Using Unikernels to Enhance the Attack-Resistance of Spire, a Network-Attack-Resilient Intrusion-Tolerant SCADA for the Power Grid

Brad Whitehead
Mike Boby

CS3551 – Advanced Topics in Distributed Systems
Class Project

Project Goal

Convert Spire to self-contained unikernels and demonstrate that:

- They continue to operate correctly and
- They exhibit the increased performance and reduced resource utilization characteristics of unikernel technology
- If possible, demonstrate the increased compromise resistance of the Unikernel-based Spire.

Why?

- While an excellent approach, security and compromise resistance may be further enhanced by discarding the use of an operating system and converting the executables into unikernels, isolated from other applications through hardware-enforced virtual machine technology
- Not only will this increase the compromise resistance, it will significantly enhance portability, performance in the areas of initialization (“bootup”) and throughput, as well as decreasing resource utilization (memory)
- Considerable thought and effort has been applied to the problem of making the Spire code resistant to attack and compromise, includes using MultiCompiler to create polymorphic versions

Anticipated Project Steps

1) Familiarization with the Spire system (obtain and compile the code, and run the supplied benchmarks
2) Research available unikernel libraries and select the most appropriate one
3) Select an appropriate paper on unikernels and security to present in class
4) Compile the Spire executables into unikernels
5) Iteratively, make necessary code changes
6) Test and benchmark Spires unikernels using the included benchmark suite
7) Investigate the compromise resistance of the Spire unikernels (this step is dependent on the availability of any existing compromise/penetration tests or test tools)
8) Document the project
9) Prepare and deliver project presentation for class

Prior Research

- While there are a number of publications on the unikernel concept and its applicability to security, since the seminal paper in 2013, only one paper was found that specifically addressed the use of unikernels in a SCADA environment:
  - Sakic E. et al. (2018) VirtuWind – An SDN- and NFV-Based Architecture for Softwarized Industrial Networks. In: German R., Hielscher KS., Krieger U. (eds) Measurement, Modelling and Evaluation of Computing Systems. MMB 2018. Lecture Notes in Computer Science, vol 10740. Springer, Cham

  In this paper, unikernels were selected not for their security properties but rather for their fast instantiation and low memory requirements
- There are two other papers that mention the possibility of using unikernels in industrial networks, but both authors felt that the unikernel orchestration systems were not mature enough
- Both papers chose to use containers instead. Containers have a number of well known security issues. We believe that unikernels are sufficiently mature and goals for Spire are achievable.