Hello I'm Roger salient today is Thursday, August 5 teens and you're listening to the information security news podcast brought to you by Northwestern University information technology our first story today is about the SSL certificates and you probably have seen this message in your browser before United connect to a website and you get a message that pops up and says you know warning in all of this certificate is not valid or the certificate is out of date care of you know things of of the snitching of the sortable messages do you want to continue and you know yes or no and no most people click yes even though they recommend that you click the cell they have funded dozens of research basically here this is somebody from Google and a grad student from Berkeley and essentially they come out and they find that different browsers handle this differently and have different success rates and so they find that the most success looks like it's coming from Firefox with the with you know basically of your chrome user may be twice as likely to actually look on the you know the linkages can't go through and click through and and ignore the warnings and so I guess it's what they're saying is it's your substance important to get people to understand what these warnings mean and that it's also important for the people within the browser industry to make the browsers you give the information in a way that's more valuable to the user so off I believe they said that for Firefox it was the word on trusted for example was a good one and the people understood what that meant so it's it's kind of interesting and I and I like this idea of looking at what kind of like the geeks you know understand and what is it really mean to the people out there I've always liked that sort of research we actually have a faculty member here at Northwestern who that's one of the things that she does know what I would've people understand versus what we really saying and it separate interesting stuff them his story that the house house a curate he smart is generation Y right so you know I mean you you look around and you see younger people you know there they are all hooked up to me and him got to be another iPhone they've they've get having everything of God is is is on the net net ready to go but what is said is security smart generation wide may not be and the is sounds like what they're really saying is look generation Y is free likely to ignore policies in the runoff that's true or not but unnecessarily also I don't know Venice so means that they're not security smart of you know you noted us was to do something but you ignore it and do it anyway it one could argue well you're smart enough to know you were supposed to do it clear that I'll know it's it's an interest it's nesting question I mean I think until I read this article I was just thinking in all these still you look at the younger generation there hooked in everything they do is online that you know whatever the latest app is they can tell you about you know the latest technologies in oh but you know maybe they do have some areas were there weaker in on me and I certainly know that if myself I'm pretty quick to make sure I'm following the policies where I can in the enough turns out that you younger folks it's not a bestseller true that is a problem in then the sauce story on the on Ars Technica about the Internet of things and essentially what this is is a story about look there's a zillion different devices out there that now have the Internet or a way to connect to them over the Internet built into them and you know that's really something and a lot of these things are not a secure is they need to be and for example they were talking about some lights are LED lights that are made by Philips and I actually pay actions concern by one since well back ago and some listed on Amazon actually and I thought were pretty cool but it looks like they've got the sump security issues and in him and in food addresses isn't a member member I like it was last week I
was talking about the security issues on the xerox machines in on who addresses those issues and it is a big deal and it's certainly nothing to be perfect but you don't really think that were given the point where Holmes need to have firewalls and those firewalls need to be configured to allow certain kinds of devices in another device is not putting a machine or device you know your year of refrigerator in this case a light whatever it happens to be just putting it on the network just seems like a bad idea you know there's all these they show these commercials you probably seen them before you know always Sosa forgot her keys let me just unlock the door for you in all it's just a matter of time before the bad guys realize that they could just search the net find these devices that are out there and bang and there in the house you know that's a real problem I think I hope that they work on securing these devices better but really I think the most important thing is easier to put it if you've if the expectation is that you're making a device and you put up these can be on the network somehow than the expectation should be that at some point you're going to have to it update that device and this device should automatically be looking for its updates and should automatically apply them without any user intervention because it's unrealistic to expect users to go and update their blue Ray player they bought it so that can play blue raise and then I can update it in oh at your job such printers thing anyway the their story another story about up of compromise for servers of potential compromise for servers but it turns out it's there you can buy servers high-availability servers and these are servers probably not like you're buying for your home rights these are servers that you would have been in corporations a new first these things like that now these servers have a essentially a stick installed a second drive on them and they're ready if you ever need to reimage it you can do it remotely turns out this stuff is not free secure and other people could potentially get in and I could really be dangerous another's that looks like there in one particular companies what they research was done on this from the University of Michigan but it actually looks like maybe there's more companies that are involved in the Sears well and it yields some of the stuff that they're being done done in know a buffer overflows and stuff like that I just don't see a man so many years later when a buffer overflows were real problem 20 years ago and you would think by now they be fixed they still happen it's just the obvious to maze by that and in the last door-to-door talk about is the is this trashcan stalking you and it turns out that in London they had smart phone tracking trash cans presented in smart phone tracking trash cans and yet you pricing regulates you wander down the street visibility trash bin over there you control your your waist and that it had a little device in it that was grabbing all the Mac addresses of smartphones as they were gone by because smartphones are constantly looking for place to connect to Wi-Fi in these trash cans were grabbing all that information now they're using in exactly the same way some stores were there for you no great information here I'll gather the stuff up as I'm passing by the coffee shop I shoot this guy over a coupon Mrs. Heyward having a specialty coffee and get that you know Dana should have price and you know maybe people take advantage that stuff but there some privacy issues here now turns out that just after this story was put up on Ars Technica they they shut these trash cans down they there at the device within the trashcan sense of the trash cans are still there but it's pretty interesting stuff cannot I would not be surprised to find out that this more viscous stuff is going to be going on and I really wish the people controlling anyway thanks for listening DNA, just suggestions please feel free to send and are – saving the northwestern.edu and is always shall find additional security
information as well as some notes to contain the links for today's podcast better websites
www.IT.northwestern.edu/security