# DT726A Spring 2025 Cybersecurity for the Internet of Things (IoT)

Jonas Colmsjö

University of Örebro

2025-03-12

# Some Benefits of Smart Agriculture

Utilizing inexpensive network and sensor platforms has led to noteworthy improvements in agricultural techniques:

- reduced water and energy consumption
- reduces excessive use of fertilizers and pesticides
- bolster farming system resilience
- reduce greenhouse gas emissions
- enhance food security
- ultimately enhances crop production while minimizing environmental impact

Source: Smart Agritech - Robotics, AI, and Internet of Things (IoT) in Agriculture, Santosh Kumar Srivastava

# Approach

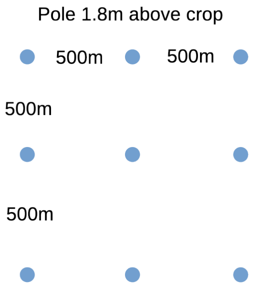
A Smart Agriculture Architecure based on Davis Instruments will be evaluated from a security perspective.

The standard ETSI TR 103 621 - Guide to Cyber Security for Consumer Internet of Things will be used

An alternative to Davis Instruments will also be briefly reviewed.

# Placement of Sensor Nodes

Type of environment deterime the necessery density for the nodes



Pole 1.8m above crop

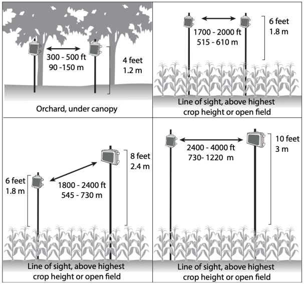
500m

500m

500m

500m

(a) Sensor density



(a) Pole height

Nine short poles can cover approx. 1km2 (or 100 hectare) on a flat landscape without trees

# Example of configuration

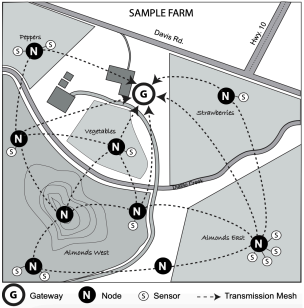


Figure 3: Sample Farm

The landscape and crops will determine the requirements in the end

The gateway should be placed where it has good cellular connectivity

The Zigbee mesh network (DavisTalk) work best if each node can reach at least two nodes and not just one

# Network Security

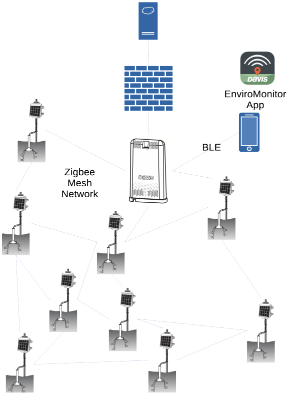
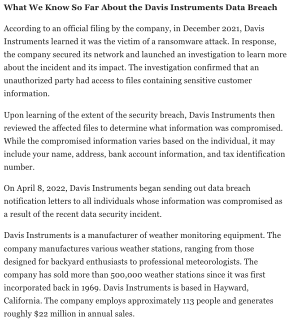


Figure 4: Network diagrram

Configuration is performed using an app that communicate with the Gateway using Bluetooth (BLE)

# Security Related Processes



**What We Know So Far About the Davis Instruments Data Breach**

According to an official filing by the company, in December 2021, Davis Instruments learned it was the victim of a ransomware attack. In response, the company secured its network and launched an investigation to learn more about the incident and its impact. The investigation confirmed that an unauthorized party had access to files containing sensitive customer information.

Upon learning of the extent of the security breach, Davis Instruments then reviewed the affected files to determine what information was compromised. While the compromised information varies based on the individual, it may include your name, address, bank account information, and tax identification number.

On April 8, 2022, Davis Instruments began sending out data breach notification letters to all individuals whose information was compromised as a result of the recent data security incident.

Davis Instruments is a manufacturer of weather monitoring equipment. The company manufactures various weather stations, ranging from those designed for backyard enthusiasts to professional meteorologists. The company has sold more than 500,000 weather stations since it was first incorporated back in 1969. Davis Instruments is based in Hayward, California. The company employs approximately 113 people and generates roughly $22 million in annual sales.

Figure 5: Breach

- David Instruments has no public no vulnerability disclosure policy. Thers is no place to report vulnerabilities. There is not public list of vulnerabilieis (CVE:s)
- But Davis Instruments did inform their customers when they were breached themselves

# Evaluation against ETSI TR 103 621 - Guide to Cyber Security for Consumer Internet of Things

Summary of evaluation:

- Requirements met: 23
- Requirements not met: 4
- Not possible to determine: 35

# Amount of data sent

4 sensors/node x 9 nodes every 5min

- 100 bytes x 4 x 9 x 12 = 43.2kb/h

# Price

- EnviroMonitor Node ($525)
- Soil: DI 6440 ($85)
- Temp/Humidity: DI 6830 ($175)
- Solar: DI 6450 ($225)
- UV: DI 6490 ($425)
- CO2: SenseCAP NDIR ($100)
- EnviroMonitor Gateway ($995)
- Cisco Secure Firewall ISA3000 ($3600)
- Total 1.435x9 + 995 + 3.600 = 12.915 + 995 + 3.600 = 17.510

| Update Intervals | Annual Service Charge/Node |
|---|---|
| 5 min | $180 |
| 15 min | $156 |
| 60 min | $132 |

# Summary for Davis Instruments

Davis Instruments have many weaknesses and many questions are not answered!

Still, they are well established vendor and any obvious off-the-shelf alternative that is more secure has not been found

Building the architecture part-by-part is an alternative where all design decisions will be knonw (since we make them ourselves)

- this should not be considred a more secure solution until it has been thourougly tested in practice though
- it is also quite certainly a more expensive solution taking all costs into consideration

# Alternative Architecture based on LoRa LPWAN

Use the same Davis Instruments set of sensors

Cambell Scientific Titan Radius Mote SDI-12 LPWAN Slave ($180)

- can take SDI-12 Sensors each

RAK RAK7391 LoRa WAN Gateway ($530)

- Raspberry Pi Compute Module 4

Cloud: Use AWS IoT for LoRaWAN with the Open Source LoRa Basics Station

- has suport for MQTT and HTTPS.

Price: $(1010 + 180)\text{x}9 + 530 = 11.240$

AWS pricing is complex but the cost for messaging seam negligible. The cost for a server need to be added though! - approx 2 million messages per year (45 sensors x 5 messages per hour) with a costs $1.20 /million messages

# Thank You!

# APPENDIX

Evaluation against ETSI TR 103 621 - Guide to Cyber Security for Consumer Internet of Things

Provision 5.1-1 “Where passwords are used and in any state other than the factory default, all consumer IoT device passwords shall be unique per device or defined by the user”. OK

Provision 5.1-2 “Where pre-installed unique per device passwords are used, these shall be generated with a mechanism that reduces the risk of automated attacks against a class or type of device”. OK

Provision 5.1-3 “Authentication mechanisms used to authenticate users against a device shall use best practice cryptography, appropriate to the properties of the technology, risk and usage”. UNKNOWN

Provision 5.1-4 “Where a user can authenticate against a device, the device shall provide to the user or an administrator a simple mechanism to change the authentication value used”. UNKNOWN

Provision 5.1-5 “When the device is not a constrained device, it shall have a mechanism available which makes brute-force attacks on authentication mechanisms via network interfaces impracticable”. UNKNOWN

Provision 5.2-1 “The manufacturer shall make a vulnerability disclosure policy publicly available. This policy shall include, at a minimum: - contact information for the reporting of issues; and - information on timelines for: 1) initial acknowledgement of receipt; and 2) status updates until the resolution of the reported issues”. NOK

Provision 5.2-2 “Disclosed vulnerabilities should be acted on in a timely manner”. UNKNOWN

Provision 5.2-3 “Manufacturers should continually monitor for, identify and rectify security vulnerabilities within products and services they sell, produce, have produced and services they operate during the defined support period”. UNKNOWN

Provision 5.3-1 “All software components in consumer IoT devices should be securely updateable”. OK

Provision 5.3-2 “When the device is not a constrained device, it shall have an update mechanism for the secure installation of updates”. OK

Provision 5.3-3 “An update shall be simple for the user to apply”. OK

Provision 5.3-4 “Automatic mechanisms should be used for software updates”. OK

Provision 5.3-5 “The device should check after initialization, and then periodically, whether security updates are available”. OK

Provision 5.3-6 “If the device supports automatic updates and/or update notifications, these should be enabled in the initialized state and configurable so that the user can enable, disable, or postpone installation of security updates and/or update notifications”. OK

Provision 5.3-7 “The device shall use best practice cryptography to facilitate secure update mechanisms”. UNKNOWN

Provision 5.3-8 “Security updates shall be timely”. UNKNOWN

Provision 5.3-9 “The device should verify the authenticity and integrity of software updates”. UNKNOWN

Provision 5.3-10 “Where updates are delivered over a network interface, the device shall verify the authenticity and integrity of each update via a trust relationship”. UNKNOWN

Provision 5.3-11 “The manufacturer should inform the user in a recognizable and apparent manner that a security update is required together with information on the risks mitigated by that update”. UNKNOWN

Provision 5.3-12 “The device should notify the user when the application of a software update will disrupt the basic functioning of the device”. UNKNOWN

Provision 5.3-13 “The manufacturer shall publish, in an accessible way that is clear and transparent to the user, the defined support period”. OK

Provision 5.3-14 “For constrained devices that cannot have their software updated, the rationale for the absence of software updates, the period and method of hardware replacement support and a defined support period should be published by the manufacturer in an accessible way that is clear and transparent to the user” UNKNOWN

Provision 5.3-15 “For constrained devices that cannot have their software updated, the product should be isolable and the hardware replaceable”. OK

Provision 5.3-16 “The model designation of the consumer IoT device shall be clearly recognizable, either by labelling on the device or via a physical interface”. OK

Provision 5.4-1 “Sensitive security parameters in persistent storage shall be stored securely by the device”. UNKNOWN

Provision 5.4-2 “Where a hard-coded unique per device identity is used in a device for security purposes, it shall be implemented in such a way that it resists tampering by means such as physical, electrical or software”. UNKNOWN

Provision 5.4-3 “Hard-coded critical security parameters in device software source code shall not be used”. UNKNOWN

Provision 5.4-4 “Any critical security parameters used for integrity and authenticity checks of software updates and for protection of communication with associated services in device software shall be unique per device and shall be produced with a mechanism that reduces the risk of automated attacks against classes of devices” UNKNOWN

Provision 5.5-1 “The consumer IoT device shall use best practice cryptography to communicate securely”. UNKNOWN

Provision 5.5-2 “The consumer IoT device should use reviewed or evaluated implementations to deliver network and security functionalities, particularly in the field of cryptography” UNKNOWN

Provision 5.5-3 “Cryptographic algorithms and primitives should be updateable”. OK

Provision 5.5-4 “Access to device functionality via a network interface in the initialized state should only be possible after authentication on that interface” OK

Provision 5.5-5 “Device functionality that allows security-relevant changes in configuration via a network interface shall only be accessible after authentication. The exception is for network service protocols that are relied upon by the device and where the manufacturer cannot guarantee what configuration will be required for the device to operate”. OK

Provision 5.5-6 “Critical security parameters should be encrypted in transit, with such encryption appropriate to the properties of the technology, risk and usage”. OK

Provision 5.5-7 “The consumer IoT device shall protect the confidentiality of critical security parameters that are communicated via remotely accessible network interfaces”. OK

Provision 5.5-8 “The manufacturer shall follow secure management processes for critical security parameters that relate to the device”. UNKNOWN

Provision 5.6-1 “All unused network and logical interfaces shall be disabled”. UNKNOWN

Provision 5.6-2 “In the initialized state, the network interfaces of the device shall minimize the unauthenticated disclosure of security-relevant information”. UNKNOWN

Provision 5.6-3 “Device hardware should not unnecessarily expose physical interfaces to attack” UNKNOWN

Provision 5.6-4 “Where a debug interface is physically accessible, it shall be disabled in software”. UNKNOWN

Provision 5.6-5 “The manufacturer should only enable software services that are used or required for the intended use or operation of the device”. UNKNOWN

Provision 5.6-6 “Code should be minimized to the functionality necessary for the service/device to operate”. UNKNOWN

Provision 5.6-7 “Software should run with least necessary privileges, taking account of both security and functionality”. UNKNOWN

Provision 5.6-8 “The device should include a hardware-level access control mechanism for memory”. UNKNOWN

Provision 5.6-9 “The manufacturer should follow secure development processes for software deployed on the device”. UNKNOWN

Provision 5.7-1 “The consumer IoT device should verify its software using secure boot mechanisms”. UNKNOWN

Provision 5.7-2 “If an unauthorized change is detected to the software, the device should alert the user and/or administrator to the issue and should not connect to wider networks than those necessary to perform the alerting function”. UNKNOWN

Provision 5.8-1 “The confidentiality of personal data transiting between a device and a service, especially associated services, should be protected, with best practice cryptography”. UNKNOWN

Provision 5.8-2 “The confidentiality of sensitive personal data communicated between the device and associated services shall be protected, with cryptography appropriate to the properties of the technology and usage”. UNKNOWN

Provision 5.8-3 “All external sensing capabilities of the device shall be documented in an accessible way that is clear and transparent for the user”. OK

Provision 5.9-1 “Resilience should be built in to consumer IoT devices and services, taking into account the possibility of outages of data networks and power”. OK

Provision 5.9-2 “Consumer IoT devices should remain operating and locally functional in the case of a loss of network access and should recover cleanly in the case of restoration of a loss of power”. OK

Provision 5.9-3 “The consumer IoT device should connect to networks in an expected, operational and stable state and in an orderly fashion, taking the capability of the infrastructure into consideration”. OK

Provision 5.10-1 “If telemetry data is collected from consumer IoT devices and services, such as usage and measurement data, it should be examined for security anomalies”. UNKNOWN

Provision 5.11-1 “The user shall be provided with functionality such that user data can be erased from the device in a simple manner”. OK

Provision 5.11-2 “The consumer should be provided with functionality on the device such that personal data can be removed from associated services in a simple manner”. OK

Provision 5.11-3 “Users should be given clear instructions on how to delete their personal data”. NOK

Provision 5.11-4 “Users should be provided with clear confirmation that personal data has been deleted from services, devices and applications”. NOK

Provision 5.12-1 “Installation and maintenance of consumer IoT should involve minimal decisions by the user and should follow security best practice on usability”. UNKNOWN

Provision 5.12-2 “The manufacturer should provide users with guidance on how to securely set up their device”. OK

Provision 5.12-3 “The manufacturer should provide users with guidance on how to check whether their device is securely set up”. NOK

Provision 5.13-1 “The consumer IoT device software shall validate data input via user interfaces or transferred via Application Programming Interfaces (APIs) or between networks in services and devices”. UNKNOWN

# Examples to meet data protection provisions for consumer IoT

Provision 6-1 “The manufacturer shall provide consumers with clear and transparent information about what personal data is processed, how it is being used, by whom, and for what purposes, for each device and service. This also applies to third parties that can be involved, including advertisers”.

Provision 6-2 “Where personal data is processed on the basis of consumers’ consent, this consent shall be obtained in a valid way”.

Provision 6-3 “Consumers who gave consent for the processing of their personal data shall have the capability to withdraw it at any time”.

Provision 6-4 “If telemetry data is collected from consumer IoT devices and services, the processing of personal data should be kept to the minimum necessary for the intended functionality”.

Provision 6-5 “If telemetry data is collected from consumer IoT devices and services, consumers shall be provided with information on what telemetry data is collected, how it is being used, by whom, and for what purposes”.

# Resources

https://github.com/weatherlink

https://manualsnet.com/davis/enviromonitor-6810

https://www.weatherlink.com/static/docs/APIdocumentation.pdf

https://www.jdsupra.com/legalnews/data-breach-alert-davis-instruments-1461698/