Cybersecurity in a Large-Scale Research Facility – The MagLab's Approach

D. S. Butcher[1], C. J. Brigham[2], J. Berhalter[1], A. L. Centers[1], W. M. Hunkapiller[2], T. P. Murphy[1], E. C. Palm[1], J. H. Smith[1],
1.National High Magnetic Field Laboratory, 2. Florida State University, Information Security and Privacy Office

Funding Grants: G.S. Boebinger (NSF DMR-2128556 and NSF/DMR-1644779) and the State of Florida

What is the finding? The National High Magnetic Field Laboratory (MagLab) and Florida State University (FSU) have developed a cybersecurity approach that *addresses the researcher's need for open network access, supports the conduct of research, and promotes maximum research impact by enabling open data and FAIR (Findable, Accessible, Interoperable, and Reusable) data management principles. Simultaneously, this approach protects critical equipment and information from unauthorized or malicious access and exploitation.*

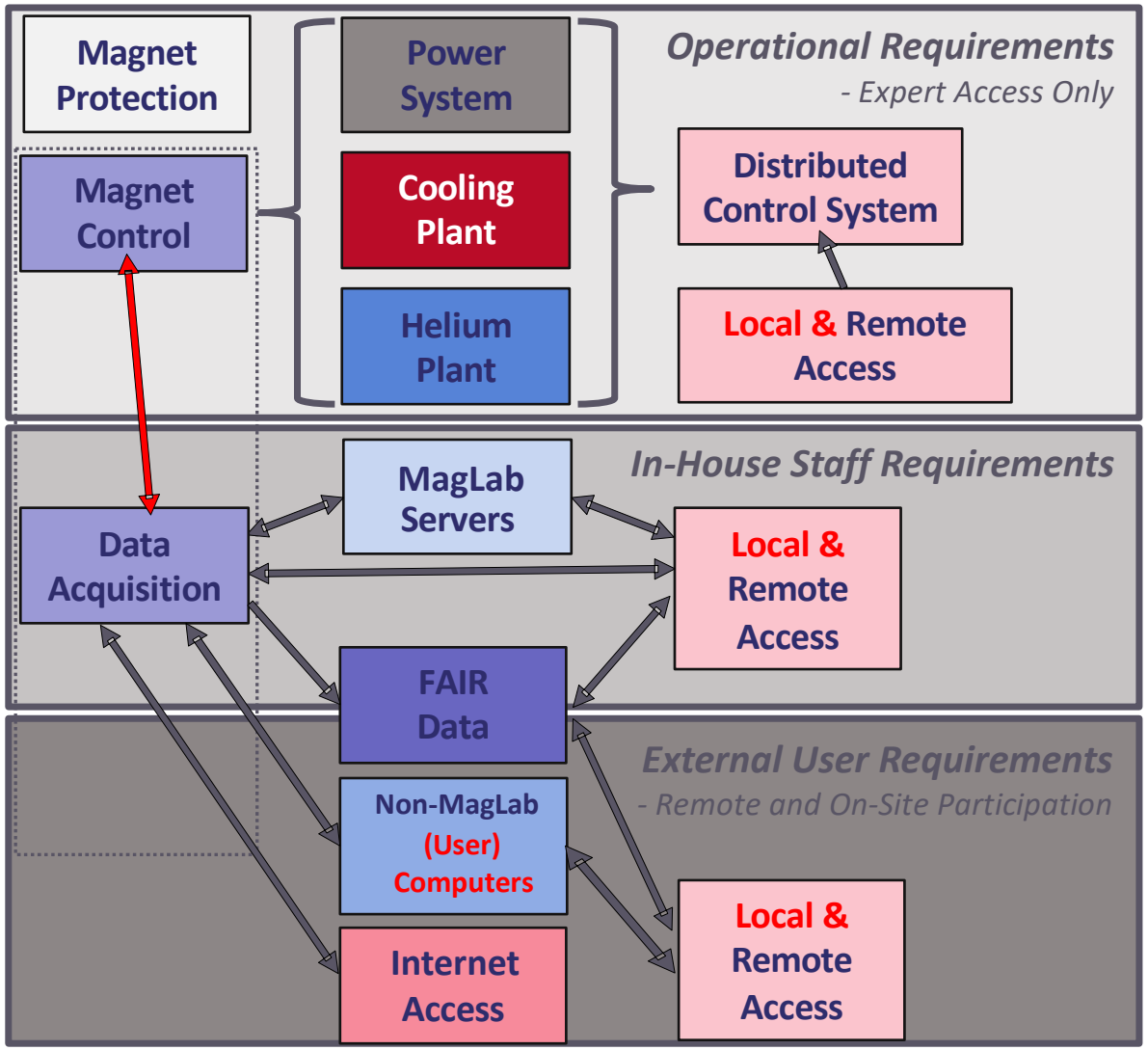
Why is this important? The MagLab provides access to the highest magnetic fields for scientific research teams from a range of disciplines. *Cybersecurity for such a large-scale user facility presents unique challenges due to the requirement to address both protection needs of a facility featuring industrial scale equipment that has associated hazards and, on the other hand, the network and connectivity needs of thousands of external users, an international community that evolves from year to year.*

Cybersecurity protocols and standards for conventional corporate applications typically fall short of addressing the range of needs that modern research facilities face. Pragmatic solutions for cybersecurity protection are needed that also protect external user access that is necessary to advance scientific research. As such, *the MagLab and FSU have developed a bespoke cybersecurity approach tailored for the MagLab's user facilities.*

Why did this research need the MagLab? As a large-scale user facility that hosts about 2,000 researchers in its facilities annually, the MagLab and its user facility staff have unique perspectives and are strongly motivated to develop suitable pragmatic cybersecurity protocols due to the access and protection needs of its people, programs, and assets.

Facilities used: DC Field Facility, Ion Cyclotron Resonance Facility

Citation: [1] Butcher, D.S.; Brigham, C.J.; Berhalter, J.B.; Centers, A.L.; Hunkapiller, W.M.; Murphy, T.P.; Palm, E.C.; Smith, J.H., *Cybersecurity in a Large-Scale Research Facility—One Institution's Approach,* **Journal of Cybersecurity and Privacy, 3,** 191-208 (2023) **doi.org/10.3390/jcp3020011**



Overview of the accessibility needs for scientific research in a large-scale user facility like the MagLab. [1]