CCST EXPERT BRIEFING SERIES:
Toward a Disaster Resilient California

Cultivating Data Security Practices in **PRECISION AGRICULTURE**

Download this **Document**

One Pager

Briefing held: **OCT. 2022**

For more details about this briefing: ccst.us/expert-briefings

SUMMARY

- Precision agriculture (PA) has the capacity to improve agricultural yields, reduce water and other inputs, and reduce greenhouse gas emissions.
- The data required to implement PA practices is extremely valuable and susceptible to theft and the data systems are susceptible to ransomware.
- By manipulating data, bad actors can negatively affect the cost of agricultural production.
- Many farmers and people involved in food production would benefit from a greater understanding of the security risks that exist in their data systems, and training or resources to prevent an attack from happening.

DATA PRIVACY AND PRECISION AGRICULTURE

THE PROMISE AND THE RISKS

To feed a growing population affordably and in a way that minimizes greenhouse gas production, the farming industry will need to rely on innovative technologies such as precision agriculture. **Precision agriculture** is an approach to farming that optimizes water, fertilizer, and other inputs by using very detailed and high spatial resolution data that is captured by a network of sensors, drones, and other means of data collection. The data are processed in real- or near-real time so farmers can make highly informed decisions on how to manage their crop.

By its very nature, precision agriculture generates large amounts of data that are extremely valuable to farmers and other people, including private industry and malicious actors. Access to, corruption of, or other perturbations to the data involved in precision agriculture may have large downstream impacts on inputs (e.g. water, fertilizer) and therefore the cost of food production.

Cyber attacks on critical infrastructure, including food

KEY THREATS
IN PRECISION AGRICULTURE

CONFIDENTIALITY
Intentional theft of sensitive data that can be published publicly or sold to negatively impact a farmer's financial status or reputation.

INTEGRITY
Intentional falsification of data into sensor or control systems that may disrupt crop and livestock sectors.

AVAILABILITY
Disrupting systems or networks at critical times such that data for navigation, decision-making, or other controls are not available.

Outcomes from a cyber attack in precision agriculture are similar to other sectors: Data theft, stealing resources, reputation loss, destruction of equipment, or gaining an improper financial advantage over a competitor.

STRONGER WITH SCIENCE FOR 30 YEARS

CCST
CALIFORNIA COUNCIL ON SCIENCE & TECHNOLOGY

CCST Disaster Resilience Initiative: Ongoing, complex, and intersecting disasters—including climate change, extreme heat, power outages, and the COVID-19 pandemic—are radically disrupting the ways in which Californians live and work. CCST is committed to delivering science and technology advice to improve our resilience to disasters, reduce harm, and improve the lives of all Californians.

SELECT EXPERTS

The following experts can advise on data security and precision agriculture:

PRAMOD KHARGONEKAR, PHD
UC Irvine
Vice Chancellor for Research &
Dist. Professor of Electrical Engineering and Computer Science
pramod.khargonekar@uci.edu

Expertise: control and systems theory, cyber-physical systems, applications to manufacturing, renewable energy, biomedical engineering

ALIREZA POURREZA, PHD
UC Davis
Assistant Professor and Director of the Digital Agriculture Lab
apourreza@ucdavis.edu

Expertise: Advanced sensing technologies for crop monitoring and precision agriculture.

LISA YEO, PHD
UC Merced
Assistant Professor
lyeo2@ucmerced.edu

Expertise: Privacy and security implications of precision agriculture.

CHANDRA KRINTZ, PHD
UC Santa Barbara
Vice Chair of Graduate Affairs and Professor of Computer Science
ckrintz@ucsb.edu

Expertise: AI systems for digital agriculture and the Internet of Things (IoT).

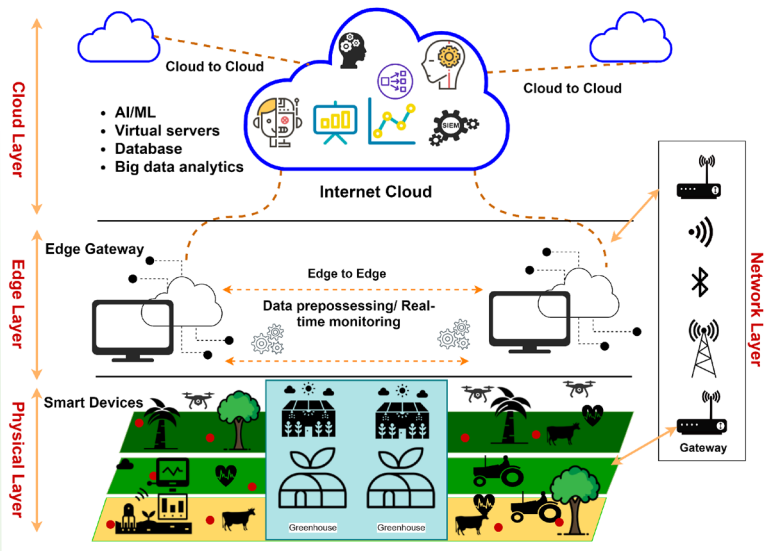
TIFFANY DRAPE, PHD
Virginia Tech
Assistant Professor
tdrape@vt.edu

Expertise: producer's understanding and misconceptions about the generation, storage, and use of agricultural data

CCST CONTACTS:

Brie.Lindsey@ccst.us
Director of Science Services

Sarah.Brady@ccst.us
Deputy Director



Yazdinejad A, Zolfaghari B, Azmoodeh A, Dehghantanha A, Karimipour H, Fraser E, Green AG, Russell C, Duncan E. A Review on Security of Smart Farming and Precision Agriculture: Security Aspects, Attacks, Threats and Countermeasures. Applied Sciences. 2021; 11(16):7518. https://doi.org/10.3390/app11167518

A Typical **SMART FARM**

A typical smart farm that employs precision agriculture may have multiple layers of data collection, processing, handling, and storage that are susceptible to data loss. These layers are referred to as physical, edge, network, and cloud layers.

Common attacks may include:

- Attacks on the hardware (e.g. IoT and other cyber-physical devices)
- Attacks on the networks and related equipment
- Attacks on data - attacking the data while being stored, transmitted, or processed
- Attacks on the code, software, or applications
- Attacks on the support chains
- Misuse attacks (e.g., misuse of physical resources to attack entities such as people or property)

and agricultural systems, are on the rise across the nation and have the potential for impacts at scales ranging from local community to global economy.

In 2021 the FBI identified five large cyber attacks on food supply systems. These events are causing disruptions in large industries (e.g. meat packing businesses) to smaller cooperatives.

Ransoms for these attacks have ranged up to **$40 million** and continue to trend up in frequency of attacks and ransom amount. Indeed, even a small Iowa farming coop was attacked and had its data ransomed for **$5.9 million**.

Agriculturally-related ransom attacks are not limited to food production. Manufacturers of farm equipment have reported attacks as well, suggesting there could be attacks impacting the world's food production at multiple points from farm equipment production and delivery, to food production and shipping.

In a time when data privacy, security, and rights are the subject of active debate, many aspects of data used to optimize agricultural and food system production and distribution—such as data generation, ownership, and security—are not thoroughly understood.

Case Study: IOWA GRAIN COOP

September 2021

A ransomware group, BlackMatter, stole **1 terabyte** (1,000 gigabytes) of New Cooperative Inc's data—including invoices, R&D work, and soil-mapping technology—and demanded **$5.9 million** to return the data.

The ransomware attack resulted in New Cooperative taking their systems offline to contain the threat. This action resulted in disabling their soil-mapping platform (i.e., software used to provide farmers with precise fertilizer and water input recommendations) and using temporary solutions to feed livestock and poultry farms that rely on the feed supplies.

Case Study: FARM IMPLEMENT VULNERABILITY

August 2021 - 2022

A hacker named Sick Codes was able to attack and access multiple systems on John Deere tractors. Sick Codes attacked the tractors' systems to demonstrate their vulnerabilities and there was no ransom or damage.

These exposed vulnerabilities showed that such system and device insecurities could be exploited by malicious actors or potentially combined with other vulnerabilities.

Such vulnerabilities could render equipment inoperable or produce erroneous data or affect guidance software to drive tractors off-course. If attacks were done during a critical period such as planting and harvesting, there could be financial loss to farmers and potential impacts on food supply chains.