2nd SoC workshop CERN - Minutes – June 11, 2021 – SysSecurity

https://indico.cern.ch/event/996093

Notes:

- These minutes were collected by P. Zejdl.
- They provide a record of the questions and answers following the presentations. For the presentations themselves including recordings, please, refer to the indico timetable.

Friday – June, 11th:

- S. Lueders, CERN-IT Security:
  - Q: This was an amazing talk. Could you please comment on context behind some of the rules that seemed to be historically targeted at simple PLCs from 10 years ago, being applied to the much more complex devices like a system on chip, which is essentially a single board computer, and I see them quite different.
    A: The rules are not really different between the PLC and the server if you just look at the basics: keep it up to date, control the input, control what's running, make sure that default passwords are removed and so on. - So there's no no big difference. … It's more discussion document where we can see what you can do. It is a document for you to check: Can I do this easily? Please do! Can't do this? Talk to us, talk to your system administrator. They may say this is something we need to have. Or this is something we can tolerate because it is sitting in a rack, on a subnet behind the gateway. This is where the controls point comes in. It's about understanding, so I completely understand system on a chip. For me it is like a PLC in the way how its functioning, but much much more powerful. And this power of course is also something which can be abused! Let's talk, let's analyze, let's talk and then make a conscious decision - by your management to say yes, we are running 1000 or 10,000 of those boards. They have no security or they have very low level of security, we accept this because we have a separate network, we even have a separate network inside of a separate network, and even if it's going down the the damage is restricted. It's more about knowing, discussing, and then deciding.
  - Q: With RedHat you get security fixes, but with Buildroot or Yocto it is up to you to apply security fixes. Did you ever have a thought about this?
    A: For me, those are devices, which are unpatched in first instance. I love devices like laptops on the office network, which are putting in the patches automatically, which is very convenient… I understand that of course you don't want to do this automatically, because you would like to control your devices and having having this targeted. So, for Yocto and similar the point is - the system administrators of such system should have a plan: When and how to update those systems, when needed: on a technical stop, annual closure, next long shutdown. But to have a plan for those things that is important! I would love and I still believe we should be very very agile and be able to do this more or less on a interfill basis. Yeah, between fills. But of course, I also see lots of control system

owners at CERN, which apparently are not completely fond of this because they don't trust their their system, or they fear that when you patch you bring something down and you have to retest everything, which are completely acknowledge. It's not black and white. I'm just saying you need to have a plan how would you patching.

- Q: As a the security team - Have you ever thought about trying to break Yocto to see if the latest version is ok, or if there are some vulnerabilities…?
  A: Nope, but if you have the setup, as I said in beginning, we are here for helping you. … We might find some things and somebody has to fix it, which is of course creating more work but you… But yes, let's talk and then we do a little bit of penetration testing those devices. And afterwards, we might be more comfortable, at least they know where the weaknesses are. It is one more step forward, than just being ignorant and saying okay I run it but I don't want to know about anything about security…