# International Workshop on Adaptive Security & Privacy management for the Internet of Things (ASPI 2013)

**Stefan Poslad**
Queen Mary University of London
stefan@eecs.qmul.ac.uk

**Mohamed Hamdi**
School of Communication Engineering, Tunisia
mmh@supcom.rnu.tn

**Habtamu Abie**
Norwegian Computing Center
Habtamu.Abie@nr.no


*UbiComp'13 Adjunct*, September 8–12, 2013, Zurich, Switzerland.

ACM 978-1-4503-2215-7/13/09...$15.00.

## Abstract

The Internet of Things (IoT) was initially proposed to connect specific things via the Internet using devices, such as RFID readers, to realise intelligent identification and management. This vision has since expanded to include a more diverse range of devices, services and networks to become an Internet of anything, anywhere, connected, anyhow. Security and privacy management for the IoT remains a core challenge.

Many IoT devices maybe may have zero or minimal security by design because they are low resource, low power devices, designed to work as closed vertical services. Security threats and risks may be higher because devices are unattended, use local wireless communication that have no or weak encryption making them more susceptible to eavesdropping and because users find security too unusable to setup and operate and hence leave devices relatively unsecure. It may also be less problematic to reproduce and fake data sources, access nodes and data sinks that interact with IoT devices in order to attack devices or the services they access. Devices can be moved between or removed from private, communal, public and hostile physical spaces. There is a higher risk of a loss of privacy for human users and organisations because of an increased ability to eavesdrop, because of wireless networks with soft boundaries, and because embedded

environment devices can sense smaller amounts of physical trails with a greater degree of sensitivity and accuracy. A specific focus is on the need for IoT security to adapt. The adaptation has multiple dimensions. We can adapt existing conventional security models to more effectively secure an IoT. We can adapt security pre-planned and unplanned context changes such as different moving around in different physical spaces. IoT systems can be designed to self-adapt. IoT systems need to adapt to the active (re) configuration and maintenance of IoT devices and systems of devices by users and by artificial agents.

The proposed workshop intends to bring together researchers and practitioners from relevant fields to present and disseminate the latest on-going research focussing on adapting security, privacy & management for the Internet of Things. It aims to facilitate knowledge transfer and synergy, bridge gaps between different research communities and groups, to lay down foundation for common purposes, and to help identify opportunities and challenges for interested researchers and technology and system developers.


## Author Keywords
Internet of Things

## ACM Classification Keywords
H.m [Information systems]: Miscellaneous.


## Motivation and Challenges
Many security researchers focus more on the review of current information security threats landscape with far less focus on emerging and future threats for the IoT. These threats are discussed below.

*Unattended devices:* devices may be left unsecured either because their owners expect that they will remain under their physical control. However, if dont, they are open to use by anyone. Embedded micro devices and macro devices may need to be left unattended for long periods, in relatively inaccessible environments, e.g., pace-makers that are implanted in the human body and remote sensors left in uninhabited physical environments. Unattended embedded devices that are used for control, e.g., pace-maker implants, require stable timing to deliver control signals at set times, over time. The security design of devices to be tamper-resistant or at least tamper-evident is a key concern. Protecting specific parts of a device may be insufficient. Some threats can manipulate the local environment to cause the device to malfunction such as heating or freezing the environment. Hence a multi-lateral approach is needed to protect unattended devices, e.g., use of materials resistant to physical attacks, use of counter-measures and other corrective measures it tampering attacks are detected, and the use of a priori preventive measures such as encryption to lessen threats.

*Low resource and low power devices:* low resource devices may lack the CPU and memory to perform the computation to encrypt and decrypt data that is exchanged. Devices that run out of power essentially cannot operate normally and this essentially constitutes a denial of service. A general type of attack on devices with limited energy reserves is to cause their energy reserves to be unnecessarily expended. For example, a common strategy to conserve power is for devices to enter various power-saving modes, e.g., various sleep and hibernation modes. A sleep deprivation attack or threat makes just enough legitimate requests to prevent a device from entering its energy-saving mode. A barrage attack bombards victim nodes with legitimate requests.

*User managed devices:* security is often in practice configured to be low: In complex cyber-physical systems, such as hospitals or control rooms, there is continuous interaction between devices and operators. In these systems, security and privacy need therefore to be studied in relation to users' needs and actual practice; otherwise, they would be systematically overridden by users because they constitute impediments to normal work. For instance, authentication methods based on logins may be introduced in a system to identify authorised users. However, users may still use weak passwords (e.g., dates, names), store passwords in unsafe places (e.g., on a mobile phone), or even share passwords (e.g., with an authorised "guest" user that is not recognised by the system). These and other workarounds not only void the introduced design solutions, but potentially create new threats to the system.

*Increasing wireless PAN/BAN/LANs of devices:* multiple types of the same type of physical and network layer may exist because multiple independent users and providers may offer overlapping wireless networks within the same vicinity. This can make it easier for a device on one network to inadvertently or maliciously breach the security and mismanage another device on another overlapping network. Targets for attack can be more readily identified by the mere fact that devices are communicating in the vicinity and because environments are more instrumented with active devices. As devices networks increasingly interoperate in the Internet, it leads devices to be more open to remote access and to an increasing risk of a remote attack.

*Changing / unknown ICT infrastructure, physical space, human-social environment:* the boundary between what is assumed to be a closed, more secure, private space and more open social and public spaces becomes softer enabling private data in personal spaces to seep out into less personal spaces. For mobile users, they may not realise as they roam that they are accessing services over public or even hostile spaces and fail to enact stronger security measures or even counter measures.

*Loss of Privacy:* In addition, to an increasing ability to eavesdrop on wireless PAN/BAN/LANs that can overlap, that have soft boundaries, the profusion of smart environment devices means that humans can be identified, tracked and profiled to a greater degree throughout the physical environment, without their consent. As more human-to- human and human to-device interactions occur over shared physical networks and shared service and social spaces, it is also possible to sense smaller amounts of physical trails of these interactions with a greater degree of sensitivity and accuracy.

*Key challenges in supporting security that can adapt to a likely dynamic IoT:* Security adaptation can take the form of parameter adaptation achieved by specific variations in the security control parameter vector, structure adaptation achieved by dynamic changes in the structure of the system, goal adaptation achieved by formally defining specific constraints on the state of the system, or any combination of these. Adaptation can take place at any layer or across-layers, i.e., vertical cooperation among multiple system layers, horizontal cooperation among multiple platforms, and universal adaptation  combination of vertical and horizontal cooperation.

The challenges in doing security adaptation are that the adaptive algorithm must respond to changes in the system on the fly and the activities of the adaptive algorithm must have only minimal deviations from the normal mode of operation of the system, must address the

reconfiguration of functional logic, the architecture as a whole, and the handling of conflicts. Additional challenges are to the implementation of adaptive algorithms are the complexity of the correct definition of goals and restrictions, the necessity for the on-going identification of both system and environment, and the required minimum reaction time of adaptive algorithms.

Self-adaptive security solutions are capable of handling changing operational contexts, environments or system characteristics and adjust their security control parameters by monitoring the environment and the underlying system itself. For the design and development of self-adaptive security systems for IoTs where their specialties are taken into account, concepts of control theory, such as control loops, are normally adapted and used in order to build flexible self-adaptive IoTs which are capable of handling dynamic changes.

## Related Literature

Kozlov et al. [2012] and Medaglia and Serbanati [2010] give an overview, categorization, and analysis of security and privacy challenges in the IoTs. They have identified that the protection of data and privacy of users is one of the key challenges in the Internet of Things. They state that lack of confidence about privacy will result in decreased adoption among users and therefore is one of the driving factors in the success of the Internet of Things. Hong et al. [2004], propose privacy risk models as a general method for refining privacy from an abstract concept into concrete issues for specific applications and prioritizing those issues. Webera [2010] argues that measures ensuring the IoT architecture's resilience to attacks, data authentication, access control and client privacy need to be established.

Roman et al. [2011] contend that for IoT to fully bloom into a paradigm that will improve many aspects of daily life, open problems remain in many areas, such as cryptographic mechanisms, network protocols, data and identity management, user privacy, self-management, and trusted architectures need to be addressed.

Suo et al. [2012] present a brief review of security in the IoTs and discuss the research status of key technologies including encryption mechanism, communication security, protecting sensor data and cryptographic algorithms, and briefly outline the challenges. According to Shnitko [2003] adaptation may be defined as the optimal control of specified object F in state S whose influence Y on the environment is determined by the influences X of the environment on the object, the relevant set of adaptable structures or factors U, and the goals Z of the adaptation as defined by specified constraints on the state S of the object.

Savola et al. [2012] discussed metrics-driven adaptive security management needs and initial solutions for E-health IoT applications especially for the treatment of chronic diseases and well-being of elderly people. They argued that adaptive security management is needed especially for setting the sufficient security requirements and for enforcing the adequate security controls in the face of changing security risks and use context, and that informed adaptive security decision-making is based on adequate security effectiveness, correctness and efficiency evidence offered by security metrics.

Abie and Balasingham [2012] presented a high-level risk-based adaptive security framework for IoT in eHealth to estimate and predict risk damages and future benefits using context-aware game theoretic models. The framework outlines how the security methods and

mechanisms should adapt their security decisions upon those risk estimates and predictions by incorporating practical and systematic evaluation models utilizing security metrics for validation of the adaptation.

## Expected Results

The proposed workshop has three primary objectives. Firstly, it intends to present and disseminate the latest accomplished and on-going research on adaptive security, privacy and management for IoT and novel applications in ubiquitous computing. This includes work on security in next generation Internets, including sensor networks, mobile device networks and distributed mobile and autonomous systems and services, context-aware systems, distributed AI, and HCI. Accepted papers will appear in the conference proceedings. In addition, selected high-quality papers will be invited to be published, after revision and extension, in a journal such as a special issue of the International Journal of Pervasive computing and Communications (IJPCC).

Secondly, the workshop aims to bring together researchers and practitioners from the relevant fields, in particular, the audience encompasses those with a wide range of expertise in modelling complex systems, developing methodologies, systems and infrastructures, application developers and users with expertise and experience in user requirements, system implementation and evaluation related to IoT security and privacy. We expect that through this workshop a research community focusing on this high interest area can be formed, and more work and contributions can be made available in the future, probably in another workshop next year.

The third objective of the workshop is to identify opportunities and challenges and facilitate collaborations and synergy between different research communities and groups and in particular to relate the security in IoT to a broader landscape of Ubiquitous Computing.

## References


1. Abie, H. and Balasingham, I. 2012. Risk-Based Adaptive Security for Smart IoT in eHealth. I: BODYNETS 2012 - 7th International Conference on Body Area Networks. Brussels: ICST - Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering 2012 ISBN 978-1-4503-1997-3, pp. 269-275

2. Hong, J., Ng, J., Lederer, S., and Landay, J. 2004. Privacy risk models for designing privacy-sensitive ubiquitous computing systems. In D. Benyon; P. Moody; D. Gruen and I. McAra-McWilliam (Eds.): Proc. of the 2004 conference on Designing interactive systems: processes, practices, methods, and techniques, (August 1, 2004), NY, pp. 91-100.

3. Kozlov, D., Veijalainen, J., and Ali, Y. 2012. Security and privacy threats in IoT architectures. In Proceedings of the 7th International Conference on Body Area Networks (BodyNets '12). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), ICST, Brussels, Belgium, Belgium, pp. 256-262.

4. Medaglia, C. M., and Serbanati, A. 2010. An Overview of Privacy and Security Issues in the Internet of Things. In The Internet of Things, 5, pp. 389-395.

5. Roman,R., Najera, P., and Lopez, J. 2011. Securing the Internet of Things. In IEEE Computer, 44, 9, 51-58.

6. Savola, R., Abie, H., and Sihvonen, M. 2012.Towards Metrics-Driven Adaptive Security Management in E-Health IoT Applications. I: BODYNETS 2012 - 7th International Conference on Body Area Networks. Brussels: ICST - Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering 2012 ISBN 978-1-4503-1997-3, pp. 276-281.

7. Shnitko, A. 2003. Adaptive security in complex information systems. In Proc. 7th Korea-Russia Int. Symposium on Science and Technology, (8023863), 206-210, (28 June - 6 July, 2003).

8. Suo, H., Wan, J., Zou C., and Liu, J. 2012. Security in the Internet of Things: A Review. In Int. Conf. Computer Science and Electronics Engineering (ICCSEE), 3, pp. 648-651.

9. Webera, R. H. 2010. Internet of Things  New security and privacy challenges. Computer Law & Security Review, 26, 1, (January 2010), pp. 23-30.