Hello I'm Roger safe in today's Thursday, February 7 and you're listening to the information security news podcast brought to you by Northwestern University information technology will start with updates and there's a new version of Java out and the it actually fixes 50 different security holes so that's pretty a pretty big deal here and glad that it's out there because is been obviously a lot of issues with Java lately and were having you know the various browsers now Safari his is not a Firefox for the just not running old versions of Java and you know I'm really afraid that if Oracle doesn't do something to get job under control so that people can rely and again to be a safe and secure way of using the Internet users can see nobody using Java anymore this is its its glad to fix this stuff again I don't want a solid complaining about that but why am complaining about is taking so long with so many different vulnerabilities and if you're looking to kill up our product line this seems like a pretty good way to do it to me so hopefully received Java turning over a new leaf fairness is can be the the end of this sort of the completely insane numbers of vulnerabilities in Java then the twitter got hit with the hacked the other day and it looks like somebody broke in and got what twitter called limited access to user information I don't know what limited axis means to you to me at it means a little you know maybe they got e-mail addresses or maybe they got some posts or something like this here but when you're getting e-mail addresses usernames you know salted passwords you know I don't see how that's limited salted passwords is not limited access you know maybe they mean only didn't get every single salted password they had they only got up order for million of them but that's still a lot and that's you know if you can get salted passwords with limited access then really that's pretty bad on the other hand though I see their twitter not only solve the problem notify the users all this is good but now they're looking to add two factor authentication to their service and my guess is they probably been a delivery similar to some of the other services or users without your smart phone will get an SMS message and you'll reply and then that'll allow your your tweets to go through so it's again not a perfect solution but it's a pretty good one song glad to see that you don't bad sit thing happens but they're trying to make the best of it they fixed the problem and the train introduced something that's going to make it more secure so kudos to the folks at Twitter for doing that I'm I were talking about keeping things to work Ars Technica put out a article on thus securing your website in Salina things that we taught if Artie talked about what it's pretty good to have all these things in one place I've always liked these guides that think they're really useful and saw a post a link to this the show notes and you hope you take a look at it Google has got the same sort of a guide a guide to saying safe and secure online and it looks that they've actually got several different guides in their you know what which can do as a parent you know what you can do is to string a regular surfing the web things of this type of nature sodium both of these will be in the show notes should be able to take a look at them and then it's right that you know like to see criminals were using the Internet for criminal purposes to be prosecuted with the current criminal laws that would not hate when you notice that while millions of dollars have disappeared and we don't have any idea how to get a hold that you know with who knows what happened there you know it's reach ridiculous when this stuff happens song glad to see here that we've got some people that were prosecuted and they stole $14 million $14 million that looks like that might be looking at 30 years in prison but $14 million that's a lot of money to be stealing and it really says something about just how vulnerable these systems are online when you can
steal so much money I mean why would anybody be a you know a regular old
criminal these days when you can just do it a lot safer it seems from the your own home
and get a whole lot more money is been a lot of talk about the the Obama administration
has essentially come out word they're saying we can order a preemptive cyber attack and
in a lot of the press are making this seem like this is it like you know what the president is
can it be able to just push the button below the Internet apart like he's got some sort of
suitcase of nuclear launch codes there but you know I don't even know how this would
work to be honest with you you know it's not like you've got a missile you know you put
a nuclear missile and missile loan you have somebody down there ready to turn the key
and that same thing is condemned work and do its job for you know many many years
not so sure that cyber attacks again work in the same way so the process that's out there
today in oh may network next week may network a year from now who knows but at
some point it's definitely not going to you know be feasible anymore which means this is
can have to be constantly evolving situation which means changes and stuff like that but
saying that the president should or shouldn't have this fear of this saying the press makes
it seem like all my God in all this is good obedient to the world and I really don't think it's
can be like that I hope I'm wrong or a Bush set up am not wrong on this one of me would
really be a tragedy if somebody could just blast the the Internet apart on the funeral some
sort of preemptive strike but I guess print to find out her you know at some point these
things always intend to come up while talking about the government's the FCC has spent
money of time telling people how they need to be secured safe and all that is good but the
same time there they're not doing a very good job on their own so that's bad now I
concede that a any large organization to the FCC you know that my own university you
know any of these places small business even its freight difficult to make all these things
get everything you need in place but you have to start somewhere and you have to if
you're a large organization you have to put a lot of resources to security in us one thing
when you're a home user in on you got a couple three machines at home and you get a
wander around the the home and you you update everything you know it's you have
to do more than that if you get a be the FCC and you certainly a minimum you have to
make sure that things are updated regularly and they're not even doing that so that's bad
so really want to see them work harder at making sure that their machines are secure
especially if you're in a been a position where your telling other people what they need to
do in order to stay secure in a somewhat close with another one of the stories on the
skater controls and basically this was a story in wired magazine about the of vulnerability
in some tritium software this is something that allows companies to control their
environmental systems in overheating the air-conditioning you know in some cases the
elevators you know what it lasted different things and there's vulnerabilities in the
systems and for the most part it turns out that these things are you a somewhat
misconfigured on not saying that the vulnerability should or shouldn't be there and it
shouldn't be right you when you're writing software like this are the controls is consistent
you should make sure that stuff is secure on the other hand when you are the person that's
using these types of systems you need to make absolutely sure that those systems are well
firewall done not on the regular network that you're sharing everything else with because
if you do you're going to have problems there's just no way around that in the reason that
I want to bring this up here is more and more regular home users are starting to put these
systems into their homes where you can control the tent that temperature will feel from
from your iPad or something like that you know you need to be very careful when you're
doing these things because you don't want somebody to use this as a way to cause
mischief in your home you know when it's you know for a lot of times it's probably not
too dangerous when you're somebody just turns off your heat oh well I turn it now I get
home I disconnect the skater system and everything is fine but if you happen to be a
vacation and hits freezing cold like it's been here in Chicago over the last couple weeks
single-digit temperatures you turn off that the heat those pipes are a star freezing your
and have a real mess so I guess I'm trying to get you think about is if you're thinking
about putting these types of automation system in your own home please make sure that
you got it really well firewall that your client updates to those systems whenever you
can and that you use really strong passwords because you don't want somebody to be messing
around with this kind of stuff in your own home anyway thanks for listing if you have
any comments or suggestions please feel free to send them to our – safe in a
northwestern.edu and is always shall find additional security information is Wells notes
that contained links for today's podcast other website W
 WW.IT.northwestern.edu/security