Digital Biosecurity Pilot Project

Problem Statement

Security models for the bioeconomy have largely been developed on risk profiles borrowed from the financial industry and, in some cases, industrial control systems. The bioeconomy, however, has unique characteristics that require domain-specific knowledge of the risks to environmental, health and economic impact from directly targeted attacks. Key questions need to be assessed and answered for any facility engaged in bioproduction. These include: how much technical information must the attacker possess in order to target a specific process or facility? Which processes cause the largest economic impact if disrupted? Can an attacker lead companies down the wrong path of research, leading to irrecoverable losses of time, resources and capital? Can attackers disrupt venture capital strategies and affect financial returns? What are the resources required to attack key workflows, and subsequently what is the cost of defense? What strategies are effective against such attackers, and what are their cost? Can government provide an active role in assurance of material, process and results for critical bioeconomic infrastructure?

The path to market for biotechnology ventures requires intricate and highly regulated R&D and manufacturing processes. The various processes involved in biomanufacturing often have shared instrumentation and human practices, making it attractive to an attacker to target a few critical steps for maximal economic impact. In biomanufacturing it is hard to develop truly robust and “defense by depth” operations. One illustrative example of this problem is in scale-up manufacturing when companies attempt to demonstrate the scalability of their production by moving from small volume bioreactors (300mL) to large volume capabilities (2,000L-20,000L). In cursory studies of this scale-up process we have identified key steps where attackers could cause the loss of 88% of cost of goods in the scale-up manufacturing and production workflows.

We are advocating for pilot project, designed to assess the economic impact, attribution capability, countermeasure design and longevity of such attacks on a real-life scale-up manufacturing workflow. This project would build on capabilities currently being developed by Sandia National Laboratories and BioBright with the support and collaboration of In-Q-Tel Laboratories. This pilot project would include both physical and computationally modelled systems to demonstrate real operations and show how the unique challenges of biomanufacturing demand an enhanced effort to protect the security, resiliency and reliability of critical biomanufacturing capabilities.

Unique Capabilities

DarwinSync – BioBright

DarwinSync is an encrypted end-to-end scientific data collection platform being deployed commercially with biotechnology, pharmaceutical, and instrument companies. Initially funded by DARPA, DarwinSync automatically collects scientific data from equipment and extracts the proprietary metadata from the files before making this data available programmatically through application programming interfaces. This platform enables the collection of real-world, ground-truth data that can be used to detect unexpected deviations from a workflow or anomalous instrument behavior.

Emulytics and cybersecurity - Sandia National Laboratories
Sandia National Laboratories has developed the Emulytics simulation and assessment platform as a technology for rapid specification and deployment of complex networked systems – including software, hardware, services, applications and hardware-in-the-loop. This tool allows event replay, component testing and assessment of complex ConOps scenarios by instantiating thousands of host components in high-fidelity. Systems using Emulytics have been deployed to model and assess cybersecurity risks in genomic, synthetic biology and industrial systems.

BrightPoseidon - BioBright & In-Q-Tel Laboratories (Q3 '20)
BrightPoseidon refers to the combination of BioBright's DarwinSync capabilities with In-Q-Tel laboratories' Poseidon software. Together, these tools are anticipated to allow the detection of attackers impersonating biological equipment on a facility's network. This capability is under development and is anticipated to come online in Q3 2020.

Access to instrument manufacturer and industrial partner data
BioBright and Sandia have worked directly with key hardware and software vendors to collect and assess material (i.e., firmware, software and hardware) from biomedical instrument manufacturers. These relationships have allowed BioBright and Sandia access to material for security assessment purposes. Additionally, our work with synthetic biology and biomedical manufacturing companies have given us first-hand knowledge of realistic experience with scale-up facility operations.

Necessary Activities
Here we advocate for a demonstration of the unique security considerations of a biomanufacturing process. Specifically, we argue for demonstration of a cybersecurity incident on a functioning scale-up biomanufacturing process, deployed *in silico.* This simulated incident would 1) Demonstrate the unique biological risk space – by showing the impact of a consequential attack on a major bioeconomic component, exercising realistic security considerations; 2) Provide impacts metrics, i.e., economic (e.g., quantity yield reduction impacting manufacturing throughput) and safety (e.g., as a result of increased impurities missed by QC); 3) Deploy network monitoring pre-attack to demonstrate the value of device-to-device and network visibility in detection, containment, remediation and event forensics; 4) Provide *post-facto* incident analysis, mitigations and lessons learned; 5) Identify and map key global biomanufacturing capabilities, vendors and operations for community-building around safe and secure biomanufacturing.

The five components of this potential simulated incident are distinctly valuable as separate components in the process of digital biosecurity incident response. The demonstration of an attack would be a minimal necessary component, however parts 2-5 provide key additional information about our understanding of realistic scenarios. The ultimate goal of this research and exercise would be a blueprint for planning and addressing cyber incidents in the future. This blueprint would provide a tool for recognizing unique cybersecurity vulnerabilities to the bioeconomy that occur in agriculture, genomics, medical device and hospital operations, biomanufacturing and pharmaceutical development. Its ultimately goal would be to establish an understanding of the risks and mitigations affecting digital biosecurity and to use that understanding to reduce threats to critical infrastructure, coordinate vulnerability information sharing and manage risks.

Model Development of a Biological Industrial Operations Cyber Emergency Response Team
The advocated activities would serve as an operational staging platform for demonstrating the value and usefulness of a government-led threat response effort – serving the medical, genomic and synthetic biology device, software and operations industries. Government, industrial and academic partners would be able to use this framework to craft a responsible disclosure plan. This would include buy-in from the relevant vendors, a communication plan and a common vulnerabilities and exposures detailing the issues, mitigating steps, and a realistic assessment of risk. This could be modeled on the DHS's existing US-CERT/ICS-CERT procedures. This pilot would require a trusted government partner for deploying this model – acting as a liaison between government, academia and industry. It would also require a trusted industry partner to serve as the industry connector – getting buy-in and support from all elements of biological equipment and operations industries.