Exercise: User Interfaces

ACME Water have decided to modernise the tools and interfaces used by instrument technicians when modifying plant equipment. They have instructed Midnight Engineering — its preferred system integrator — to develop an iPad based solution. Once deployed, the solution will allow instrument technicians to make changes to Programmable Logic Controllers (PLCs) in water treatment plants, both locally and remotely.

Midnight Engineering are considering a solution based on *HMI Pad (*http://www.sweetwilliamsl.com/hmi-ipad). They will develop user interfaces for the controllers using this framework. Instrument Technicians will download the interfaces to their iPad, allowing them to interact directly with the control system. The project files for the interface will be stored in ACME's control software repository.

When answering the questions, you may find it helpful to refer to and update the *ACME Water* demo CAIRIS model (downloadable from https://github.com/cairis-platform/cairis/blob/master/examples/exemplars/ACME_Water.cairis).

Questions

1. What threats or vulnerabilities does this *HMI Pad* based solution explicitly try to address?

This isn't really spelt out anywhere, but — based on p.131 on the HMI Draw Reference Manual — we can draw out 3 areas of concern.

- *It seems that WPA / WP2 should be used for 'local connections' and VPN for 'remote connections'. Further investigation will find that these refer to the connection between the iPad and PLC, so there seems to be some [as it turns out highly justified] concerns about spoofing or tampering with the data flows between the HMI View app and the PLC.*
- *There are also references to a 'Validation Code' to stop unauthorised access to HMI Draw. The concern here seems to be about malicious HMI Draw projects being downloaded, e.g. Victor creates a malicious HMI project containing a logic bomb, authenticates using his own account so this can be downloaded onto the iPad and subsequently used by someone else. However, given that iPad are likely to be used by individual technicians, and it seems unlikely iPads will be shared, it's unclear how significant this attack is. It's also likely that an insider with site access will be able to determine the validation code anyway.*
- *Unauthorised access or theft of the iPad itself. Password-based authentication can be setup to prevent this, but it does entail turning off automatic login.*

2. How much does the design meet the security expectations of (i) Instrument Technicians, (ii) ACME Water in general?

(i) It seems unlikely that the iPad will replace the laptop, so this could be seen as another device for Barry to carry around. Depending on what training Barry receives before using the device, he may assume that authenticating with the app is enough to address ACME's security concerns. This isn't the case though as it appears the channel between the app and the PLC is open, and thereby vulnerable to passive attacks, e.g. attacks that infer the validation code to the PLC.

(ii) iPads are certainly cheaper than touchscreen interfaces, so are easier to replace if iPads are lost or damaged. It appears the validation tags are coded into the interfaces, rather than configured by instrument technicians; this seems to safeguard the code to some extent if the tablet is lost. The biggest concerns seem to be between with the [open] channel between apps the PLC, and the externalities that arise because of that. For example, adding validation codes to PLC raise the question of how such codes should be added, where they should be stored, and how to deal with revocation.

3. How might you enlarge or reduce the solution's system image to make it more usable and secure?

There needs to be a secure channel between the app and the PLC, so any changes should focus on this. This could entail modifying HMI Pad itself, but this may not be possible given HMI Pad is an off-the-shelf product. Suitable policies and guidelines on the use of HMI App would be useful, e.g. how to setup a VPN, together with information on what to do if iPads are lost, and how validation codes should be setup and stored.