Comprehensive Exam - Question #2

Rob Gillen

Question

What impact do Real Time Operating Systems have on the vulnerabilities of cyber-physical systems. In other words, what characteristics do RTOSs have that make them more or less vulnerable (than general purpose operating systems), and what are some schemes attempted to mitigate these vulnerabilities.

Answer

The landscape for embedded systems is wide and varied in both form and function.

Custom logic (i.e. FPGA, ASIC)

Bare Metal programming (microcontroller, microprocessor)

RTOS (FreeRTOS[1], QNX[2], VxWorks[3],)

Pros: - (near) determinisim - reduced attack surface

Cons: - (near) determinisim - sometimes less robust outward-facing connectivity

While not explicitly focused on RTOS-based devices, Formby et. al. [4] performed a three-year longitudinal study of the network traffic within a power company's substations for the purpose of characterising the traffic and they uncovered a number of interesting items that are relevant to this topic.

The traffic was *not* nearly as regular and predicable as one would expect, even given a highly over-provisioned network. There is an assumption among many that in a relatively isolated network that has more capacity than needed and contains only embedded systems devices (RTOSs, bare-metal) monitoring a physical system, the traffic should be highly regular and consistent. This type of enviornment should (logically) be a perfect fit for anomaly detection systems as the model of "normal" should be clear and easy to build and abnormal traffic should be clear and obvious. Contrary to this assumptions, they found significant variance in response times, in inter-packet timings, etc. They performed the majority of their work in one substation and validated it in two others (all the same company, however).

The traffic was unpredictable in predictable ways. What I mean by this, is that they were able to model and cluster the features from their traffic analysis and, given their access to ground truth, could confirm that the devices from a given manufacturer behaved consistently. This allowed them to monitor the traffic and then predict with high accuracy the manufacturer of a given device on the network (fingerprinting). We have long been able to do similar assesments in the traditional IT network realm to predict device operating systems and versions (e.g. NMAP[5]) but not the hardware manufacturer. The assertion of Formby et. al. is that this is likely due to the fact that the devices under consideration were initially designed (as were their programming logic) to perform a particular function such as monitoring current and voltage and then opening a relay if either are two high. Pressures to integrate systems have driven manufacturers to add LAN/WAN capabilities which were secondary to the primary objective of these systems and were therefore possibly under-supported via system resources. The network interactions become, essentially, "best effort" relative to the primary device functionality.

References

[1] A. W. Services, "FreeRTOS - market leading rtos." [Online]. Available: https://www.freertos.org/.

[2] a subsidiary of B. QNX Software Systems Limited, "QNX operating systems." [Online]. Available: https://blackberry.qnx.com/en.

[3] I. Wind River Systems, "VxWorks." [Online]. Available: https://www.windriver.com/products/vxworks/.

[4] D. Formby, A. Walid, and R. Beyah, "A case study in power substation network dynamics," *Proc. ACM Meas. Anal. Comput. Syst.*, vol. 1, no. 1, pp. 19:1–19:24, Jun. 2017.

[5] G. Lyon, "NMAP: THe network mapper." [Online]. Available: https://nmap.org/.