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

Real-time Operating Systems (RTOSs) are, in many ways, similar to general purpose OSes and have, in recent years, gone through similar adjustments due to increasing threats. The primary difference is that RTOSs started out targeting disconnected/private networks and therefore were less suseptible to malicous actors. The developers of such systems focused on the scheulding and real-time nature of their systems (the key objective of the system) rather than hardening them from outside influence. As these systems have been increasingly connected to corporate networks and eventually to the Internet itself, the maintainers of these OSes have had to adopt techniques and protections that have long been present in general purpose OSes but must implement them in a manner that does not impede their schedulers. What follows is a list of advantages, disadvantages and some mitigations for these related to RTOSs.

There are many RTOSs available but some common ones include FreeRTOS[1], QNX[2], and VxWorks[3].

Security Advantages

From the standpoint of platform security, there are some significant advantages to utilizing an RTOS. Some of these include near determinism, reduced attack surface, and limited hardware resources.

Determinism: RTOSs do not provide the same level of clock syhnchronicity available in an FPGA or ASIC, but the are designed to support time-dependent repeating tasks. This regularity can be a significant asset when monitoring the data coming into/going out of one of theses systems - the traffic patterns should exhibit a consistency that eases the tasks of anomaly detection.

Reduced Attack Surface: Becuase these OSes are not general-purpose, they are generally streamlined for a specific category of tasks or operations. As such, the software packages included in the OS and code compiled into the kernel is often far less that would be present in a general OS.

Limited Connectivity: While not a factor specifically of an RTOS, many of the control systems running an RTOS in cyber-physical sytem run in a private network or, at least a segmented network. As mentioned above, however, the increasing connectedness is rapidly diminishing.

Security Disadvantages

- (near) determinisim

- sometimes less robust outward-facing connectivity
- limited hardware resources
- less automated patching/updates
- more often "stuck in a closet"
- less robust (securly).
- Shared Memory (Whiteboard)

Lack of Enterprise Management Features

Mitigations

Since the public disclosure of Stuxnet, there has been an increase in the amount of research in the area of cyber physical systems. Many security researchers are taking a closer look at the devices and software that control the systems that affect our daily lives. Some of the mitigation work is listed below:

Security-Focused RTOS: Much like the general OS market has security-hardended versions of the most common OS variants, there have emerged security-enhanced RTOSs. asdfasdf

Ingegrity RTOS by Green Hills Sofware[4]

Memory Isolation:

System-Call Based Anomaly Detection: In their paper[5] Cheng et. all present an anomaly-detection system that monitors system calls to attempt to determine if someone is performing data-injection attack. They are specifically focused not on network-based attacks, but local-device attacks wherein an attacker attempts to modify the memory locations holding the data on which the control system responds. In these cases, the logical control flow of the application has not been violated, but the data is simply wrong, causing the program to respond in a fashion consistent with its programmed logic but contrary to the actual physical state of the system. Systems such as this could be used to help mitigate the risks of shared memory models in deployed RTOS platforms.

A Potential Bellwether

While not explicitly focused on RTOS-based devices, Formby et. al. [6] 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[7]) 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] G. H. Software, "Integrity real-time operating system." [Online]. Available: https://ghs.com/products/rtos/integrity.html.

[5] L. Cheng, K. Tian, D. Yao, L. Sha, and R. A. Beyah, "Checking is believing: Event-aware program anomaly detection in cyber-physical systems," *CoRR*, vol. abs/1805.00074, 2018.

[6] 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.

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