Why Pervasive Monitoring Is Bad

Stephen Farrell • *Trinity College Dublin*

Since June 2013, we've seen numerous revelations about hugely intrusive Internet surveillance, a significant subset of which involves what we call *pervasive monitoring* (PM). Many in the Internet community, myself included, consider this a serious abuse, one that doesn't just threaten users' privacy, but also affects important freedoms and public and private enterprise on the Internet. In this column, I describe why I think PM is bad. Work to mitigate PM is ongoing in various places, but is out of this column's scope.

What PM Is and Is Not

PM isn't a targeted attack. Listening to the German chancellor's phone isn't PM, and I don't deal with that here. But although targeted attacks aren't PM, targeted attack techniques can be used to set PM up — for example, by breaking into a specific switch so a bad actor can later exfiltrate user credentials, keys, application data, or metadata. Interestingly, those who discover that they've been the target of such surveillance appear to react with outrage (real or feigned). My guess is that this would be the same for the general population — if shown that their specific communications have been recorded without permission, people are likely to be as outraged as the German chancellor. On the other hand, most people don't seem to be outraged by PM if they believe they're unaffected. To me, this indicates that a prerequisite for "successful PM" is secrecy. But at scale, we see that secrecy hasn't, in fact, been maintained, so arguing for PM seems foolish unless you go as far as arguing that all information should be published always.

Even from the narrow perspective of an organization allergic to taking positions on topics such as this, the IETF has documented its consensus in RFC 7258[1] that PM represents an attack that should be mitigated during Internet protocol design. (As an author of that document, I should say that although the IETF has reached consensus on its content, this article goes well beyond areas in which the IETF does or should take positions, and is purely personal. And because that document has been the subject of extended debate in the IETF community, I won't repeat its arguments. I'd encourage you to read it, though; it's short but defines PM better than I can here, and describes purely technical reasons why it ought to be mitigated.)

Before considering why PM causes harm, we should first dispel a couple of falsehoods that have promulgated. PM involves gathering information; once a copy is made for possible later review (even if only temporarily), then the information has been recorded, and surveillance of the sender and intended recipients has occurred. The idea that surveillance happens only when someone looks at the information is simply wrong, akin to saying that an oncoming train won't hit me because I've covered my eyes. Similarly, the idea that recording metadata isn't surveillance is at best misinformed and at worst disingenuous. Indeed, a PM system recording the fact that someone makes a DNS query for example .com at some time and place is obviously surveillance — as is any similar recording of other metadata — because it reveals significant information about user behavior. Once such data is recorded, it's vulnerable to future examination, as are those involved, regardless of whether the data has yet been examined or whether audio content — from a VoIP call, for example — has also been recorded.

Direct Damage

Moving on from correcting misconceptions to its other harms, PM creates a chilling effect — if you're conscious that everything you're doing is being recorded for unknown purposes by unknown entities, as appears to be the goal of those conducting PM, then you'll self-censor.[2] Such self-censorship is damaging and threatens a fundamental benefit of the Internet — its ability to enable people anywhere to communicate with one another in whatever manner

1089-7801/14/$31.00 © 2014 IEEE

those people consider sufficiently private. This actually follows from the end-to-end argument — we should not have to depend on network internals for our privacy. This argument also shows another way in which PM is inherently damaging. If we accept that innovation at the network edges is a beneficial consequence of the end-to-end argument, then requiring that the network can usefully (for the bad actor) record communications puts a straitjacket on innovation because endpoints can communicate only in ways that allow PM.

PM also requires signals intelligence agencies to undermine everyone's security (as with the NSA's "BULLRUN" program[3]), including that of their "customers." This stupendous waste (reportedly US$250 million per year!) seems so single-mindedly short-sighted and stupid that it can be hard to pick apart exactly why it is so bad. First is the obvious problem that damaging Internet security is damaging to everyone who uses the Internet, friend and "foe" alike. Less obviously, this practice feeds a market for exploits (you need them to keep coming in all the time), likely resulting in many more dangerous ones both arising and remaining secret than would otherwise be the case. If signals intelligence agencies feed this market for zero-day exploits, then even if those agencies reform, the market will continue and will find new customers. Sellers also have no real incentive to sell items only once, and are probably not people to whom we would want to entrust such dangerous tools.

The dual mandate of some signals intelligence agencies is also problematic — if part of their mission is (supposedly) to defend their own stakeholders from attack, BULLRUN and creating a market for exploits seem hugely counterproductive unless we assume that somehow exploits will remain secret, which isn't the case. Often, once these tools are used on the Internet, then the tool itself is exposed, and others can and will copy it. Even patching systems to protect against exploits can expose the vulnerability, allowing many people to reverse engineer the exploit. This kind of "weapon" is one where as soon as you fire it, you hand your enemy the blueprints for making their own — truly, a foot-gun.

No matter how highly you think of any one bad actor (and those doing PM are bad actors, even if they don't believe so), there are always other, equally capable bad actors about whom you'll have a very low opinion. And these will compete at PM, which creates a vicious cycle of increasingly intrusive technologies that will, with probability 1.0, be used for repression somewhere in the world. Those doing PM or developing PM technologies are contributing directly to such repression no matter how they justify their own actions.

Collateral Damage

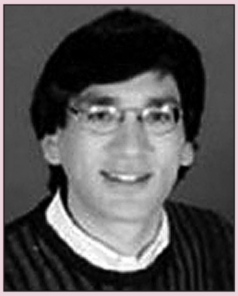
PM represents a perversion of the network — that is, it causes the network to do something (surveillance) for which it wasn't intended and which isn't openly described. Those who design applications and network technologies

Technical cosponsor:
IEEE COMMUNICATIONS SOCIETY

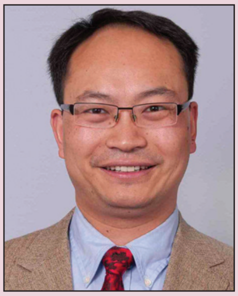
IEEE Internet Computing
IEEE Computer Society Publications Office
10662 Los Vaqueros Circle
Los Alamitos, CA 90720 USA

Editorial. Unless otherwise stated, bylined articles, as well as product and service descriptions, reflect the author's or firm's opinion. Inclusion in *IEEE Internet Computing* does not necessarily constitute endorsement by IEEE or the IEEE Computer Society. All submissions are subject to editing for style, clarity, and length.
Submissions. For detailed instructions, see the author guidelines (www.computer.org/internet/author.htm) or log onto *IEEE Internet Computing*'s author center at ScholarOne (https://mc.manuscriptcentral.com/cs-ieee). Articles are peer reviewed for technical merit.
Letters to the Editors. Email lead editor Linda World, lworld@computer.org
On the Web. www.computer.org/internet/.
Subscribe. Visit www.computer.org/subscribe/.
Subscription Change of Address. Send requests to address.change@ieee.org.
Missing or Damaged Copies. Contact help@computer.org.
To Order Article Reprints. Email internet@computer.org or fax +1 714 821 4010.
IEEE prohibits discrimination, harassment, and bullying. For more information, visit www.ieee.org/web/aboutus/whatis/policies/p9-26.html.

IC Welcomes New Editorial Board Members



Arun Iyengar does research, development, and consulting in distributed computing, fault tolerance, and Web performance at IBM's T.J. Watson Research Center. His caching and load balancing techniques are widely used to improve performance for websites and distributed applications, and he's developed widely used techniques for dynamically generating Web content that have been incorporated into Web content management systems. Iyengar received a PhD in computer science from the Massachusetts Institute of Technology. He is founding coeditor in chief of *ACM Transactions on the Web*, chair of IFIP Working Group 6.4 on Internet Applications Engineering, and a founding executive committee member and former chair of the IEEE Computer Society Technical Committee on the Internet. He is a fellow of IEEE.



Weisong Shi is a professor of computer science at Wayne State University, where he directs the Mobile and Internet Systems Laboratory (MIST) and codirects the Laboratory of Sustainable Computing (LaST) and the Wayne Wireless Health Initiative, investigating performance, trust, power- and energy-efficiency issues of networked computer systems and applications. Shi received a PhD in computer engineering from the Chinese Academy of Sciences. He is chair of the IEEE Computer Society Technical Committee on the Internet, and serves on the editorial board of *Elsevier Sustainable Computing*, the *Journal of Computer Science and Technology*, and the *International Journal of Sensor Networks*. He is a senior member of IEEE and ACM, and a member of Usenix.

are thus forced to deal with a network that's doing something radically different from what it says on the box, which will cause collateral damage. I wouldn't be surprised if some critical system running over the Internet fails badly because of design, implementation, or deployment issues with a PM system. I would guess that this has already happened. We know that adding any new component to a complex system will often cause failures; I see no reason why attempts to secretly inject the complex systems required for PM would be anything but more problematic.

State actors doing PM also bolster the privacy-unfriendly actions of commercial entities in at least a couple of ways. They might, via public or secret administrative or legislative actions, compel commercial entities to retain data that those entities would otherwise discard. Some of those entities will inevitably use such data for privacy-unfriendly purposes. Why would a profit-seeking company not use such an asset? Even if some wouldn't, and really mean it when they say that they "take privacy seriously," it's hard to see how they could resist increasing profits in the long term (such profits accruing from marketing and customer profiling). In addition, the knowledge that state actors are doing PM provides "cover" for commercial entities who in fact don't "take privacy seriously" (no matter how often they repeat the phrase), in that they can quite reasonably argue that what they're doing is nothing compared to what governments do.

BULLRUN also does more subtle damage to the Internet in that a non-negilgible number of people involved in Internet security are worried that colleagues might have (wittingly or not) been helping the BULLRUN agenda. Quite likely, this is truly the case, but it's equally true that a lot of people who have worked with or for signals intelligence agencies have in fact done really good, honest work. And those people are now unfairly viewed as tainted — basically, it's guilt by association. I personally know some people who feel this and who have self-censored where they see a potential for accusations that they are in league with, for example, the NSA.

But assigning that kind of guilt by association is wrong, even in the face of a demonstrated conspiracy to damage the common good that Internet security represents. Why? Well, we should recognize that the guilt-by-association fallacy is in part what leads governments to conduct PM — they wrongly conclude that everyone in even indirect contact with a suspect is themselves suspect. We shouldn't fall for this bad logic and conclude that everyone who works for a signals intelligence agency is a bad actor.

In fact, this issue isn't new: in standards fora, we deal with similar issues with commercial entities all the time: "Is this person saying this because it's technically correct or only because they will make more money from it?" Our defense in such cases remains the best answer here, too — we should require that Internet technologies be developed as openly as possible and also be openly scrutinized to determine if they are fit for purpose. Given that this is our best defense, an immediate consequence is that we must take people at face value and ensure that their technical contributions are properly scrutinized and treated on their merits. This technical scrutiny will, of course, need to consider the new information we have about the overall threat landscape.

My conclusion is that the case against PM is simply overwhelming, and those of us involved in developing Internet technologies of whatever sort should consider how we can each work to make PM harder, so that when and if societies reach agreement on the damage from PM, we'll have sufficiently usable and easily available tools to mitigate that damage. I hope you agree.

References

1. S. Farrell and H. Tschofenig, *Pervasive Monitoring Is an Attack*, IETF RFC 7258, May 2014; https://tools.ietf.org/html/rfc7258.
2. *Chilling Effects: NSA Surveillance Drives US Writers to Self-Censor*, tech. report, Pen American Center, 12 Nov. 2013; www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf.
3. J. Ball, J. Borger, and G. Greenwald, "Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security," *The Guardian*, 5 Sept. 2013; www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

Stephen Farrell is a research fellow at Trinity College Dublin and one of two IETF security area directors. His research interests include security and delay/disruption-tolerant networking. Farrell has a PhD in computer science from Trinity College Dublin. Contact him at stephen.farrell@cs.tcd.ie.

Selected CS articles and columns are also available for free at http://ComputingNow.computer.org.