KATHY SCHNITT: Welcome to the Evolution of the DNS Resolution Work Party Teleconference on Thursday the 13th of July 2023. Barry, back over to you.

BARRY LEIBA: Well, I'm happy it's not tomorrow. So Friday the 13th. No, you wouldn't want that, so Thursday the 13th is better.

Yeah, so Andrew has Section 8 queued up on the screen. I'm sorry, Steve, who is Andrew for the day, has Section 8 queued up on the screen. And I'll just let Steve take it away. We're going to go through it.

STEVE SHENG: Yeah. Thank you, everyone. So some context here. Section 8 is about implications of Ambiguous Internet Name Resolution. Geoff Huston wrote some really good text, and then Andrew made quite some comments. This part of the call is to review Section 8. And then I'll probably start resolving things and taking people's notes for changes to the section.

So with that, does everyone on the call have a link to the document?

TARA WHALEN: I got it.

STEVE SHENG: Okay. Then let's start reviewing Section 8. I'll give people probably three, maybe four, four to five minutes. Review up to the paragraph. So don't review these bullet points. Just after the paragraph. So I'll give people four minutes.

RUSS HOUSLEY: I don't know if this is worth raising, but in the first paragraph, the remote server was the correct one. [At that era], it was the remote host. We're talking Telnet. Very—

GEOFF HUSTON: [inaudible]. You kind of slip into current nomenclature, [don't you]?

RUSS HOUSLEY: Yeah, right. I just don't know if that is worth highlighting or not.

GEOFF HUSTON: Well, what I wanted to highlight was the fact that if you addressed a packet to the intended destination address, you could always believe the answer. And it was kind of, in retrospect, gee, that was naïve. But that was what we assumed. The entire DNS just relied on that, and so did everything else.

BARRY LEIBA: I think the word that we really want to put there is "service."

GEOFF HUSTON: Okay.

RUSS HOUSLEY: [Sure].

BARRY LEIBA: Because we talk about services later on, and I think it's a good segue into it if we start with that word there.

WARREN KUMARI: It's certainly somewhat true that ... I mean, this sounds like nobody believed that there was such a thing as a man-in-the-middle attack. Or I'm completely misunderstanding this.

RUSS HOUSLEY: Nobody was worried about it because they all knew each other.

BARRY LEIBA: Yeah. I get what you're saying, Warren, but the ... Sure, a packet could still be sent to the correct address, but it wasn't really the one you thought it was. And you don't really have the right thing. I think that's out of scope for what we're trying to talk about here, though, and I'd rather not confuse things by trying to throw that into it.

GEOFF HUSTON: The point that I was trying to make, and I think it's certainly true from my sketchy memory of the 1980s, was that addresses were the glue. You know?

BARRY LEIBA: Yes.

GEOFF HUSTON: If you had an address, you were connected. And if you sent a packet to that address, the thing at that address answered. And you never really questioned that as a general assumption. So the protocols we built were based around addresses because, why wouldn't you, you know? And that's the informal sense that I'm trying to convey here.

WARREN KUMARI: Okay. So I guess I kind of got that. I think it's also, it used to be much more, that an address and a—I'm going to say service, but that's not really what I mean—were largely interchangeable, right? It was that if you sent a packet to a server, there was only one web server listening on that, and it only believed that it was one thing. Right? Like, name-based virtual hosting didn't really exist [that far back].

GEOFF HUSTON: Oh, oh.

RUSS HOUSLEY: Oh, that's true. But Telnet and FTP were very common on mainframes.

WARREN KUMARI: Yes.

GEOFF HUSTON: Right. Telnet, FTP, Gopher. You name it.

RUSS HOUSLEY: Exactly.

GEOFF HUSTON: They're all lumped on the same mainframe, and your multiplexing was basically the port address.

WARREN KUMARI: Yes. But also, that's ... We might be saying very similar things. But also, when web stuff came around, it was still ... 192.0.2.3 was www.foo.com, and 192.0.2.4 was www.bar.com. The address and port uniquely identified the thing. Whereas now, that's not true.

RUSS HOUSLEY: I think the thing you're talking about is what Barry was striving for, the remote service identified by the IP address and port number.

WARREN KUMARI: Yes. Which I don't ... I don't think that's [inaudible].

RUSS HOUSLEY: That's no longer necessarily true.

BARRY LEIBA: Right.

WARREN KUMARI: Now we have multiplexed or overloaded the address and port so that the way that you request a resource is its address and port and name.

GEOFF HUSTON: Right. And that's the point I'm trying to get to. And I'm also going to go one step further and say you know addresses don't matter. It's actually the name.

WARREN KUMARI: Yep. Yes. Yes and no, I mean [inaudible].

BARRY LEIBA: Well, yeah. I mean, it's not absolutely so, but it's increasingly moving in that direction, is the point.

GEOFF HUSTON: Well, I can go to Akamai, and so can you. And I bet you we get different IP addresses to go to the same website.

BARRY LEIBA: Right.

WARREN KUMARI: Yes [inaudible].

GEOFF HUSTON: And that's my point. The address doesn't really matter.

WARREN KUMARI: Yeah. But this also is based upon the service that you're talking about, like WEB. If I SSH to Akamai or I SSH to my home, there's definitely some difference there. Certain services like WEB are overloaded. Or, you know, the name is ... The address ... The name is more important than the address. Other—

GEOFF HUSTON: Right.

WARREN KUMARI: —that's not true, like SSH [inaudible].

GEOFF HUSTON: Right. But in terms of the Internet, as consumers see it—you know, the mainstream Internet—names assume primacy of role, not addresses anymore.

WARREN KUMARI: Yes.

GEOFF HUSTON: So when we start talking about ambiguity of resolution, you're actually talking about a big topic then. That was the whole idea of these paragraphs.

WARREN KUMARI: Yep. I think I'm just trying to say, you know, we can't be too absolute in [inaudible].

BARRY LEIBA: No. And I don't think what's here is absolute. It's talking about a trend. I think this ... To me at least, this is the direction I think is where we want to go, so ...

WARREN KUMARI: Yep.

STEVE SHENG: Okay. Sounds good. So [inaudible].

RUSS HOUSLEY: Do you want me to that change?

WARREN KUMARI: [inaudible] wasn't the correct address [that would] still make [me] twitch slightly. But not enough that I care.

BARRY LEIBA: Okay.

RUSS HOUSLEY: Do you want to make that change there, Barry, for "remote service," comma, "identified by the host and port"?

BARRY LEIBA: Yes. By the address and the port.

RUSS HOUSLEY: Address [inaudible].

BARRY LEIBA: Yeah. So "service"—

RUSS HOUSLEY: IP address. Right.

BARRY LEIBA: "Service" or ... Here, Steve, do you want me to type it? Let me ... Oh, he's got it. Okay. "Identified by the host, by the address and the port," comma. Okay.

[RUSS HOUSLEY]: Good.

[GEOFF HUSTON]: Yeah.

STEVE SHENG: All right. I want to get us ... I want people to read through the paragraph and get a general sense if these are okay before we start accepting things. Anything that jumps out [in front of] you that things are missing, areas that require significant improvement?

BARRY LEIBA: I'm going to make a little tweak here.

GEOFF HUSTON: That's right. That's more English. I think my expression was more Germanic. Maybe I should have put the verbs to the end.

BARRY LEIBA: Yeah, because one of ... The angle that I'm going for with this change is to get the sense that it's still increasing. That this is something that's—

GEOFF HUSTON: Oh, yeah. Yeah.

BARRY LEIBA: —been happening and is continuing to happen more and more.

RUSS HOUSLEY: Well, interestingly—Geoff will probably take issue with what I'm about to say—but because TLS, which was raised earlier, binds a domain name to a public key, that is another ... That is why the trust is moving to the name and not the address.

GEOFF HUSTON: Oh, geez, Russ. Cart and horses.

RUSS HOUSLEY: I know. But it's—

GEOFF HUSTON: And you're right. We know where we are, but who dragged us there?

RUSS HOUSLEY: Oh, yeah.

GEOFF HUSTON: It is entirely coincident, fortunate, whatever.

RUSS HOUSLEY: The CAD Forum.

GEOFF HUSTON: Right. But, no. But we actually certified names.

RUSS HOUSLEY: Yes.

GEOFF HUSTON: And I guess if addresses really had been important, we might have got into certifying them earlier, but the thought and the impetus was never there because by the time we thought hard about—

RUSS HOUSLEY: Exactly.

GEOFF HUSTON: —the name folk were there, and it's kind of, "Yeah, fine."

RUSS HOUSLEY: That's right.

BARRY LEIBA: Well, and [the thing is]—

RUSS HOUSLEY: I agree with that, but I think it ... The statement about the trust in the integrity is tied to the name just because that's what we certify.

BARRY LEIBA: Right. The address is what's important for the protocols to work, but the name is what's important for the trust model to work.

RUSS HOUSLEY: Right. And I don't know ... Well, the bits are all here. We don't really say that, and maybe that's what we need to say at the end. I don't know.

BARRY LEIBA: Because then that brings us to different trust models or different trust roots. I don't know. I don't think I want to say "root."

RUSS HOUSLEY: Trust stores. Right?

BARRY LEIBA: Yeah, trust stores.

RUSS HOUSLEY: I mean [inaudible].

BARRY LEIBA: There you go. Different trust stores are now operable with different naming systems.

GEOFF HUSTON: You see, I don't think it's accidental that NATS came before even the early versions of SSL. You know [inaudible].

RUSS HOUSLEY: So SSL was shoved in the stack where it was because Netscape couldn't change the kernel.

GEOFF HUSTON: Right. It was a Netscape—

RUSS HOUSLEY: Right?

GEOFF HUSTON: —sort of experiment. Yes.

RUSS HOUSLEY: You know, it's really true that when you got that stack of floppies in the mail and you wanted to install the Netscape browser, there's no way you

could do a kernel mod. You know, all these people who were installing them on their houses, so it had to live in user space.

GEOFF HUSTON: Right. But it also had to live ... Because in theory, you could drag the address back out of the protocol stack, the underlying libraries. But using the name was both convenient for what you're saying. It was there already.

RUSS HOUSLEY: Yeah.

GEOFF HUSTON: And B, if ... Even the folk at the time, if you thought about it, this whole NATS thing, it made the address notion somewhat rubbery.

WARREN KUMARI: But, I mean, the whole ... Part of the reason that we have names instead of addresses is because they're easy to remember. But also, more usefully, it's an abstraction or decoupling mechanism so that you can take the same content or thingy and move it about. And I think that had been true for a long time. So having—

GEOFF HUSTON: But the telephone—

WARREN KUMARI: So having a certificate or assertion or anything similar about an address doesn't really, really make a huge chunk of sense because that removes your ability to move the resource that you're talking about.

RUSS HOUSLEY: Yeah. Renumbering has always been painful. And if you had to renumber and recertify, it would be even worse.

GEOFF HUSTON: Yeah. But I would argue the telephone network did that with the equivalent of 1-800s, 1-300s, all those mapping services. And although it was a pain in the butt, they did map number to number and kind of got away with it.

WARREN KUMARI: Sure [inaudible].

GEOFF HUSTON: It wasn't necessary that you had to move to another identifier abstraction—i.e., names—in order to get where you wanted to go to [inaudible]. It wasn't a necessary thing.

WARREN KUMARI: No, it's not necessary, but it was a [convenience].

GEOFF HUSTON: Right.

WARREN KUMARI: And, I mean, it was possible to get—

GEOFF HUSTON: Right.

WARREN KUMARI: It is possible to get number certification, certificates. It's weird and difficult as all hell, but it is doable.

BARRY LEIBA: But you can't compare this with the telephone system because the trust model is entirely different. And people do base their trust on the phone number, but it's an informal thing. And that's one of the things that's made STIR and SHAKEN more difficult.

RUSS HOUSLEY: Oh, let—

BARRY LEIBA: [inaudible].

RUSS HOUSLEY: Okay. Let's not go there because that has nothing to do with name resolution.

GEOFF HUSTON: [inaudible] down a big hole.

BARRY LEIBA: I'm just saying that you just can't compare what we're talking about with the phone system. And there's no—

GEOFF HUSTON: Yeah.

BARRY LEIBA: —trying.

STEVE SHENG: Can we focus on—

WARREN KUMARI: I mean, it was also clear that using numbers as identifiers was always weird. Like, 1-800-MATTRESS and "leave off the last S for savings." Right? That was a common ad for a while.

RUSS HOUSLEY: Yes.

WARREN KUMARI: And it was clear that was something that didn't work well. Right? "1-800-MATTRESS, leave off the last S for savings." People are trying to overload a naming scheme and put—or, sorry, a numbering scheme—and encode some sort of semantic into it. And I think that's also kind of true of the DNS. Right? The DNS was not supposed to be something where you could sell business.com for however many millions of dollars it was sold for. But that's a separate rant.

BARRY LEIBA: Right. And Steve was about to say let's get back to focusing on the text at hand.

STEVE SHENG: Yeah. Let's focus on [text]. We have a few sections to go through. I have not heard anyone that these texts that Geoff wrote that Andrew edited is in the wrong direction, so I started accepting them.

One question I have is a easier comment to address in page 31. Geoff, you're saying "names are increasingly [become] invisible." What Andrew suggested: "increasingly becoming inconspicuous" or "less salient."

GEOFF HUSTON: This was borrowed text from a prior version of the same document, and I just—

STEVE SHENG: Okay.

GEOFF HUSTON: —sort of folded it back in. And the point that Andrew—I think it was indeed Andrew, but it was an early discussion of this group—was even the names themselves are now QR codes. They're now not necessarily the anchor points that users actually use to say, "Where did I get to?"

STEVE SHENG: Right.

GEOFF HUSTON: And it was almost a parenthetic comment about QR codes and invisibility. And—

WARREN KUMARI: Well, actually—

GEOFF HUSTON: Sorry, go ahead.

WARREN KUMARI: Sorry.

GEOFF HUSTON: No, no. [inaudible].

STEVE SHENG: I will change this to "less conspicuous" because it covers a broader aspect. Even the QR code, if you click on it, you hover over and you can still see the URL. It's just, users don't usually do that. And the—

BARRY LEIBA: I had put this as less relevant to the end user.

WARREN KUMARI: I think we should keep ... "You know, "less conspicuous," I think, is useful, but I think we might also want to add something about "and sometimes invisible" or something. Because my standard example of this is when I go to Facebook on my phone, I have no idea what the name is that the Facebook app is connecting to. Right? It uses some address in the back, some name in the back. I have no idea what it is.

STEVE SHENG: Okay.

WARREN KUMARI: And my app abstracts the name away from me [or sort of] [inaudible] the name.

STEVE SHENG: Right. So I changed to "a name increasingly becoming less conspicuous and [inaudible] is invisible to the end user."

BARRY LEIBA: Okay.

WARREN KUMARI: Thank you.

BARRY LEIBA: I just made a comment. What do you think about that text?

WARREN KUMARI: Okay.

BARRY LEIBA: So not "invisible," but "less visible." That works, I think. And the point also, to me, is relevance that—

WARREN KUMARI: Yeah. I think that works. I mean, I think in some cases, it is actually invisible. I believe that iOS ... The Facebook app on iOS does not connect to facebook.com. It actually connects to fbcdn.net or something, which is only visible if you TCP dump.

GEOFF HUSTON: Well—

WARREN KUMARI: Don't care. Not important.

GEOFF HUSTON: I have a problem with "less relevant." And even though something's not up-front and in your eyeballs, it's still astonishingly relevant. It is my understanding, and indeed fervent hope, that were I ever likely to connect to Facebook and hell freezing over, that my connection would be both secure and authentic.

BARRY LEIBA: Right. [inaudible].

GEOFF HUSTON: And what that means in my mind is that, you know, the app that I'm using has done some kind of name-based TLS authentication and session encryption to establish that. And for the app, the name is really important. And that means it's really important to me the user, even though I don't know the name.

BARRY LEIBA: My point here is that it's ... Yes, it's relevant behind the scenes. It's not relevant to the user. You don't care whether it's facebook.com or fbpotato.net or whatever, as long as it gets you to Facebook. That part [inaudible].

GEOFF HUSTON: As long as the app gets to the place it intended to get to.

BARRY LEIBA: Exactly. So from your point of view, the app needs to do the right thing, but the name is not relevant to you. [inaudible].

WARREN KUMARI: A good example of that is Morgan Stanley. Right? I don't know if it's S-T-A-N-L-A-Y or E-Y. And even if I did know, I wouldn't trust my typing. I go to Google and I type in "murga staldaly", and it turns out that it's morganstanleyclientserv.com, is the actual name. That name, sadly, I don't know whether it's truly correct.

To some extent, the thing that ends up first—and I realize this is a terrifying statement—but the thing that ends up first is the thing that I am often trusting. Right? Like, the most searched for thing on Google, I believe, is still Facebook or YouTube or TikTok. I just don't remember which at the moment.

STEVE SHENG: Okay. Thanks, Warren. Barry, I would make the point that "relevant" is a judgment call.

BARRY LEIBA: Yes.

STEVE SHENG: But "conspicuous" and "invisible," those are observables. So those are not judgment calls. So for me, I cannot tell if your user's considered relevant or not. That's a judgment that an end user makes, but we can

observe these ... These names are less conspicuous and invisible. So in that line of thinking, I will argue to keep the current text.

BARRY LEIBA: So I think that the fact that ... And I don't think it's that much judgment, really. I think it's becoming ... It's pretty easy to demonstrate. And I think the fact that the users themselves are not concerned with the names the way they used to be is important to the conclusions we're drawing in this, and to the motivations behind and success of the alternative naming systems.

STEVE SHENG: But how do we know users don't care? For example—

BARRY LEIBA: Exactly what—

STEVE SHENG: —I as a user cares a lot even though they may be invisible. But once I understand it, it's relevant to me. So I'm just pointing that it's—

BARRY LEIBA: Right.

STEVE SHENG: It's not universal in that regard.

BARRY LEIBA: [It's not]. What I'm saying is first of all, we can't judge what end users think based on us because we're weird people. But even so, Warren's example of Morgan Stanley or how you actually get to Facebook, what name you actually wind up using to get to Facebook, is not something that Warren cares about. Warren cares that it got to Facebook or that it got to Morgan Stanley. And, again, as he said, the most common thing to search for in Google is Facebook. That's how people get to Facebook. They don't type facebook.com, and they don't care whether it's facebook.com or some other string as long as it's Facebook.

STEVE SHENG: I will argue maybe in the first instance, they don't care. But in subsequent instances, they may actually care.

BARRY LEIBA: Okay. I'm not going to ... I've said what I needed to say. I'm not going to argue the point anymore, so ...

STEVE SHENG: All right. Let's move on. There's one text Andrew flagged here. It says "informally." Andrew's point [is:] is it really informal?

GEOFF HUSTON: I'm acutely aware on this call that there are a number of folks who know a lot more about this than me, and therefore I prefaced it with "informally" that if I got the details wrong, I had an out.

STEVE SHENG: Do we delete this "informally"?

BARRY LEIBA: Yeah. I'm fine with that.

STEVE SHENG: Okay.

RUSS HOUSLEY: Why don't we just delete to "now, names are increasingly the foundation"?

BARRY LEIBA: [inaudible][don't] start the sentence with "now."

RUSS HOUSLEY: All right. Just "names."

STEVE SHENG: What? I'm sorry. What was it?

GEOFF HUSTON: Not the sentence with the word "names."

RUSS HOUSLEY: "Names are ..." Just [delete] three more words.

STEVE SHENG: Oh, okay.

BARRY LEIBA: That was what Russ was saying before.

STEVE SHENG: Okay, sure.

WARREN KUMARI: I mean, do we actually note anywhere, and I can't remember, the fact that what we actually ... Like, when you get the pretty lock icon, what that is actually saying is that the name that you have entered and the name and the certificate that was presented match.

BARRY LEIBA: Right. It's—

RUSS HOUSLEY: But that's no longer the case.

BARRY LEIBA: Right.

RUSS HOUSLEY: Because now it's not an address bar. It's a—

BARRY LEIBA: Right.

RUSS HOUSLEY: I don't even know [inaudible].

BARRY LEIBA: So what it's saying is that the path in the URL that you wound up going to matches the name in the certificate.

WARREN KUMARI: Yes.

BARRY LEIBA: But that is less often something the user understands than it used to be.

WARREN KUMARI: Yeah, yeah. I fully agree. But what's actually being certified is the name. Right?

BARRY LEIBA: Yes. The string [inaudible].

WARREN KUMARI: I don't know if we mention at all in here in the document that the name—

GEOFF HUSTON: I didn't, Warren. The previous sentence, I sort of slid across this at a enormously high altitude. "The service name was cast into the role of service identifier, and the trust model in the authenticity of the service was built upon this framework, i.e., the name as the service identifier."

WARREN KUMARI: Okay.

GEOFF HUSTON: [I said] trust is based on names, and that was all I said.

WARREN KUMARI: And, I mean, one sentence ... I mean, I'm sorry, one paragraph up, we do also mention TLS.

RUSS HOUSLEY: Yeah.

GEOFF HUSTON: [Right.]

BARRY LEIBA: [Right.] I think that sentence that was just highlighted that Geoff just read is accurate and sufficient for the purpose that we're writing this. I like it.

WARREN KUMARI: Yes. I largely agree. Just, I think that it's useful for people to understand that when they see the lock icon, that means I don't entirely know what I think it means. But, you know, that the name is the important bit here. I don't [inaudible].

BARRY LEIBA: Yeah. There are many studies that show that the lock icon is actually pretty useless for users, but that's out of scope for this.

WARREN KUMARI: Okay.

STEVE SHENG: Okay? All right, moving along. Andrew provided this comment regarding, the sentence starts with "The obvious response." Any thoughts?

UNIDENTIFIED MALE: Well ...

GEOFF HUSTON: But there would be various folk who want to get certification for Tor names, for .local names, for blah, blah, blah names because they want the lock to appear in strange and odd contexts. And I was, it was just head nodding to that problem.

STEVE SHENG: Okay. So you advocate that we should keep this sentence. Right?

WARREN KUMARI: I mean, this kind of sounds like SSAC is endorsing that somebody go off and do this, and I don't really know if we are endorsing, you know ... We're suggesting the CAB Forum should have something. You know, add to the sand that instead of its DNS, it's, you know, [sandblockchain: wkumari.heath]. So I think we should be careful what we're ... Is that what we want to recommend? Right? The obvious response—

GEOFF HUSTON: No, no, no. It was just observing. Once you get there—

STEVE SHENG: Yeah. It was an observation. Yeah.

GEOFF HUSTON: Yeah. Once you get there, good or bad—and it is bad—then if folk also want a padlock, then you're going to have to synthesize a padlock with ingenious methods of magic bullshit, you know? That's really what—

WARREN KUMARI: I mean, I don't know—

GEOFF HUSTON: Yeah? There's no enforcement.

WARREN KUMARI: I don't think it's really that hard to actually do. I don't know if it's a good idea. Right? Like—

GEOFF HUSTON: Well, you can add the sentence "This approach has many pitfalls." Many obvious pitfalls, you know? It's a nightmare. Yeah. "Such an approach has many obvious pitfalls from a security perspective."

WARREN KUMARI: Okay.

STEVE SHENG: So what do we say? "Such ..."

GEOFF HUSTON: "...an approach ..."

WARREN KUMARI: I mean, would it actually have—

GEOFF HUSTON: "...has many obvious pitfalls from a security perspective."

STEVE SHENG: Okay. All right. So we keep this?

GEOFF HUSTON: Well, no one could say we're endorsing it then.

STEVE SHENG: Yeah, yeah, yeah. No. Regarding Andrew's comment, how do I respond to him? Keep the sentence? All right. So let's come back. Okay. How about that? [inaudible].

GEOFF HUSTON: "... to the user." Oh, yes. Right. Sorry, you've got that. You've got that.

STEVE SHENG: Yeah.

GEOFF HUSTON: Ignore me.

STEVE SHENG: Barry, is that okay with you?

BARRY LEIBA: Oh, that's the problem. I'm looking at the text in my copy rather than where you are in the text, so ...

GEOFF HUSTON: "Over time" is two words.

BARRY LEIBA: Yeah. Yeah, that works for me.

UNIDENTIFIED MALE: [inaudible].

BARRY LEIBA: Two words split in a different way than that. Yes.

WARREN KUMARI: At some point, I have to explain the obvious pitfalls from a security—

GEOFF HUSTON: [inaudible] back in the previous paragraph.

WARREN KUMARI: One of the very few, if not the only place where I can think of where the resolution context is actually explicit is in TLS certificates. Right? Like, the TLS certificate for mail.google.com says [subjectAltName: dNSName,

mail.google.com]. If it said [subjectAltName: Ethereum Name ..." it's the only place where the resolution context is actually explicit.

I don't know. We can just, like, [hand wave] this away and hope that nobody calls us on that. But from [inaudible].

GEOFF HUSTON: Well, the issue is, Warren, if you resolve a name in a certain context and then you pass the name onward, and its resolution, without passing the context, then all hope is lost about the credentials that are associated with that name. Isn't it?

WARREN KUMARI: Well, the sentence says "The obvious response is to modify the trust credentials"—which I don't entirely know what exactly you're meaning by "the trust credentials," but whatever—"to include some form of context of resolution." That's exactly what this would be, so—

GEOFF HUSTON: I'm going to certify [local.printer (ingeoffshouse)].

WARREN KUMARI: Well, that one might be dumb, but it's better than just certifying printer.local and—

GEOFF HUSTON: But my point is: if I hand someone the resolution of printer.local and an associated certificate—

WARREN KUMARI: Are you saying "in Geoff's house" because you're saying that is built into the—

GEOFF HUSTON: No. I'm saying the context is in Geoff's house [inaudible] on the certificate in the resolution without the context, then that's pretty daft.

WARREN KUMARI: So in that case, the sentence where it says "The obvious response is to include the form of context resolution," so then you would actually be saying [printer.local (ingeoffshouse)]. That would be where the trust credential is including [inaudible].

GEOFF HUSTON: So what does that have pitfalls?

WARREN KUMARI: [inaudible].

GEOFF HUSTON: When you talk about—

WARREN KUMARI: —[inaudible] pitfalls they're not including the context of resolution.

RUSS HOUSLEY: No.

GEOFF HUSTON: No—

RUSS HOUSLEY: Printer.local has got many, many, many different printers that it would work for depending where you were connected. However, only one of them will have the corresponding private key.

WARREN KUMARI: Yes.

RUSS HOUSLEY: So you'd get lots of authentication failures unless you were in Geoff's house.

WARREN KUMARI: I's better than not—

UNIDENTIFIED MALE: [inaudible].

WARREN KUMARI: It's better than not getting the failure. Isn't it? Which is worse?

RUSS HOUSLEY: Better to have adequate resolution in your name, but we don't.

WARREN KUMARI: I think that we're speaking past each other here. What the sentence says is that—

GEOFF HUSTON: Warren, I'm trying to, without taking up huge amounts of text, to simply respond to your observation that: are we endorsing this? And the answer is, well, no, we're not.

WARREN KUMARI: Okay, okay.

STEVE SHENG: Let's keep it this way. Warren, I invite you to propose alternative text because that's easier for the committee to react to. So if you have text, you can just write [below] here in the alternative, as alternative text, or write in the chat [inaudible].

WARREN KUMARI: Okay.

STEVE SHENG: Okay?

[WARREN KUMARI]: [Sure].

STEVE SHENG: And we need to move on. So let's move on to Findings. Are people okay? Let's give people one last look at this section before we move on to Section 11.

Okay. And when you're done, I'd like you to indicate a status on this section on your participant pane. When you're done reviewing [inaudible], you can do reactions, thumbs up. Or raise hands if you have issues. Okay? Sounds good.

All right. Having heard no objections, let's move on. And, Warren, [if you have] your text, feel free to paste into the chat or in the document, and let us know.

Let's move on to Section 11, our findings. So based on Section 8, Andrew added Finding 7, which reads "Increasing ambiguity in Internet name resolution undermines trust in the integrity of services on the Internet. Additionally, because domain names are increasingly invisible to end users, it's getting more difficult to signal anything to the users with names."

Any reactions on this finding? I think it's essentially kind of a quick, high-level summary of Section 8. Any thoughts?

GEOFF HUSTON: Why does it need to be "increasing ambiguity"? Isn't it just "ambiguity undermines trust"?

STEVE SHENG: Okay.

BARRY LEIBA: Yeah. I'll buy that.

STEVE SHENG: I would agree. Okay. Good.

GEOFF HUSTON: I don't know what the second part ... The second sentence to that finding, it's not clear to me what it's saying. What are you trying to signal to users but names?

STEVE SHENG: My understanding, this goes to, for example, what Barry was saying. Because it's becoming less visible over time, it's becoming less relevant. Right?

BARRY LEIBA: Yes.

STEVE SHENG: So when a user sees a name, they will engender some sort of trust, some reaction. Right? So in that sense, it kind of acts as a signal. Because it's, overtime, less relevant. That signal, the value of that signal reduces. Right? So I think that's what Andrew was trying to say.

GEOFF HUSTON: That doesn't seem to talk to the issue about ambiguity, and I'm trying to understand what it is talking to.

TARA WHALEN: Are you saying we have two things that are two different aspects that are—

BARRY LEIBA: I think [I see]—

TARA WHALEN: —yoked together?

BARRY LEIBA: Right.

GEOFF HUSTON: Well, yes. And I'm not sure I even understand the second one, still.

BARRY LEIBA: Right. I do agree that ... I think the issue of, yeah, of ambiguity and the issue of relevance and signals are different.

STEVE SHENG: How about that?

BARRY LEIBA: That works for [me].

WARREN KUMARI: Yeah. I still don't understand what exactly is "would be signaled to the user with a name." Like, I don't really understand. Is this, like, the fact that it ends in .org means that it's more likely an organization? I don't really understand what the signaling is.

RUSS HOUSLEY: How about, it begins with "www"?

WARREN KUMARI: Oh, okay. I mean, most ... Very, very few people actually go to a website by typing in "www."

RUSS HOUSLEY: Exactly. So these are the ... Or it begins with "ftp."

WARREN KUMARI: Yeah.

RUSS HOUSLEY: It's less and less.

WARREN KUMARI: I guess I would not really have viewed that as a signal to the user, but, I mean, I guess—

RUSS HOUSLEY: But it is.

BARRY LEIBA: And it is, as is facebook.com being where Facebook lives, but not so much anymore. There are other names, and the users don't even realize it.

TARA WHALEN: And why do we even care about having meaningful strings if—

BARRY LEIBA: Right.

TARA WHALEN: —we're all just going to—

WARREN KUMARI: Yeah. I mean, I—

TARA WHALEN: [inaudible] hex strings and just [give] our hands up and give up. Maybe we should.

WARREN KUMARI: I don't think I've ever woken up and thought, "I really want to signal something to the user by having my name start with www." And if that is what we're saying, I think we need more words there.

Also, for Finding 6, the .alt thing is basically published. So I don't know if the tenses are still correct there.

GEOFF HUSTON: Before we get sidetracked on that, I want to come back to that Finding 8—

[STEVE SHENG]: [inaudible].

GEOFF HUSTON: —[and even] the prototype of it. Because to my mind, I see two things at work here, and I'm just not sure which fits in this document and which is kind of interesting but a different problem.

You see, the first side of this is what-you-see-is-what-you-get. It's the same, the homoglyph situation. That as long as it looks like the real thing, people believe it's the real thing. And it's really crude. And what-you-see-is-what-you-get kind of underpins a whole bunch of reasons why people trust names. And at that level, names are still important, you know? And they are. And in the browser world, names are still vitally important.

In the app world, we're in this entirely different piece of, "Well, you ran the app. Whatever happens is good. You can't tell what's going on. Sucks to be you. I hope you're running the right app." And there's nothing there for anyone to hang on to that the app is genuine. And to my mind, that's way beyond the topic of name resolution and its evolution. This is this different world of now you've buried everything behind an app. Where's the rock on which you're building foundations of trust. "Meh, it's a good app. It's really cool. Comes in lots of colors." How do I know that's my bank when I run the banking app?

WARREN KUMARI: Well, when you—

GEOFF HUSTON: I'm just relying on Apple or Google or their portal about loading apps into their app store, am I? Am I—

WARREN KUMARI: When you go to www.mybank.com, why are you really, really believing that is your bank? And don't say because they provided a CERT. Right? You're believing that—

GEOFF HUSTON: Well, because they've got a gray lock, a gray—[count it]—gray lock icon in the bar.

WARREN KUMARI: No—

GEOFF HUSTON: Do you see what I'm saying here, Warren? That—

WARREN KUMARI: Well, wait [inaudible].

GEOFF HUSTON: —at least there's a façade—

WARREN KUMARI: Yeah.

GEOFF HUSTON: —a façade of names in browsers that aren't in apps.

WARREN KUMARI: Except that at the ... You don't necessarily trust the app because you don't know that the app is good. Why do you believe that the version of Chrome on your machine is good?

GEOFF HUSTON: [inaudible].

RUSS HOUSLEY: Oh, now we're going to add code signing?

WARREN KUMARI: Well—

GEOFF HUSTON: Yeah—

WARREN KUMARI: I mean—

STEVE SHENG: Look, guys, I think we're going beyond this document. I mean [inaudible].

RUSS HOUSLEY: Indeed.

STEVE SHENG: So—

GEOFF HUSTON: Well, my point was: I think Finding 8 has gone too far. It's getting into concepts that we haven't explained. I think they're true, but I just don't think it's in scope for Evolution of Resolution.

STEVE SHENG: Right. How about—

GEOFF HUSTON: That was all I was trying to express.

STEVE SHENG: So I delete that last one, but this is a factual statement. Right?

UNIDENTIFIED MALE: Yes. I think we all agree it's a factual statement. And I think it is, but it is within the Charter of our work party to talk about? I think so.

STEVE SHENG: Yes.

GEOFF HUSTON: Well, I don't.

WARREN KUMARI: Even this sentence? This last one?

GEOFF HUSTON: Yeah, even that last sentence. I think it kind of needs a whole bunch of commentary about why, how, and the context that we're not going to be providing.

RUSS HOUSLEY: Wait a minute. Those are things we have bullets for back in Section 8 that we're going to arm-twist people to write text about.

GEOFF HUSTON: Ah, well, okay. It's conditional because I appreciate—

RUSS HOUSLEY: Oh, yeah.

GEOFF HUSTON: I appreciate it's a reference—

RUSS HOUSLEY: Right? Because—

GEOFF HUSTON: It's a reference to a sentence earlier on, and we did discuss it. That's true. Finding 8's pretty presumptuous, that's all.

WARREN KUMARI: We have said that names are becoming less visible and less conspicuous because of apps. Right? That's a sentence that we just wrote, like—

RUSS HOUSLEY: Yeah.

BARRY LEIBA: Yep.

WARREN KUMARI: —eight minutes ago. And so if they were less visible and less conspicuous, they're less relevant to users. I think we have the supporting text for that.

RUSS HOUSLEY: Yes. And I think we're going to have more when we flesh out that list of bullets.

GEOFF HUSTON: Okay. I will reserve judgment.

RUSS HOUSLEY: Okay. Yeah. If we don't get there—

GEOFF HUSTON: I have my crosshairs aimed at it.

RUSS HOUSLEY: That's totally fine.

STEVE SHENG: Okay, all right. All right. Let's do Finding 3. All right. This is what Andrew put the last time, I think.

RUSS HOUSLEY: Yeah. I think that we'd—

BARRY LEIBA: [We'd] discussed it.

RUSS HOUSLEY: —talked about the basics, and he edited it. We talked about it last week. He edited it and then renumbered the findings.

BARRY LEIBA: Yep.

WARREN KUMARI: Yep.

STEVE SHENG: All right, good. All right, folks. Let's move on to Section 5.5. I have a tight script I need to follow. I need to get [them through].

BARRY LEIBA: Well, [and any one of you go].

RUSS HOUSLEY: And you have four minutes.

STEVE SHENG: I have four minutes. So here, Warren, we added this sentence you requested last time as a reference. Okay? "The [inaudible] describing the Internet draft."

WARREN KUMARI: Yes. Actually, should we put a "to-do" around that? Because by the time this is published, there will almost definitely be an RFC.

RUSS HOUSLEY: Okay.

WARREN KUMARI: I don't know if we have an easy way to have a ... Like, you know?

RUSS HOUSLEY: Is it going through the individual, or is somebody sponsoring it?

WARREN KUMARI: It's gone through to the ISC, and it's been approved by the ISC.

RUSS HOUSLEY: Okay.

GEOFF HUSTON: Oh, well. Done.

WARREN KUMARI: At least I believe it's actually formally approved. Let me double-check.

STEVE SHENG: So we'll say "Check the status of this draft at the time of the publishing."

WARREN KUMARI: "Sent to the RFC editor."

GEOFF HUSTON: Oh, well. [Unstoppable].

BARRY LEIBA: We do need to spend a minute before we close the meeting talking about the next couple weeks.

STEVE SHENG: Yes. Barry, please go. Yeah.

BARRY LEIBA: Yeah. Just make a note, Steve, also, that, as Warren pointed out, the Finding 6 needs tenses checked because things have been published.

But, anyway, the next two weeks. I know that in the next week, people are going to be traveling to the IETF meeting, and the week after that is the IETF meeting. We're definitely canceling the one during the IETF meeting. Will enough of us be here next week to make it work? So Geoff said he can be on because he's already in [inaudible].

GEOFF HUSTON: I'm good.

WARREN KUMARI: I will not be available because I'll be in San Francisco doing the setup.

BARRY LEIBA: Right.

RUSS HOUSLEY: [inaudible] I will not be available.

BARRY LEIBA: And Russ won't. I will be available. But if it's just me and Geoff, that's not going to be useful, so ...

WARREN KUMARI: [You] might get more accomplished.

BARRY LEIBA: Possibly.

GEOFF HUSTON: But we'll have to undo it again, Warren.

STEVE SHENG: So let's cancel the next two meetings?

BARRY LEIBA: Yes.

STEVE SHENG: Okay. All right.

BARRY LEIBA: All right. So if we're going to do that, we need people to look at the bullet points in Section 8 that are after the text that's written and start fleshing out some of it in the intervening two weeks. And I know that's going to be difficult for those of us who are setting up for and going to the IETF meeting, but if we have two weeks of non-progress, we're not going to get enough done before the workshop. So let's really try to pick some of these topics out, ones that interest us, and flesh out the text before then.

GEOFF HUSTON: When you say, "these topics," which are you referring to?

BARRY LEIBA: The list that's on the screen now.

STEVE SHENG: Yeah.

RUSS HOUSLEY: The bullet points.

GEOFF HUSTON: So that's fleshing out the text of—

BARRY LEIBA: It's kind of a—

RUSS HOUSLEY: Yeah. Make text from bullets.

BARRY LEIBA: Right. It's kind of an outline for where the rest of this section might go and—

GEOFF HUSTON: Got you.

BARRY LEIBA: —what people have to say about these things. And we're going to ask the folks—

RUSS HOUSLEY: I mean, these were brainstorming from, like, the first month that we were a work party.

BARRY LEIBA: Right. Not all of this is going to wind up in the document, but we need to see what of it we can put some meat onto in the intervening couple of weeks.

STEVE SHENG: Okay. So who will do that?

BARRY LEIBA: [inaudible] [all of us].

STEVE SHENG: [Ask people to put their] names?

BARRY LEIBA: Yeah. I don't think we can put names on topics right now. I don't think we have time. We wanted to do that. But let's all of us look at this, and just please do your best to pick a few topics that interest you and write some text. And I will certainly do that—

STEVE SHENG: Okay.

RUSS HOUSLEY: —as well.

STEVE SHENG: All right.

BARRY LEIBA: [And I will] post a message to the mailing list asking people to do that as well.

STEVE SHENG: Okay. Sounds good. All right. With that, we reached the top of the hour, and we will adjourn for the meeting. We have one item we didn't go through, Section 5.3. But I'll flag to Andrew to pick up the discussion next time. And then the working group will cancel the next two meetings, so the following meeting will be on August 3rd.

BARRY LEIBA: Yes.

STEVE SHENG: Okay.

WARREN KUMARI: Also, well done to Steve for at least kind of managing to keep us on track and not too much going [inaudible] track.

UNIDENTIFIED MALE: Thank you.

RUSS HOUSLEY: Thank you, Steve.

BARRY LEIBA: Yes. Thanks, Steve.

RUSS HOUSLEY: Thank you all.

STEVE SHENG: Bye-bye.

[END OF TRANSCRIPTION]