Sector: Agritech

Cybersecurity for Food Security (CyFoo)

Sharad Agarwal
Prof. Awais Rashid
Joseph Gardiner
Dr Barnaby Craggs
University of Bristol

INTRODUCTION

With the everyday updates in technology, farming has also been shifting to adopt more and more smart/automated devices. This can be seen as Agritech being highly disruptive in a sector with historically low profitability. CyFoo studies the impact of malicious actors and vulnerabilities on the food supply through adoption of agritech.

AIM

The project aims to investigate vulnerabilities and their impact in order to develop a risk analysis framework and policy guidelines to support users in understanding and mitigating the cybersecurity risks from sensor-driven digital infrastructure.

HOW / METHODOLOGY

The CyFoo project deploys Agritech field studies to investigate user understanding, perception, and behaviour towards risk. In particular, the project considers sensor-driven technology used for food production, such as precision agriculture (PA) and precision livestock farming (PLF). We are also deploying a table-top smart dairy farming testbed in our lab where we will conduct security assessment and risk analysis of the devices that we install in the testbed.

Figure 1: Smart Dairy Farm

What are the key security concerns with regards to smart farming and Agritech and which ones might keep us awake at night?

EXPECTED IMPACT

With the dairy farming testbed, we will study the attack surfaces of such systems and perform a security assessment to identify the current security trends in the devices used in a smart dairy farm. We will follow responsible disclosure process for any vulnerabilities identified. The interviews will help us understand risk perceptions and risk decision-making of those who procure, deploy, and use such devices in Agritech and help us understand where risk perceptions align (or not) with technical vulnerabilities in systems.

KEY OUTCOMES

We will build a smart dairy farming testbed in our lab which will provide a platform to study security issues and test countermeasures. A policy briefing will be developed which will be shared with relevant stakeholders including manufacturers, government, and other farmer bodies.

MAJOR FINDINGS UP TO DATE

1. There is a lack of understanding and awareness about security in the agritech sector.
2. The farms have a trust relationship with their suppliers regarding their products and any updates to the systems. Security does not appear to be a primary concern.
3. We have identified and engaged with new stakeholders such as analytics companies and vets who can access the APIs or data through the devices deployed in farms directly. This introduces new attack surfaces that can be used to introduce vulnerabilities.

USER PARTNERS

Mage Control

DISSEMINATION

https://www.fginsight.com/news/farmer-input-wanted-for-cyber-security-research-123071

ACKNOWLEDGEMENTS

Bristol Cyber Security Group

PETRAS
UK Research and Innovation
University of Bristol
Bristol Cyber Security Group