Establishing a Chain of Trust in a Sporadically Connected Cyber-Physical System

Silia Maksuti[1,2], Michael Pickem[1], Mario Zsilak[1], Anna Stummer[1], Markus Tauber[1,3], Marcus Wieschhoff[1], Dominic Pirker[4,5], Christoph Schmittner[6] and Jerker Delsing[2]

[1]*University of Applied Sciences Burgenland* - Eisenstadt, Austria
[2]*Luleå University of Technology* - Luleå, Sweden
[3]*Research Studios Austria FG* - Vienna, Austria
[4]*Infineon Technologies Austria AG* - Graz, Austria
[5]*Graz University of Technology* - Graz, Austria
[6]*AIT Austrian Institute of Technology GmbH* - Vienna, Austria

***Abstract*—Drone based applications have progressed significantly in recent years across many industries, including agriculture. This paper proposes a sporadically connected cyber-physical system for assisting winemakers and minimizing the travel time to remote and poorly connected infrastructures. A set of representative diseases and conditions, which will be monitored by land-bound sensors in combination with multispectral images, is identified. To collect accurate data, a trustworthy and secured communication of the drone with the sensors and the base station should be established. We propose to use an Internet of Things framework for establishing a chain of trust by securely onboarding drones, sensors and base station, and providing self-adaptation support for the use case. Furthermore, we perform a security analysis of the use case for identifying potential threats and security controls that should be in place for mitigating them.**

I. Introduction

Cyber-physical systems (CPS) are systems that include engineered, interacting networks of physical and computational components. A special case of such systems are unmanned aerial vehicles (UAV), or drone based applications, which can be used for assessing the health state of vineyards. Compared to satellite technology, the use of drones in agriculture provides a more effective view of the vineyards, whilst still remaining close to the terrain and thereby providing more precise evaluations [1]. However, in some cases, the vineyards are located in rough environments with poorly connected infrastructure.

To address this issue we propose a CPS, where a small compute unit is mounted on the drone and small sensors with compute units are positioned in the field creating a wireless sensor network (WSN). The drone will act as a gateway by collecting land-bound sensor data and multispectral images of the grapevines and sending this data to a base station for further analysis. Two different vineyards in Burgenland, Austria, are used for field tests and test flights. By fusing the measurements of land-bound sensors and multispectral images from the drone, certain diseases and conditions can be monitored and detected at early stages. In this paper, we have identified a set of representative diseases and conditions that will be monitored by land-bound sensors and multispectral images. In order to achieve accurate measurements, it is important to identify the precise position of land-bound sensors in the field. To address this, the LAYERS tool is used to analyse the multispectral images taken from the drone. Precision vineyard management requires a high level of data confidentiality, integrity and availability. Modern crop management has a high impact on quality, profitability, productivity and sustainability. Incorrect, compromised or incomplete data can lead to false selection of pesticides or chemicals, delayed reactions to water stress and in consequence to crop failure or loss of quality.

978-3-903176-32-4

Due to remote and poorly connected infrastructures, the compute unit integrated in the drone is not always connected with land-bound sensors and base station, thus it is a sporadically connected CPS. To ensure confidentiality, integrity and availability of the data, the communication should be trustworthy and reliable. Only by trusting and relying to the data, the system can adapt itself to a changing environment e.g. using autonomic elements to adapt the sensor reading interval. We use Eclipse Arrowhead [2], as a representative example of an Internet of Things (IoT) framework, for securely onboarding the drone, sensors, and base station. Secure onboarding creates a chain of trust by using a chain of X.509 certificates [3]. This will ensure that only valid data is retrieved, damaged sensors are detected and only authorized components participate in the communication. Thus, the main contribution of the paper is to establish an end-to-end secured communication.

We perform a security analysis of the UAV communication use case. We identify a number of threats by performing threat modeling and show the results of one representative micro use case. Threat modeling is a process by which potential threats can be identified, enumerated, and mitigations can be prioritized. We investigate security standards and extract a number of security controls that should be integrated in the use case to mitigate the identified threats.

The remainder of this paper is structured as follows. Section II provides an overview of the related work. Section III describes the use case, representative diseases, and sensor positioning. Section IV presents the security analysis, including the identified threats and the security controls for mitigating them. Section V outlines findings and future work.

II. Related Work

Technology advances in UAVs have enabled the development of monitoring possibilities and surveillance of vegetation and environmental parameters in agricultural industry [4], [5]. Drone based applications are used to monitor environmental parameters with the scope to optimize the usage of the fields and to improve the efficiency by estimating the right time for harvesting. Additionally, they are used for disease monitoring, giving the possibility to detect plant diseases at an early stage and prevent their spread [6].

Vanegas et. al. [7] show the usage of UAV remote sensing to detect phylloxera infested regions in Australian vineyards. They use cameras (RGB, multi- and hyperspectral cameras) attached to the drone to collect data from two vineyards. The data are used to provide a digital model of the vineyards to highlight possible phylloxera infestation and provide information for crop management. Another drone application in the agricultural industry, is the displacement of animals. This is important to protect the plants from being eaten by animals before the harvest takes place [8], [9]. Compared to other devices, such as satellites and aircrafts, one of the biggest advantages of using UAVs is the low cost of operation. Besides the high costs of satellite images or a certified pilot for aircrafts, UAVs equipped with sensors can provide a remote sensing platform and operational flexibility [10].

Polo et al. [11] propose an agricultural WSN by using sensor nodes on the ground. A drone collects the data and sends them to a base station using wireless communication. To show the functionality of the WSN, several flights are carried out and the authors provide different measures such as the time required to retrieve the data, altitude and velocity, and number of measurements. However, the authors do not emphasize the need for an end-to-end secured communication, which is the main contribution of our paper. We propose to use Eclipse Arrowhead secure onboarding procedure for establishing a chain of trust in such sporadically connected CPS and to add a hardware-based security layer via secure elements.

The approaches presented above show the importance of using UAVs for monitoring vineyards and how to collect the data from sensors in remote areas. Since the sensor nodes in the field are located in unprotected and remote areas, they require security measures. This does not only mean protection against physical manipulation, but also the need for a trustworthy wireless communication. Various approaches have been proposed addressing security in UAV communication such as [12], where the authors are focused on flight safety, and consider security mainly in terms of people. There are other works considering security of WSN such as [13], [14], [15]. They focus on evaluating attacks, countermeasures, data aggregation, and intrusion detection, but none of them uses security standards or best practice guidelines to extract security controls and mitigate threats. In this work, we investigate ISA/IEC 62443 series for deriving use case related security requirements and identify a number of security controls that should be integrated to address these requirements.

III. UAV Communication Use Case

This section provides a general description of the use case architecture, a representative set of diseases/conditions, the parameters that should be monitored, the sensors that will be used to monitor them, and sensor positioning.

A. Use Case Architecture

As shown in Figure 1, the drone will act as a gateway by collecting land-bound sensor data and multispectral images of the grapevines and sending this data to a base station for further analysis. A modified DJI M600P is used to capture the multispectral and daylight images and to collect the measurement results of the land-bound sensors. In accordance with the legal regulations in Austria, the UAV has a second flight controller. DJI A3Pro flight controller with autonomous flight operation mode is used, which offers special hardware interfaces and flight data can be made accessible with onboard and mobile software development kits (SDKs). The gateway integrated in the drone consists of a single board computer e.g. Raspberry Pi, referred to as host controller later in the paper.

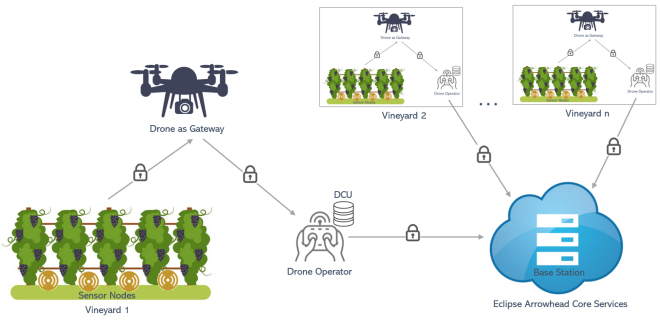

Fig. 1. UAV Communication Use Case

The sensor node consists of a single board computer, which can be a Raspberry Pi, an Orange Pi or an Arduino, referred to as host controller later in the paper. The sensor node is connected to several sensors, e.g. Air Temperature, Air Humidity, Air Pressure, Rainfall, Wind Speed, Wind Direction, Sunlight, Soil Temperature, Soil Moisture, Leaf Wetness, etc., which are used to collect environmental data.

The sensor node searches continuously for the compute unit integrated in the drone. When the drone is in range, a protected communication channel between the sensor node and the drone gateway is established. Since in some cases the vineyards are located in rough environments with poorly connected infrastructure, the sensor node sends first the data to a Data Collection Unit (DCU) that is with the drone operator. Thus, after the connection with the drone is established the sensor node will try to connect with the DCU, which consists of a single board computer, e.g. Raspberry Pi, that is connected to a touch screen. It is required for user interaction. When the connection with the DCU is established, the data transfer process begins. For the communication link, Wireless Local Area Network (WLAN) IEEE 802.11 is used. After the data is transmitted, the connection will be terminated and a

notification will be displayed in the DCU. On the sensor node, the transmitted data will be deleted to save space. Since the land-bound sensors are placed in remote locations, the data has to be transported to the base station via a vehicle. Thus, the DCU is connected to a base station and the data is uploaded for further processing.

To establish a chain of trust in such a sporadically connected system, Eclipse Arrowhead [1] framework is used. The objective of the Eclipse Arrowhead framework architecture is to facilitate the creation of local automation clouds, which enable local real time performance, security, interoperability, simple and cheap engineering, and scalability through multi cloud interaction. The architecture is built based on the service-oriented architecture (SoA) fundamentals: (i) loose coupling, which supports autonomy and distributed services, (ii) late binding, which makes possible to use the information any time by connecting to the correct resources and (iii) lookup, which can be used to discover already registered services.

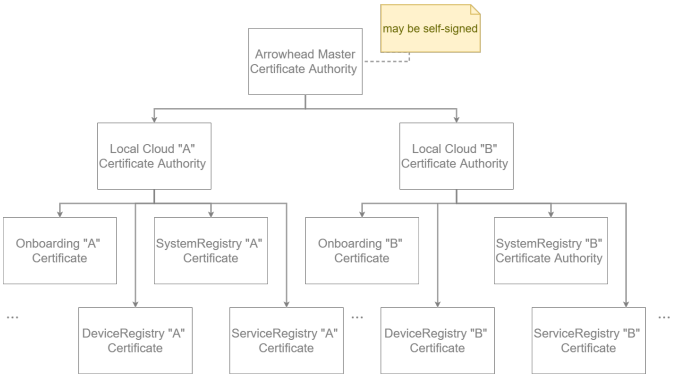

Fig. 2. Certificate Hierarchy in Arrowhead

The drone, sensors and base station should be securely onboarded in the Arrowhead local cloud. The onboarding procedure [3] enables a secured and trusted communication between the application systems and the core systems of Eclipse Arrowhead framework by using a chain of X.509 certificates [16] that are generated at run time. When a device (e.g. drone, sensor or base station) wants to interact with the Arrowhead local cloud, it should authenticate itself with a manufacturer issued certificate, which can be stored in a secure element e.g. Hardware Security Module (HSM). Each system hosted in this device should be provided with an Arrowhead issued runtime certificate. Thus, as shown in Figure 2, every local cloud should have a central Certificate Authority (CA) system that issues and signs the system runtime certificates. The CA system is the root of trust within its local cloud and it may be signed by a central Arrowhead consortium, establishing a chain of trust and allowing different Arrowhead local clouds to interconnect.

Only by trusting and relying the data, the system can adapt itself to a changing environment. To support this task, the generic autonomic management system (GAMS) [17] of Arrowhead can be integrated. GAMS is utilized to implement autonomic elements, without having to (re)implement the generic control mechanisms. Autonomic elements can be used for various adaptations e.g. to adapt the sensor reading interval, to check if the certificates in the drone are still valid, etc.

Thus, the integration of the Eclipse Arrowhead framework has a twofold benefit for the use case: (i) establishing a chain of trust by securely onboarding the drone, sensors and base station in the Arrowhead local cloud, and (ii) providing self-adaptation support for the use case using GAMS.

B. Diseases/Conditions and Sensor Mapping

Many biotic and abiotic factors can influence the health of grapevines. Biotic factors include funguses (e.g. botrytis, oidium, peronospora, phomopsis, guignardia, pseudopezicula tracheiphila), viruses (e.g. fanleaf disease, leafroll, rugose wood-complex), bacteria (e.g. agrobakterium vitis, Xylella fastidiosa), phytoplasma (e.g. bois noir, flavescence dorèe), and pests (e.g. mites, cicadas, phylloxera). Abiotic factors include weather, environment, nutrition and land management conditions. The data shown in Table I are needed for monitoring and forecast models:

Name	**Sensor**
Air Temperature	Temperature Sensor
Air Humidity	Relative Humidity Sensor
Air Pressure	Air Pressure Sensor
Rainfall	Rainfall Sensor
Wind Speed	Wind Speed Sensor
Wind Direction	Wind Direction Sensor
Sunlight	Light Sensor
Soil Temperature	Temperature Sensor
Soil Moisture	Dielectric Soil Moisture Sensors
Leaf Wetness	Leaf Wetness Sensor

TABLE I
DATA SETS FOR MONITORING AND FORECAST MODELS

For test purposes, we have identified a set of representative diseases and certain conditions (e.g. under watering or over watering that can make the leaves dry) as shown in Figure 3. For each disease and condition we have identified the parameters that should be monitored and the sensors that will be used to monitor those parameters.

Normalized Difference Vegetation Index (NDVI) is a graphical indicator that can be used to analyze remote sensing measurements, assessing whether or not the target being observed contains live green vegetation. NDVI values range from -1 to +1. For example, when NDVI value is close to -1, it corresponds to water, whilst when NDVI value is close to +1, it indicates temperate and tropical rain forests. But when NDVI is close to zero, it generally corresponds to barren areas of rock, sand, or snow, e.g. it could be an urbanized area. NDVI is the most widely used spectral vegetation index by ecologists and agriculturalists today. However, regions with sparse vegetation or soils that generate high reflectance values (e.g. dry sandy soils) can severely influence the reliability of the NDVI as an accurate estimator of green biomass, saturate remote sensors or produce biased estimates of green biomass and

[1]https://www.arrowhead.eu/eclipse-arrowhead/

vegetative cover [18]. The Optimized Soil Adjusted Vegetation Index (OSAVI) is an alternative of NDVI that accommodates greater variability due to high soil background values.

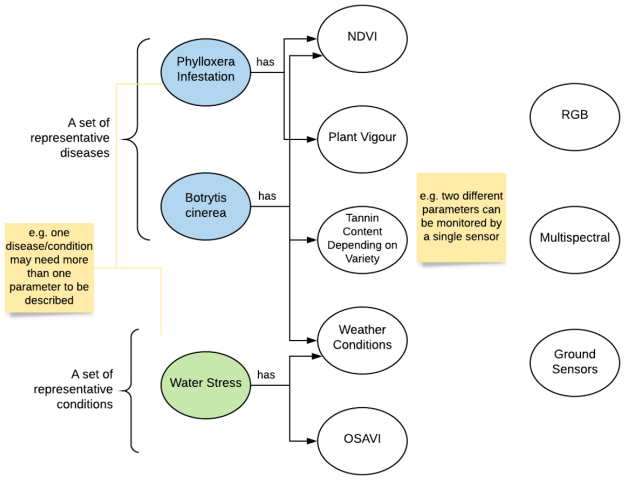

Fig. 3. Diseases/Conditions and Sensor Mapping

The reliability of such models depends on measurement location, data update intervals, interpretation of the already collected data and forecast time frame.

C. Sensor Positioning

For field tests and test flights, two different vineyards are monitored. The vineyards have different terrains with different grape varieties. By fusing the measurements of land-bound sensors, visual and multispectral images from a drone, the winemaker can monitor the condition of the soil as well as single vines. Thus, it is of utmost importance to identify the best positions for sensors in order to get accurate measurements, which can help detect diseases and conditions at early stages. We have used the LAYERS [2] tool to measure the water status for both vineyards. LAYERS is a platform that combines agronomical knowledge, earth observation remote sensing (drones, satellites, etc.) and artificial intelligence to obtain a proactive field monitoring system. It's constituted by a webtool, containing a map viewer and a field analytics dashboard, along with iOS and Android field sampling application.

The water status is used as an indicator to characterize the spatial variability in the vineyard and to identify homogeneous sub-areas. To monitor the microclimate inside the first vineyard, sensor nodes will be deployed along every 6th vine row and every 66 meters as shown in Figure 4 (a). To monitor the microclimate inside the second vineyard, sensor nodes will be deployed along every 6th vine row and every 50 meters as shown in Figure 4 (b).

[2]https://hemav.com/

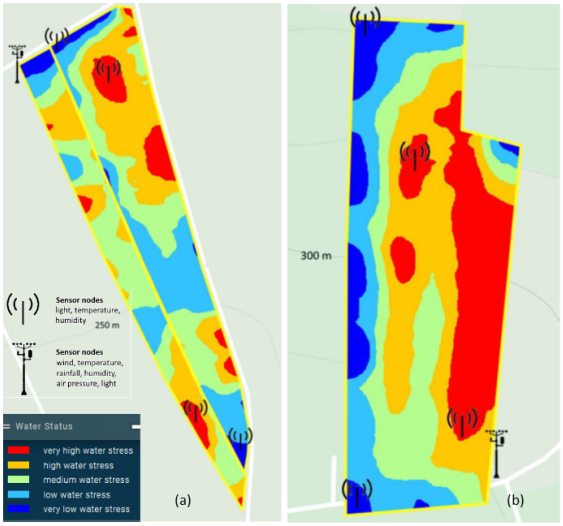

Fig. 4. Sensor Positioning in Vineyard (a) and Vineyard (b)

To acquire detailed information about the microclimate (the climate within a few rows of a vineyard), sensor nodes should be positioned at different heights: (i) grapevine area (100 cm), (ii) leaf-covered area (130 cm), (iii) top of the leaves (200-220 cm), and (iv) soil (5/20/50 cm under ground). Additionally, one senor node should be placed at the borders of each vineyard to monitor the macroclimate (the overall climate of the vineyard).

IV. Security Analysis

The most important asset of the application for the end user, e.g. the winemaker, is the sensor reading, its integrity and availability. We have performed a security analysis of the UAV communication use case for identifying potential threats. If the identified threats violate the above security objectives, it is of utmost importance to investigate standards and best practice guidelines for extracting a number of security controls that should be in place for mitigating them. Since the identified micro use cases provide similar results, in this section we present one representative micro use case.

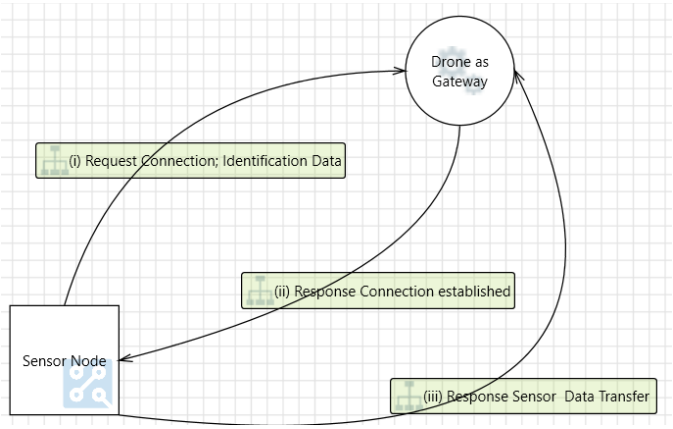

Fig. 5. Data Flow Diagram (DFD) of the Micro Use Case

A. Threat Modeling

Figure 5 shows the data flow diagram of the micro use case "Establishing Connection" and "Data Transfer" between the sensor node and the drone as a gateway: (i) the sensor node tries to establish a connection with the drone, (ii) the drone establishes a connection only if all identification data sent in step (i) is correct, and (iii) the sensor data is transmitted.

First, we identify potential threats of the selected micro use case and use STRIDE [19] as threat modeling technique. Threats are circumstances or events that potentially affect the operation of a system via unauthorized access, destruction, disclosure, modification of data, and/or denial of service [20]. Table II shows the threat analysis results using STRIDE.

STRIDE Threat Category	Nr. of Threats
S - Spoofing	8
T - Tampering	13
R - Repudiation	2
I - Information disclosure	2
D - Denial of Service	0
E - Elevation of Privilege	9

TABLE II
THREAT ANALYSIS RESULTS USING MICROSOFT STRIDE

The highest number of threats was found in the category "Tampering", which affects the integrity of data. Two example attack vectors of this category are:

- Man-in-the-middle attack, e.g. an adversary may attempt to intercept encrypted traffic sent from the sensor node.
- An adversary may tamper sensor node and extract cryptographic key material from it. For example, an attacker may leverage extracted key material to intercept and suppress data from the device on the communication path and replace it with false data that is authenticated with the stolen key material.

The STRIDE tool did not classify any of the found threats into the "Denial of Service" category. One reason for this could be that there is no internet connection in the micro use case, neither the sensor node, nor the gateway and the DCU are connected to the Internet. However, in the context of WSN, jamming is a type of DoS attack that interferes with the radio frequencies used by sensor nodes, causing disruptions of WSN proper function. Thus, the integration of security controls against jamming in WSN is of utmost importance.

The security analysis is only focused on malicious threats, however a more general risk analysis of the use case would probably reveal that non-malicious threats are also dominant, e.g. animals and weather conditions are more likely to destroy the land-bound sensors than intentional human tampering.

As a next step we will work on the threat modeling database and tooling regarding the development of a drone-specific threat modeling environment, based on ThreatGet [21], a threat modeling tool developed for the automotive domain, but also CPS in general. Here we will focus on developing a threat overview and survey for drone systems and a toolbox, containing the most common elements used.

B. Standards and Best Practice Guidelines

The components of the UAV communication use case present different security risks depending on the threats they are exposed, the likelihood of the threat arising and the consequences if the component is compromised. In order to mitigate these threats, it is of utmost importance to identify a number of security controls that should be in place.

Several international security standards and best practice guidelines can be used to extract security controls such as ISO 27000 series, NIST SP 800 series, ISA/IEC 62443 series, etc. We have selected the ISA/IEC 62443 series because they distinguish between system and device security controls.

We have investigated IEC 62443-4-2 [22] that provides technical security requirements for industrial automation and control system components (component requirements (CR), embedded device requirements (EDR), host device requirements (HDR) and network device requirements (NDR)), and IEC 62443-3-3 [23] that provides system security requirements and security levels. IEC 62443-4-2 provides four requirements (CR 1.5, CR 1.9, CR 1.13, and CR 1.14) highlighting that enhanced protection can be achieved by using hardware mechanisms, such as HSM. Also, it provides six requirements (CR 1.9, CR 2.1, CR 3.4, CR 4.3, EDR 3.12 and HDR 3.12) addressing the trust between two components based on public/private key cryptography.

The following section represents security controls, which will be integrated in the UAV communication use case for addressing the above mentioned requirements.

C. Security Controls

To achieve certain security related communication parameters such as confidentiality, integrity and availability, it is recommended to establish a protected communication channel. As discussed in Section III-A, we propose to use Eclipse Arrowhead framework to establish a chain of trust by securely onboarding the drone, sensors and base station. However, as recommended by IEC 62443-4-2, additional security controls should be in place to mitigate the identified threats. The communication protocol shall be extended by the Transport Layer Security (TLS) protocol [24], which is a protocol used to establish an authenticated communication channel. TLS can introduce some overhead, but in regards of security it is always a trade-off between overhead and security.

As identified during the threat analysis, the most critical threat category is tampering. Attack scenarios, based on tampering are hardened by supporting the host controller with an HSM. With that measure, confidential key material is kept protected and invulnerable against certain attacks. This extension shall be implemented for both parties of the communication link, the drone's gateway and the single board computer of the sensor. Further, an HSM shall also be supporting the base station in regards of outsourcing security critical function, while communicating with the drone's gateway. Specifically, the TLS layer is partitioned between the respective host controller and the HSM, in order to outsource security critical functionality. A typical partitioning is depicted in Figure 6.

In [24], a typical TLS handshake sequence supported by an HSM is depicted. The most important step, is calculating the signature for verifying that the client (UAV in this case) possesses the private key, which corresponds to the certificate used for client authentication. This step is performed by the HSM in order to ensure, that the private key is never leaving the HSM. This measure, allows mitigating threats against the respective host controller.

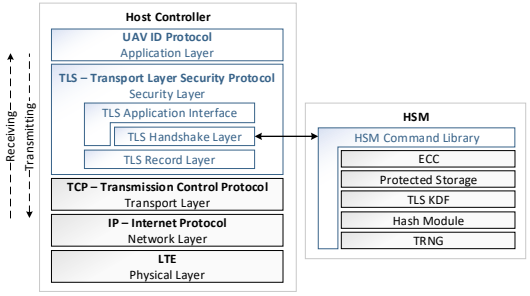

Fig. 6. Extended Communication Protocol Stack [24]

Even if an adversary is tampering with the hardware in order to perform side channel attacks, the keys remain protected within the HSM, and therefore key cloning can be prevented.

V. Conclusion and Future Work

In this paper, we have proposed a sporadically connected CPS that creates a drone based application for vineyards. We have used LAYERS tool to identify the precise position of land-bound sensors in the field, and we have identified a set of representative diseases/conditions (e.g. phylloxera infestation, botrytis, water stress) to be monitored by these sensors. The Eclipse Arrowhead framework is proposed for establishing a trusted and secured communication of the drone with the land-bound sensors and base station, and for providing self-adaptation support for the use case. We have performed a security analysis to identify the security controls that should be integrated in the use case for mitigating potential threats. E.g. software-based security mechanisms are not sufficient to protect against existing security threats because data may be collected by potentially untrusted devices. Thus, we propose to add an additional hardware-based security layer via HSM, which provides tamper resistant storage for holding and protecting important key material against several attack scenarios, even including physical access to the device.

As future work, we will evaluate additional requirements for security and self-adaption. We will use GAMS [17] to develop autonomic elements for smart and secure drone based applications in a vineyard management. This will be based on an extension of existing work with domain specific aspects.

Acknowledgment

This work has received funding from ECSEL Joint Undertaking (JU) under grant agreement No 826610 Comp4Drones project. The JU receives support from EU's Horizon 2020 research and innovation programme and Spain, Austria, Belgium, Czech Republic, France, Italy, Latvia, Netherlands.

References

[1] P. Tripicchio, M. Satler, G. Dabisias, E. Ruffaldi, and C. A. Avizzano, "Towards smart farming and sustainable agriculture with drones," in *International Conference on Intelligent Environments*. IEEE, 2015.
[2] J. Delsing, *Iot automation: Arrowhead framework*. CRC Press, 2017.
[3] A. Bicaku, S. Maksuti, C. Hegedűs, M. Tauber, J. Delsing, and J. Eliasson, "Interacting with the arrowhead local cloud: On-boarding procedure," in *2018 IEEE industrial cyber-physical systems (ICPS)*. IEEE, 2018, pp. 743–748.
[4] F. Vanegas, D. Bratanov, K. Powell, J. Weiss, and F. Gonzalez, "A novel methodology for improving plant pest surveillance in vineyards and crops using uav-based hyperspectral and spatial data," *Sensors*, vol. 18, no. 1, p. 260, 2018.
[5] L. Pádua, J. Vanko, J. Hruška, T. Adão, J. J. Sousa, E. Peres, and R. Morais, "Uas, sensors, and data processing in agroforestry: A review towards practical applications," *International journal of remote sensing*, vol. 38, no. 8-10, pp. 2349–2391, 2017.
[6] R. Calderón, J. A. Navas-Cortés, and P. J. Zarco-Tejada, "Early detection and quantification of verticillium wilt in olive using hyperspectral and thermal imagery over large areas," *Remote Sensing*, 2015.
[7] F. Vanegas, D. Bratanov, J. Weiss, K. Powell, and F. Gonzalez, "Multi and hyperspectral uav remote sensing: grapevine phylloxera detection in vineyards," in *2018 IEEE Aerospace Conference*. IEEE, 2018.
[8] S. Bhusal, K. Khanal, S. Goel, M. Karkee, and M. E. Taylor, "Bird deterrence in a vineyard using an unmanned aerial system (uas)," *Transactions of the ASABE*, vol. 62, no. 2, pp. 561–569, 2019.
[9] Z. Wang, A. S. Griffin, A. Lucas, and K. Wong, "Psychological warfare in vineyard: Using drones and bird psychology to control bird damage to wine grapes," *Crop Protection*, vol. 120, pp. 163–170, 2019.
[10] T. Adão, J. Hruška, L. Pádua, J. Bessa, E. Peres, R. Morais, and J. J. Sousa, "Hyperspectral imaging: A review on uav-based sensors, data processing and applications for agriculture and forestry," *Remote Sensing*, vol. 9, no. 11, p. 1110, 2017.
[11] J. Polo, G. Hornero, C. Duijneveld, A. García, and O. Casas, "Design of a low-cost wireless sensor network with uav mobile node for agricultural applications," *Computers and electronics in agriculture*, 2015.
[12] D. Popescu, F. Stoican, G. Stamatescu, O. Chenaru, and L. Ichim, "A survey of collaborative uav–wsn systems for efficient monitoring," *Sensors*, vol. 19, no. 21, p. 4690, 2019.
[13] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," 2006.
[14] A.-S. K. Pathan, H.-W. Lee, and C. S. Hong, "Security in wireless sensor networks: issues and challenges," in *2006 8th International Conference Advanced Communication Technology*, vol. 2. IEEE, 2006, pp. 6–pp.
[15] T. Kavitha and D. Sridharan, "Security vulnerabilities in wireless sensor networks: A survey," *Journal of information Assurance and Security*, vol. 5, no. 1, pp. 31–44, 2010.
[16] R. Housley, W. Polk, W. Ford, and D. Solo, "Internet x. 509 public key infrastructure certificate and certificate revocation list (crl) profile."
[17] S. Maksuti, M. Tauber, and J. Delsing, "Generic autonomic management as a service in a soa-based framework for industry 4.0," in *IECON 2019-45th Annual Conference of the IEEE Industrial Electronics Society*, vol. 1. IEEE, 2019, pp. 5480–5485.
[18] R. R. Fern, E. A. Foxley, A. Bruno, and M. L. Morrison, "Suitability of ndvi and osavi as estimators of green biomass and coverage in a semi-arid rangeland," *Ecological Indicators*, vol. 94, pp. 16–21, 2018.
[19] M. Howard and S. Lipner, "The security development lifecycle, vol. 8," *Redmond: Microsoft Press. Google Scholar Google Scholar Digital Library Digital Library*, 2006.
[20] I. E. Commission *et al.*, "Iec 62443-1-1, industrial communication network–network and system security. part 1-1: Terminology, concepts and models," 2016.
[21] C. Schmittner, S. Chlup, A. Fellner, G. Macher, and E. Brenner, "Threat-get: Threat modeling based approach for automated and connected vehicle systems," in *AmE 2020-Automotive meets Electronics; 11th GMM-Symposium*. VDE, 2020, pp. 1–3.
[22] IEC, "62443-4-2:technical security requirements for iacs components," 2019.
[23] IEC, "62443-3-3:system security requirements & security levels," 2013.
[24] D. Pirker, T. Fischer, C. Lesjak, and C. Steger, "Global and secured uav authentication system based on hardware-security," in *2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*. IEEE, 2020, pp. 84–89.