The IETF and pervasive monitoring in a post-Snowden Internet

Internet security is a perennial issue, and one that the Internet Engineering Task Force (IETF) has always pursued as a major concern. But the revelations from Edward Snowden about pervasive monitoring by the NSA and other agencies have rocked the Internet community and thrown a sharper focus on the IETF’s security work. Jari Arkko, chair of the IETF, spoke to Netnod recently about the IETF’s response to pervasive monitoring and how that response fits within the broader context of the IETF’s history and current work. As disturbing as these revelations have been, do they change in any fundamental way the mission of the IETF? And can we even see this current turmoil as an opportunity for progress?

[Note: A condensed version of this longer discussion was included in the Netnod News magazine in Spring 2014]

The Edward Snowden revelations about pervasive monitoring by the NSA and other agencies have rocked the Internet community. You have said “My vision of the end goal is that we try to build a more secure Internet based on the assumption that there are all these threats around us”. How do we get there from here?

The first step in getting somewhere is to realise that you have a problem and, of course, I want to emphasise here that there are many threats to the Internet and this is one of them. We at the IETF have been for years trying to improve the security of the Internet in various ways. But last year’s revelations point to a changed model of how we view what kinds of vulnerabilities there are and what kinds of attacks are possible. And that of course has an impact on what we can do and what we should do.

You wrote on your blog in November that the current IETF audit of all applications for vulnerability to pervasive monitoring is "not a reaction to specific revelations, but a wholesale upgrade to our view [of] what the threats in the Internet are and how they need to be addressed". I guess that’s what you’re pointing to there, but can you elaborate on that?

Yes, so again, it’s not to make a response to a particular threat – even though it’s significant – but to start to understand that [for] all the different applications and aspects of Internet technology that we have, what can we do for those different things to make them more secure? A while ago, I said that in some sense the surveillance revelations were a wake up call. Now, we’ve been working on security for a long time,
but the wake up call is more about how broad the kinds of dangers really are. Since you know we try to improve the technology, and of course technology improvements are just one aspect of the overall security situation, so we try to do our part, but technology doesn’t all questions. But we certainly try to improve the technology.

**Can you even guess at how long that application-by-application process of “strengthening the Internet” could take?**

It will take forever, because we will be doing it continuously. And obviously some aspects we are looking at in a prioritised manner so at the IETF we created this new working group that is looking at how to apply TLS for various applications – the UTA, or Using TLS for Applications Working Group – so that’s going to address some of the things like email, using TLS for email, and what can we do with TLS and instant messaging. We’re also looking at web traffic – what can we do there? – and we’re looking at improvement in DNS and how we can make that confidentiality friendly and how can we improve some of the basic protocols like TCP, that’s been one question. Can we provide some security technology there?

**You mentioned the UTA Working Group. How far will TLS and HTTP updates go towards improving the situation, and what issues will these not fix?**

The HTTP work, which is nearing completion, and the TLS work, which I hope will complete this year, they are short term updates, or they are steps along the path. And they are important, but they are not the only thing that is needed. So the technology development is one thing at the IETF, but even more important is what’s happening out there in the real world. What are service providers doing and what kinds of technology are they adopting? There is a trend, and it has been going on for a couple of years already, and it started even before the Snowden revelations, of turning on more security for web traffic – TLS, HTTPS – and that seems to be continuing and now many service providers are doing that and that’s a key result. We at the IETF try to improve the technology itself, but that’s still one step. Turning things on by the service provider is one step. Us improving the technology is another step. But going even further, I think that it will be required for things like email. Obviously, we can do certain things with email security like, from my client to the server, but end-to-end security for email, for instance, is a difficult thing and it would not be helped by TLS.

**You’ve also said before that even if the security benefits of things like HTTP 2.0 aren’t enough to convince operators, the actual performance improvements in that protocol might push deployment. Does the IETF need to be more engaged in standards promotion?**

I’d like to respond to that by saying that our mode of operation has always been voluntary adoption. So we don’t try to convince people that you should use or must use standards. The good standards sell themselves. That’s what we will try to do here as well. Both HTTP 2.0 and TLS 1.3 are major projects ongoing. They have some aspects which are not security related and they have some security related aspects as
well. Depending on who you are and what your situation is, you may be preferring to switch to the new technology because of these different aspects. For some people it might be that it’s a little bit faster to set up. For some others, it might be that it’s more secure.

I don’t see it as our role. Of course we have to speak about the technology, but it’s not in my mind so critical to market the technology. It’s far more critical that we do something that responds to the needs of the users and operators.

Bruce Schneier has argued for approaches that make widespread surveillance administratively and economically unattractive. Does that strategy fit with the current IETF priorities?

I think it does. So one of the things that we are doing, both the community and at large, is turning security more on – encryption for instance, is turned on more widely. And we’re trying to, obviously, encourage that, but also build tools that make it possible more easily. A small example of that is that maybe TLS 1.3 will have a slightly quicker set-up time because of less round trips and this will lead to a situation where it’s perhaps more acceptable to a wider range of operators. So I think it does fit Bruce’s overall strategies quite well.

The current guidelines for RFCs require a section on security considerations, but that is frequently a short paragraph at the end of the document that almost looks like an afterthought. Does this requirement need new emphasis?

Well, I think I would pay not so much attention to the existence of the section itself, but rather what the content is. I think the surveillance revelations and the discussions surrounding them have certainly put this into the mindset of all the IETF participants so I think that alone will have an effect on how they think about their technologies or new things they are developing or how they write these sections.

Now, we’ve had a discussion of how we view the surveillance – or this “pervasive monitoring”, as we like to call it – and it’s been said that it is a vulnerability that needs work to address. Whatever we do, we need to have an opinion about how this is affected by possible pervasive monitoring. It’s not a special class of vulnerability or a special class of situation, but it’s one of those many things that we looked at.

We recently approved an RFC that says that you actually have to – for any new thing that you develop – you have to have an explanation of what is the relationship of this work to pervasive surveillance. How does it take into account these worries? And you don’t have to have a particular answer. It might be that for some aspects of technology, pervasive surveillance is not an issue at all, or is something that can’t be dealt with. But you have to have done the leg work and have done the analysis, just like we already do for many other things.
You mentioned before about the work that’s required on email and how that’s in some ways a bit more complex. Now, SSL on websites asks basically nothing of the end user. But today encrypted email remains complex and messy, even for relatively advanced users. Is there any need in the IETF for a cultural shift that better recognises the realities of the non-technical community?

Absolutely it's required, and I think it is recognised. We recognise the situation, for instance, with regards to end-to-end email protection. It works quite well with current systems in enterprise environments, as an example, but it works much less well in the global Internet. It's been recognised that that's an issue. I don't think that the recognition itself is a problem, but it's a question of what are the technical means that could overcome these challenges -- and that's a big question.

You've also mentioned a few times in presentations and blog posts about moves for "opportunistic keying". Can you explain very briefly how that works?

Right, so that's still a hot debate. So in the IETF meeting that we just had a week ago in London, we had a workshop between the IAB and the W3C -- a very well-attended workshop by the way. The STRINT workshop. During the workshop, we split into different groups and one of the groups focussed on opportunistic keying. That is still seen as something very desirable, but at the same time, somewhat challenging. So some of the earlier discussion that we had on this topic last year focussed on, you know, if you turned on opportunistic keying and there was no guarantee of the identity of the other sides, you would not authenticate the other side and that would be confusing to users. Now I think this year we've realised that if we do something like that, then it has to be invisible to the user. We're doing something security-wise, but we hide it from the user, at least in terms of browser user interface: you would not see a key-lock on your screen because you're using opportunistic keying underneath. It might still help against pervasive monitoring, but it's not a guarantee that you are talking to the right party here. The use of HTTPS in the usual authenticated mode remains the best option for securing web traffic today.

The STRINT workshop goals for London noted the baseline assumption that pervasive monitoring is an attack, but that "dissenting voices are expected and need to be heard". Were there any dissenting voices?

We've certainly had lots of discussion about that at the IETF when we approved the BCP that says pervasive monitoring is a threat that we need to consider. When we made that decision at the STRINT workshop itself, we did not really have a lot of discussion of that. We really focussed mostly on how can we improve things. That, I think, is the current mindset at the IETF. Now, securing the Internet is obviously not trivial, otherwise it would already have been done. But we are really focussed on the small or larger things that we can do.

I guess I was just wondering on what a potential dissenting voice might have dissented on, on that point.
The IETF discussion focused on a couple of different things. One of them was "do we have enough guidance to say that we need to do something?", for example. We don’t yet know how to deal with this in different areas. One example of that would be opportunistic encryption, I think. It’s potentially desirable, but we can immediately recommend today? So the statements are somewhat high level at this moment.

You have said previously that the surprise in the Snowden revelations was not the existence of governmental surveillance, but rather the "scale and some of the tactics". In your view, what are the most troubling tactics revealed so far?

Since we work at the standardisation forums, one critical thing for us, of course, has been whether there has been – as claimed – there has been some influence by the intelligence organisations on standards. We obviously take that very seriously and while we’ve heard of complaints in some other standards organisations, I don’t at the moment believe that we have cases like that in the IETF standards. This is not to say that we have no problems in our standards. Our standards have many problems. Again, Internet security is hard, and we work on improving it.

On that topic, there has been a controversy around an NSA employee co-chairing the Crypto Forum Research Group (CFRG). Without going into that specific case, in an open, trust-based organisation like the IETF, how do you deal with people who don’t come to the party in good faith?

We have to understand that it’s a more general concern. It’s not just about the surveillance incident...

Yes, and I’m asking in the general sense as well, from a corporate interest position as well as a government one.

Right, and people are different, even in different organisations. Some of them might have commercial interests; some of them might have other interests, like this case shows. But the way that we deal with that, is that in all of the situations that we have open participation and broad input on any topic. So when we have broad review of cryptographic standards, for instance, or selection of some security technology then that’s our best chance of combatting any undue influence, whether it’s commercial or personal or governmental. And that’s the way – rather than trying to block particular persons or particular organisations from the work, make sure that we have enough broad participation, many people commenting on the topic. Then we can be more certain that the results are good.

Changing direction a little bit, what was your reaction to the recent NTIA announcement about relinquishing control of the DNS?

Right – and I think that actually, despite the text that is in the announcement, they actually do talk about not just DNS, but about addresses and protocol parameters as
well. All those are in the same contract. I think that the reaction from the different Internet organisations has been fairly positive. We see this as part of the evolution that has been going on around IANA for a long time. The Internet organisations, I think, are strong enough to handle these functions and our communities are broad enough to deal with any issues there. So this is a step in the evolution path, and its a good step.

Finally, Edward Snowden’s leaks have unleashed a metaphoric avalanche on your workload, but I believe you recently found yourself in a literal avalanche. What’s worse? Obviously the actual avalanche was a great danger...

I guess that’s over quickly though. It is over quickly. But from the perspective of Internet work, the Snowden revelations and everything else that’s going on, I don’t take it negatively. I think these are opportunities for us to do better for the Internet. That’s a very good thing. I see a lot of very constructive, good work in IETF and elsewhere. I think it’s a happy thing, improving the security of the Internet, even if you learn of some new issues.

Is there anything else you would like to add?

One more thing. I just wanted to reemphasise that this is not a single event. It’s something that has been going on a long time – improving the security of the Internet. And even the intelligence agencies were previously involved in some similar discussions. In the late ‘90s, early 2000s we had a discussion on whether to use encryption technology at all or whether to use weak or strong encryption. At the time, some countries and some intelligence agencies were of the opinion that those technologies should be limited. But the Internet community chose to do strong encryption and they chose to use encryption to begin with and I think that’s the basis of things like e-commerce today. It was obviously the right decision at the time. And last year’s and this year’s discussions are just another similar situation. We just have to make sure that we have the communications tools that we need for all our tasks.