IETF Technical Plenary Session
3 March 2014
London, England

Transcript provided by Brewer & Darrenougue
Corrections provided by Cindy Morgan and Dave Thaler

--BEGIN TRANSCRIPT--

>> RUSS HOUSLEY: Welcome to the London IETF. I hope you've had a good first day.

First thing I'd like to share with you is the change in membership for the IAB. We have four outgoing members of the IAB that I just called to the stage a minute ago. We have a plaque to present to each of them. So we'll start with that. Bernard, you're first. Alphabetical.

>> Thank you.

>> RUSS HOUSLEY: In addition to the plaque, the IAB members have gotten together to get you a little something. You've got a bag to help you get it all.

[Applause; plaque and gift bag presented to Bernard Aboba.]

>>RUSS HOUSLEY: Now, Ross Callon.

[Applause; plaque and gift bag presented to Ross Callon.]

>>RUSS HOUSLEY: Next is Alissa.

[Applause; plaque and gift bag presented to Alissa Cooper.]

>>RUSS HOUSLEY: Thank you so much. And, finally, Hannes. And your gift from all of us.

[Applause; plaque and gift bag presented to Hannes Tschofenig.]

>>RUSS HOUSLEY: Incoming we have four members -- Mary, Ted, Joe, and Brian. You'll get to meet them at the end at the open mic. And of the people who were up this year that are continuing is Marc and Eliot. And Eliot was getting a one-year term. The one-year term is because Alissa had to resign because of the job she's taking on Wednesday, as the RAI area director.

Few things that have gone on since we were last together. The IAB

issued a statement on the draft-farrell-perpass-attack document. Two RFCs were published on the IAB stream, one about the list of the official protocol standards. Basically, every 100 RFCs, we were publishing an RFC that listed the official standards. And we've replaced that with a web page. And we published one on Architectural Considerations of IP Anycast.

We were asked to appoint two people to the ICANN Technical Liaison Group, which is a group that existed for a while and then went dormant and is being revitalized. So we went through a process for nominations from the community. We set this up assuming it was going to not go back in hibernation. So we need two people for that. So we selected one, that's Daniel [Migault] for the one-year term and Warren [Kumari] for two-year term. And next year we'll replace one of them or at least go through the process to seat one of them.

Finally, the I* leaders had a meeting in Santa Monica. And out of that meeting a statement was issued that was signed by the CEO or chair of each of those organizations. The link is on the slide, if you download it from the site.

The IAB has approved starting the assignment of digital object identifiers for each RFC. We were going to assign them to the old ones and to the ones in the future. There's an example of what one might look like on the slide.

And, finally, the draft-iab-doi is a document that describes how this is going on. Basically, what's in it now is the motivation. As the mechanisms get figured out, that document will be updated as we go along.

These are the documents that the IAB is working on right now. I'm not going to run down the list, but you can see the ones and what status they are in. The only one that is kind of different than the normal IAB document is the first one because we're working with the IESG for that one to become a BCP.

We did have an appeal this go. There will be more of this in Lars' report. But I, basically, say here at the end of the appeal, the IAB chose to take no action.

We have an ongoing appointment right now. We have a call for ISOC Board of Trustees. We sent out a first call. We sent out a reminder call. And, based on the people who have volunteered, we will soon be seeking comments from the community on the willing candidates. Please provide your input when that happens, probably next week.

We've had two workshops, first one in December and the other one just last week.

And there will be a brief report on the first one on Internet Technology Adoption and Transition here tonight. And the second one was about strengthening the Internet against pervasive monitoring. That one is a little too new in terms of having a report tonight. We just did that right before this meeting. And, if you really want to know what happened, grab Stephen Farrell. He did a great job organizing that workshop.

So these are the current IAB Programs. I'm not going to go through the status of any of them. I've asked the Program leads for each of these Programs to make sure their page was up to date and current. If you go to the URL at the top of the slide, if you're interested in any one of these programs, you can find the status there.

Moving on then to the next presentation, which I believe is Lars. If the outgoing IAB members would be more comfortable in the audience, they're welcome to go.

>>LARS EGGERT: I'm Lars Eggert. And I chair the IRTF, which is the daughter organization or sister organization or brother organization of the IETF on the research side. This is the short version of these slides. I'm going to give a longer version of this in the IRTF open meeting, which I think is Wednesday morning.

Seven out of the nine research groups that we've currently chartered are meeting this week, which, as far as I remember during my time, is a record. You can see them there. Some of them already met today. Some are still working.

Again, we have a group that is sort of newly forming which is the GAIA group, Global Access to the Internet for All, on the bottom of the page. They have a meeting that isn't on the agenda. The reason for that is they needed to meet on a specific day and for a time that's sort of longer than a normal meeting slot. They also are meeting in a room that isn't as large as the other IETF rooms and, therefore, can't hold, you know, the hundreds of people that might otherwise show up. But there's a mailing list at GAIA@IETF.org. If you're interested in the topic, send me an email there. Warren Kumari and Arjuna Sathiaseelan -- I hope I'm pronouncing correctly -- are running this group. And I'm guessing we'll see future meetings at future IETFs.

Other than that, we're reviewing the ICCRG tomorrow morning with the

IAB. And we have an open meeting on Wednesday.

This is my personal take in terms of where we are in terms of activity. Most of the research groups are in the active set, specifically, the CFRG is very active. I'll get to that in a little while.

And we have a new working group on Network Coding that got formed I think right after the IETF meeting in Vancouver.

Some of our research groups are dormant. That's normal. Activity happens in bursts. The Routing Research Group has been pretty silent for a while. We tried and reboot it for the London meeting, but there wasn't any group of interested people that would put enough energy into it to actually pull together an agenda that made the meeting worthwhile. But Wednesday morning I'll meet with a few routing guys for breakfast to discuss what we can do.

We're giving ANRP prizes to routing papers. And it seems odd that the routing research group is inactive at the same time.

We closed the SAMRG on scalable multicast. They published the final two RFCs.

And those are the ones that you see there in the green. This is our IRTF stream. Publication is bursty, and the bursts are not very big. But we currently have three or four documents with the RFC address. Before the next meeting there will be a little spike in this plot.

That's the RFC that we published out of the SAMRG.

Just before Christmas there was an email sent by Trevor Perrin to the CFRG list -- the CFRG is the Crypto Forum [Research] Group -- ccing the IAB and me.
There was a request to replace one of the two co-chairs of the research group.

Since this was Christmas, it took me a little while to actually review this.

I sent my reply on January 7th rejecting the request to replace Kevin. That decision was appealed. I will note that there isn't really any very formal appeal process defined for the IRTF. But, since I serve at the discretion of the IAB, they may replace me. And so we decided to take the matter there and let them decide whether this decision was warranted or not.

And the IAB responded to Trevor on January 24th.

Switching topics, the Applied Networking Research Prize, we've been handing this out for, I think, three years now together with ISOC. This is to bring sort of new interesting relevant academic research to the IETF meeting. Hopefully, it's sort of to inspire you to look at things that are new and upcoming. We had 46 nominations for papers in 2014. This is the largest number we had. Every year I think we're growing by about 20-30% or 50%. We had 36 last year. 46 this time. So, hopefully, we'll scratch the 50 for the 2015 cycle.

We have a selection committee made up of academics, former prize winners, IETF people, IRTF people. And we chose six winners for 2014. Two of them, Kenny Paterson and Keith Winstein, are presenting at this meeting on Wednesday morning. One is a talk that describes attacks on TLS, so that should be interesting to the security guys in the room. The other one presents a algorithm for doing congestion control for media traffic, so that's interesting for the RTC Web community, I'm guessing. We have four more talks, two at each of the next two meetings this year coming up. And, since we want to generate publicity, I'm not going to tell you who the winners are now.

The award period for 2015 will start probably in the fall. I'll send an announcement and talk about it at the next meeting. So, if you come across good research papers, please nominate them so that we have a good selection of winners next year. Thank you.

>>HEATHER FLANAGAN: Hello. I'm Heather Flanagan, the RFC Series Editor. We have Alexey Melnikov. He's the chair of the RFC Series Oversight Committee. We wanted to go ahead and combine the -- sort of the whole RFC RSOC report into one. Give you the quick highlights to what the RSOC is up to. The membership and details of the program are online, as Russ indicated earlier.

We completed the annual review of the RFC production center and publisher in 2013, which I put together and was reviewed by the RSOC. That's available online for anyone to see. And the RSOC also performed this sort of initial review of the new style guide and the digital object identifier drafts on their way to the IAB.

Some of you may be aware, I've been working on format for RFCs. So there has been quite a bit of progress since the last IETF meeting. We have several drafts posted that describe different areas of what's going on with the format, including the XML vocabulary. What we have, what's going to change, what we're -- what I'm looking at for using non-ASCII characters, and then some more details about the publication formats.

The work is not done, but good progress is being made. And we'll discuss it further on Wednesday at 5:20.

So the next steps, if you don't have a chance to make it to the BoF, to give you the conclusion, the punchline for the session, for all the drafts that we currently have posted, we'll want to incorporate feedback received as we consider appropriate and finish what drafts we can and start the formal publication process, which includes additional community review.

We'll create a statement of work to write the specs and start the community process for that before IETF 90 and then hope to start actual development of tools based on those specs by IETF 91.

And I want to take a moment, again, if you can't make it to the BoF, to thank the design team for participating and putting so much time into making this work. It's been greatly appreciated. And the list of who's on the design team and a lot of what we're discussing is available on the Wiki. And I have a link on that later on the slides.

The style guide has been something I've been working on almost as long as I've been working on format effort. And it is now in the IAB call for comments. That should be wrapping up very soon now. And you can expect it to come out from the IAB to the IETF community in calling for review there very, very soon.

You've seen this slide. I just wanted to make sure we were being very transparent in the work we're going do start, because we will be starting this before this is an actual RFC. There was a little chicken and egg problem of wanting to actually document things like what DOIs we would be assigned and how that would work. So that's why we'll just keep updating the draft as we go until we get to document everything. Last, but not least, the RFC Editor has been accepted as a member of the International Association of Scientific Technical and Medical Publishers. This is a trade association of publishers. A lot of other people -- a lot of other organizations publishing documents like us, standards documents, technical publications. And they have a lot of experience we can learn from. So we're doing this, basically, to learn more about the best practices in the technical publishing space and to, you know, get out there and make sure the name of the series, the RFC series and the documents we publish, is better known.

If you want to know what's going on in my part of the world, I have a Wiki which I try to keep updated with things I'm working on. And there is, of course, the RFC-interest mailing list, which goes through surges of activities. So, depending on how you filter your mail, you may get

flooded or not, depending on what day it is.

That's what I got. Thank you all very much. I hope to see you Wednesday.

>> ELIOT LEAR: I'm here to talk about the Internet Technology Adoption and Transition workshop. This occurred in December. And it, basically, looked at the problems of can we do a better job at seeing that the technology developed in the IETF is, in fact, deployed widely.

This is not the first such activity that the IAB has engaged in. RFC 5218 has looked at this before. We are going to talk a little bit about that.

Our premise, though, was to question whether the neck itself has been closed for business and whether we're seeing good deployment in areas that we think we should be. There's a little error on the slide that should be DCCP.

For instance, what are the inhibitors to DANE? What are the inhibitors to DNSSEC deployment? How do we get new RRs? These are some thoughts we had going into the workshop. And one of the thought exercises I was playing with is: What would you do if you wanted to do the MPLS-ng? Anyone want to start that?

So that gets right to the motivations. At this point we have a lot of interesting work going on. How do we see WebRTC deployed is one question we used going into the workshop. HTTP has been looking at -- HTTP2 being run primarily or almost exclusively over TLS, how will that play? We looked at -- we were going to look at ROAs and BGPsec. The speaker for that unfortunately couldn't make it, but we did accept a paper on that.

We were contemplating the notion of mandatory to implement in the marketplace.

You can see the workshop information at the URL below. There is a report that's been posted today that's a draft, and we will be announcing that.

So we started out in this using RFC 5218 as a base. And on the right side, you will see what's described as initial success factors and then wild success factors. There's also the notion of failure.

I want you to at least take a look at these success factors for just a moment because one of the outcomes of the workshop was that the IAB and

the IESG should take a look at these factors in the context of reviewing BoF proposals.

So I am going talk the rest of my few minutes, I will give you a brief overview of some of the papers that were presented, not all of them. I will probably run out of time but not slides.

So Andrei [Robachevsky], who I believe is in the audience, did a great job of talking about averting the tragedy of the commons. And the question is how to provide more resilience in the routing system. And he was looking at some of the problems other people face. One of the examples was fishermen that overfish without some form of regulation.

The solutions that he contemplated were you turn the commons into private property and that way essentially you internalize externalities or account for all that's changing.

You tax and regulate, which is a classic way to do it.

Or you find a bottom-up cooperative model.

Guess which one Andrei picked to go for?

So some of the ways in which you need to have it lined up is you have to have a common understanding of the problem, solutions, and individual benefits. And you have to have an ability to assess risks.

So his goal and his effort has been to build critical mass, particularly in the routing system, which is where he's working and, since Andrei is here, if you have more questions, not only can you read his paper but you can go find him.

An interesting area that we looked at was the bundling of technology. So if you have two independent services and you put them together, can you actually improve the deployability? And so you can imagine a quadrant in which when you do this, either nothing changes, you get the same amount of deployment, things get better or things get worse.

And so Steven Weber and Roch Guérin and Jaudelice de Oliveira presented a paper on this. One of the issues we questioned was, well, what happens if there are dependencies like there might be between DNSSEC and DANE? Or WebRTC and SCTP? How does that change? And his answer was: I don't know yet.

One of the big take-aways was that he would like to work with interested working group chairs, authors and other people to validate

some of the model that he built out.

I am going to encourage people who are interested to come talk to me, and I will facilitate that.

Another area that we looked at was DNSSEC and deployment. Here Anne-Marie Eklund and Patrik Wallström joined us remotely and talked about the heavy lifting that they've done. Which they've learned if you make people pay more to implement DNSSEC, they don't. And if you actually give them an incentive through cash, in fact, they do. And the interesting results of this paper is that 300,000 out of 1.3 million domains in .SE are, in fact, signed. That's a tremendous accomplishment and something that I wonder can be replicated, perhaps not with .com or .net but perhaps other domains.

We talked with Rainer Böhme, who was an economist, and he was looking at Bitcoin success factors. And the key messages I would like to just bring to you here are that there are success factors such as early mover advantage and having a way for participants to capture the value that is being provided to others as well.

And these are some interesting aspects of Bitcoin. We're going to hear a lot more about Bitcoin today, so I won't spend any more time on that because I'm running out of time already.

We heard from Dave Meyer about some work he and John Doyle are doing that compares systems biology which has a bowtie model to the hourglass model. There's something called ATP in systems biology, which is a common building block that transmits energy between cells. And there was a comparison to that between the common control function which is I.P.s, as he put it. This scenario where I think it was the one that needs the most work and further research. And Dave's interested in working on that and continuing it, and he's interested in a research area as well.

He also talked about the domain of the robust versus the domain of the fragile and how robustness actually requires a certain amount of complexity in order for work to succeed. Again, this was interesting, but when asked: What are our lessons learned here? He said, well, it works too early. I am not quite sure to translate it into operational things for the IETF.

So Hannes [Tschofenig] talked a little bit about getting to TLS 1.3, what are the things we can do. We had a little bit of a roundtable discussion about that. Just a couple of things to quote out of that, maybe there is a little marketing that's needed in terms of the name.

That was just something that was thrown out. Another thing that was thrown out was maybe some test harnesses might assist. And the problem statement here is that we see a heck of a lot of TLS 1.0 much less 1.1 out there right now. And it seems very hard to manage the tail, as it were.

One point I will say is I believe the HTTP working group is pondering the idea of requiring TLS 1.2 for deployment. So that's another thing that has come up since.

So here's some next steps. There is a research group, not a working group, that may be formed called GAIA which is, as Lars described so I won't go into further detail there.

We're going to try to facilitate some of Steven Weber's research. The IAB and IESG should probably take a good look at 5218, again, as we do our BoF reviews. And we'll have some possible discussion about facilitating interoperability. Maybe ISOC might be interested in playing a role there.

We want to do a better job of tracking successes, wild successes, and failure.

With that, I'm done. Thank you, Russ.

[Applause]

>> DAVE THALER: Welcome to the IAB's technical topic this time. We talked about payment systems in relationship to the Internet. It is interesting, when I checked into this hotel on Saturday and picked up the newspaper in the lobby, there were two articles in the front section that talked about the Internet.

The first one was on the front page, and it talked about Bitcoin. And the second one was about on page 8 and was much longer, and it talked about China and moving to things like credit card systems and so on. And by coincidence, those are two things that are very closely related to what our two speakers are going to talk about.

So let me introduce our two invited speakers today. Malcolm Pearson, stand up or wave or something.

Malcolm Pearson is the director of development at Microsoft China for eCommerce protocols and mechanisms. He's going to talk about how different payment ecosystems actually work around the world and what some of the protocol challenges are today. So if you have ever wondered

what happens when you actually register for IETF or you actually book a hotel room and what happens to the money, Malcolm's going to educate us on that and the protocols and so forth.

Steve Kirsch, go ahead and stand up.

Steve is a serial entrepreneur based in Silicon Valley. His company is a pioneer of technology such as the optical mouse, Web search, WYSIWYG text editing and anti-spam. Two years ago he decided to take on the problems with digital identity and password proliferation by starting OneID. And he's going to talk about a number of security issues that occur with payment systems and sometimes more generally. And then he's going to talk about the future of Bitcoin.

And so with that, I will turn it to Malcolm to come up. Let's welcome Malcolm and Steve both. Give them a hand.

[Applause]

>> MALCOLM PEARSON: So let me just give a very quick introduction to myself. Actually, the beginning of my career I spent about 20 years working in email followed by so far about five years in eCommerce. The email experience is kind of relevant because the situation I think we're in in eCommerce is kind of similar to the beginning of email or at least email about 25 years ago.

Back then it was a very diverse space, just about every single vendor had their own email standards, some of them like IBM had three. And the company I originally worked for, its whole existence was based on gatewaying between these different systems.

About ten years into that career, it became clear that things were converging around SMTP and S/MIME.

My last ten years were converging Exchange. Used to a very X.400-oriented system, moving that into SMTP and (indiscernible) system and even moving some of the defense messaging systems off of X.400 standards and onto SMTP.

I'm hoping we get the same kind of benefits out of some convergence of protocols around payments. Little joke: I'm hoping to do SMTP again. It would be "simple money transfer protocol."

My time in commerce has been pretty fascinating, especially the last two years where I've been working in Shanghai. Before that, I had been located in the Seattle area.

It's been very interesting because just being in the culture and being in the country, you get to see how very different the payment mechanisms and how very different the sort of social assumptions about money are.

Some of it is very technical in the way that you use different cards and different payment mechanisms.

Another one is, it gets into scenarios. For the first six months or so when I was there, I got a lot of feedback from the engineering team that said they were sort of disappointed that we weren't working in the forefront of eCommerce. It took me a while to parse what they really meant.

And what it was, was that eCommerce as an application itself or as an experience itself is much more prevalent in China. So you have experiences like settling a check at a restaurant. And it's very normal for you to have an app on your phone that will go and let you spread out the charges for that amongst your friends and you'll settle the money amongst your friends and one person will go and pay it.

Another one is gifting or payments to friends. It's much more built into the culture and built into the mobile experiences there.

I think we're starting to really get that feedback in, and we now actually have a prototyping group there in China. I tend to probably weekly -- built into the end of some meeting, someone will come up to me and say have another five minutes of "hey, here's another a cool scenario you probably haven't seen." Each time it is a breakthrough. So I'm finding that fascinating.

Just give you a quick roadmap of how I want to try and go through this content. Try to give you a little bit of a structure to the payment space and some of the key challenges, base ourselves in some of the scenarios. I will be talking about the different payment methods, and I think you will get a sense for just how diverse this space is. And, finally, a slide trying to summarize some of the big areas where I think we can use some standardization.

Here I'm trying to give you a structured picture of the online or, you know, immediate user interaction part of payments. First, let's talk about the merchant. Full disclosure, I probably count as a merchant being part of Microsoft. We are trying to sell stuff.

First thing is the merchant will show an invoice, which is basically a contract between -- hey, for some amount of money, here's some

fulfillment, some kind of product you should get. That's really presented to the user.

Conceptually, what really should happen is the user should go to their source of money and instruct that source of money, "Hey, I'm authorizing you to transfer some money to the merchant for those goods."

Third step, that merchant should then be making authoritative statements back to the merchant -- sorry, that source of money should then be making authoritative statements back to the merchant that says, "Hey, not only has our user convinced us they want to transfer this money but also funds are available." And then, finally, the merchant's responsible for fulfillment.

Just want to highlight, there's kind of a network issue here of many merchants working with many sources.

Another thing I want to highlight is that this potentially is a cascading effect here where source of funds will be transferred maybe to a merchant and that merchant in a way may become a source of funds to another one of these interactions.

I also want to highlight that when we think about commerce, we have to look beyond just the online interaction of paying for stuff. There's also a lot of mechanics of something called cash settlement, making sure that the money that has been made available in a source actually gets audited and flows into banks that the merchant cares about.

Another one, I want to talk about the governmental issues of making sure that both tax information gets reported correctly and that financials get reported correctly.

Just to give you some perspective, we probably put as much effort into both a taxation and the financial reporting as we do on some of the online interactions with different payment instruments.

Just highlighting some of the challenges that I'll point out as I go through payment instruments, the network effect in this space is huge. In email, it was many, many different vendors which caused diversity. Each one of those vendors thought they should have their own standard.

Now, countries have currencies, and I think they may have a stronger claim to actually having a need for diversity than the vendors. So there's some real force in the system that's going to cause a lot of diversity that we need to deal with and support.

Even when you get within a country and a currency, there are a lot of different mechanisms that exist to go and transfer money within that country.

Another one, very interesting tension, is between security and convenience. You can really see this especially in North America. The credit card networks that we have in North America are extremely convenient. I can give my wife my credit card and she can go spend money on it.

I can supply a credit card to a merchant that I trust, and they will even keep track of this for me, and they'll make it very easy for me to make subsequent charges on this.

In contrast, a number of places consider that very insecure. In China, if you provide that kind of experience, many of the users will reject it and feel that you're not providing enough security. And I would say truthfully you are not providing enough security in that kind of experience. So you can see there's kind of a tension here.

And it is not a simple tension, right? It would be easy to say, "Hey, you know, we should just have a high security system here." But there's arching interaction between the merchant, the user, and the payment source where you have to describe what is being purchased and what the pricing of that is, and that needs to be able to flow through all these participants and be able to be understood by them in order for the system to work.

So I actually think there's an interesting email analogy here. Spam was certainly, and continues to be, a challenge in email. We could have taken an approach where we locked email down, at which point it would become uninteresting and ineffective. I think there was a lot of work to find incremental improvements to the security of email rather than taking a dramatic approach to locking down.

Obviously, business is another factor. There are many big entities involved in commerce. Another angle on business is the unbanked. It's very easy for us in North America to think about a world where everyone has a bank account. Huge portions of the population that we're trying to reach with commerce don't actually have a bank account. Most of their interaction is around hard currency. And so you've got to keep that in mind that we're dealing with cultures that don't have bank accounts, don't have charge cards.

We also think about that from the point of view -- even in North America, you talk about kids who, if you do want to sell games to them,

you need some mechanism that is appropriate and also has the appropriate controls.

I also want to emphasize emerging markets from a cultural point of view. I think I've mentioned already how, you know, different cultures have different assumptions or different expectations about how money should be handled. Another angle to this is to think about the social and economic impacts of some of these very cash-heavy cultures. There's some statistics that a lot of these emerging markets without an e-commerce solution, people will spend two working days a month just dealing with bringing cash maybe to family members or going and paying bills, which is just a big load on their life.

So there's some good that we can potentially do by solving this.

Let me take a look at this from a scenario point of view. I want to pull a few of these out. One dimension to look at is the latency. You can really see a continuum from high latency payment experiences. When you go to a sit-down restaurant, you don't really care if it takes 10 minutes for a payment to complete. If you are sitting in a game and you're trying to purchase some consumables that are part of that game, you expect a very immediate experience. On the other end, you can go and look at subscriptions to business services like email. There we probably have tolerance of two or three days in payments. The merchant can probably afford to even suffer the loss of payment for a few days on those items and latency is unimportant.

Another thing to think about pricing, sort of ties in to this interaction when you're looking at how the end user, the merchant, and the sources of money interact. The thing is you run into -- sometimes prices are very clear at the beginning. I'm purchasing this item. You get a little bit more abstract when you talk about recurring subscriptions where, you know, it's $12 a month. But we can imagine how to express that.

It can get pretty complicated when you talk about pricing that's variable based on usage. And so one of the challenges is to figure out a good way to go and express that, give parameters around payments. You can already see this showing up in some of your online banking experiences where you're maybe trying to automate the payments for a phone plan. And your kids are sending lots of SMSs.

I've talked a little bit about the e-commerce as an experience itself in terms of gifting, in terms of giving money within family. Again, emphasizing that that shows up a lot in Asia or at least my experience is it's predominant in Asia.

Another angle that we don't think about always too much is disputes and returns, especially with the convenience in North America on charge cards. That system really relies on the ability of the end user to go back and dispute a charge if the charge was not actually intended. Even without that system, even without the relatively weak authorization there, there's need for things like returns where a customer says, "Hey, I didn't actually want this product" and a mechanism to both return the product, give money back.

We can't forget about the security issues, especially around credit cards. Neiman Marcus and Target, for example. In my group we spent months working on designs, you can imagine a system where there's 500 engineers involved in an e-commerce system, including operations folk.

You don't want all those 500 people to have the ability to go and steal those credit cards, because they may be very tempted, so engineering a system to go and lock down and always reducing the number of people that have the ability to access credit cards. And, finally, I talked a little bit about back-end issues around cash reconciliation and tax reporting.

Now lots of pictures here. The point of this slide is there's many, many payment instruments. And I'm going to try to jump into these in a structured way. I want to talk about a little bit of perspective on mobile billing. This is interesting from two angles. There is an unbanked angle. It's very interesting that in a lot of countries, the mobile operators are the companies that have got the most presence within those countries. And they have the ability to go and do cash transactions with end users. So this becomes a very rich -- people in those geographies that otherwise wouldn't be able to participate.

Not just a selfish interest of merchants, but this also enables the money transfer issues I was talking about where, you know, an individual may need to transfer money to a spouse that lives in another city, which can be common in these geographies.

There's another angle to this, which is convenience. And you definitely have seen the cases where, you know, people want to be able to use their cell phone very much like a wallet or credit cards and not have that complexity of many credit cards that they need to manage.

Just jump down into a fairly low tech scenario of mobile payments. The point here is using SMS messages as a way that you can authorize payments. This ends up being a very easy way to get a lot of reach because there's so many devices out there that support SMS.

A slight variant of this, getting to more sophisticated devices that will rely on either the fact that the transaction is being initiated over the network that the mobile operator controls so they have an ability to authenticate the request that's being made or use some material in the SIM in the mobile device.

A scenario that I find kind of interesting is the interaction between mobile devices and other systems that you might want to make payments for. So you can imagine a game or an online experience where you've selected something that you want to purchase. Those systems can put up a bar code or a QR code to, essentially, be -- have the merchant express the invoice or express that contract between what is being purchased and what the price is and, ultimately, where the money is intended to be delivered. It's a very nice scenario that the phone can then go scan that. The phone can also be the place where you have the material where you can make a strong claim that the user was present, authorize those payments.

Just a little bit of a flow to summarize this, the point I'm trying to make on this slide is that the authentication here can be really tied around the device, the mobile device, and then be transferred on to the carrier. The carrier has good ways to be able to trust the mobile device and then pass on a strong proof to the merchant that funds are available. I'm going to skip through this.

Things to just highlight in this space, I kind of glossed over the issue of is the possession of a device enough to say that the user is present? Certainly in some cultures, in Japan, if I lose my cell phone, it's going to come back to me. And it's not going to be abused along the way.

That's not going to work in every culture. Another level we'll also want to be thinking about the hackability and the security of those devices, if they're used to make strong claims about the presence of the user.

Another fascinating area. This one was quite a shock to me when I first started to understand it. The retailer and kiosk scenario. So there's a thing called Boleto in Brazil. And Brazil has a big history of not liking online commerce. I think people have probably been mistreated. One of the most common patterns there is you'll actually go up to a Web site, and you'll see an order form that says I'm trying to get something. It could be something for physical delivery. It could be something for digital delivery. You say, okay. I want to pay with a Boleto. And what happens is you can see this little invoice thing in

the middle of the screen here. You get -- you actually get an image that renders that includes a bar code at the bottom. And encoded in all of that is, essentially, what I meant by an invoice that says here's the goods you're getting. Here's the price. Here's the account number of me, the user that's trying to purchase something. And here's also the account where the money should be delivered.

The user prints this out, this nice little piece of paper, walks to their local convenience store, brings cash in hand, takes it to the cashier, cashier counts the money, checks it off, and sends a signal back to the banking system to signal this payment. Quite dramatically different from what we're used to in the western world, but you can see how that fits the patterns of that culture.

There's some other variants of this. I have a little bit more direct experience just with China Unicom. And all the mobile carriers have this pattern. You can go up to a kiosk, if you're trying to recharge your phone, a prepaid model. You go up to the kiosk. You type in your cell phone number. You say how much money you want to top off. You get a little receipt. You walk up to the cashier, hand over the cash, and the same kind of interaction.

It's also interesting because this is one that can cascade. So, for example, there's a streaming video company within China called BestTV. They actually get their funding indirectly through the China Unicom networks and I think other networks. So you can go to your local Family Mart, pay into your cell phone plan, transfer money from your cell phone plan into your streaming video plan and have it work.

Just another scenario in Russia. A slightly more direct pattern where you actually walk up to a kiosk. You identify who you're trying to pay money to. Money is scanned, and payments are made.

In this space, you know, one of the biggest challenges is actually identifying where the money is getting sent and making sure that that's reliable.

I'll mention Bitcoin so that no one can claim I wasn't paying attention.

I want to quickly shift to eWallets. This term has been used in many ways. The way I'm using it is a concept where the eWallet behaves a little bit like a bank account. It has the properties that there's a balance there of money that's been accumulated. Generally, the companies that implement these have actually stronger off model. So we're a little bit better than what I'll point out for credit cards.

The value that these guys produce is, especially in some of these more offline payment methods, like I just talked about with Boleto, where you have to go to your local convenience store to go and make payments. So you can imagine that the kiosk mechanism gets money into these eWallets. And then you have a very convenient way to go and make payments either, you know, person to person, or into some kind of online experience that you're trying to use.

This is actually relevant in North America as well. I'll get to ACH or bank transfers a little later.

Jumping ahead, these pictures should be fairly familiar. Western credit cards. Kind of the point of this slide is it doesn't quite work the way we imagine it might work. I was kind of emphasizing how a lot of these systems there's actually quite the strong connection from the end user straight through to the source of money to make sure that that authentication and authorization works quite nicely. You can see in this picture it's kind of reversed. You, as the end user, work directly with a merchant. When you hand over your card to the merchant, you're essentially saying, "Hey, merchant, I trust you to go and handle this correctly and fulfill my intentions with those payments." And you can see how this works through a number of steps in the system, ultimately, through the card networks and then to your source bank to go and collect money.

There was a lot of trust in this system, built into this system.

I think in the early stages, it was probably a fairly small system. And so it was actually practical to make sure that all the parties were adhering to the standards. I think this system is sort of getting stretched beyond, definitely, its original design point. And we're seeing some of the challenges there.

What I want to emphasize is that all the participants in the system have to make guesses about the fraudulentness of the transactions. So as a merchant, we get charged by how much fraud we let into the system. We're really not in a good position to judge this. We end up having a team as big as our payments team that works on statistical models to try to predict whether this particular transaction is fraudulent. So a lot of motivation. But doesn't seem like quite the right solution.

Just a picture of how I'd like it to be. This is probably the heavy handed solution to spam, and we'll never get here. I will go quickly to get to bank transfers. When you do online payments for utilities, has the structure actually a little bit similar to credit cards. The

interesting thing is it can, actually, flow two ways where either you, as the user, can go to your online banking and initiate payment out. That's, actually, a very high security model. It's very much like the kiosk where you, essentially, have cash in hand. You can make sure that things work nicely. But it also has the pull effect where, you know, as a merchant, you, basically, just with your account information, they can pull money. And so there's an incredible amount of trust that they're actually doing the right thing there.

Again, this one, I think, is a little bit easier to get wired up in such a way that it's safe, you know, as long as you really emphasize the push model.

I want to spend a little bit of time here to summarize where I think the opportunities are for standardization. I don't know enough about the behavior and structure of IETF to know how to find interest and how to find engagement on these.

My email address is on the front page, so please reach out to me. Email will be delayed, because I'll usually be in Shanghai. I will be moving back to North America this summer along with my family. So I should be easier to reach.

Let me just emphasize -- the first series here I talked about invoice, talked about the relationship between prices and the goods that you're getting. User authentication, making sure that the user is present and that they are making their intention known when they talk user payment authorization, authorizing that payment.

I talked a little bit about the complexity of pricing, so you would want that user authorization to be able to express some of these usage-based models. Good challenge there.

Next step: Even though the user decided to spend some money, you actually want the source money to say that the funds are available. You want a good mechanism to make this extensible so that you can add new merchants and new money sources into the network without having significant reconfiguration to have to go on, which does today. I talked a little bit about cash reconciliation, so that we don't forget about it, and then reporting both for financial reasons and taxation.

Currently this world is very diverse and some of that is due to business interest. We found that it is actually possible to get convergence. One place where we've been applying pressure is just to do cash reconciliation protocols, just file formats, getting those

converged. And we actually have found that the participants are pretty willing to play. So there is, in fact, hope that the parties do want to work towards convergence. So I would say that this is an area worth engaging in.

That's all I've got. Thank you.

[Applause]

>>STEVE KIRSCH: Like, Malcolm, I also got my start in email. I wrote the email system that was used by Jon Postel and the rest of the gang at UCLA Network Measurement Center and the ARPANET. So I was there at the very beginning of the Internet.

And I cranked away code on an ASR33 teletype, and Jon was actually pretty nice to me. He said if you came at 4:00 a.m., we would let you use the data point terminals. And they ran at 2400 baud. So those were the good old days. A lot of has changed since then.

So I'm here to talk about payments and talk about identity. And I'm going to talk about secure payment authorization.

And, actually, authentication and secure payment authorization are actually almost the same thing. So when you talk about logging into a site, you're just basically if you are doing it securely, you say, "Hey, log me into HSBC," signed Steve. If you are talking about a transaction, you are saying, "Hey, I want to purchase so and so from this merchant" and you are signing it with your digital identity. And so they're really quite the same.

And so we can use the same protocols, and it is just what we sign that's different. And so I'm going to be talking about identity, talking about secure authorization. But they're really interrelated.

I'm going to talk about 15 myths today, and I'm going to try to bust 15 myths. How many people have seen the show "Mythbusters"? Oh, great. So, normally, they say is the myth busted or not. And, actually, I'm going to have all myths here and I'm going to bust all 15 of them today for you, which is quite a feat because usually on the show they only bust one or two. So we're going to do all 15.

So the first myth I want to bust is that there is no way to fix this mass password breach problem and mass credit card breach problem. It seems like every day we hear about some company. Right now it is Sears who is under the gun and they may or may not be breached. We're not sure about that.

But I made a list of some of the companies that have been breached over the last few years. It's pretty much everybody who has done business is on that list. I think if I put every logo here, it would be too small for you guys to read. You know what? The problem here is really simple. The problem is that we use shared secrets. This actually looks like the Target logo, but the reality is I was trying to show that on the perimeter, you have all, you know, people with shared secrets like credit card numbers and passwords. And in the center, the same secrets are in that center part where they can be breached. And so any resemblance to the Target logo is purely coincidental.

The problem is magnified because half the users -- in fact, there's an admission by the former CISO of PayPal, was that half the people at PayPal use the same password on all Web sites. So whenever a site gets breached, then you get messages from every other site telling you to change your password for this very reason.

So, how do we solve this problem once and for all? Now, the solution seems to have alluded us, hasn't it? What we need is something that's equivalent to the U.S. passport, right, where it's got digital identity encoded in that. We hand it over, and everybody trusts the U.S. passport. You take your U.S. passport. And it is trusted in all these countries. Why don't we have the same thing on the Internet?

I always go to these identity conferences and ask the question of the audience: Why don't we have this? Or what's the equivalent for the U.S. passport for the Internet? I always get blank answer. Nobody knows.

Well, the solution to the problem is actually pretty easy. The solution to this breach problem is that we just get rid of all the shared secrets. So all the stuff like usernames and passwords, one-time passwords TOTP, oauth, your pet's name, Social Security number, tokenization, API keys, secure I.D.s, Google auth, credit cards. Once we get rid of all those, we won't have any mass breaches. Easy enough, right?

So the thing is that we've had actually the ability to do this for many, many years. And the problem is not that we don't have the technology to do this, the problem is that we're not using the technologies that we have.

So, for example, when Forbes got broken into, I got an email from them saying, "Hey, your password is in jeopardy. Why don't you change it here and change it everywhere else you use that same password."

What was not said and what nobody ever says is that, well, give you an option in the future to log in without using a shared secret.

Change is hard. Even if you lose a billion dollars, change is hard. I don't think they're going to move off of shared secrets at Target even after losing billions of dollars in the breach.

And as far as I know, not one company that has been breached with a password breach or a credit card breach has ever offered a consumer the ability to log in without using a shared secret, even as an option. Not one company, ever, as far as I know. Changing behavior is hard.

I tried to do this with OneID. I said, here's a way to get rid of shared secrets. You know what? I created this handy list. It seems like somebody has this list because I am always getting something off this list of the 19 reasons as these are excuses for inaction. These are nice. You can present it to management, and management looks at that and says, "Yeah, yeah, yeah, that looks good. Let's stick with shared secrets."

But the reality is these are just excuses. If you don't want to change, this is a great slide to have handy and you don't even have to say the reason. You can just say "Number 3" or "Number 19." Why bother? Just use one of the excuses. It is a great list.

Okay. So the thing is that people say we'll adopt two-factor auth. Whenever they get broken in, they say two-factor auth, that will eliminate our password breaches, solves the problem.

But you know what? Two-factor auth basically prevents key-logging tasks. It does nothing to prevent the mass breaches because typically all of these two-factor auth solutions are another shared secret. Guess what? The massive file's got shared secrets. And there is a password shared secret, and there is a two-factor auth shared auth secret, and maybe there is a token shared secret that once you do the two-factor auth, they drop a token and they have that.

So they breach two files instead of one. The breach happens again. And people think, hey, two-factor auth, it solves the problem. It doesn't.

And the other problem is that the users hate it. You know, the Google stat -- less than 1% of the people adopted two-factor auth. If nobody uses it, what kind of solution is that?

Okay. Myth Number 3. This is out of band two-factor auth. Banks use this so it must be safe. In fact, HSBC is using not the RSA secure ID; they are using someone else's token. But they are using this technique and they are giving it out to consumers saying, "If you want to do a certain transactions, use our out-of-band two-factor auth. This is secure. We are HSBC. This is secure."

Sorry. That's in-band two-factor auth because you're entering that code from that device on the same computer that you used your username and password. If I compromise that computer, you're done. It's not digitally signed. These things are like signing a blank check. When you enter that code in, you got malware on that machine. Malware takes that code, does whatever it wants. Thank you for the blank check that you just gave over to me.

And we actually have proof. There was a study done that -- two years after FFIEC guidance to implement two-factor auth, look at fraud rates. What happened to fraud rates? Did they go down? No. They went up. Wow. Effective solution.

Now, this is an example of real out-of-band two-factor auth. What happens is the transaction is rehashed, and it's digitally signed on the original device. And then it comes of a separate channel. The transaction is shown to the user. The thing that's shown to the user is rehashed and digitally signed on a second device ideally using a second private key. That's real two-factor auth that's out of band.

Myth Number 4: Biometrics will fix all of this. Well, turns out biometrics are kind of like a password that you can't change. They're kind of like a shared unsecret. And if you're using it remotely, you're screwed. If you are using it locally, as long as you control the hardware, you're actually in good shape.

Myth Number 5: Storing credit cards cannot be made secure. That's a very commonly believed myth. That's not true. You can actually use crypto on a user's device to encrypt their credit card, store it in the cloud. When you need to use it, you take it down from the cloud, you decrypt it on the user's device and hand it over to the merchant. It is not perfect, but it at least eliminates the chance that you can have this mass compromise of stored credit cards.

So here's a diagram of that. We have encrypted cards that the user has encrypted his card, stored it in the cloud. The user brings it down, decrypts it, and gives it over to his favorite vendor to use and not store.

Myth Number 6. This is my favorite of all the myths that everybody is now programmed to think that passwords are bad, right? Well, passwords, it turns out, are inherently good. You know, when you talk about three-factor auth, there are three factors, something you know, something you have, and something you are.

Now, if we get rid of passwords, we get rid of one of those factors, something you know. We're left with two factors. That's no good. Security is all about three factors. Passwords are great.

What's wrong with passwords is how we use them today because on almost every system in the world, passwords are used as shared secrets. Bad. Wrong way to do it. You take your password, you put it in, maybe you hash it on your computer or you send it up to PayPal and they hash it there and store it and compare it. Whatever. Not the way to do it. This is the way everyone does it. It is not the way to do it. Yes, this wrong way is something that we should eliminate.

The right way to use passwords is to never disclose them and never share them off of your local device. So what you do is you take your password, you combine it with a local salt on your default on your device and that creates a signing key, ideally an elliptic curve, digital signature algorithm signing key. And that's used to sign a challenge that comes from your merchant, say, a log-in challenge or authenticate-this-transaction challenge, and then you send that back. So that's the right way to do passwords.

Now, as part of this, because people use passwords as shared secrets, you have these things you see on the Internet that longer passwords are more secure. That's bullshit. If you do passwords right, the way I'm talking about, you only have to protect your device from your kids. And how hard is that? Because you know they will only get a few guesses before the device then locks.

I have a one-character password. Here's my OneID account. Here's my username. I have a one-character password. I'm telling you my username and password. And I know people -- I checked. People actually looked at this presentation before I got up here. They tried to log in as me. Ha, ha. You didn't get in. Nice try. But the point is that my password can be one character. I can disclose to you my username and password and there is no way for you to log into my account, as those of you who have tried already know.

Myth Number 7: PKI, RSA crypto and EMV are all safe technologies. Commonly held myth, I know most of you believe that.

Okay. So they're not as safe as you thought. PKI is not end-to-end secure. My proof is simple, DigiNotar, QED.

One of the simplest proofs ever.

RSA crypto, there was a presentation at Blackhat conference saying, We may be able to find some algorithms that may break RSA, and that may happen three or four years from now. It may happen five years from now. It may not happen, but there's a risk. You should use elliptic curve cryptography.

EMV, not digitally signed at the far end. You put your credit card in. Yes, it says $65 or whatever, but there's no guarantee that that machine has not been tampered with. It is not end-to-end secure. "End-to-end secure" means it is your device that's signing it, not someone else's device.

Myth Number 8: FIDO will fix all of this, the dog. FIDO stands for Fast Identity Online Alliance. There is their URL. And some people are enamored by this thinking, "Of course, this will solve the problem. Look at all these companies that are using FIDO."

Sorry. FIDO is authentication only. It doesn't do transactions. Darn. And it can't eliminate the risk of cloning your private key on your device. But, geez, it is not a federated identity system. It solves part of the problem, but really doesn't -- it kind of moves past the password phase of 500 passwords you have to remember to lots of devices that you have to have that you have to authenticate to each RP. And if you lose a device, you're screwed.

Okay. So the answer is federated identity. So the myth would be that all federated identity providers are untrustable. Now, this myth is actually mostly true. Unlike some of the other ones.

So you can't trust most of these guys who do federated identity. So all the guys that you use today as a consumer, Facebook, Google, LinkedIn, Twitter, you can't trust those guys, apple. You know, any breach or goof at any of these identity providers, your identity is toast.

So the reason is you're authenticating to Facebook and Facebook uses some magic to say "Oh, yeah, you're Steve" and then they authenticate to airBNB. If there is a problem at Facebook, you're screwed.

So the right way to do it is called trustable federated identity. Now, "trustable" means that the IdP, the identity provider, can ask around.

And that's because he doesn't have enough stuff to go and assert your identity without your consent. So no matter what happens at the IdP, they cannot assert your identity without your consent.

And this requires a crypto secret to be loaded on your device. That means if you create a new device, you better use one of your old devices in order to authenticate that new device because if you don't, there's something wrong because that secret that you have on device one has to be transferred using some sort of Diffie-Hellman or some sort of modification of that to device number two in a way that can be snooped by the network that may be helping you to transfer that.

Trustable IdPs use end-to-end secure protocols, meaning it is signed by my computer at my end and then it is verified at the far end by the relying party like an airBNB.

Trustable federated identity, there are no shared secrets. The security is guaranteed by the architecture and not by the people running it so people can goof up and modify the code and change around things. And it doesn't affect the security of the system.

It's got ECDSA, probably, as the digital signature algorithm that replaces everything. Simple protocols -- Adam Back, which designed our protocols, always told me that, hey, complexity is the enemy of security. Really, really important thing to remember.

There is no single port of compromise in these systems so we have to assume that people's laptops are going to be breached. So the trustable federated identity will take that into account and assume that's going to happen and still be immune to that single point of compromise.

So here's an example of a trusted federated identity system. Unfortunately, I had to use my own because that's the only one that I know about that exists.

But it is really -- it's an award-winning clever algorithm that does all these things. It uses multiple ECDSA prior keys so there are actually three keys used on three different devices. And it authenticates whether the device has been stolen and so forth.

It would take about eight minutes to explain, and that is unfortunately more time than I have today.

But here are the benefits for trusted federated identity. You can securely store things like private keys to your Bitcoin account, for log-in and so forth. You can store secret keys. If you're into

symmetric cryptography, sometimes secret keys are useful. You can store personally identifiable information like your name, address, phone number, and so forth, all securely in a way that nobody but you can access. And the nice thing is that the public keys that you give a relying party or Web site and so forth are stable for the life of your identity. So you can change your password, you can change your devices, and all that. You do not have to go and reprovision any of the public keys at any of the relying parties that you go to. So you can add this capability to your SSH, your VPN, your login or whatever. One password, one PIN that you have to remember across all sites. Wouldn't that be nice? I think so.

Myth number 10: Trustable federated identity is too hard to use and it's not as safe as our proprietary identity that our security staff has created. I always ask really? Would you like to do an audit? We can compare the trustable federated identity system versus your system, and we'll see who wins. And it turns out that these trustable federated identity systems are immune to all known attacks. It's not perfect immunity. Nothing is. But compared to anything else? Like night and day difference. You can take any well-known, world-famous security crypto expert and compare the two systems. And it's night and day difference.

Myth number 11: An IETF standard is the best way to fix any problem like this.

No. Actually, I want to ask you all to do me a favor. Do not treat this presentation as a shared secret. Okay? So, you know, we're now all in the know here. And, you know, the worst thing you can possibly do is keep the secret. Right? I know it's going to be kind of hard for some people to -- hey, been doing this wrong all these years. But it's great if you can spread the word and walk the talk. So you know when you get this email once a month from the IETF saying you're on these mailing lists and, by the way, in the clear, here are your passwords for all these things. Okay. It is time -- that technology was invented 50 years at MIT where I went to school. And it's time. It's time to start walking the talk at IETF and start actually using technologies that are newer than 50 years old for your mailing lists and some other things. The IETF tools also can be password protected for some of them.

You can go home and you can deploy this technology on your Web site, use it with VPN, SSH. Share this presentation with your friends on Facebook and secure the other insecure trustable federated identity.

Tell people at Target, AT&T. Gosh, AT&T you have, like, five different log-ins. You just need one. You don't really need all these things.

It's crazy!

We're going to switch on to Bitcoin. I have seven minutes left.

Okay.

Myth number 1: A Bitcoin is going to die. This is the new Mt. Gox logo. Nuclear cloud over, I guess, Japan and what not. Bitcoin is going to die, and people predicted this. The two-bit idiot posting, "Hah, I fear this is the end of Bitcoin. That people will lose faith in the currency."

So I checked with Satoshi, and he said that, "Rumors of my death are greatly exaggerated." His vital signs are still stable after this incident, although the Bitcoin price has dropped. And, if you go to Mt. Gox now, there's nothing there any more. There's something saying hey we're working on it. Here the phone number to call.

So nothing on the horizon as far as anyone knows is going to go kill Bitcoin.

Okay. Bitcoin myth number 2: Bitcoin is the future of payments. How many people believe that? Oh, wow. You guys are really trusting me, huh? Okay. So the future of payments is end-to-end security.

What that means is I take my device, I digitally sign it on my device, and I hand it over through some chain. And they can't muck with it because it's digitally signed. And, at the very end, the merchant gets it. And he can't mess with it either. He gives it to the payment provider, my bank. My bank looks at it. And they can verify my signature. And they're the guys with the funds. They release the funds to the merchants, digitally signed. That is the future of payments. That's how it's going to be done. It's going to be done just like with Bitcoin. Instead of these proprietary APIs like ACH and Visa net and stuff that none of us have any access to unless we're special people, it's going to be open API just like Bitcoin is. Anyone can do it. It's going to be all crypto based. It's will be as simple as this. Do you want to send 1.32 Bitcoins to Amazon in payment for an invoice? You shouldn't have to type anything more complicated than this on your computer to go in and make that payment. We've got to make it really simple. So a simple money transfer protocol, as Malcolm would say.

Bitcoin myth number 3: Bitcoin cannot be regulated. Hmm. Okay.

So you know what? I did a little research. And Satoshi, it turns out, he did not talk to any regulators. And he did not sit down with any

bank presidents before he designed Bitcoin.

And so, therefore, he created something that he really didn't think about regulation when he invented it. And so, therefore, Bitcoin is inherently difficult to regulate.

And, in fact, they had these hearings at the New York Department of Financial Services. And they heard from a whole bunch of Bitcoin companies. And they issued subpoenas to a thousand Bitcoin companies asking for what should we do. They asked people, "Hey, what do we do to regulate Bitcoin?" They got all sorts of conflicting messages. Some people said, "Eh, you should loosen the regulations." Other people said, "We should tighten the regulations." And the head said, "Ooh, I don't want -- money laundering is a bad thing. I don't want -- I'll kill a thousand Bitcoin companies before I will let one money launderer through the system." Sounds like tightening to me. If you tighten it, oh, okay, I'm a Bitcoin company. I have to get licenses in 50 states. Let's see. How long does that take and how many millions of dollars do I need to do that?

Turns out there are solutions to this regulation problem that the regulators actually like. In fact, they love it. And you can even protect consumers against things like another Mt. Gox happening. Cointrust is an example of one of the companies that's doing this. So I think it can be regulated.

Bitcoin myth number 4: It is safe to keep my Bitcoin in Coinbase or Bitstamp. I actually have a Bitstamp account. It's a very reliability system. They've not been breached so far. I have one Bitcoin in Coinbase. Took the other thousands and socked them away. I had predicted this back in December. And I was quoted, and Tech Review picked it up. I was speaking at a Bitcoin conference. I said if you have any amount of Bitcoin in any of these other Bitcoin places today, you're a fool. I should have been a little bit nicer when I said that, but, you know, I probably should say, "You should rethink that."

Okay. So it turns out that Coinbase and Bitstamp use the same protocols as your friendly bank. In-band 2FA. Ouch. That means compromise your machine, Bitcoin is all gone.

So I suggest -- and, you know, we've tried to talk to these companies and say, hey, there's a better way. There is a better way to secure this. But they are just -- they have an excuse list. Someone gave them that 19 list of excuses. It's not invented here. We're going to do it ourselves. Not interested. Too busy to really talk about it.

Okay. So, if you have any amount of Bitcoin, my suggestion is you keep it offline for now.

And the best place to do that is Bitcoin Armory. Now, it's not necessarily very easy to do that, but it is secure.

It's absolutely secure. Adam Back was the guy who told me about that. Adam is known as the grandfather of Bitcoin. And Adam kind of taught me everything I knew about Bitcoin, including to use the tip on using Bitcoin Armory, which I quickly downloaded and used. And then I spent about three days figuring out what the protocol was to keep the keys for my Bitcoin safe so that, if California were to be hit by an atomic bomb, I would still have access to my Bitcoin and I wouldn't have to have USB keys in multiple banks all across the country.

So safe and easy for Bitcoin storage is coming. It's not available now. But what everybody wants is safe -- is keep my Bitcoin safe and make it easy for me to access the Bitcoin. Coming in 2014, I'm sure. Not available now.

Okay. How can the IETF help? I'm not sure yet. Got to be honest on that one. When I don't know, I'll tell you. I do not know how the IETF can help at this point. But maybe in the future, things will be more clear.

So this is my contact information, if you'd like to contact me. And, if you like the presentation, great, you can use these things. If you did not like them, you can send email to devnull and that will work as well. Okay. Thank you.

[Applause]

>> DAVE THALER: So we're going to open the mic lines for about 15 minutes of technical Q&A. If you have comments or questions, get in the mic lines for right now. And we'll go for about 15 minutes. And, if you have any comments as to what actions you think the IETF can do in this space, those would be great to hear from the community on.

Russ is going to help me moderate the time and the queue here. Go ahead, Phil.

>> PHIL HALLAM-BAKER: Phil Hallam-Baker. I've been doing Internet payments now for about 20 years. My big fear of Bitcoin is that, when it crashes and dies horribly -- and it will -- it's going to be the cold fusion of Internet currencies. If you look at the inflated claims, they're claiming that there's a $7 billion market cap. Best that we can

make looks like there's about a million dollars maybe in these exchanges. So, if somebody wanted to cash out today, there would be maybe a million to cash out. Almost no commerce. This is the thing that gets me about Bitcoin. The whole point of a medium of exchange is its people have to spend it. And, if you have a currency that is deflating at 100 times in a year, as Bitcoin did last year, that is a sign of abject failure. The whole point of money is to spend it. And, if people aren't spending it, then you've not got a digital currency.

If you want to respond, go ahead.

>> STEVE KIRSCH: Yeah. Well, it's definitely deflationary. And that's why people tend to horde it. If you look at the stats, most people buy Bitcoin for investment. When I got into Bitcoin, it was $125 per coin. And I bought a 10th of a Bitcoin, so $12 worth. Three weeks later it had tripled in value. I said that's interesting. And so then I put a million dollars in at about 320. And three weeks later it had tripled to being $3 million. And I said that's kind of interesting.

So it always turns out that, when you invest a little amount of money, that's when you get the big gains. And then when you say oh, that happened, then you put the million dollars in and then you see it all disappear, right? So I think the thing about hoarding is that the Bitcoin's price will adjust so that people will, in fact, sell it at some point and decide to trade it. And there is commerce that is going on with Bitcoin. If you look at when Overstock started accepting in Bitcoin, there were lots of people who were paying in Bitcoin. And the fact of the matter is that Bitcoin doesn't always go up in price, as we've seen, that it peaked at about $1,200 per coin.

And now it's at what? Like 500, 600 -- so about -- low 600s per coin right now.

And, you know, some people will hold on to it. And other people will spend it. It just depends on what you believe in the future. Some people think that the Bitcoin price is going to $10,000 per coin. Other people think it will cap out at about a thousand. Okay.

>> PHIL HALLAM-BAKER: It's only a profit when you can sell.

>> DAVE THALER: We're going to close the mic lines for those who are up right now. We're going around in a circle right here, except for you in the yellow are after the person up front. I can't see, because I'm blinded. So go ahead.

>> ???: Just looking end points. The positives that we suffer in this

country, test guys are all Microsoft XP. And I'm just wondering, with a good combination, even weak mechanisms can give you strong security. And I think this is demonstrated by Steve's pitch as well.

So here's the question: Does the IETF potentially have a role in having an open set standards to monitor all the end points insofar as they're on the network and, if they start behaving oddly, we can pick it up?

>> DAVE THALER: Okay. Next. Reminder to state your name and keep your comments brief and to the point.

>> RIGO WENNING: Rigo Wenning, W3C. Just wanted to announce that W3C is having web payments workshop 28 of March and that we address many of the questions that were raised. So it's all available on the Web site.

>>DAVE THALER: Would you be willing to post a link to the workshop's Web site to say the IETF discussed this? Okay. Great, thanks.

>>KATHLEEN MORIARTY: Kathleen Moriarty, global lead security architect for EMC Corporation. I have a bunch of questions. I'm going to limit it to one. Can you explain the RSA token myth and how a physical token is not a second factor? We'll start there.

>>STEVE KIRSCH: How it's what?

>>KATHLEEN MORIARTY: How it's not a second factor? Pretty much that's what I surmised after several of the slides, from that specific -- I have lots of other questions, but --

(Talking simultaneously.)

>>STEVE KIRSCH: If you're from EMC, you're from RSA. So you must know -- so I think you must be challenging me on something. I said it wasn't an out of band -- it's normally not used as out of band second factor because it doesn't digitally sign anything. It's just a number.

>>KATHLEEN MORIARTY: I think you said it was in-band 2F.

>>STEVE KIRSCH: Yeah. It's in band 2 factor, not out of band. Out of band is when you digitally sign something on a second device and use a second channel, use a second -- it's independent. So that a compromise of the main computer, then it's not susceptible to that.

>> Maybe you can chat off --

>>STEVE KIRSCH: We can talk later. I'll be happy to --

>>KATHLEEN MORIARTY: I mean, there's no known attack against it. I'm not going to bother.

>>DAVE THALER: You're next.

>>DAN BOGDANOVICH: Dan Bogdanovich, Juniper Networks. In one of the slides, you were saying you were sending a challenge in the NONS (phonetic). Then you did the local calculation and then with a response back. This is what is used today in mobile telephony and SIM cards. And there are a couple of issues there as well because there is a shared secret at one point. And then you can go with the open algorithm or with an obscure algorithm. There is a problem as well.

So I don't know -- you were saying that you were breaking one of the myths with when you are doing the local computation to send it.

>>STEVE KIRSCH: Careful because SIM cards, I believe, are using a shared secret. So what I'm talking about is signing with a private key and not a secret key. So private keys are asymmetric. Secret keys are symmetric. So we're not talking about signing with a private key. I'm talking about signing with an asymmetric key. Big difference.

Anytime you use symmetric cryptography like that, you have a point of failure. Well-known.

>> MATTHEW KAUFMAN: I sat patiently through your list of myths, and I did enjoy the flexibility with which you alternately assumed that the machine could be compromised.

And then relied on the machine not being compromised.

Specifically, I would note the cases where you assumed that the mobile device is independent, despite the fact that the user routinely plugs it into the same computer to do things like update it.

And then uses that same mobile device to install the Facebook application whereupon they grant it privileges to do everything, including perhaps read the private keys from other applications. I'm not sure exactly what you're selling.

But I'm not sure I want one either.

>> STEVE KIRSCH: Okay. So... You know, it is unfortunate that manufacturers like Google have phones that can be easily compromised.

But you know what? Apple iPhones are actually really hard to compromise in comparison to an Android phone which I'm sure everyone will agree.

>> ???: Can I borrow your phone, Steve?

>>STEVE KIRSCH: So, you know, there is some truth to that. And people make compromises all the time. And if you have multiple devices and you have a mobile phone which you are using for secure auth, you have an option to just use it for secure auth and nothing else.

I happen to have a Pebble watch. I have got the new Pebble Steel. It is $250. It is a cool watch. You know, these things can be used to digitally sign transactions, just like a TREZOR or other dedicated devices.

These things, you don't load software on it very often, if at all. And they become very hard to compromise. And so you can store secrets here like storing your private key to sign transactions. So we have choices, and we have choices in terms of our mobile phone habits and how much we want to use our mobile phones and download things and how easily mobile phones can be compromised. And those things will be compromised less and less over time than they are now as we get smarter about things.

But the point is that what you're trying to do -- and there is no perfect system, and I'm not claiming there is a perfect system. I didn't claim that anything was impervious.

I claimed there are better ways to do things, folks, because you know what? Right now we have an attack surface that is huge, and it is shared secrets.

And, you know, you can have all these, you know, clever remarks that say, "Oh, your thing is not secure either." You know what? You're right. But my thing is about 100 times more secure -- a couple orders of magnitude, maybe three, four orders of magnitude more secure than what we're doing today.

And you know what we should be doing is moving in a direction that makes things more secure and not hanging on to what we're doing today, which is 50-year-old technology and which is totally insecure, and it is being proven insecure every single day.

>>DAVE THALER: Okay. I think that takes us to the end of our open mic time. I think we have drained the Q&A time. So let's give our speakers a hand here because it has been very interesting.

[Applause]

Thank you, guys. I think both of them are willing to be contacted afterwards and look forward to hearing from people. So I will hand it back to Russ for the last portion.

>>RUSS HOUSLEY: Thank you. Okay. Could we have the IAB incoming, outgoing and continuing all come to the stage, please.

Would you introduce yourself?

>> Hello. I'm Erik Nordmark.

>> Mary Barnes.

>> Bernard Aboba.

>> Andrew Sullivan.

>> Hannes Tschofenig.

>> Joe Hildebrand.

>> Heather Flanagan.

>> Xing Li.

>> Lars Eggert, ex officio.

>> Russ Housley.

>> Alissa Cooper.

>> Dave Thaler.

>> Eliot Lear.

>> Jari Arkko.

>> Joel Halpern.

>> Brian Trammell.

>> Ted Hardie.

>> Marc Blanchet.

>> And Ross Callon.

>>RUSS HOUSLEY: Open microphone. Do you have any questions for the IAB?

>> SEAN TURNER: Sean Turner, soon-to-be a former IESG member. One of the things that I find interesting having been around for a while is filling out the feedback in NomCom. And one of the things I have thought about doing, IESG feedback, it is pretty straightforward about what you can do, like this guy didn't produce documents fast enough, he didn't help this or that.

With the IAB, sometimes it is interesting to try to figure out what kind of feedback we should have because we don't know sometimes what additional things they would like to do now that they're on.

So I'm curious if the new IAB members and maybe the ones that are staying on, not now but maybe in the soon-to-be future, would like to give us an idea of the things they would like to do in the next year to two years. So that there is some way we can kind of figure out whether or not they did that.

I mean, I don't know. So IESG, it is pretty straightforward, right? You start working groups. You do stuff. It is kind of like -- very functional. You go through telechats and things.

And the IAB is a little bit more nebulous, and that's perfectly okay. But I would like to think that you guys got put on the IAB to do architectural work, whatever that is, for you to define it. And it would be nice if you could tell us what that is.

>> JOE HILDEBRAND: So I think that's a fantastic suggestion. It is completely reasonable, and I will sign up to do that at some point in the next month or so.

>> SEAN TURNER: Yeah, it doesn't have to be done now. You could do it in six months. I don't care when.

>> BRIAN TRAMMELL: Me, too.

>> SEAN TURNER: Great. I mean, you don't have to do it.

>> HANNES TSCHOFENIG: Sean, as I'm leaving, I can say something.

>> SEAN TURNER: Are you throwing the hand grenade back?

>> HANNES TSCHOFENIG: No. But joke aside, from my past four years, I particularly enjoyed working with the community on the workshops. I think that was something that was quite interesting for me getting to know a lot of the IETF participants from different areas.

And from the feedback I had gotten after the workshop, sometimes it was a difficult workshop. But I thought, like the others, like, the socializing and networking aspects as well, I thought bringing new work to the IETF is certainly an interesting aspect of the work. And, hopefully, some of the other guys will continue that as well.

>> ALISSA COOPER: Can I also comment as an outgoing member? I would just say that like many other jobs, there's some parts of the IAB work that are really not predictable in advance. Like, I don't know who's going to say, like, when we have a falling out with another organization with which we would liaise, I want to handle that well. No one is going to say that in advance. Sometimes those are some of the really more important things that IAB can do in a pinch. Or I want to appoint really good people to the (indiscernible) I received or whatever.

So I would just say, think about that. Everyone's going to state their goals in terms of the affirmative architectural things they want to achieve. But there is other really important functions of the IAB that should be taken into account as well.

>> SEAN TURNER: Absolutely. And those are clearly demonstrable, though.

>> ALISSA COOPER: I don't know about that.

Some of it is behind the scenes.

>> RUSS HOUSLEY: Okay. Eliot and Marc, and we will go to the next person.

>> ELIOT LEAR: Having just been reappointed, there are a couple of things I would like to accomplish. One of which is to help the Internet community get through the next year in terms of Internet governance relatively unscathed and to work with interested players to see that that happens.

Talking about that in terms of Internet governance, yeah.

>> MARC BLANCHET: I will resume by: We're doing all the dirty work so that you guys, IESG, do the real work.

>> RUSS HOUSLEY: Okay, Russ and then Mike.

>> RUSS MUNDY: Russ Mundy. Thanks. I'm actually here more as a comment and to stand up so people know me. I'm your liaison to the ICANN NomCom for the IETF, the IAB. And this is the time if you're interested in helping out and getting more technology expertise into ICANN, consider volunteering for the ICANN NomCom. If you want to know more, look me up later in the week. I'll have an ICANN hat on. And be happy to talk to you about what's going on there.

>> RUSS HOUSLEY: Thanks, Russ. And we appreciate you accepting that job.

>> MICHAEL RICHARDSON: Michael Richardson. One of the things I learned recently is that it has always been a role of the IAB to be involved in BoFs and creation of new working groups. And this is not a new thing that they have done more recently.

And I notice this because I want to compliment all the people at the table. The last two years I have really, really noticed the presence of IAB people in the BoF formation process. It is much more obvious and maybe more explicit. It has been really, really cool.

As far as I'm concerned, most of the BoFs I have been to have been pro forma, were already done. So I want to say I think that's an excellent, excellent thing and I think it is extremely useful because we had a lot of people coming with new, crazy ideas and figuring out what -- whether they even belong in the IETF is sometimes daunting.

I want to say I think it is really, really good and I think it is really a good thing, and I hope it is something you continue to do well. So thank you.

>>RUSS HOUSLEY: Thank you.

>> ALISSA COOPER: I would just say, we should probably give a bit of thank you to Spencer Dawkins for his initiation and getting us a little formalized in how the IAB engaged in BoF creation. So, thank you, Spencer.

[Applause]

>>RUSS HOUSLEY: Spencer, are you trying to reply or are you running?

>> SPENCER DAWKINS: All of the above. Spencer Dawkins. I was going to say this was all part of my plan to have you all helping me.

>> RUSS HOUSLEY: Wes.

>> WES GEORGE: Just a quick question. Could you talk a little about how you vet the speakers for the tech plenary?

And whether or not you review their slides ahead of time to determine whether they're a sales pitch.

>> RUSS HOUSLEY: You want to lead that one?

>> DAVE THALER: So the first question is how, in general, do we vet speakers. And the second one is how do we review the slides.

Let me just tell you what we do. So, first, we try to get speakers. We get a bunch of people that are potential ones and we say what are the topics we think are the most relevant to the IETF. So this is the first part of the question, which is -- one of the rules that we have for plenaries or one of the guidelines we try to follow in general is a plenary should be ideally informative or entertaining, preferably both. In other words, we don't want people to fall asleep and we want the audience to get educated on some topic. And so we look for a topic that kind of fits both criteria that can keep people awake and that they can learn something. So that's how we choose topics.

Then how do we choose speakers? We say, who would be a good speaker on these particular topics? We look at the news. We said, "Boy, Bitcoin is a popular topic. We think that's something that would draw people. That's something that there's a lot of passion about learning about. A lot of people don't know how it works. Payment systems are in the news." We talked about that in the newspaper. And so we say: Who is it that can actually speak on these things?

So on the Bitcoin topic, we learned that there is actually a Bitcoin workshop going on right now. And so some of the people that are directly involved with Bitcoin are actually off the table, although we did try to talk to some of them.

We said who else can talk about Bitcoin? Who else can talk about payment systems?

So we go through a bunch of names. And we say who are the best people to talk about these particular topics: The security aspect, mobile systems aspect, and so on. That's the general process that we follow.

On the slides, we do vet the slides. The slides go through the IAB. I think both slides went through, I don't know, four to seven different iterations each. That's normal for each plenary.

This time I think we actually went through more iterations than we normally do. Often we don't get the slides until fairly late. This time we started getting slides at least two weeks in advance, which doesn't always happen.

So we can do better, but we're actually better than some previous plenaries as far as when we get slides and things. That's the general process we follow.

>> WES GEORGE: Were you pleased with the result there?

>> RUSS HOUSLEY: One thing we have been doing for the past few meetings is including on the end of the meeting survey questions about whether you like the plenary topics and so on and that we will definitely be continuing to do that. So please continue to give us your feedback.

>> HANNES TSCHOFENIG: I just want to respond directly to the question. In general, sort of we prefer, obviously, if there's from outcome of plenary, is if there's any idea for us on what we could be doing. And the payment topic is rather new. That type of payments, crypto currencies and these type of thing, something we haven't worked on in the IETF so far. Thomas Roessler mentioned they're doing a workshop. And there's an interest group, sort of a research group in the W3C terms looking at that topic. And maybe, at some point in time, there would be a chance to have a look at some of these protocols. Obviously, there's a lot of deployment and other aspects that are happening with the IETF itself doesn't have a lot of influence on directly. So we need to keep an eye on this. And maybe some of the folks in the audience have been involved in some of those payment protocols in one form or the other. I'm aware of people who use OS with extensions as a payment protocol. So that would be interesting to socialize, see whether the IETF can actually help to improve some of those things. On the SSO solutions we're already working on, it's making good progress.

>> DAVE THALER: Sometimes, when we look at plenary topics, we have to make sure they appeal to all areas, not too focused on one of the seven Areas that we have and, secondly, that it's not too focused on, say, North America. So we look for topics that might have a worldwide appeal or a multi-regional appeal as well as multi-Area appeal. Topics that would be not just for a single Area but of interest to all of us as end

users or all of our Areas.

So, for example, in Malcolm's topic, he talked about the different types of ecosystems all around the world. We might be familiar with our part of the world but much less familiar with the [other] ecosystems around. In
the IETF we need to be designing solutions for all of them. So part of the question, when we have these topics, is it's not clear is that is there to the IAB or for the IETF to do? So part of the point to the plenary is to say is there some work for the IETF to do in this area? And often we don't know, and part of the point of this is to get feedback from the community to see if there is. So an example of the payment systems, we learned that protocols that they use are proprietary systems and they're so diverse, there's so many different ones, there's no standardization whatsoever.

So kind of the question there is, well, that's kind of an interesting topic that kind of goes on behind the scenes. Is this something that should be part of the IETF or not? And we don't know. So we said that's actually kind of an interesting topic that should the IETF be trying to standardize protocols in this space? Or is that the job of somebody else? Or what? So just educating the community there was an example of something we thought would be valuable to learn about and get feedback is this something for us to do here? I didn't see any specific comments or feedback on that. So I wasn't as happy with the fact that there weren't discussion of what, if anything, should the IETF do around payment protocols. So that's something I would encourage people to follow up with Malcolm or on the list about to say we'd still like to find out is there anything that we need to do here given that there is no standardization going on right now across these different protocols.

>> MARY BARNES: Okay. My point was that I wanted to make a more general comment and not explicit on this plenary is that we do welcome input from the community. Russ sent an email; it's probably been about a year. We do have a list of proposed topics. We have been following up with some of the suggested speakers and stuff. So, if you guys have things you want to hear about, let us know. Otherwise we have to kind of work from our own -- you know, our own ideas and people that we know.

>> MARC BLANCHET: To your point with, I think, probably most of us would say there are some plenaries that are more interesting, some less. And maybe the more or less depends on each person and may not be the same. I would like to point out that it's not necessarily easy to get, you know, speakers organized all this. And you know, and if you remember, not that far away, we actually changed the plenary time to

accommodate to have -- you know, a speaker we wanted. So -- you know, so it's not easy.

Moreover, for the speaker point of view, I was always more, quote, unquote, more interested in plenaries that were not from our, you know, people that we know, our community, from people outside. So we get -- you know, different perspective. But then the challenge is that those people that come here never come here -- don't know -- you know, exactly how we work, what we do and stuff. So that's the challenge. It's difficult.

>>ELIOT LEAR: Yeah. I was going to follow up on a point that Dave made. I'll be brief. The chip and PIN that we use here in Europe is a perfect example of a system that has been demonstrated to have flaws, in fact, by a professor at Cambridge who hosted the ITAT workshop. And one of the key issues he raised publicly was a lack of open standards. It's an absolutely valid point. One of the questions that IETF and IAB should be looking at is what are the bounds of work that gets done here? And I think, generally, the answer is, well, if you come here and you bring the work here, then we can at least consider that. So not only -- now that we're aware, maybe one of the things we need to be doing is doing outreach to those communities and say why don't you follow the principles that we use that give you fine review. You can spot security problems earlier rather than when you have a two billion person deployed base or something like that.

>>KEITH MOORE: I'd like to make a comment about speakers and just a comment about IAB in general. What I'll say is about speakers. It's not necessarily a bad result if people don't find themselves agreeing with a speaker. If the speaker has provoked thought, if he's encouraged anyone to do better, if he's encouraged to refute what he's saying, even in their own minds or in discussions within IETF, those are good things. So please keep bringing speakers that cause us to think.

The second point I'd like to make, I think, is perhaps more to the function of the IAB, main function of IAB. My impression over the years has been IAB spends a lot of its time doing what I would call political work. I'm glad that -- I think IAB has generally done a good job at those things. I'm glad that we have senior people looking into those areas, although I do think -- suspect that a role that has been somewhat back seated since Cobi for those who remember that, is architectural direction. And one way I would interpret that is anticipating and managing tussles. That's a difficult and subtle kind of work. I know IAB spends some of its time doing it. But I feel like more than ever, it's been something that's -- we've struggled with for years. And I think more than ever we need to strengthen IAB's role in that. IAB's

powers are limited, and that's perhaps unfortunate. But I think, perhaps, the community needs to see what we can do structurally in the organization to anticipate and manage tussles.

>>RUSS HOUSLEY: So, Keith, I didn't put the slide up this time because we had a lot of material to cover in the reporting time.

But we are publishing more guidance RFCs in the last couple years than we have for a long time. We are trying to do that. You saw in the list of documents we're working on, some of them are RFC editor, some of them are guidance, and some are PCP related. So we heard that in other parts of the community and are doing our best to do so.

>>JARI ARKKO: I just wanted to say that, even if you're not necessarily seeing the IAB here declare all kinds of architects or thoughts from the podium or directly publish themselves RFCs on topics or drive new things, I think most of the work actually happens in -- look at some of the workshops that they have happen like the security workshops just before this sponsored by the IAB. So I think that's the value of the IAB, making things like that happen. And it's not necessarily the IAB members themselves, you know, writing documents or driving discussions, but making these discussions happen. I think that is happening.

>> Dan.

>>DANIEL MIGAULT. Here's a proposal for a speaker at one of the next IETFs. It would be interesting to hear about RINA Recursive Internet and the Internet Architecture. And that would be some, you know, thought provoking, you know, subject that they could bring up.

>>RUSS HOUSLEY: Thank you. Phil.

>>PHIL HALLAM-BAKER: So, over the past few months, due to Snowdenia, there's been a huge amount of interest in pervasive surveillance. I think that we should make sure that we don't take our eye off the other ball, which is just how fragile this digital world we have created is. And we saw some evidence of that recently with the Russian invasion of South Ossetia. And if, like me, you followed the cyber attacks that were part of that invasion, they rerouted BGP so they could take over the Web sites, so they could impersonate the government of Georgia and tell people to lay down their arms. We've seen -- since seen a great deal of enthusiasm about the role of the Internet in the Arab Spring. But I think that we need to start looking at how do we make the Internet robust against attack, not just in terms of how do we stop people breaching confidentiality, but how do we stop people from stopping the

Internet and impersonating people and governments and all that stuff and not get distracted into thinking that Snowden is now the only problem that we have to face?

>>TED HARDIE: So one of the main reasons that I joined the IAB or threw my hat in to join the IAB was, in fact, to take the security and privacy programs and to really, seriously, ramp them up. I think that the IAB needs to do a great deal more than it has been able to do in the past. And that means one of the main things we'll be doing is recruiting, reaching out into both this community and some other communities that have been identified for people who can help develop, frankly, systems engineering approaches to the problem. A lot of what we've done in the past is describe particular parts of the issue or describe the roles of particular network elements in the network.

And we have to go beyond that to describe a systems engineering approach that enables us to describe how you put all pieces the IETF builds together to create an Internet that is both effectively confidential end to end and robust against certain types of attacks. In the STRINT workshop there was a point made that I agree with and also don't agree with. And the point is, to some extent, what we're talking about is an engineering quality issue. And that's true, but I think it masks the extent to which this engineering quality issue is a threat far beyond the Internet. And the reality is the Internet has become a tool for communication sufficiently important that disrupting it is potentially harmful at the scale of humanity itself. And the parallel I made in the workshop in sort of the small was, if you were a water quality engineer and discovered anybody had the capability to divert the water supply of your major river through their own property, even if the one you saw diverting it did it because they wanted to look at the pretty fish, you'd be rearchitecting to protect it from people who would do it for far more harmful reasons. And I think that's the scale of problem we have in front of us. And it crosses well outside of the usual security area through every single one of the areas of the IETF and beyond into territories like user experience that we're not very comfortable with.

But that's the task we have ahead of us. And I think the IAB recognizes that it has that task and is willing to take it on by reaching into the community for the people we need to work on it. Because there's no way in hell these 13 people, even with the people who are leaving, could do it by themselves. So thanks for volunteering. And we look for more.

>>RUSS HOUSLEY: Okay. We've run over time. And there's no one at the mics, so have a good evening.

[Applause]

--END OF TRANSCRIPT--