Why Organizations Need a Secure Domain Name System
Transcript

Part 1: DNS as Internet Phonebook

Julia Allen: Welcome to CERT's Podcast Series: Security for Business Leaders. The CERT program is part of the Software Engineering Institute, a federally funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. You can find out more about us at cert.org. Show notes for today's conversation are available at the podcast website.

My name is Julia Allen. I'm a senior researcher at CERT working on operational resilience and software assurance.

Today, I'm pleased to welcome Alex Nicoll. Alex is a member of CERT's Enterprise Threat and Vulnerability Analysis team. And today specifically Alex and I will be kicking around the Internet Domain Name System and talking in a little bit more detail about its security extensions, which are starting to be used in some organizations and why these security extensions are critical for protecting your organization's digital information and networks and computers.

So, welcome, Alex, really glad to have you with us today.

Alex Nicoll: Thank you for having me.

Julia Allen: So, just to set the stage, can you say a little bit about what for those not intimately familiar -- what is the Domain Name System and why it's such a critical component of operating effectively on the Internet?

Alex Nicoll: Well in general, people tend to remember names and concepts far better than they do numbers. Internet addresses are essentially just long strings of numbers. And, unfortunately, they don't really seem to have a whole lot of logical sense to people. They make great amounts of sense to computers but in terms of people, we don't really seem to relate what the numbers are to where they intend to take us.

So for instance, if I give you the address for CNN's website, you'll probably forget that in the next couple of days. But if I just tell you to go to CNN, that's something that will stick with you for a little while, or if I tell you to go to CERT.org's website.

So the idea is to provide a way for people to associate words and concepts with the numbers and then let the computers take care of the messy business of actually translating those concepts into the appropriate numbers and taking us where we want to go.

Julia Allen: So Alex, would it be fair to say that there's a unique number associated with every computer and every server on the Internet? And if that is the case, is there software somewhere in the Internet that reconciles these numbers to a specific device?

Alex Nicoll: The Internet itself is divided up into a large number of what we call subnetworks, or subnets, that are assigned to specific geographic regions or they're assigned to specific companies. And there's a huge backbone called the Internet Routing System that essentially serves as a map for the entire Internet.

So if every server is given one or more specific numbers that are supposed to be unique across the entire world and to address that particular number you go out to the Internet Routing System and say, "Here, here's the number for the thing I want to talk to. Tell me how to get there."

And the Internet Routing System then, based on a series of maps that it has -- it's the equivalent of you going out and using your global positioning system to go find a specific address in a city--the Internet routing backbone knows where various things are and how to get there. And so based on the number that you give it, it knows how to get there.

Julia Allen: Well, that makes a lot of sense. And I think as we were kicking around ideas for the podcast today, you also used the analogy of there's not a single monolithic phonebook for the entire world; there are phonebooks for every particular region. Would that be a fair analogy for what you're describing?

Alex Nicoll: Absolutely. That's pretty much the way the entire Domain Name System is put together. In the Internet routing schema, all it ever really cares about is numbers. It doesn't care about a particular name or a particular concept. And so we need a way of mapping those names and concepts to the numbers that form the Internet backbone and that's what the Domain Name System is all about.

And so you can think of the domain name system as a phonebook. Every person in a city has an entry in the phonebook. You can say, "This is my home telephone number. And this is the telephone number associated with this particular address." So what we can do is say, "I need to look up in the Internet phonebook where Sears is." And the computer will go out and query the great Internet phonebook that we call the Domain Name System. It says, "Tell me where Sears is." And it'll get back an answer that says, "Sears is at this particular address." The part about this, however, is that there is no one monolithic Internet phonebook.

Everybody is responsible for their own little piece of it, and the great piece -- or the great thing about DNS -- it is a very distributed system. Every individual network across the entire world is responsible for sticking up their own, small piece of that phonebook, which is then linked together and sort of aggregated into this great Internet phonebook. And each individual is your sole responsibility and nobody else can stomp on that individual piece.

So if I own the namespace associated with CNN or CERT.org, then it's me and me alone that can affect what happens within that namespace. The other phonebook providers out there, those ones that are responsible for, oh, say, the namespace in Great Britain or the names that are over at News of the World cannot affect what I'm doing over in my chunk of -- or in my own particular namespace.

Part 2: How Security Extensions to DNS Mitigate Hijacking

Julia Allen: Okay well, that makes a lot of sense and I think the analogies really help. So this is a security podcast series, so let's turn our attention a little bit to the specific part of the Domain Name System that is about the security extensions, trying to make the Domain Name System more secure and sometimes that's referred to as DNSSEC.

So what's that? What do we mean when we say security extensions to DNS or DNSSEC? Can you introduce that to us a little bit?

Alex Nicoll: Sure. The Domain Name System was basically created back when the Internet was a very nice place. Nobody really had any intention of behaving badly or doing bad things. And it turns out that we really didn't think too much about the security aspect because the Internet at that point was limited to a series of academics, some government agencies, and a few defense agencies.

And we were all expected to do the right thing and cooperate with each other. But as the Internet got more commercialized, more and more commercial companies came online, and there turned out to be a relatively reasonable amount of money to be had by doing bad things on the Internet.

And so the DNS system then 11 was considered inviolate, because if you messed with the naming system, you really had no way of guaranteeing that anybody was going to get anywhere of any importance.

Julia Allen: So you could actually do something to the Domain Name System that would redirect someone to a place that they didn't want to be and they would think they were still going to CERT.org or CNN.com, right?

Alex Nicoll: Right. And that's what happened -- back in the mid 1990s, a particular tack was proposed that said: "If we don't do something about the Domain Name System, it could get hijacked. And people who think they're going to a legitimate website or people going to a legitimate news site won't be able to get there. They'll instead be redirected somewhere else." And everybody nodded their heads and said, "Yes, great and wonderful, but we're not sure how to address this just yet."

Starting in about 2000, they said, "Okay, that's becoming more of a possibility." Because the hijacking took a reasonable amount of computing power and prior to about 2000, it wasn't -- that kind of computing power wasn't available to the average person. But with all things, computers got faster, computers got more powerful, people got a little bit more -- smarter about the way they did things. And that security hole started looking far more and more likely to be exploited. And it turned out it was several times.

So the Internet Engineering Task Force started developing a backwards-compatible add-on to the DNS system that was supposed to provide some resilience against attacks that would allow people to hijack your web traffic.

Julia Allen: So what kinds of features, just in a summary description, what kinds of features typically are in the security extensions? What kind of things helps make DNS a little bit more bulletproof?

Alex Nicoll: Well, the whole idea is that DNS is based on what we call a "chain of trust." The idea behind a chain of trust is that I make an assertion that this is the right answer and then you can go off and ask somebody else if that really was the right answer and get verification that I'm not lying to you.

Julia Allen: So like a trusted third party?

Alex Nicoll: Very much so. It's exactly what it is when it comes down to it. Since the Internet is this hierarchical place, the more what we call labels you tack onto something -- so the more numbers of dots in the name that you try to use, the more different layers of the naming system

you have to go through. It actually gives you more opportunities for people to sign off on it and say, "Yes, that is really the right answer."

So what the DNSSEC system does is it allows a name server to assert, when it hands you back a name that says, "Hey, you want to go to CNN.com? Here's the name. Here's the address you want to go to. And I'm going to sign that and say that that is the right answer." And then you can take that signature that it hands off to you and verify it with the next level up in the Internet -- say, "Well, okay, I don't really quite trust you that that's the right answer," or "I don't quite trust that that was not spoofed by somebody sitting in the middle or hijacking things, so let me go ask your parent domain."

So in this case, if we're talking about CERT.org, you can say, "Let's go ask the guys over at .org really quick if that signature that came to me from CERT.org was real." And so you go pass that signature onto the guys over at .org and they say yes or no, as the case may be. And it better be yes in our case. And they can sign off on it and say, "Yep, that's the right answer." And then if you really get suspicious and you think that the guys over at .org are lying to you, you can actually go up and ask the root of the Internet itself and say, "Hey, is that really the right answer that the .org guys gave me?" And it'll say yes.

Julia Allen: So you can keep working yourself up the address tree or up the naming tree and get more and more levels of verification, correct?

Alex Nicoll: Essentially, yes, that's exactly the way the chain of trust is supposed to work. You get an answer and then you can keep going up and up and up in the levels to make sure that the answer is absolutely correct all the way up to the very root of the Internet itself.

Part 3: Challenges to Implementing DNSSEC; First Steps to Take

Julia Allen: But it strikes me there would be a certain amount of overhead involved in this, unless it's all automated or streamlined. So aren't you adding processing time to each transmission or each verification step, or is that really been taken care of because of the speed of the software that does the checking?

Alex Nicoll: No, you're absolutely right that it does add a little bit of a burden. For instance, the signature that your domain name server provides to the client who's asking for this name-to-number translation, does take up more space. So it takes longer to transmit on the Internet. It requires more traffic for every transaction that goes through. And since there are millions of transactions on a given DNS server per day, that can add up over time to a lot of additional bandwidth that actually needs to be utilized.

In terms of processing power, the cryptographic algorithms themselves are only really run on the client system. The servers have essentially pre-canned answers that you ask for. So it doesn't really require a whole lot of thought on the server end, but every time you get one of these signatures back on the client end, who's actually doing the requesting, they have to go through all the mathematical gyrations to actually verify it, which does take a little bit of additional time.

Julia Allen: And while we're talking about challenges, are there some other things that organizations need to think about that they may run into as challenges or hurdles when they're implementing DNSSEC?

Alex Nicoll: Well, the hardest part about DNSSEC in and of itself is that it's based on what's called public key cryptography. And public key cryptography requires you to have this private key that only you know and you can keep absolutely secret from everybody else in the known universe, and a public key which you give to everybody else in the known universe so that they can verify that you were the guy who signed the things with the private key. They're essentially two halves of a whole. And so if an organization doesn't have somebody who really understands the notion of public key cryptography, then their DNSSEC deployment is going to become a lot harder.

The other thing they really need is somebody who really understands the concepts of key management. And you'd think that keeping a private key private is easy; you go take it up, you go lock it in a safe, and you never see it again. Well, it turns out you can't do that with DNSSEC. You have to keep using that private key over and over and over again as things change. And so training somebody for the proper handling of that information and being able to sign the records that need to be signed and then putting the key back away, keeping the key safe across this whole process, turns out to be non-trivial.

Julia Allen: So just to connect the dots, so the public and private keys and the use of cryptography have to do with the signing of the verification that the domain name is what it claims to be. Am I correct about that?

Alex Nicoll: Yes. That's essentially what it is. And to make the whole system work so it was backwards- compatible with the old DNS system, they essentially added a couple of new fields, or what they call records, that get sent along with the original stuff that says, "Hey, this is the name and the number that you were interested in." And those signatures form the core of the whole chain of trust.

Julia Allen: Well, that makes sense. And I think you had also pointed out to me that one of the other challenges is that the packets that this domain name information is being exchanged in, when it has the security extensions they're a little bit larger, and so you have to worry about memory and other types of load balancing. Does that factor in?

Alex Nicoll: Memory and load balancing, not quite so much. But it really does significantly increase the amount of information that you have to push out your Internet connection, especially if you have a very busy website. And a lot of companies are starting to see that increase become tenfold increase in just the amount of DNS traffic that they have, simply because the packets are that much larger when they get sent across the Internet.

And so then it can translate into an additional cost for whatever size connection you have to the Internet, because you'll have to size it, again, a little more appropriately for the amount of traffic that you're now expecting.

Julia Allen: And you mentioned that this whole effort started with the Internet Engineering Task Force around 2000. Do you have -- I know there's not a lot of good hard data -- but do you have any anecdotal data, or a sense of uptake? In other words, are organizations slowly but surely starting to implement DNSSEC, or are they in a wait-and-see mode? Do you have any feel for that?

Alex Nicoll: A lot of organizations are definitely starting to adopt DNSSEC, especially the big what we call hosting companies online. There are a number of folks out there who cater to the companies that don't want to run their own DNS servers. And they don't want the additional

burden and so they actually pay somebody else to do it. And those companies we call hosting companies because they essentially host the service for you.

And those are a lot of the early adopters for the DNSSEC extensions because essentially they're high-value targets. They have a lot of information and a very small footprint and they have a lot of vested interest in making sure that information is not tampered with. And so a lot of those folks are definitely the first adopters of the DNSSEC protocol. Other adopters would include Google. The U.S. government actually is -- the Office of Management and Budget has issued a memorandum requiring all government agencies to utilize DNSSEC extensions.

The governments of the Netherlands and Sweden have mandated that those countries go entirely DNSSEC to provide a more secure and stable environment for their citizens. So the adoption is not slow. It's not as rapid as we might like it to be but it is definitely going and going quickly.

Julia Allen: Great. Well, thank you for those examples. So let's say I buy it. So I hear what you're saying, I understand how dependent I am -- my organization is -- on this being a robust capability, So as a business leader or as the head of IT, if I was going to think of this, what would be some good, concrete first steps to take?

Alex Nicoll: Well, first concrete first steps to take are to figure out what your exposure is. A lot of companies, it turns out, don't actually have a good handle on where or what domains they actually have registered to them and where those domains are being hosted from. So are you running your own DNS servers? Are you paying somebody else to run your DNS servers? Really what is the footprint you have on the Internet and how much is it going to take to protect it?

The other question is do you already have the infrastructure in place to do this? A lot of the most recent domain name server software, like Microsoft Server 2008, actually comes with a DNS server built into it that already does DNSSEC. So there really isn't an additional cost. BIND, one of the most popular DNS servers out there on the market, is absolutely free.

And so you -- and chances are, you already have the infrastructure for pulling this off already in your organization. So what you're really looking for then is figuring out what your exposure is, and what kind of people you have in your organization that understand these things, or what kind of training you need to get your folks to allow them to understand these concepts to be able to implement the DNS record set and signing practices.

Julia Allen: And you mentioned earlier the ability to understand and manage keys -- public keys, private keys. That's a really key capability, correct?

Alex Nicoll: Absolutely. That forms the core of the whole thing. Once you understand the public and private key management and implementation, the rest of this flows out naturally.

Julia Allen: Excellent. Excellent. Well, I feel like we've just discussed the tip of the iceberg but I sure do appreciate your insights and this perspective that I think would be very helpful to our listeners. So just by way of a last question, do you have some places, some references where our listeners can pick up a few more details?

Alex Nicoll: Well, for all the gory technical details, the Internet Engineering Task Force website is by far and away the best place to start. Although there are a lot of different resources

available, particularly PowerPoint presentations and walkthroughs for how to go about planning a DNSSEC deployment at a specific website called dnssecdeployment.org.

Julia Allen: Excellent, excellent. Well, Alex, I can't thank you enough for your preparation and time and giving this perspective to our listeners so they can think about this important topic. So thank you very much.

Alex Nicoll: Well, thank you again very much for having me.