISP is there for. They're the way I get to the Internet. Equipment that has been installed by Phorm in the ISP's facility intercepts this query. And it looks to see whether my browser has a cookie that is in the CNET.com domain for something called WebWise. WebWise.net is the domain owned by Phorm. So WebWise - and if you look WebWise.net up in WhoIs, you'll see Phorm, Inc., in New York, NY, and the names

of the technical and administrative contacts for Phorm. So they're intercepting my bringing up a CNET page to see whether I have a CNET cookie that they planted in the CNET domain. Now, let's take this from the beginning. So initially I would not. If there's not, if I don't have a WebWise cookie in the CNET domain, they block my access to CNET. A server steps in and - get this, Leo - pretends to be CNET.

Leo: Oh, see, that should be completely prohibited, banned.

Steve: It pretends to be www.cnet.com...

Leo: Because it's a proxy, you can do that.

Steve: Well, it's in the ISP's facility. It answers the connection and this query that I've made.

Leo: If I were CNET I'd be - all right.

Steve: Oh, wait, we're just getting warmed up here. And so it responds as the CNET server and returns what's called a "307 temporary redirect." A 307 - normally when you bring up a web page you get a 200 response, 200 and, like, an okay, which is like, here's the page you asked for, no problem. A 307 response tells your browser that that URL you have asked for has been temporarily relocated to somewhere else. It tells it that it has been relocated to WebWise.net. So the CNET request you made comes back to your browser from this intercepting server, and your ISP is saying, oh, CNET is moved. It's now WebWise.net. And then there's a - then it says /bind/ and a question mark, and then some parameters which include the original URL at CNET that you were trying to access because they have to hold onto that since they've just intercepted you and redirected you.

So now your browser, not knowing anything the wiser, goes, oh, the page I want is moved. So it now makes a query to WebWise.net with this fancy thing on the end which contains the original CNET URL and parameters that you tried to access. The reason it does that is, if your browser has a WebWise.net cookie, that it will give it up. That is, that WebWise.net cookie that your browser has will then be sent along with this redirected query to WebWise.net. Once again, that's intercepted at the ISP, doesn't actually go to WebWise.net. Their server located at the ISP intercepts it and checks to see whether that redirection query contained a WebWise.net cookie. If so, they now know who you are. That is, there's a WebWise.net domain cookie on your machine if you've ever used this ISP before. So then they know who you are. If there's not a WebWise.net...

Leo: When you say "who you are," you don't just mean, oh, they've seen you in another session before. They know who you are, Steve Gibson, Leo Laporte. They know who you are.

Steve: Well, your ISP...

Leo: Because you're their customer.

Steve: Exactly. Your ISP knows everything about you.

Leo: Right. So they know where you live, they know your credit card number, they know who you are.

Steve: Right. Now, there can be and probably is a hands-on relationship between your ISP and the Phorm people.

Leo: I hope so.

Steve: But again...

Leo: But who knows?

Steve: That's the kind of thing that changes in the fine print of the license agreement. And then, oh, wait, you didn't read the license agreement? Okay. So now if there's not a WebWise cookie, which there would not be if you were just like, you know, Mr. Virgin, never used the Internet before, they would assign you one. That's a 128-bit pseudorandom value. So it's just a random token, but it uniquely identifies you to their system. So they respond to this, your access to WebWise.net, by again giving your browser a 307 temporary redirect response, this time back to CNET, to a special fake page at CNET. But since it's the WebWise.net pseudoserver which is serving you, if you didn't have a WebWise.net cookie, you do now. And notice that it's a first-party cookie because you went directly, your browser went to WebWise.net, requesting a resource from that URL. So it's a first-party, most privileged cookie which your browser has now received.

Leo: So unless you block all cookies, you've got it.

Steve: Yes. So now your browser receives another redirect, a 307, from WebWise.net, telling it, oh, we were wrong, CNET turns out to be where you want to go after all. Except it's another fake page at CNET. Now your browser re-requests a CNET.com address. Because of the way it's formatted, the technology, the Phorm technology again steps in, pretends to be CNET, fakes it out, and answers the query. In that fancy URL is still hanging on there for dear life the original URL you tried to go to at CNET. And encoded is the unique ID for WebWise in this query. That allows the server, which is again for the second time pretending to be CNET even though it's not, that allows it to obtain from your CNET query the WebWise UID, unique ID, and it sets a - this is where it sets a WebWise cookie in the CNET domain because your browser thinks it's at CNET. And a server has stood in and intercepted the CNET server and is faking it out.

So your browser, in getting the response back, back comes a WebWise cookie for the CNET domain containing your unique ID. And that response is another 307 temporary

redirect, finally, to the actual page you wanted to go to on CNET. So your browser receives that along with the WebWise.net cookie, which is now in the CNET domain, and makes the request to CNET. Now every time your browser brings up any CNET assets, it includes, in addition to any cookies, the real CNET cookies which CNET has given it; a WebWise cookie containing your Phorm unique ID.

And so all of the work you do on the 'Net, any time your browser is making a query, there's this spy server that checks to query to see if the query contains for that domain, no matter where you're going, Apple.com, CNET, CNN, MSNBC, TWiT.tv, no matter where you go, what's happened is essentially every single site you visit is given an extra cookie. So your browser ends up filled with these WebWise cookies for every single domain you visit. And those are first-party cookies. And any query you make outbound is checked for the presence of one of these WebWise.net cookies. If it's missing, it sends you on that multiple server dance, the triple 307 temporary redirect dance, jumping you around between fake servers in order to get your WebWise cookie, in order that it can essentially migrate that over from the WebWise.net domain into the domain you're attempting to go to.

Leo: So is the whole process, the intent of the whole process just to get these cookies, these WebWise cookies on your system for every site you visit?

Steve: Yes. That's the whole...

Leo: That's why they're doing this dance.

Steve: That's what these people have achieved with this horrible...

Leo: And a first-party cookie, to boot.

Steve: First-party cookie planted in the domain of every domain you visit, and one in the WebWise.net domain which is essentially replicated among all the other domains that your browser ever visits.

Leo: With your unique ID.

Steve: With your unique ID. Now, imagine a couple things.

Leo: Now, I just - I want to say something because there's some confusion in the chatroom because you used CNET as an example. CNET has nothing to do with this. No site you visit has anything to do with this. This is Phorm doing this.

Steve: Yes. In fact...

Leo: In fact, I'm sure CNET would hate this.

Steve: Well, yes, because your relationship with them is being polluted by a cookie that they never set for your browser and that someone else's server is pretending to be them, giving your browser multiple redirection commands, bouncing it around URL space for the purpose of planting cookies across all the domains you visit.

Leo: Now, there are some companies that do want this because there's no value in doing this unless you can sell this information to an advertiser.

Steve: Well, okay. So notice that what this does - okay. The other thing happening. So now imagine a query to CNET that does contain the WebWise cookie, as it will after this three-redirect dance that your browser is taken on. So now finally the result of that final third redirect is you actually - the browser is allowed to contact CNET. In the process, this system removes the WebWise cookie component from the query. So CNET does not see the WebWise cookie that is essentially - they're trying to corral it so it only stays between you and the ISP in sort of an ISP, you and ISP private dialogue. So they do remove the WebWise cookie if they can. When can't they? Well, if I take my laptop to Starbucks, and I'm on T-Mobile...

Leo: You're not using their ISP.

Steve: I'm not using my ISP at home that was the source of this infection. So every site I visit cannot have that WebWise cookie stripped out on the fly. It goes out. And so this ID that I've been assigned is visible to every site that I visit. And that's a common ID. Normally sites give you their own ID per site. There's no aggregation. This aggregates your identity across all the sites that you might visit because your browser has been polluted with a common cookie for every domain you've visited while you were under the influence of this Phorm-based ISP. The other instance where they are unable to strip out their cookie is over secure connection because they're not, at this point in the game - and god help us if our ISPs ever start requiring us to accept an SSL certificate as part of our agreement to use the ISP because that would allow them to intercept our secure socket connections. But at this point the whole system is blind to any secure conversations we have, any secure traffic. So any time I am using HTTPS, I am bypassing, even from my ISP, my Phorm-ridden ISP, I am bypassing that technology, and the WebWise cookie again is leaking out and is visible to any sites I'm visiting over a secure connection because there's no way that the Phorm system can filter SSL connections at this point.

Leo: So again, to underscore this, this isn't CNET doing anything. This isn't TWiT.tv doing anything. This is your ISP in collaboration with Phorm doing something to essentially track what you're doing on the Internet.

Steve: Yes. A highly comprehensive, cross-Internet tracking.

Leo: It goes far beyond anything third-party cookies ever could do.

Steve: Oh, yeah. Well, because, now, look what else happens. So finally my request to the real CNN page gets through because it's been - it's had this WebWise cookie embedded in the domain that my browser is carrying. When the page comes back, this system inspects the page. This system reads the page that is being sent back to me and does an analysis of it to determine what I'm interested in. So it's reading - this is where the spying really comes in, beyond identity tagging. Now it's reading everything I'm reading and building a profile of who I am and associating it with this tag which it has built up. And over time it builds a database of it knows every page that I go to. They say they are not maintaining a record of that. What they're doing is they're scanning the page, doing some sort of semantic analysis, determining within categories, they say they have over a thousand...

Leo: They're looking for keywords.

Steve: Yeah. Well, they have a thousand categories. And so they, like, put checkmarks in categories for people of, like, oh, this person is interested in the following sorts of things, based on their history of their Internet usage.

Leo: But that's not what this is limited to. They could do more. That just happens to be what they say they're doing.

Steve: Well, and there again, I mean, this notion of inserting themselves in the pipeline means, well, wouldn't it be more valuable if I could also read this person's email coming and going between the ISP? You know, web, oh, that's, you know, that's really not as specific because these are those pages that have been pre-prepared. Imagine if I could read the email content of the conversations. And oh, don't worry, we're not going to save it. We're not going to keep it. We're just going to scan and analyze it, determine more about who you are.

So one of the things that's different about this from DoubleClick is the level of visibility. That is, say that only one, only one company hosted ads from Phorm. Well, that one company has the advantage of all of your surfing. That is, the ad being served is about you, even if only one, only if you go to one place. Whereas DoubleClick needs to - it's only able to build up a profile based on the places you go. This system builds a profile based on everywhere you go and makes that available to any of the people who are using their ad network for advertising revenue.

Leo: Is any Internet Service Provider in the U.S. currently using Phorm?

Steve: I don't know. The hope is...

Leo: Nobody would admit to it, probably.

Steve: Well, I mean, this has now become a real hot potato. Our guest in two weeks is going to give us the inside skinny on what's been going on over in the U.K.

Leo: It's illegal in the U.K., isn't it?

Steve: Well, I mean, there are people who are really up in arms. And I'm glad. I mean, again, my role is to explain what this thing does, what the technology is. There can certainly be people who say, well, wow, I like the idea of more relevant ads. Or I like the idea of...

Leo: Well, that's the other side of this, which I was going to get into; but we've gone way over, so I don't want to get into it too much. And that's the case that, for instance, Charter was making, is all it does is give you ads about stuff you care about. What's wrong with that?

Steve: Right.

Leo: I mean, we're not trying to steal your personal information. I guess your point is that the technology could do that.

Steve: The technology could. And I'm concerned about drift and migration of capability.

Leo: Right.

Steve: I would have no problem, for example, if this was an opt-in system. If you had to go to your ISP's page or a Phorm page and say hey, I'd like a $3 a month discount on my bandwidth, please. I'm happy to contribute my profiling habits on behalf of this technology in return for a discount on my bandwidth. I mean, if it were an opt-in system, that makes sense. I love that the language I read somewhere said, well, the reason we made it opt-out is that we feel that more people will be able to benefit from it than an opt-in system. What happens, of course, is that people are furious when they find out that this kind of game is being played.

Leo: Yeah, well, I'm furious already, and I'm really glad that you actually raised the issue and talked about this because this is pretty appalling. But as you say, it's not necessarily how it's used. And I think that this is why people like Charter are kind of surprised when we stand up on our hind legs and say, well, wait a minute, we don't want that.

Steve: Yeah, this is not for us, this is for them. This is for Charter. Charter is getting [indiscernible]...

Leo: Benefit to them, yes.

Steve: ...from Phorm in return for letting Phorm profile us.

Leo: But their spin was totally this is to your benefit because you're going to get ads that are more targeted at you.

Steve: And my feeling is, fine, make it opt-in.

Leo: Yeah. Simple.

Steve: Intercept the first time I try to go to the 'Net. I mean, they have the capability of intercepting, you know, god himself. So the first time I go to the Internet, my access to CNET.com is blocked, and I get this wacky page, I go what the heck is this. And it says, hey there, we're offering a new service that will allow advertising by selected advertisers on websites to target you and serve you ads that are more specific, blah blah blah. So, I mean...

Leo: I got a big bulls-eye pointed on my forehead, that's what they mean.

Steve: Entirely possible for them to make it an opt-in where...

Leo: Well, I love the idea they can say we'll cut five bucks off your bill every month. They're going to make a hundred bucks. But, you know, give me some.

Steve: And I guarantee you a lot of people would say heck, yeah, I don't care about privacy, I care about my wallet. And so I don't mind that.

Leo: And we should really underscore that we are at the mercy of our ISP anyway. I mean, they see everything we do. If they you know, the FBI put boxes in every Internet Service Provider's center years ago.

Steve: In order to scan email.

Leo: Yeah. So the Internet Service Provider has all this information; right?

Steve: Yup.

Leo: All right. I'm not going to get angry, and I'm going to keep my blood pressure down. Steve, thank you so much. What a great show. It was a lot of fun. Fun. I mean fun in the sense that we get to really understand, as usual on this program, a very deep and a difficult topic. You've done a great job of explaining it and of raising our awareness about it, too.

Steve: I just - it's horrific what these guys have done.

Leo: And, you know, I don't think there's any - there's no mainstream media outlet anywhere that can explain how this works. And this is where we're really, I think, increasingly in a situation where technology has outpaced the general public's ability to understand what's being done to them. And I think we're doing a very important job getting the word out. Now, all the geeks who are listening who understand this, now you need to figure out a way to explain it to your friends and family and to stand up to your Internet Service Providers and let them know this is not something we want.

Steve: Yeah. The good news is there does seem to be a lot of outrage that this is causing. It's certainly causing the ISPs to back off and, you know, rethink that this is - oh, look, it's free money. No.

Leo: Right. It isn't free money. We're going to get the money out of them in one way or the other. Make them let us have the choice, I guess is the idea. Hey, if you want 16KB versions of this show - I know some people say, oh, the audio quality's good, but it's big, I'm on dialup. We have listeners all over the world, many of whom don't have the high speed that you might want for the large version. We do have a small version. It's available at Steve's site, GRC.com. You can go there and download that. He also has transcripts. And I think on a show like this it's very helpful to be able to read along as Steve's talking. You can find transcripts, the 16KB version, complete show notes, and of course SpinRite, Steve's bread and butter, his ultimate disk recovery and maintenance utility. It's all at GRC.com. And Wizmo, too. How would you find Wizmo? You just go to the front page there, Steve, is that...

Steve: Yeah, GRC has now a really nice sitewide menu, you may remember, that does not use any scripting. And so under - I'm not even sure where it is now. But it's right there under the top-level menu, under freeware and utilities, is Wizmo. And that'll get you there. And I'll remind people who are inspired to send in a question or write for next week's Q&A, by all means, please do, GRC.com/feedback. And I will read your stuff, and we'll do 12 questions next week.

Leo: That'll be a lot of fun. And that way we get a little more variety. We've spent a lot of time with Phorm. And we're not done with this topic, I think.

Steve: Nope. I think, well, clearly people are passionate enough. I think it'll be fun to talk with a Phorm world insider who has been, I mean, who is rapidly anti-Phorm. We're going to do that in two weeks.

Leo: Good. All right, Steve Gibson. Thank you very much. Thank you all for being here. A little side note, you can also watch us do this show live if you're so inclined. We record on Tuesdays at 11:00 a.m. Pacific - that's 2:00 p.m. Eastern time, or 18:00 UTC - at TWiTLive.tv. And everybody was saying, Steve, in the chatroom, as you were talking, they loved watching you because you gesticulate with your hands. They said it's actually easier to understand Steve because you can see his thought

process. You can see how he's working. And they really enjoyed it. So I thank you for allowing us to do the video. I think it's really great. They want to know if you're Italian.

Steve: We figured out - there is some Italian in there, yeah. We figured out a way to do video and audio both over separate Skype channels.

Leo: And the audio quality is great. We're back to our usual audio quality. I think that's really what's most important, yeah, because most people listen to it in audio. But, you know, there are around 3,000 people who are watching and enjoying your performance, your bravissimo performance every Tuesday on TWiTLive.tv. Thank you, Steve. We'll talk to you again next week.

Steve: Thanks, Leo.