Contribution ID: **29** Type: **not specified**

Dealing with insecure and/or cyber espionage enabled COTS devices

Sunday, 8 October 2017 12:35 (25 minutes)

Manufacturers and companies distributing COTS devices don't necessarily give cyber security a high priority, or for small outfits, may not have the expertise to make sure their devices are 'cyber safe'. As more and more controls devices now come with Ethernet interfaces and many come with some sort of embedded operating system, making sure these devices are 'safe'to connect to our networks is becoming a more and more overwhelming task. In this round table discussion, we will share our experiences with COTS devices that were either found to contain malware, act as malware portals (attempt to connect to some sever), or are suspected to be portals for cyber espionage. We will share methods we use to cope with such devices and brainstorm on possible ways to improve our security around them.

Summary

Presenter: BROWN, Kevin (BNL)