Securing the Internet of Things A Military Perspective

Konrad Wrona
NATO Communications and Information Agency
The Hague, Netherlands
Email: konrad.wrona@ncia.nato.int

***Abstract*—The Internet of Things (IoT) has the potential to become one of the most disruptive technologies that have emerged in recent decades. It can influence both civilian and military applications. One of the biggest challenges to successful deployment of IoT systems is security. Security is particularly important in military applications of IoT. In this article we discuss security challenges related to military applications of IoT and propose a possible approach to solving some of them, based on Object Level Protection and cryptographic access control.**

I. Introduction

The Internet of Things (IoT) has the potential to become one of the most disruptive technologies that have emerged in recent decades. It can influence both civilian and military applications.

The IoT is in itself not a radically new technology - rather it is an integration of several existing technologies such as wireless sensor networks, embedded systems, machine-to-machine communications, cloud computing and mobile applications. The integration was made possible by recent advances in these individual technologies, which enable cost-effective and relatively easy implementation of cyber-physical systems, and involve physical sensing, networking, data analysis, and context-aware workflows and applications. The integration, although a natural step in the the development of information systems, has the potential to cause a phase transition in the way we interact with the physical environment and dramatically increase both our situational awareness and the amount of data processed by information systems.

One of the biggest challenges related to wide-spread deployment of the IoT is security. Security of the IoT has been a subject of active research in recent years, including several research projects funded by both the European Commission and DARPA.

In this paper we provide a military perspective on the security of IoT applications and we show how IoT applications can be supported by the Content-based Protection and Release paradigm proposed for future military operations [1].

II. Role of IoT in military applications

There are several high-impact use cases for deployment of the IoT in a military environment. Some of the most important use cases are briefly discussed below. A more detailed discussion of the applicability of the IoT to military operations can be found in [2].

A. Smart equipment

The Internet of Things can be applied to a large variety of military equipment such as vehicles, supplies, and even weapon systems. Many such network-enabled objects have already been demonstrated to have significant security flaws and vulnerabilities. In particular, several serious vulnerabilities have been identified in cars [3]–[6], leading to massive vehicle recalls. There are also known examples of the enemy exploiting weaknesses in the security of military cyber-physical systems [7]. Similarly, researchers have recently identified important security vulnerabilities in commercially available smart rifles [8].

B. Situational awareness

One of the most important aspects of every military operation is proper situational awareness. Most armed forces already use a wide range of sensors and unmanned vehicles for gathering intelligence. Incorporating civilian IoT solutions into military IT systems could improve the operational picture available to a commander and could substantially contribute to augmenting overall situational awareness. Nevertheless, positive effect of such augmentation can be only achieved if an adequate availability and integrity of information delivered from the IoT systems can be assured. Therefore, the COTS IoT systems need to be carefully evaluated in this respect before being integrated as trusted and reliable sensors within cyber situation awareness capability.

C. Logistics

Use of the IoT, including sensors and RFID, is fundamental for improving the efficiency and effectiveness of logistics operations. This includes interoperability with third-party logistics systems, since many of the supplies required during military operations consist not only of military equipment, but also of subsistence and medical materials for forces. The use of IoT systems in logistics could also contribute to increased safety of logistic operations, e.g., by preventing a joint transportation of some goods such as chemical components, which could result in dangerous chemical reactions, or parts of cryptographic equipment, which should not be intercepted by an adversary [9]. However, it was shown in the past that improper integration of RFID tracking solutions with the backend system could lead to new attack paths on the enterprise information systems [10]. Also, lack of an adequate

978-1-5090-0366-2/15/$31.00 ©2015 Crown

protection of confidentiality could enable an adversary to perform better targeted attacks on the delivery convoys or use the information as a side channel for reasoning about planned military operations. Similarly, inadequate integrity and availability protection could be exploited by an adversary to severely impact the logistics operation, e.g., by maliciously re-routing the goods. All these risks need to be taken into account when designing IoT-enabled logistic applications for military.

D. Medical care

Assistance in treatment of medical conditions and injuries during combat operations is one of the most commonly discussed applications of wearable and stationary IoT systems in military environment. However, in addition to high potential for improving speed and accuracy of delivering, often life-saving, medical treatment to soldiers, smart medical care systems may also introduce some new risks. Modern medical systems and health monitoring systems are typically equipped with wireless functionality and enable communication between devices and towards medical back-end systems. These wearable - or implantable - medical systems were demonstrated to have some security vulnerabilities [11]–[13]; in fact it has recently emerged that some prominent public personalities were aware of the issues and sufficiently concerned to disable remote connectivity in their implanted medical devices [14].

III. IoT as a new attack surface

Like every new technology, IoT potentially introduces a new attack surface in the military IT system. This attack surface consists of:

- IoT devices (i.e. sensors and actuators)
- Communication channels between the devices as well as between the devices and the back-end system
- IoT-specific back-end applications
- Back-end data storage.

From an enterprise perspective, some interesting new security challenges are also introduced through the implementation of the Bring Your Own Device (BYOD) concept in relation to personal IoT devices. Although most of the current work on BYOD security policies and mechanisms is focused on relatively powerful traditional mobile devices, such as laptops and smartphones, it is conceivable that in the near future employees will be bringing to the work place a large number of smart devices, with all their related security risks and opportunities. How this situation could be exploited in order to increase the security of the enterprise by taking advantage of the additional sensing capabilities, rather than it only opening new attack vectors for the enterprise system, is still an open question. One of the open challenges is the management of potentially complex security policies applicable to IoT BYOD. In this respect formal approaches may offer an interesting solution.

A. Attacker model

IoT systems used in military environments are faced with determined attackers with varying technical capabilities. Although some of the adversaries faced by NATO and NATO nations in their recent operations are not technically sophisticated, this situation changes rapidly. Insurgents in Iraq being able to access unencrypted surveillance streams from American drones is the best example of a risk introduced by underestimating the capabilities of an adversary. Also, many historically unsophisticated enemies have substantial financial resources and control large parts of the population. This provides them with the ability to procure by purchase or coercion the required expertise externally.

Depending on the IoT use case, the attacker may be more (e.g. in the case of ground seismic sensors) or less (e.g. in the case of unmanned vehicles) likely to have physical access to a device. Nevertheless, it is reasonable to assume that the physical integrity of the device cannot be guaranteed and the devices should be equipped with embedded secure elements and a trusted execution environment [15] in order to protect the cryptographic material as well as the capability for remote wipe.

It must also be assumed that the attacker has access to a wireless communication channel between the IoT devices, as well as between the IoT devices and the gateway to the back-end system. Therefore these communication channels must be authenticated and secured against eavesdropping as well as, to the extent possible, against jamming.

The attacker's accessibility to the IoT back-end system, typically located in a cloud, may vary depending on the exact location of the back-end system. Accessibility may be reduced by existing network defences in the case of systems located within the private NATO cloud, but systems hosted by third-party providers may use a public cloud or expose their interfaces to the public Internet.

Therefore it is important that a proper vulnerability assessment and penetration testing, including scenarios involving compromised IoT end devices, be performed regularly on the back-end system.

B. Vulnerabilities

A recent study [16] of 50 smart home devices found that none of the devices enforced strong passwords, used mutual authentication, or protected accounts against brute-force attacks. Almost two out of ten of the mobile apps used to control the tested IoT devices did not use Secure Sockets Layer (SSL) to encrypt communications to the cloud. The tested IoT technology also contained many common vulnerabilities. In particular, some of the web portals used to control IoT devices had serious vulnerabilities, allowing unauthorized access to the back-end systems.

The Open Web Application Security Project (OWASP) List of Top Ten Internet of Things Vulnerabilities [17], which define the attack surface of IoT applications, is:

1) Insecure web interface
2) Insufficient authentication/authorization
3) Insecure network services
4) Lack of transport encryption
5) Privacy concerns
6) Insecure cloud interface

7) Insecure mobile interface
8) Insufficient security configurability
9) Insecure software/firmware
10) Poor physical security.

C. Privacy

Privacy implications of the IoT have been a subject of research and public interest in both Europe [18] and the US [19]. Although privacy is not a primary concern during military operations, NATO and NATO nations have to comply with the national privacy regulations applicable to the deployed personnel. Thus it is important that the implemented IoT solutions not unnecessarily infringe on the privacy of personnel and that all collected personal information be adequately protected both in transit and in storage.

IV. IoT as a security enabler

Despite the security and privacy risks introduced by IoT systems, the IoT can be used to provide an additional source of security-relevant information and thus enable context-aware security mechanisms and support defence-in-depth principles. For example, context information received from IoT systems could be used as input to authentication mechanisms (e.g. using behavioral biometrics) or be used to dynamically adapt the level of deployed security measures, based on the perceived threat level and operational picture. Our recent results on behavioral biometric authentication are promising [20]. Although our implementation was limited to the standard sensors included in a typical smartphone, the same approach could be applied to distributed scenarios, in which the behavioral pattern of the user is collected from multiple IoT devices, if sufficient trustworthiness of this information can be guaranteed.

V. Security requirements for military IoT

The security requirements for military IoT systems do not differ from the security requirements for any other IT systems deployed in the military environment, and concern confidentiality, integrity and availability.

A. Confidentiality

Confidentiality is an important aspect of any military operation. In the case of IoT systems, confidentiality protection is required for all communication channels, as well as data stored and processed both at the end nodes and in the back-end system. For example, in the case of wireless sensor networks or unmanned vehicles, compromising confidentiality may both endanger the forces and the goals of operations by giving clues about the military plans, and provide unintended support to the enemy by providing him with data streams and increased situational awareness. A real-life example of such a threat was observed in December 2009 when militants in Iraq obtained access to the unprotected down-link transmission used by the US drones [7].

B. Integrity

Integrity is critical for many aspects of military IoT systems. Clearly it is important that the information delivered to the command and control center by smart things has not been modified and is trustworthy enough to be incorporated into the operational picture and used for command decisions. However, it is equally important that the command and situational information provided to the smart objects be of appropriate integrity. For example, it is stipulated that in December 2011 Iran had successfully brought down a US reconnaissance RQ-170 Sentinel UAV by spoofing the GPS signals it received to navigate back to its launch point. Integrity is not only a feature of information but also of a system, where it refers to ensuring preservation of a secure state and configuration of a system. A violation of integrity of the system may have catastrophic impact on confidentiality, integrity and availability of data processed by this system. Example of such attack was observed in in September 2011, when a virus-infected military system was used for keylogging command and control of a US UAV fleet at Creech Air Force Base in Nevada [21]. These events led to the development of the DARPA research program in High Assurance Cyber Military Systems [22], [23].

C. Availability

The full potential of the IoT in military environments will not be achievable if required availability of the information delivered from the sensors and devices cannot be assured. Similarly, it is important that command and control information be available to actuators and smart devices when required. A specific aspect of availability related to the IoT is so-called *sleep-deprivation attack*. This type of attack targets specifically battery-powered devices, which are common among smart things, by preventing them from entering an energy-saving mode. This leads to depletion of battery power and replenishing batteries may be extremely difficult, if not impossible, in combat situations, thus zero-power technology and energy scavenging may be important for survival of the IoT systems. These are subjects of recent large DARPA research programs [24].

VI. Applying Object Level Protection to IoT

A. Object Level Protection

The concept of Object Level Protection (OLP) [25] was developed to support NATO Network Enabled Capability (NNEC) [26]. OLP is a system-wide standard approach to data protection; it is built on two fundamental pillars:

1) Protection is applied to individual data objects (or portions thereof) instead of to a collection of data objects and systems.
2) Metadata is bound to data objects and is used by protection enforcement mechanisms to determine the protection requirements for a data object.

OLP also complements the cyber defence component of a cyber security architecture by supporting data leakage prevention and defence-in-depth. In particular, OLP capability

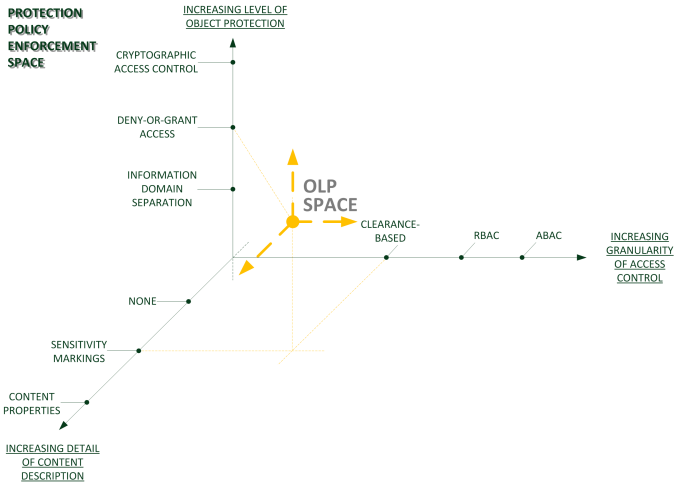

Fig. 1. The OLP Space extends into all directions of the PPES.

strengthens resilience to unforeseen threats in the sense that if perimeter protection appears to be insufficient, then there is a second layer of protection at the object level, especially when cryptographic access control is deployed [27].

B. OLP dimensions

The OLP space (OLPS) can be defined by the following three dimensions:

1) The level of detail in the description (i.e. metadata) of the content of an information object, in short *detail of content description*
2) The granularity of the information about the actor (i.e. human user or automated process that requests access to a data object) and the environment that can be supported by the protection policy enforcement capability, in short *granularity of access control*
3) The *level of object protection*, i.e. to what extent it is possible to protect an object regardless of its location and the time.

There may be multiple ways in which mechanisms related to each dimension can be implemented. The individual dimensions are discussed in more detail below.

1) Detail of content description: An information object can be described using metadata. The metadata is used by protection mechanisms to determine the protection requirements for a data object. The level of detail with which an information object is described determines the precision with which the protection requirements can be formulated and enforced; it also depends on the type of metadata that is used. In the state *none*, protection mechanisms do not rely on any metadata. Instead a protection policy is enforced at the system (or network) level and is applied to all data objects (e.g. as in the *system high* approach). As there is no protection at the object level in this state, it is not part of the OLPS. However, *none* is included in the discussion in order to clearly establish the distinguishing characteristics of OLP (and the OLPS). In the state *sensitivity markings* the metadata comprises a sensitivity marking. A sensitivity marking does not provide information on the contents of a data object; it is an expression of the protection requirements and release conditions that apply to a data object. In the state *content properties* the metadata describes the content represented by the data object. Contrary to sensitivity markings, content properties do not express the protection requirements and release conditions. The correspondence between the protection requirements, the release conditions and the content properties is recorded and managed in separate protection and release policies [28].

2) Granularity of access control: The information about the actor and its environment can have different granularity depending on the targeted state. In the state *clearance-based* [29] the information about the actor and its environment is limited to the actor's clearance level or the classification of the system (or network) from which the actor requests access to a data object. In the state *Role-Based Access Control* (RBAC) [30] the use of a clearance level for actors is expanded with the concept of roles, which allows for a more fine-grained expression of an actor's authorizations. In the state *Attribute-Based Access Control* (ABAC) [31] the use of clearance levels (and system/network classifications) and roles is expanded to include more detailed sets of attributes describing the actors involved in the accessing of data objects, and the technical capabilities of the systems used for access. The protection policy enforcement capability that implements this state will support ABAC.

3) Level of object protection: Enforcing a protection policy at the data object level requires the ability to apply a protection policy to an individual data object regardless of its location and the time. The extent to which this can be realized is referred to as the *level of object protection*, for which three general states are distinguished. The state *information domain separation* takes its name from the practice of enforcing a protection policy at the information domain level, where the policy is inherited by all systems that constitute the information domain. In this state a data object is protected based on its information domain membership and it must not be transferred to an information domain under a different (i.e. less stringent) protection policy. Currently, prevention is commonly realized by separating systems or networks (where the systems or networks contain information and form an information domain). As there is no protection at the object level in this state, it is not part of the OLPS. However the state is included here to clearly establish the distinguishing characteristics of OLP (and the OLPS). In the state *deny or grant access* (DOGA) protection mechanisms are introduced that can enforce a protection policy at the object level. The enforcement can be coarse-grained, i.e. access control is enforced on a data object as a whole, or fine-grained in the sense that it is possible to enforce a protection policy on portions of a data object. If an actor is allowed to access a data object, then access is granted by releasing the data object to that actor (where the data object is transferred from the data object's information domain to the actor's information domain). An example is the release of data objects from one domain to

another through the use of a cross-domain guard, such as the NATO Medium Assurance XML-labelling Guard [32], which makes release decisions for (portions of) data objects. In the state *cryptographic access control* (CAC) [33] the protection policy is not enforced according to the DOGA principle, but instead by encryption of data objects (or portions thereof). The use of CAC increases the level of object protection because an encrypted data object is protected regardless of its location, whereas in the case of DOGA once the data object has been released, the protection policy of the originating information domain can no longer be enforced. When CAC is used, the access control decision is not enforced in direct response to a request for a data object. Instead data objects are encrypted and the access control decision is delayed until a decryption attempt is made. When an actor is able to decrypt the data object, this implies that the correct key material has been used and it is concluded that the actor is authorized to access the data object. When decryption fails, this implies that the actor is not authorized. Note that the decision to release decryption key material to an actor will be based on whether or not the actor has authorization. However, when CAC is used the request for key material can in principle be made independently of the attempt to decrypt (i.e. access) the data object.

C. Applicability to IoT

Describing information generated by the IoT using content properties is a natural step, as much of the data is sensor-type data, often described as an XML structure. Use of ABAC takes advantage of the availability of content metadata in IoT systems and supports fine-grained information sharing between partners relying on federated IoT systems. The traditional approach to protection of data in military systems, by relying on security markings and Bell-LaPadula [29] security policies, is not applicable to the IoT because it is too large and potentially cannot control its devices. Similarly, enforcing DOGA principles in IoT applications may be overly complex and unscalable.

D. Cryptographic access control for military IoT applications

We argue that OLP with CAC provides an attractive solution for protecting data in military IoT systems. The advantage of using cryptographic access control on an information object level, instead of network layer confidentiality mechanisms, is that objects can be protected end-to-end, including during possible interim storage. Also, fine-grained access control offered for OLP facilitates sharing of information generated by the IoT systems with external partners, such as local civilian authorities, non-governmental organizations, the International Committee of the Red Cross, and the United Nations. Implementing a flexible information-sharing capability within the IoT from the beginning is crucial because such a large amount of data can potentially be generated by IoT systems, and that data would be impossible to analyze and release using the classical (manual) process.

In public-key encryption schemes, every entity holds both a private and a public key according to predetermined global parameters. In order to securely transmit a message to a recipient, a sender first encrypts it using the public key of the recipient. The recipient can then upon receipt decrypt the message using his private key. Public keys are usually distributed via public-key certificates, which contain a copy of a public key, some owner identity information and a signature on the certificate provided by the central authority for the public key infrastructure.

Identity-based encryption can be seen as a variant of public-key encryption that does not make use of public-key certificates, but for which instead the public key for a recipient can be determined directly from the global parameters of the scheme and the public identifier associated with a recipient. Unlike the case in a regular public-key infrastructure, in which every entity can generate its own private key, in identity-based encryption schemes private keys are typically generated and distributed by the central authority.

Attribute-based encryption (ABE) can be seen as an extension of identity-based encryption, in which decryption can be enabled based on the outcome of a predicate on a number of attribute values associated with the recipient. This is accomplished via prior assignment of a number of private keys corresponding to these attributes. Attribute-based encryption allows for fine-grained control of the decryption capability for a message; the sender does not necessarily need to know the precise identities of the appropriate recipients but can instead define an attribute-based policy for the recipients.

Attribute-based encryption can be further abstracted into predicate encryption and functional encryption. Hidden-index predicate encryption schemes are useful when the access policy or the attributes themselves consist of sensitive information and should therefore also remain hidden to unauthorized parties. Attribute-based encryption and predicate encryption can be seen as special cases of a higher-level functionality called functional encryption. Functional encryption schemes allow messages to be encrypted in such a way that decryption of the resulting ciphertext produces an evaluation of the message with respect to a key-dependent function.

In our recent work, we have investigated use of ABE schemes for object level protection [27]. These schemes can be combined with classical symmetric encryption schemes, similarly to the approach commonly used with traditional public-key cryptography in order to construct a hybrid encryption scheme. Such hybrid encryption scheme limits the performance overhead introduced by use of ABE. Several researchers have investigated use of ABE in the context of the IoT [34], [35].

VII. Conclusion

We have discussed several use cases and related threats applicable to the use of IoT systems in military applications. We also presented the concepts of Object Level Protection and cryptographic access control, which are currently considered to be possible security models for future NATO operations. We conclude that OLP and CAC can be applied to the IoT

in order to provide end-to-end data protection, both in transit and in storage.

The deployment of cryptographic access control in the IoT introduces several challenges, including the key management and implementation of cryptographic algorithms in constrained environments. Although, the computational overhead of introduced by many modern cryptographic mechanisms is too large for many of todays IoT devices, experience has shown that the performance of devices improves much faster than anticipated and that devices can in a short time improve sufficiently to perform even complex cryptographic algorithms. Although there will always be a market space for low-end IoT devices, e.g. nano-things [36], the majority of IoT devices will be powerful enough to support state-of-the-art encryption mechanisms such as ABE before the regular life cycle of military systems results in wide-spread adoption of IoT technology.

An interesting open research issue is to what extent data can be kept in an encrypted state through its entire life cycle. This was a topic of a recent research program at DARPA [37].

REFERENCES

[1] K. Wrona and S. Oudkerk, "Content-based Protection and Release Architecture for Future NATO Networks," in *Military Communications Conference (MILCOM)*, San Diego, CA, USA, 2013.

[2] D. Zheng and W. Carter, "Leveraging the internet of things for a more efficient and effective military," Center for Strategic & International Studies, Washington, DC, Tech. Rep., 2015.

[3] I. Roufa, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Grutser, W. Trappe, and I. Seskar, "Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study," in *Proc. of the 19th USENIX conference on Security*, 2010.

[4] S. Checkoway, D. Mccoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, "Comprehensive Experimental Analyses of Automotive Attack Surfaces," in *SEC'11 Proceedings of the 20th USENIX conference on Security*, 2011.

[5] C. McCarthy, K. Harnett, and A. Carter, "Characterization of Potential Security Threats in Modern Automobiles: A Composite Modeling Approach," National Highway Traffic Safety Administration, Washington,, Tech. Rep. October, 2014.

[6] C. Miller and C. Valasek, "A Survey of Remote Automotive Attack Surfaces," Tech. Rep., 2014.

[7] J. A. Marty, "Vulnerability Analysis of the MAVLink Protocol," Ph.D. dissertation, Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, 2014.

[8] A. Greenberg, "Hackers can disable a Sniper Rifle - or change its target," *Wired*, Jul. 2015.

[9] A. Sorniotti, L. Gomez, and K. Wrona, "Secure and trusted in-network data processing in wireless sensor networks: a survey," *Journal of Information Assurance and Security*, vol. 2, no. 4, 2007.

[10] M. Rieback, B. Crispo, and A. Tanenbaum, "Is your cat infected with a computer virus?" in *Proceedings of the Fourth Annual IEEE InternationalConference on Pervasive Computing and Communications (PERCOM)*, Washington, DC, USA, 2006, p. 169179.

[11] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel, "Security and Privacy for Implantable Medical Devices," *IEEE Pervasive Computing*, vol. 7, no. 1, Jan. 2008.

[12] D. Halperin, T. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel, "Pacemakers and Implantable Cardiac Defibrillators : Software Radio Attacks and Zero-Power Defenses," in *Symposium on Security and Privacy*, 2008.

[13] W. H. Maisel and T. Kohno, "Improving the security and privacy of implantable medical devices." *The New England journal of medicine*, vol. 362, no. 13, Apr. 2010.

[14] R. Luscombe, "Dick Cheney feared assassination by shock to implanted heart defibrillator," The Guardian, Oct. [Online]. Available: http://www.theguardian.com/world/2013/oct/19/dick-cheney-heart-assassination-fear

[15] GlobalPlatform Inc., "GlobalPlatform Device Technology TEE Internal API Specification - Version 1.0," GlobalPlatform, Tech. Rep., 2011.

[16] M. B. Barcena and C. Wueest, "Insecurity in the Internet of Things," Symantec, Tech. Rep., 2015.

[17] D. Miessler, "Securing the Internet of Things : Mapping Attack Surface Areas Using the OWASP IoT Top 10," in *RSA Conference*, 2015.

[18] M. van den Berg, P. de Graaf, P. O. Kwant, and T. Slewe, "Mass surveillance - Part 2: Technology Foresight," European Parliament, Tech. Rep., 2015.

[19] E. Markey, "Tracking & Hacking : Security & Privacy Gaps Put American Drivers at Risk," Tech. Rep., 2015.

[20] A. Buriro, B. Crispo, F. Del Frari, and K. Wrona, "Touchstroke: Smartphone user authentication based on touch-typing biometrics," in *New Trends in Image Analysis and Processing–ICIAP 2015 Workshops*. Springer, 2015, pp. 27–34.

[21] K. Hartmann and C. Steup, "The vulnerability of UAVs to cyber attacks - An approach to the risk assessment," *Cyber Conflict (CyCon), 2013 5th International Conference on*, pp. 1–23, 2013.

[22] K. Fisher, "HACMS : High Assurance Cyber Military Systems," *HILT'12 Proceedings of the ACM SIGAda annual conference on High integrity language technology*, 2012.

[23] L. Pike, P. Hickey, J. Bielman, T. Elliott, E. Hamberg, and T. Dubuisson, "Building a High-Assurance Unpiloted Air Vehicle," in *MEMOCODE'13 Eleventh ACM-IEEE International Conference on Formal Methods and Models for Codesign*, 2013.

[24] U.S. Defense Advanced Research Projects Agency, "N-ZERO Envisions 'Asleep-yet-Aware' Electronics That Could Revolutionize Remote Wireless Sensors," *Communications of the ACM*, Apr. 2015.

[25] S. Oudkerk and K. Wrona, "A Common Approach to the Integration of Object Level Protection in NATO," in *Proc. of the STO Symposium on Cyber Security Science & Engineering*, Tallinn, Estonia, 2014.

[26] A. Domingo and H. Wietgrefe, "A NNEC-compliant approach for a Future Mission Network," in *Proc. of the Military Communications Conference (MILCOM)*, 2012.

[27] S. Oudkerk and K. Wrona, "Cryptographic Access Control in support of Object Level Protection," in *Proc. of the Military Communications and Information Systems Conference (MCC)*. St. Malo, France: IEEE, 2013.

[28] A. Armando, S. Oudkerk, S. Ranise, and K. Wrona, "Content-based Protection and Release for Access Control in NATO Operations," in *Proc. of the 6th International Symposium on Foundations & Practice of Security (FPS)*. La Rochelle, France: Springer, 2013.

[29] L. J. LaPadula and D. E. Bell, "Secure Computer Systems: Mathematical Foundations," MITRE Technical Report 2547, Volume II, Tech. Rep., 1973.

[30] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, and R. Chandramouli, "Proposed NIST Standard for Role-based Access Control," *ACM Trans. Inf. Syst. Secur.*, vol. 4, no. 3, 2001.

[31] V. C. Hu, A. R. Friedman, A. J. Lang, M. M. Cogdell, K. Scarfone, R. Kuhn, D. Ferraiolo, A. Schnitzer, K. Sandlin, and R. Miller, "Guide to Attribute Based Access Control (ABAC) Definition and Considerations (Draft)," National Institute of Standards and Technology, NIST, Tech. Rep., 2013.

[32] K. Wrona, S. Oudkerk, and G. Hallingstad, "Designing medium assurance XML-labelling guards for NATO," in *Proceedings of the Military Communications Conference (MILCOM)*. San Jose, USA: IEEE, 2010, pp. 1794–1799.

[33] M. Kiviharju, "Towards Pervasive Cryptographic Access Control Models," in *SECRYPT*, 2012.

[34] X. Yao, Z. Chen, and Y. Tian, "A lightweight attribute-based encryption scheme for the Internet of Things," *Future Generation Computer Systems*, vol. 49, 2015.

[35] J. Hernández-Ramos, J. Bernabe, M. Moreno, and A. Skarmeta, "Preserving Smart Objects Privacy through Anonymous and Accountable Access Control for a M2M-Enabled Internet of Things," *Sensors*, vol. 15, no. 7, 2015.

[36] I. Akyldiz and J. M. Jornet, "The Internet of Nano-Things," *IEEE Wireless Communications*, no. 12, Dec 2013.

[37] M. C. Libicki, O. Tkacheva, C. Feng, and B. Hemenway, "Ramifications of DARPAs Programming Computation on Encrypted Data Program," RAND National Defense Research Institute, Tech. Rep., 2014.