Integrated Technology and Policy Enabling Large-Scale Deployment of UAVs: Trustworthiness and Threat Mitigation

Bertrand Cambou
EECS Department
bertrand.cambou@nau.edu

Paul G. Flikkema
Informatics & Computing Program
paul.flikkema@nau.edu

Constantin Ciocanel
Mechanical Engineering Department
constantin.ciocanel@nau.edu

Northern Arizona University

Abstract–The risks associated with the deployment of Unmanned Aerial Vehicles (UAVs) are such that only a fraction of their commercial possibilities can be currently exploited. Among other applications, UAVs have the potential to vastly increase the operational capability of a broad range of Internet of Things (IoT) services, and applications, and could become a critical component of IoT-based systems. In this position paper, we envision how future technologies, including nanotechnologies and emerging cryptographic primitives, UAV sensing, and lightweight structural materials with power storage capability can mitigate threats to safety, security, and privacy. Specifically, this paper proposes the integration of a connected crypto-processor architecture and distributed UAV sensing, together with a new set of policies to enhance their trustworthiness, detect and identify potential UAV-based threats, and spur development of UAV's with increased energy storage capacity and flight range. We argue that together, these technologies can unleash a larger range of viable commercial uses for UAV-based technologies.

1. Positioning of the opportunity, and threat mitigation.

Very few new technologies have the potential to profoundly change our way of living as much as UAVs. For example, in support of booming e-commerce applications, foundational UAV technologies are already mature enough to deliver part of the postal traffic [1-2], in particular within congested cities and suburban areas. UAVs can also save lives by assisting doctors and healthcare providers with the delivery of medications in emergency situations. Multi-site industrial complexes can reduce inventory, cost, and cycle time of manufacturing by expediting delivery of spare parts for maintenance. Public safety agencies can rapidly respond and intervene during natural disasters and terrorist attacks. More broadly, UAV technologies can introduce aerial mobility that supports transport of both information and mass to a wide range of existing services and applications, including IoT, smart cities, cyber-physical systems (CPS), and distributed automation.

Threats to privacy, protection, security and safety. Conversely, very few emerging technologies also have the potential to threaten national security, public safety, damage infrastructure, and compromise privacy when under the control of malicious entities, terrorists, drug dealers, and others. Flying objects can invade privacy when equipped with cameras, directional microphones, and thermal imagers. From a logistical standpoint, when the batteries powering UAVs run out of power, the chances of collisions between UAVs and other aircrafts increase significantly, creating unacceptable safety hazards. These risks are so serious they hamper entrepreneurs from pursuing new business opportunities, thereby limiting the development of new UAV applications.

Remedies. In this environment, legislators and the Federal Aviation Administration (FAA) [3-5] are working to design and implement policies that will allow businesses to further develop and deploy UAV technology. The recently implemented FAA policy, to register all UAVs, is in our opinion an excellent step in the right direction. Other policies, such as limiting the flying range of an UAV to the airspace visible for the pilot, are also sound, and will facilitate the development of the UAV industry. However, only a fraction of what the UAV technology can offer to our society is reachable with the current restrictions, and leaves the door open for malicious use.

New strategy. In this paper we outline a new, comprehensive strategy that would rapidly expand the deployment of UAVs through a creative suite of policies, combined with technologies aimed at enhancing UAV's safety and security. Several of these new technologies are described below, with the understanding that many of them are also implementable in other IoT applications.

2. Suggested end to end trustworthy architecture for UAVs.

In this section we are presenting the key steps to implement our recommended architecture, with the objective to create a safe, secure, and trustworthy UAV-aware environment, to enable its large scale commercial deployment. It is important to note, that in this section we are only recommending the **use of mature technologies**, already proven in different segments of the secure cyber-space, and financial services.

Insert a secure element, also called smartcard, in every UAV. Microcontrollers with crypto-processors are widely used to store cryptographic authentication keys in applications such as mobile phones, banking cards, ID cards, and smart passports. About 8 billion of these portable "vaults", called secure elements or smart cards, are produced every year. These elements store ID numbers, pin codes, public and private keys, AES keys, passwords, biometric prints, and other secret information. The embedded crypto-processor can encrypt and decrypt data. Typically, the cost of a secure element is below $0.25. The global smart card alliance has leveraged an industry standard, ISO/ISEC 7816, and driven application programming interfaces (API) with two main operating systems: Javacard and Multos [6-7].

Personalize each UAV with secret keys. This operation can be done in synergy with the FAA policies requiring registration of all UAVs. The secure element inserted in each UAV should be loaded with its unique set of secret cryptographic keys that can provide trusted authentication and non-repudiation [8]. As with banking cards, the downloading of the secret keys (or personalization) is managed in a highly restricted secure facility. Only accredited officials should have access to the secret information, on a need to know basis. The equipment and standards to personalize secure elements have been driven by industry consortiums such as EMVco.

Connect UAVs to the internet. Modems allowing communication through existing wireless networks are cheap and commercially available. Many IoT systems are already connected through these networks, including mobile point of sales terminals, personal medical devices, and cars. Embedding wireless modems in the UAV electronics can be performed following a range of wireless standards, including cellular telephony. The technologies to secure UAVs that we describe here are not dependent on a particular communication standard.

Host authentication on a secure server. A distributed, secure server, accredited by an institution such as FAA, and hosted in the cloud for resilience to failures or attacks, can host a secret database containing all UAV users and their authentication factors. Prior to takeoff, a UAV should be in communication with a local wireless base station connected to the internet. The secure server can then recognize it as a registered unit (Fig. 1). The current public key infrastructure (PKI) can be implemented to offer 2-way security: authentication of the UAV, and authentication of the network (protection against malicious base stations). The software stacks driving such a server, called card (or client) management systems (CMS) are commercially available, standardized, and in use by telecom and internet service providers.

Enable flight planning and registration via the web. A service can be offered on line for UAV users to register flight plans for their devices. As done in aviation, prior to flight, the user can enter departing and arriving points, and schedules. As the UAV enters the wireless network, the secure server can: i) authenticate the UAV, ii) validate and approve its flight plan; and iii) verify that the UAV is following its approved route (Fig. 2). The design of such a flight planning and registration service can be implemented with commercially available software tools at low cost. Technologies that are synergetic with this service include automatic wireless user positioning, local maps, and GPS to provide accurate information on the behavior of the UAV.

Integration. The combination of wireless modems and secure elements integrated in each UAV enables two critical safety factors: i) trusted authentication of the UAVs, and ii) the ability to track where they are flying. The wireless infrastructure and secure server enable real time tracking of flying routes of certified UAVs. This infrastructure can be administered by FAA, or other agency, in such a way that continuous improvement in technology can be adopted to further enhance safety. Licenses to fly should be periodically re-issued with replacement of the secure element to incorporate additional cryptographic security features. Financial institutions are already issuing new cards every two to four years to incorporate stronger encryption and download fresh cryptographic keys. As presented in section 3, we foresee that the recommended UAV architecture will open the opportunity to bring to market disruptive technologies that will further strengthen safety, and security, mitigating threats.

Vulnerability analysis. Such a new architecture might create new opportunities for malicious users. The potential vulnerabilities and corresponding mitigation strategies have to be comprehended, here a few examples:

- ***Replacing the secure element and the modem by a commercial phone to fool the system.*** Such vulnerability exist with existing configuration. Remedies include the use of additional recognition technologies, see section 3.4 below, and if necessary the dedication of a unique communication protocol to UAVs that use existing wireless infrastructure.
- ***Stealing an UAV or a secure element to install it in a malicious UAV***. Without the correct user password the malicious host will not be able to register the UAV with the stolen secure element.
- ***Stealing a secure element and the user password.*** Additional protections are required such as use of biometric prints to double check the identity of the user, as well as the detection of abnormal behavior of the user, and the UAV.
- ***Side channel attacks, and extraction of secret keys.*** In sections 3.1 & 3.2 below we present new technologies that can further reduce the risk.
- ***Virus hidden on the embedded software of the UAV***. In section 3.3 below a method to secure the software environment is suggested.
- ***Malicious base station taking over the UAV.*** This type of attack, in addition to other "man in the middle" attacks, should be protected by the encryption technology between the UAV and the wireless infrastructure. The UAV should authenticate the malicious network, and react to the threat.

The suggested new architecture to operate UAVs should significantly enhance trustworthiness, safety, and security, and this compared with the current art. This vulnerability analysis is also highlighting the importance to develop new concepts specifically aimed at further strengthening the safety, and security of UAVs.

3. Threat mitigations through advanced technologies.

In section 3 we are looking at several new enabling technologies, that are directly synergetic with the architecture presented in section 2, each has the potential to significantly strengthen UAV's trustworthiness and viability: use of nanotechnologies, make secure elements even more secure; hardware authentication technology called PUFs; secure software environments; aerial vehicle sensing tracks UAV; trajectory and speed; and enhancement in the battery technology to makes UAVs much safer.

3.1 ***Use of nano-materials for secure elements.*** Current secure elements mainly use embedded flash memory to store secret information, the operating system, and client data. While flash is doing the job well and design engineers know how to handle flash to produce solid secure elements, embedded flash is now an aging technology. Crypto-analysts and sophisticated hackers are making progress toward breaking flash-based secure elements. Emerging memory technologies based on Nano-materials are gaining acceptance, in particular Resistive RAM technology. ReRAM leverages the physical properties of metal-oxide to consume a fraction of the power of flash and operate orders of magnitude faster [9-10]. The relevance for UAV security is increased compute power for cryptography, making UAV systems harder for hackers to break. Flash, the mature incumbent, is a way to start securing UAVs as presented Section 2, with gradual transition to solutions based on Nano-material based components as they become available.

3.2 ***Hardware authentication and PUFs.*** Physical Unclonable Functions (PUFs) [11-13] are emerging cryptographic primitives that act as "digital fingerprints" (Fig. 3). Electronic components are subject to micro-variations during the manufacturing process that makes each of them unique; PUFs exploit these differences to create trustworthy authentications. When embedded in secure elements, PUFs have the potential to make each UAV unique, and differentiable. During personalization it is possible to extract a reference pattern of the PUF called a "challenge". Thereafter, during the life of the UAVs, the PUF can generate fresh authentication patterns called "responses". A matching challenge-response-pair is a trustworthy method of authentication, which is extremely protected from third party attack, and easy to use, (Fig. 4). PUFs are excellent candidate technologies to further secure UAVs (as well as many other IoTs).

3.3 ***Protected software environment.*** Securing software embedded in UAVs is still at an exploratory phase, however, the impact on their trustworthiness could be extremely significant. Here the objective is to restrict all software running in the UAV to only those which can be authenticated by the secure element with cryptographic primitives such as PUFs (Fig 5). Any third party software, malware, Trojans and other threats

should be prevented from running [14]; see Fig. 6. This environment has to be transparent to software developers; thus translators are needed to convert non-secure software to protected and certified software automatically. This technology could have a wider impact in several IoT applications such as securing cell phones and automobiles and smart transportation.

3.4 ***Aerial vehicle sensing of UAVs.*** This idea, also at the exploratory phase (see [15-18] for related work), stems from a vision of using networks of wideband radio- and audio-frequency sensors with significant computational power to collaboratively sense UAVs; see Fig. 7. Given the need for operation at any time and in any weather, the approach uses passive and active sensing of radio-frequency (RF) energy and passive sensing of acoustic energy. Such acoustic-RF sensing would enable detection, classification, and localization of small aerial vehicles. Aerial vehicle sensing (AVS) networks could initially be deployed in environments where the risk is highest, e.g., public spaces and essential infrastructure, but could eventually become more widespread as the cost of microelectronics decreases.

3.5 ***Carbon-based/lightweight structural materials with power storage capability (a.k.a. structural supercapacitors).*** The battery technology of UAVs is of prime importance for commercial applications where improved range, speed, and payload capacity are needed. However, one has to consider valid concerns based on potential hazards to the public due to the risk of fire and other unexpected failures of batteries. To minimize such risks, one can use emerging carbon fiber-based supercapacitors, integrated directly in the frame/ mechanical structure of the UAV [19-20]. This approach has the advantage of not only leading to a reduction in size, and weight, of the battery, but also to a reduction in charging time of the powering system (i.e. battery-supercapacitor), ultimately leading to shorter delays between flights. In addition, embodiment of the light, mechanically strong, thermally stable, and eco-friendly carbon fiber-based supercapacitors in the bulk of the UAV structure facilitates an increase in range of operation of the UAV, as the peaks in power demand during flight can be accommodated by the supercapacitor (characterized by higher power density), while the power needed for cruising can be supplied by the battery (higher energy density).

The implementation of these five concepts would directly support the architecture presented in Section 2, and be part of a comprehensive roadmap to develop, and gradually adopt enhancements as they become mature. The frame of suggested policies is to enable a larger-scale use of trustworthy UAVs while stimulating this type of development, and many others, for continuous improvement in trustworthiness.

4. Recommendations and implementation.

The step by step implementation of the new architecture, as presented section 2, is based on the adoption of mature technologies, and policies, synergetic with FAA regulations: registration of all users, and certified users can register flying schedules in a way similar to private and commercial aircraft. To enhance the trust in the new architecture, we are recommending that strict restrictions and regulations should be in place before initial implementation of the suggested architecture: i) no-fly zones around public places, airports, and areas critical to national security; ii) limit the number of UAV flying in the same area at a given time; iii) limit the speed; and, iv) regulation of the flying conditions in term of elevation, min and max, and deviation to approved flight schedule. The combination of these restrictions, with the deployment of the new policies and technologies, is expected to largely increase public confidence in UAVs, reduce potential threats in safety and security, and un-leash significant portions of the related commercial space that has been off limit so far. This should create new business opportunities for the general market, and for emerging enterprises eager to be part of the effort surrounding the new architecture.

Sizing the business opportunity. We are recommending studies to size the business opportunities that could benefit from an expansion of the use of UAVs. With UAVs, existing corporations can simply enhance their efficiency, and reduce operating costs, they can also offer extended services to their clients, thereby increase revenues. Examples include delivery of packages and light goods, medical supplies, and others, such as traffic control, security monitoring, emergency response, and photography. It can be anticipated that eventually tens of millions of UAVs could be allowed to operate with hundreds of monthly flights, each generating tens of dollars per flight. Such a study can further motivate technology and policy makers, and clarify the priorities (i.e. work on big ticket item first).

Need to involve industrial partners. The administration of the architecture presented in section 2 can also open multiple new business and job opportunities. We are recommending to involve upfront the partners who are potentially going to be part of the deployment of this new architecture on UAVs, for example:

- For component and system suppliers of wireless modems, navigation and altitude control, and new secure microcontrollers: Infineon, NXP-Freescale, STMicro, Atmel, Gemalto, Safran, Oberthur, G&D…
- For personalization and security suppliers: financial transactions & secure data processing companies, First data, Wells Fargo, Verisign, CyberTrust, Rambus…
- Potential users: Amazon, Postal services, Walmart, Home depot, Medical suppliers…
- Research institutions and entrepreneurs to develop new enabling technologies: use of nanotechnologies for the components, cryptographic and security based solutions, new secure software apps and CMS, AVS infrastructure suppliers, suppliers of carbon based UAVs with integrated supercapacitors.

An important aspect that is not part of this position paper is to analyze the business implications of the use of UAVs specifically to replace a portion of the road traffic, thereby reducing pollution.

5. Summary

The architecture described in this paper should pave the way for large scale use of UAVs, with significant commercial impact. The initial implementation can leverage mature technologies, UAVs can be wirelessly connected to the internet with commercial modems, secure elements can be integrated into their electronics, host and server based services can be quickly developed. The suggested policies are synergetic with current FAA regulation, for example: the request from certified users to register flying UAVs schedules in a way similar to private and commercial aircraft. The disruptive concepts presented in the paper can further enhance the trustworthiness in the new UAV architecture: use of nanotechnologies, new cryptographic primitives, secure software, AVS combined with wireless, and carbon based/lightweight structural materials with power storage capability. The entire proposal is also greatly applicable to many other IoT systems and services in general, such as transportation, and smart-cities.

ACKNOWLEDGEMENTS

The technical ideas presented in section 3 were originated, and/or discussed with the following colleagues:

- Section 3.1: **Dr. Marius Orlowski** from Virginia Tech and his research work on metal oxide Resistive RAM, and D**r. Michael Kozicki** from Arizona State University and his research work on CB-RAM
- Section 3.2: **Dr. Fatemeh Afhgah**, **Dr. James Palmer**, and **Dr. Derek Sonderegger** all from NAU and their research work related to the coding and decoding of PUFs, and statistical analysis.
- Section 3.3: **Dr. Omar Badreldin** from NAU for his exploratory research work on software.
- Section 3-5: **Dr. Cindy Browder** from NAU for her research work on structural super-capacitors.

REFERENCES

1- Switzerland begins postal delivery by drone; *AFP, The Guardian, July 7th, 2015.*
2- Finnish post office tests drone for parcel delivery; *Reuters, Sept 14th, 2015.*
3- Register your UAV – Federal Aviation Administration, Aug 2015: https://www.faa.gov/uas/
4- Overview of Small UAS Notice of Proposed Rulemaking, part 107, April 2014, FAA, : https://www.faa.gov/regulations_policies/rulemaking/media/021515_sUAS_Summary.pdf
5- Recommendations and report of the task force on US drone policy, June 2014: http://www.stimson.org/images/uploads/task_force_report_final_web_062414.pdf
6- ISO/ ICT 7816 Smartcard standard overview, 2004: http://www.smartcardsupply.com/Content/Cards/7816standard.htm
7- Global smart card alliance – standard and specifications, 2015: http://www.smartcardalliance.org/smart-cards-intro-standards/
8- H.X. Mel, Doris Baker; Cryptography Decrypted; *Addison-Wesley, 2000.*
9- Gargi Ghosh and Marius Orlowski; 2015; Write and Erase Threshold Voltage Interdependence in Resistive Switching Memory Cells; *IEEE trans. on Electron Devices, 62(9), pp. 2850-2857.*
10- Bertrand. Cambou; June2, 2015; ReRAM architectures for secure systems; *US Application No 62/169957.*
11- David. Naccache and Patrice. Frémanteau; Aug. 1992; Unforgeable identification device, identification device reader and method of identification; *Patent US5434917.*
12- B. Cambou; Physically Unclonable Function Generating Systems and Related Methods; *US Patent application No. 62204912; August 2015*
13- An Chen; 2015; Comprehensive Assessment of RRAM-based PUF for Hardware Security Applications; *978-1-4673-9894-7/15/IEDM IEEE.*

14- Zheng Gong, Marc X. Makkes; 2011; Hardware Trojan Side-Channels Based on PUF; *Inf. Security, Vol. 6633, Notes in Comp. Science pp 294-303.*
15- Hack, D.E., Patton, L.K., Himed, B., and Saville, M.A; Detection in Passive MIMO Radar Networks; *IEEE Transactions on Signal Processing 62(11):2999----3012, June 2014.*
16- Qian He, Lehmann, N.H., Blum, R.S., and Haimovich, A.M; MIMO Radar; Moving Target Detection in Homogeneous Clutter; *IEEE Transactions on Aerospace and Electronic Systems 46(3):1290----1301, 2010.*
17- 13 Patwari, N. and Wilson, J. 2010. RF Sensor Networks for Device-Free Localization: Measurements, Models, and Algorithms; *Proceedings of the IEEE 98(11): 1961----1973, 2010.*
18- 14 N. Patwari, L. Brewer, Q. Tate, O. Kaltiokallio, and M. Bocca; Breath finding: A Wireless Network that monitors and Locates Breathing in a Home; *IEEE J. of Selected Topics in Sig. Proc. 8(1):30----42, 2014.*
19- Luo, X. Chung, D.D.L; Carbon-fiber/polymer matrix composites as capacitors; *Composite Science and Technology,2001, 61, 885-555.*
20- Constantin Ciocanel and Cindy Browder; Structural Supercapacitor; *US Patent pending, NAU 2012-007.*

AUTHORS

Dr. Bertrand Cambou is a Professor of Practice at Northern Arizona University where his primary research interests are in cyber-security and how to apply nanotechnologies to strengthen hardware security. Dr. Cambou is directing the cybersecurity effort at NAU as part of the newly formed School of Informatics, Computing, and Cyber-Systems. Dr. Cambou has previously worked as a CEO in Silicon Valley in nanotechnologies where his organization won a contract with IARPA with applications related to quantum cryptography. He worked in the smartcard industry at Gemplus (now Gemalto), and in the POS/secure payment industry at Ingenico. He spent 15 years at Motorola Semiconductor (now NXP-Freescale), where he was CTO for five years and was named Distinguished Innovator and scientific advisor of the BOD. He is the author or co-author of 37 patents in microelectronics and cybersecurity with over 350 citations. Dr. Cambou holds a Doctorate degree from Paris-South University, France and an Engineering degree from Supelec, France.

Dr. Paul Flikkema is Director of the Informatics & Computing Program and Professor of Electrical Engineering at Northern Arizona University. Dr. Flikkema's primary research interests are in networked communication and computation systems, with applications to networked embedded systems, wireless sensor networks, and genomic information networks. He is also interested in education in communications, signal processing, and active learning in engineering education. He has held visiting positions at Helsinki University of Technology, Sony Computer Sciences Laboratories (Tokyo), and Yokohama National University. Dr. Flikkema holds a PhD and a MS in Electrical Engineering from the University of Maryland, College Park, and a BS in Computer Engineering from Iowa State University. Dr. Flikkema is leading the development of an exploratory project at NAU on aerial vehicle sensing for UAVs.

Dr. Constantin Ciocanel is Associate Professor in the Department of Mechanical Engineering at Northern Arizona University. His expertise is in modeling and characterization of smart materials and systems, and in development of carbon based composite materials with power storage capability. Magnetic shape memory alloys, magnetorheological fluids, shape memory alloys and piezoelectric materials, and their applications in sensing, power harvesting or actuation, are the focus of Dr. Ciocanel's research . He holds a DSc from ""Gh. Asachi" Technical University of Iasi, Romania, and a PhD from the University of Toledo, Ohio, both in Mechanical Engineering.

FIGURES

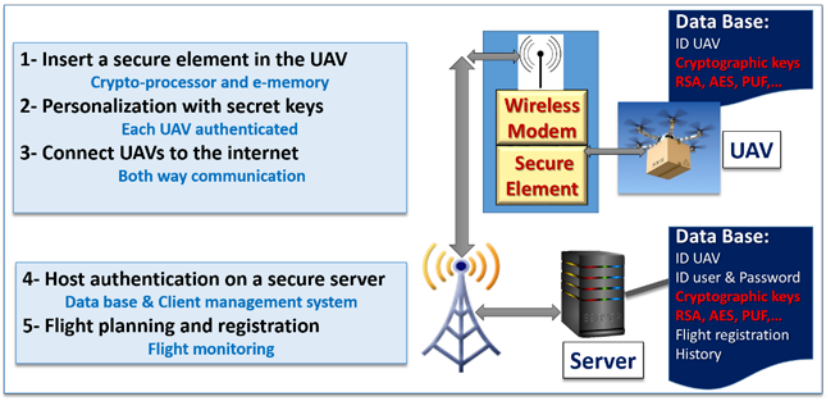

Figure 1: Architecture to create trustworthiness with UAVs

Figure 2: User Interface and monitoring

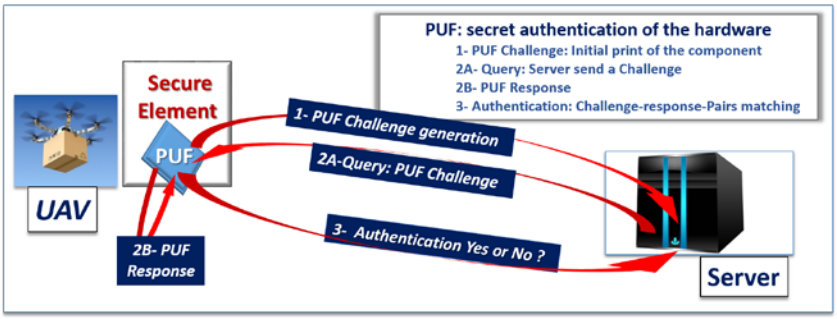

Figure 3: Physically Unclonable Functions (PUFs): "digital fingerprint"

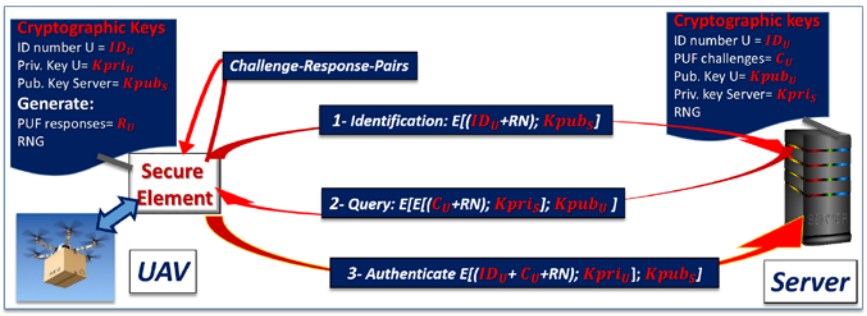

Figure 4: Cryptographic communication

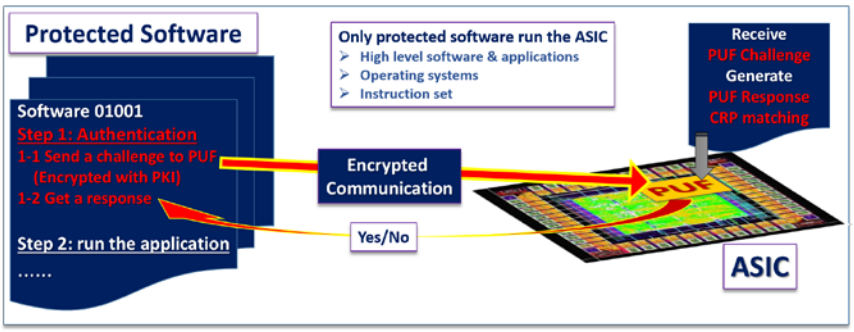

Figure 5: Use of PUF for software protection

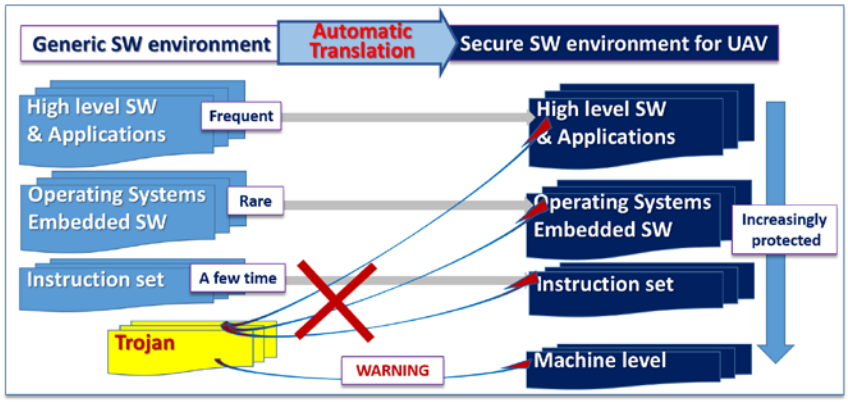

Figure 6: Translation and Trojan protection

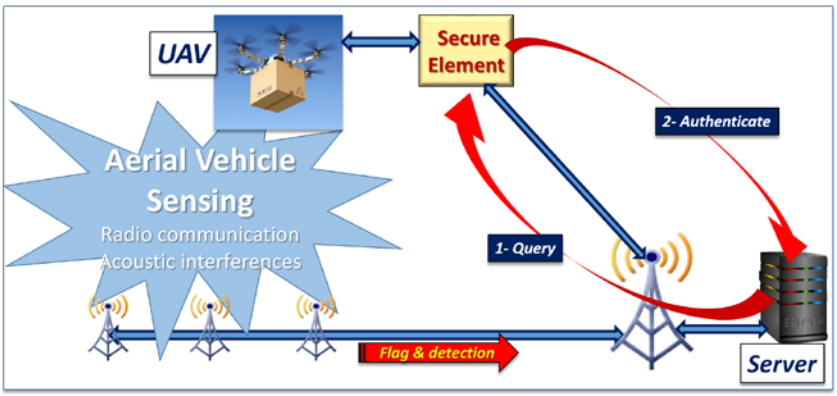

Figure 7: Use of Aerial Vehicle sensing