



# Securing the Internet of Things

Rodrigo Roman, Pablo Najera, and Javier Lopez, *University of Malaga, Spain*

**In the Internet of Things vision, every physical object has a virtual component that can produce and consume services. Such extreme interconnection will bring unprecedented convenience and economy, but it will also require novel approaches to ensure its safe and ethical use.**

In the Internet of Things (IoT), everything real becomes virtual, which means that each person and thing has a locatable, addressable, and readable counterpart on the Internet. These virtual entities can produce and consume services and collaborate toward a common goal. The user's phone knows about his physical and mental state through a network of devices that surround his body, so it can act on his behalf. The embedded system in a swimming pool can share its state with other virtual entities. With these characteristics, the IoT promises to extend "anywhere, anyhow, anytime" computing to "anything, anyone, any service."

Several significant obstacles remain to fulfill the IoT vision, chief among them security. The Internet and its users are already under continual attack, and a growing economy—replete with business models that undermine the Internet's ethical use—is fully focused on exploiting the current version's foundational weaknesses. This does not bode well for the IoT, which incorporates many constrained devices. Indeed, realizing the IoT vision is likely to spark novel and ingenious malicious models. The challenge is to prevent the growth of such models or at least to mitigate their impact.

Meeting this challenge requires understanding the characteristics of things and the technologies that empower the IoT. Mobile applications are already intensifying users' interaction with the environment, and researchers have made considerable progress in developing sensory devices to provide myriad dimensions of information to enrich the user experience.

However, without strong security foundations, attacks and malfunctions in the IoT will outweigh any of its benefits. Traditional protection mechanisms—lightweight cryptography, secure protocols, and privacy assurance—are not enough. Rather, researchers must discover the full extent of specific and often novel obstacles. They must analyze current security protocols and mechanisms and decide if such approaches are worth integrating into the IoT as is or if adaptations or entirely new designs will better accomplish security goals.

The proper legal and technical framework is also essential. To establish it, analysts must thoroughly understand the risks associated with various IoT scenarios, such as air travel, which has many interrelated elements, including safety, privacy, and economy.<sup>1</sup> Only then is it possible to justify the cost of developing security and privacy mechanisms.

All these requirements underline some critical first steps in successfully implementing IoT security measures: understand the IoT conceptually, evaluate Internet security's current state, and explore how to move from solutions that meet current requirements and constraints to those that can reasonably assure a secure IoT.

## INFRASTRUCTURE SEEDS

The "Objects in a Superconnected World" sidebar describes some of the characteristics of the things in the

## OBJECTS IN A SUPERCONNECTED WORLD

Since the IoT's inception, governments and other organizations have tried to capture its essence in words, some more successfully than others.<sup>1</sup> In a nutshell, the IoT is a worldwide network of interconnected objects. Each object that surrounds a person, from books and cars to appliances and food, has a virtual avatar that behaves as an active entity. In this context, all IoT objects have five main characteristics:

**Existence.** Things, such as a car, exist in the physical world, but specific technologies, such as an embedded communication device, enable the existence of a thing's virtual personas.

**Sense of self.** All things have, either implicitly or explicitly, an identity that describes them, such as car, Porsche, or license plate number. Objects can process information, make decisions, and behave autonomously.

**Connectivity.** Things can initiate communication with other entities. As a result, both an element in their surroundings and a remote entity can locate and access them.

**Interactivity.** Things can interoperate and collaborate with a wide range of heterogeneous entities, whether human or machine, real or virtual. As such they produce and consume a wide variety of services.

**Dynamicity.** Things can interact with other things at any time, any place, and in any way. They can enter and leave the network at will, need not be limited to a single physical location, and can use a range of interface types.

An optional sixth characteristic is environmental awareness. Sensors might enable a thing to perceive physical and virtual data about its environment, such as water radiation or network overhead. This characteristic is optional because not all things will exhibit it, such as an object enhanced with a lower-end radio frequency identification (RFID) tag.

The combination of various technologies has enabled objects to exhibit these characteristics, allowing them to become virtual beings. Energy-efficient microcontrollers act as brains, imbuing objects with embedded intelligence. Sensor technology provides

objects with sensory receptors, and RFID provides a way for them to distinguish one another, much like people recognize a face. Finally, low-energy wireless technology, such as specified in IEEE 802.15.4, supplies the virtual counterparts of voice and hearing.

Multiple applications already use these and other technologies, such as machine-to-machine communication, virtual worlds, and robotics. To be a virtual being, an IoT object needs only enough technology to realize its role and complete its mission. A tire can simply provide information about itself and its state, but a car will be much more technologically complex because it must be aware of its surroundings as well as its own state.

RFID in pharmaceutical environments, location-aware mobile applications, and smart metering systems are all essentially "intranets of things," in which objects are isolated from those in other scenarios and domains. IoT applications will have greater scope and flexibility, being able to interact not only with objects in other scenarios and domains but also with real and virtual entities.

Figure A shows an application involving a smart meter with current capabilities—an intranet-of-things scenario—and a smart meter as part of the IoT.

Another example is weather stations, which will send anonymous queries to pedestrians' personal networks to create a city temperature and humidity map that business owners can integrate with other data to decide the best place to build an ice cream shop. Likewise, virtual supermarket goods will interact with a clerk to notify him of a strawberry yogurt shortage; with a potentially allergic shopper to provide her with ingredient information; and with third-party applications, such as event planners, to reveal if the shopper's friends like strawberry yogurt.<sup>2</sup>

At present, only partial IoT instances exist, mainly those that provide information services through centralized systems and interfaces. These IoT application forerunners hint at the possible benefits of a full-blown IoT and can serve as foundational elements for building this new virtual world. New companies are providing a centralized interface to access raw sensor data worldwide. Such data can help launch an IoT application. The personal network paradigm is another example of a partial instance. Local entities, such as wearable objects, interact indirectly with external services, such as a fitness monitor, through a central server such as a smartphone. In this way, users and their objects interact with their environment, deciding what data they want to share and with whom. These and similar applications are a start, but to attain the IoT's full benefits, work must continue.

These and similar applications are a start, but to attain the IoT's full benefits, work must continue.

## References

1. H. Sundmaeker et al., eds., "Vision and Challenges for Realizing the Internet of Things," *IoT European Research Cluster*, Mar. 2010; [www.internet-of-things-research.eu](http://www.internet-of-things-research.eu).
2. E. Fleisch, "What Is the Internet of Things? An Economic Perspective," white paper, WP-BIZAPP-053, AutoID Labs, Jan. 2010; [www.autoidlabs.org](http://www.autoidlabs.org).

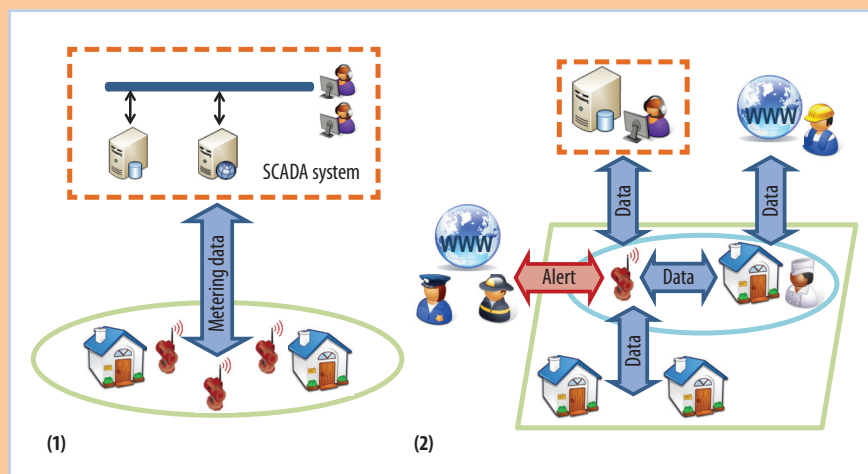


Figure A. A smart meter application in two scenarios. (1) In the intranet-of-things scenario, the meter interacts only with the supervisory control and data acquisition (SCADA) system. (2) In the IoT scenario, the meter interacts with the SCADA system, household members, other houses, and emergency personnel.

envisioned IoT and some existing applications that are arguably partial IoT instances. The path to the IoT is not a single step; rather it is the gradual incorporation of IoT applications into the real world, which involves giving objects virtual personas and thinking outside the box. For example, researchers could enhance fishing vessels with sensors and communication systems that offer shared services about the state of the sea and other facets. Objects that belong to a virtual world can be made aware of objects outside that world—including the services that other objects and entities provide. Sensors that monitor agricultural fields can access weather reports for the area and adapt the irrigation systems accordingly. Developers can also decrease system dependence on a centralized architecture, creating autonomous applications. Mobile phones without Internet connection in a disaster area can collaborate to propagate the location of a sensor-enabled water source.



**Traditional public-key infrastructures will almost certainly not scale to accommodate the IoT's amalgam of contexts and devices.**

With this staggered approach, society might be able to enjoy IoT's benefits, while analysts and researchers tackle the infrastructure complexities. The problems will be both technical and semantic, requiring interoperable mechanisms that can connect entities as well as help them understand each other. Distributed services must be reliable, not only offering availability but also adapting themselves in case of malfunction. A governance model must scale to billions of devices all over the world. Within these metachallenges are issues such as bootstrapping, mobility, scalability, data processing, standardization, and billing.

### **COPING WITH OLD AND NEW THREATS**

Not surprisingly, even a staggered approach to developing the IoT presents a daunting task for security. What protection measures are possible as billions of intelligent things cooperate with other real and virtual entities in random and unpredictable ways? The IoT's highly distributed nature and use of fragile technologies, such as limited-function embedded devices in public areas, create weak links that malicious entities can exploit. Easily accessible objects in unprotected zones, such as city streets, are vulnerable to physical harm. Like compromising botnets, some objects would try to hinder services from the inside. Additional threats include the existence of a domino effect between intertwined services and user profiling through data collection and other methods.

To avoid these threats, the IoT must have strong security foundations built on a holistic view of security for all IoT elements at all stages—from object identification to service provision, from data acquisition to infrastructure governance, all security mechanisms must consider each object's life cycle and services from the very beginning of that object's existence.

### **Protocol and network security**

Heterogeneity greatly affects the degree of infrastructure protection. Highly constrained devices that use low-bandwidth standards, such as IEEE 802.15.4, must open a secure communication channel with more powerful devices—for example, sensor nodes scattered in a smart city would communicate with smartphones or PDAs. Securing this channel requires optimal cryptography algorithms and adequate key-management systems, as well as security protocols that connect all these devices through the Internet. Although it is not clear how many resources will be available to such constrained devices once the IoT truly takes off, it makes sense to optimize security as much as possible to improve future service provision.

In a bottom-up approach, cryptography is the cornerstone for network infrastructure protection. Although standards such as AES might work for some IoT devices, others, such as passive RFID tags, might be extremely constrained. Cryptographic mechanisms must be smaller and faster but with little or no reduction in security level. Mechanisms could include symmetric algorithms, hash functions, and random number generators.

In this approach, if cryptography is the brick, the mortar is key-management infrastructures that establish keying material, for example, shared secret keys. Making this mortar requires associating previously unrelated and sometimes highly constrained objects in an extremely dynamic environment. Manual configuration works only in small and personal environments, and traditional public-key infrastructures will almost certainly not scale to accommodate the IoT's amalgam of contexts and devices. There is also the issue of rekeying devices to keep information flow safe in the long run.


Further up the network infrastructure are the communication layers. Clearly, the IoT must extensively use Internet standards for communication and service provision. Still, some devices, such as sensors that check the state of runway lights, will lack the resources to implement the Internet security mechanisms that normally protect these kinds of interactions. Therefore, security protocols require some forward-looking adaptation. Subtle differences between IoT and Internet protocols might lead to gaps in end-to-end security. Thus, adaptations should not only fulfill the IoT's performance requirements but also provide the protocol's original security properties in the context of the Internet architecture.<sup>2</sup>

## Data and privacy

Privacy is one of the most sensitive subjects in any discussion of IoT protection. The data availability explosion has created Big Brother-like entities that profile and track users without their consent. The IoT's anywhere, anything, anytime nature could easily turn such practices into a dystopia. Users would have access to an unprecedented number of personalized services, all of which would generate considerable data, and the environment itself would be able to acquire information about users automatically.

Although a dystopia is the worst-case scenario, the IoT could certainly exacerbate a range of undesirable situations. Facebook accounts already affect a user's employability and personal interactions. Imagine exponentially more such exposure opportunities.

**Privacy by design.** One viable solution is privacy by design, in which users would have the tools they need to manage their own data. The solution is not too far from current reality. Whenever users produce a data fragment,



**As developers create a worldwide object network, they must build an infrastructure that allows mutual object authentication.**

they can already use dynamic consent tools that permit certain services to access as little or as much of that data as desired. Taking that idea a step further, a user in Central Park could provide a location-based service with the information that he's in New York City, but not that he's in a specific park.

**Transparency.** Transparency is also essential, since users should know which entities are managing their data and how and when those entities are using it. Stakeholders such as service providers must be part of this equation, which might make take-it-or-leave-it license agreements obsolete. Businesses will adjust their services according to the amount of personal data the user provides.

**Data management.** A huge issue is deciding who manages the secrets. Technically, cryptographic mechanisms and protocols protect data throughout the service's life cycle, but some entities might lack the resources to manage such mechanisms. In other words, one data management policy will not fit all situations. Consequently, there must be policies on how to manage various kinds of data as well as some policy-enforcement mechanism. Developing and enforcing such data management policies is not trivial. It requires interpreting, translating, and optimally reconciling a series of rules, each of which might be in a different language. And any policies must align with legislation on data protection, which itself could change.

## Identity management

In the IoT, identity management requires considering a staggering variety of identity and relationship types, all of which must follow four object identity principles:

- An object's identity is not the same as the identity of its underlying mechanisms. The x-ray machine in the radiology department might have an IP address, but it should also have its own identity to distinguish it from other machines.
- An object can have one core identity and several temporary identities that change according to its role. A hospital is always a hospital, but it can temporarily be more significant as a conference locale or a shelter.
- An object can identify itself using its identity or its specific features. A food's virtual identity is defined by its ingredients and quantity.
- Objects know the identity of their owners. The device that controls a user's glucose level should know how that information fits in that user's overall health.

Objects can also be in groups, which some mechanism must manage. A house could have several appliances that only certain residents and visitors can use at particular times. The refrigerator could lock itself after midnight to any resident or visiting teenagers, but remain open for the adults.

Proving identity is an important part of identity management. As developers create a worldwide object network, they must build an infrastructure that allows mutual object authentication. There must be a balance between centralized management and a distributed, hierarchical approach.

Mechanisms for anonymization and the creation of pseudonyms are also important building blocks. Because the IoT deals with multiple contexts, an entity is not likely to reveal its identity all the time. In a vehicular network, for example, a police car can reveal its identity to cars and staff at the police station, but keep its identity hidden during undercover work unless it is interacting with other police cars.

As these examples illustrate, identity management in the IoT offers both challenges and the opportunity to improve security. A promising approach is to combine diverse authentication methods for humans and machines. With this combination, a user could open an office door using bioidentification (such as a fingerprint) or an object within a personal network, such as a passport, identity card, or smartphone. Combining authentication methods can prevent any loss of overall system security. Such combinations typically take the form of what I am + what I know or what I have + what I know.

Authorization is also an identity management concern. Authentication and authorization share open research issues, such as finding a balance between centralized and

distributed systems to answer the question of who's in charge of defining and publishing roles. However, specific topics, such as delegation, fall mainly under the authorization umbrella. An IoT element can delegate certain tasks to other objects for a limited time. For example, an object in the user's personal network, such as his phone, can check on his behalf to see if his suitcase contains all the needed clothes for an upcoming conference.

Granularity is another authorization issue. The services that an object provides would depend on the number of credentials presented. For example, a classroom could provide anyone who asks with the name of the course being taught, but it would release the syllabus of that course only to students with authorization certificates from the dean.

### Trust and governance

Trust is essential to implement the IoT. In this context, trust is more than the mechanisms that reduce the uncertainty of objects as they interact, although such mechanisms are important in helping objects choose



**Although governance offers stability, support for political decisions, and a fair enforcement mechanism, it can easily become excessive.**

an adequate partner for their needs. In the IoT, such mechanisms must be able to define trust in a dynamic, collaborative environment and understand what it means to provide trust throughout an interaction.

But trust also encompasses how users feel while interacting in the IoT. Feelings of helplessness and being under some unknown external control can greatly undermine the deployment of IoT-based applications and services. There must be support for controlling the state of the virtual world. Users must be able to control their own services, and they must have tools that accurately describe all their interactions so that they can form an accurate mental map of their virtual surroundings.

Governance will help strengthen trust in the IoT. A common framework for security policies will support interoperability and ensure security's continuity. Defining adequate enforcement mechanisms will go a long way toward simplifying data protection.

A governance framework can also help reduce liability. If someone can attribute a malicious action to a particular user or agent, it will be possible to punish that user or the agent's owner. But governance is a double-edged sword. On the one hand, it offers stability, support for political decisions, and a fair enforcement mechanism. On the other hand, it can easily become excessive, fostering an environment in which people are continuously monitored and

controlled. If the current Internet's partially solved governance problem is any indication, it will take the combined efforts of several research communities to address the challenges of a governance framework when countless stakeholders and billions of objects join the mix.

### Fault tolerance

Clearly, the IoT will be more susceptible to attack than the current Internet, since billions more devices will be producing and consuming services. Highly constrained devices will be the most vulnerable, and malicious entities will seek to control at least some devices either directly or indirectly. In this context, fault tolerance is indispensable to assure service reliability, but any solution must be specialized and lightweight to account for the number of constrained and easily accessible IoT devices.

Achieving fault tolerance in the IoT will require three cooperative efforts. The first is to make all objects secure by default. Aside from designing secure protocols and mechanisms, researchers must work on improving software implementation quality, since it might not be feasible to provide a software patch for billions of devices.

The second effort is to give all IoT objects the ability to know the state of the network and its services. This system would need to give feedback to many other elements; for example, a watchdog system could acquire data as part of supplying qualitative and quantitative security metrics. An important task in this second effort is to build an accountability system that will help monitor state.

Finally, objects should be able to defend themselves against network failures and attacks. All protocols should incorporate mechanisms that respond to abnormal situations and let the object gracefully degrade its service. Objects should be able to use intrusion-detection systems and other defensive mechanisms to ward off attackers.

Once an attack affects their services, IoT elements should be able to act quickly to recover from any damage. Such elements can use feedback from other mechanisms and IoT entities to map the location of unsafe zones, where an attack has caused service outages, as well as trusted zones—areas with no service outages. Such information can be the basis for implementing various recovery services, such as having objects access trusted zone services first. Mechanisms could also inform human operators of any damaged zone and then perform maintenance operations. This infrastructure self-management is a key IoT tenet.

### WORK IN PROGRESS

Researchers, governments, and industries are committed to developing and standardizing identity and security mechanisms for IoT building blocks. Table 1 lists some of the more mature efforts, excluding work-in-progress standards and government recommendations such as EU

**Table 1. Standards for IoT technologies.**

Standard	Purpose	Security	URL
ISO/IEC 14443	Architecture for contactless proximity cards	Information flow protection (AES)	<a href="http://www.iso.org/iso/identification_cards.html">www.iso.org/iso/identification_cards.html</a>
IEC 62591 (WirelessHART)	Protocol for industrial wireless sensor networks	Encryption, authentication, key management	<a href="http://www.hartcomm.org">www.hartcomm.org</a>
GS1 keys	Identification system	Unique identifier definition	<a href="http://www.gs1.org/gsmp/kc/epcglobal">www.gs1.org/gsmp/kc/epcglobal</a>
uicode	Hardware-agnostic identifier	Unique identifier definition	<a href="http://www.uidcenter.org">www.uidcenter.org</a>

**Table 2. IETF standards that might be implemented in the IoT.**

Standard	Purpose	URL
6LowPAN	IP connectivity	<a href="http://datatracker.ietf.org/wg/6lowpan">http://datatracker.ietf.org/wg/6lowpan</a>
ROLL	IP connectivity	<a href="http://datatracker.ietf.org/wg/roll">http://datatracker.ietf.org/wg/roll</a>
CoRE	Lightweight REST Web service architecture	<a href="http://datatracker.ietf.org/wg/core">http://datatracker.ietf.org/wg/core</a>
CoAP	Generic Web protocol definition	<a href="http://datatracker.ietf.org/wg/core">http://datatracker.ietf.org/wg/core</a>

recommendation C(2009) 3200.

Although these standards and mechanisms are good first steps, much additional work is required to build a robust and secure IoT. Again, a holistic view is vital: it is important to protect the IoT's building blocks, but its features create new requirements that are equally significant.

The design of specific security IoT mechanisms is still in its infancy, but recent developments are encouraging and could provide some degree of protection to existing IoT applications, such as the different instances of the IBM Smarter Planet initiative ([www.ibm.com/smarterplanet/us/en/?ca=v\\_smarterplanet](http://www.ibm.com/smarterplanet/us/en/?ca=v_smarterplanet)) or ventures such as Pachube (<https://pachube.com>) and Arrayent (<http://arrayent.com>).

### Cryptography and protocols

Researchers are already making strides toward developing better cryptographic algorithms and modes for IoT devices. The ISO/IEC 29192 standards aim to provide lightweight cryptography for constrained devices, including block and stream ciphers and asymmetric mechanisms. As of August 2011, these standards were still under development, but some algorithms are available. Sony's CLEFIA is a novel block cipher that supports 128-bit keys ([www.sony.net/Products/cryptography/clefi/about/index.html](http://www.sony.net/Products/cryptography/clefi/about/index.html)). The eSTREAM project ([www.ecrypt.eu.org/stream](http://www.ecrypt.eu.org/stream)) studied the robustness of stream ciphers such as Salsa20/12 and Trivium, which are extremely useful in embedded systems.

Research on lightweight dedicated hash functions has just started. The winner of the SHA-3 competition—scheduled to finish in late 2012—should lay the foundation for more work on a new class of hash functions for long-term security. The competition's goal is to develop a new cryptographic hash algorithm that converts a variable-length

message into a short message digest. The digest will be part of generating digital signatures, message authentication codes, and many other security applications in the information infrastructure (<http://csrc.nist.gov/groups/ST/hash/sha-3/index.html>).

It is already possible to construct lightweight hash functions based on lightweight block ciphers. As an alternative to these lightweight algorithms, existing optimizations in operational modes can make data processing more efficient. Both AES-CCM and AES-GCM offer data integrity and confidentiality. Another optimization is algorithm management in a cross-layer architecture, where various security mechanisms share one algorithm.<sup>3</sup>

Other communities, such as the Internet Engineering Task Force, aim to implement Internet standards in the IoT. Table 2 lists these standards and their purpose.

Although researchers have met some interim implementation goals, various constraints make it difficult to fully achieve security through Internet standards.<sup>2</sup> Developers can tweak the IPsec protocol to provide network-layer security between Internet hosts and constrained devices,<sup>4</sup> but the remaining challenges are formidable. It will be no small task to deal with the coexistence of strong link-layer security and IPsec, for example, or the negotiation of keying material. Preshared keys are usable with previously known devices, and public-key cryptography is useful when the constrained object behaves as a client,<sup>5</sup> but the negotiation of dynamic keys between previously unknown entities is still an open problem.

### Identity and ownership

In certain IoT contexts, single-sign-on (SSO) mechanisms can be useful, since users need to authenticate only once to interact with various devices. However, traditional

Web 2.0 SSO (openID and Shibboleth, for example) were not designed to fulfill certain IoT requirements,<sup>6</sup> such as giving the user control over the choice of identity provider. Other mechanisms force users to employ a particular protocol, which can be problematic in a heterogeneous environment. Another issue is the lack of support for directional identities, in which objects broadcast their identities.

These issues strongly imply the need to adapt existing SSO mechanisms or create new ones that better fit the IoT. Although some approaches address this need through a hybrid architecture that combines all mechanisms through specially crafted middleware,<sup>6</sup> this topic still needs research.

One approach to verifying device ownership and owner identity is digital shadowing,<sup>7</sup> in which a user projects his virtual identity onto logical nodes. Digital shadows are based on the notion that a user's objects act on his behalf but do not store his identity, only a virtual identity that contains information about his attributes and the objects' sessions and interactions with the architecture. Therefore, digital shadows only implicitly indicate their owner's identity.

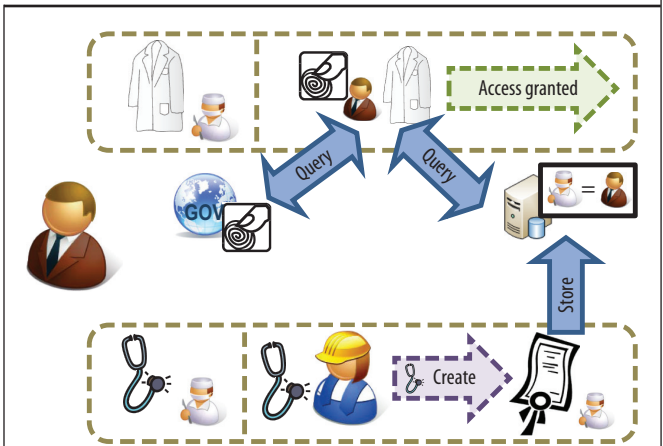
Figure 1 illustrates how digital shadowing might work with an electronic stethoscope and white coat. The doctor's fingerprints prompt a query to the government database, while his coat provides the digital shadow to the hospital database, which checks the doctor's role. Both authentication aspects (what I am + what I have) enable the doctor to enter a certain hospital area. The stethoscope records and stores the patient's heartbeats, signs the data on the doctor's behalf, and stores the data in the hospital database. The stethoscope can also check for any heartbeat anomalies by accessing other systems inside or outside the hospital.

The coat and fingerprint authentication scenario in Figure 1 might also benefit from revocable access delegation,<sup>8</sup> in which an RFID tag (the logical node) returns a valid ID (the virtual identity) only if the tag's owner has authorized the reader. These tags are essentially part of the user's digital shadow because they provide no user information (only a number), but any reader with explicit user authorization will know that they belong to that user. Because a tag's ID is not easy to link to its owner and the user can revoke authorization at any time, the digital shadow approach also accounts for privacy.

## Privacy protection

Various approaches are in development to protect the personal information of IoT users. The delegation mechanism is one privacy preservation proposal. An unauthorized RFID reader will retrieve only a random value, so it will not be able to track the user.

However, limited user access is not the only protection scenario. In some cases, users will want to provide information without revealing too much about themselves.



**Figure 1. Instances of digital shadowing for a doctor. The doctor's white coat and electronic stethoscope store his virtual identity and act on his behalf. (Top) The coat and the doctor's fingerprints are elements of an authentication method. (Bottom) As the doctor uses the stethoscope, it not only records and stores the patient's heartbeats, but also signs the data on the doctor's behalf and stores it in the hospital database.**

Some solutions in this context let the user find others who best match his preferences, without actually revealing such preferences to everyone. Other schemes let users maintain their location privacy even when making location-dependent queries.<sup>9</sup> For example, a user could try to locate someone nearby who likes Beethoven, without explicitly providing his own location and music preferences.

An interesting idea is the privacy coach,<sup>10</sup> in which an RFID reader in a mobile phone scans the tags embedded in some object, such as a loyalty card, and downloads the companion privacy policy. If the object's privacy policy does not match the user's preferences, the user can choose not to use the object. Conversely, whenever an RFID reader tries to read the mobile phone's signal, the phone can check the reader's privacy policy and ask for user consent. Finally, the privacy coach can protect the user's private physical space, such as a house, by scanning for malicious items or undesirable entities, such as objects left to monitor the house without the user's permission.<sup>11</sup>

**T**he IoT is already more than a concept. By complying with security requirements, it can fully bloom into a paradigm that will improve many aspects of daily life. Open problems remain in a number of areas, such as cryptographic mechanisms, network protocols, data and identity management, user privacy, self-management, and trusted architectures. Future research must also carefully consider the balance of governance and legal frameworks with innovation. Governance can

sometimes hinder innovation, but innovation in turn can inadvertently ignore human rights. The right balance will ensure stable progress toward realizing and securing the IoT as envisioned, and the benefits to humanity will be well worth the effort. **□**

## Acknowledgments

This work was partially supported by the European Union under the 7th Framework Programme for R&D (FP7) through the NESSOS (IST-256980) project and by the Spanish Ministry of Science and Innovation through the ARES (CSD2007-00004) and SPRINT (TIN2009-09237) projects. The latter is cofinanced by the European Regional Development Fund.

## References

1. B. Daskala, ed., *Flying 2.0—Enabling Automated Air Travel by Identifying and Addressing the Challenges of IoT & RFID Technology*, European Network and Information Security Agency, 2010; [www.enisa.europa.eu/media/press-releases/flying-2.0-study-of-internet-of-things-rfid-in-air-travel](http://www.enisa.europa.eu/media/press-releases/flying-2.0-study-of-internet-of-things-rfid-in-air-travel).
2. O. Garcia-Morchon et al., "Security Considerations in the IP-Based Internet of Things," IETF, Mar. 2011; <http://tools.ietf.org/html/draft-garcia-core-security>.
3. R. Roman, J. Lopez, and P. Najera, "A Cross-layer Approach for Integrating Security Mechanisms in Sensor Networks Architectures," *Wireless Comm. and Mobile Computing*, vol. 11, no. 2, 2011, pp. 267-276.
4. S. Raza, T. Voigt, and U. Roedig, "6LoWPAN Extension for IPsec," *Proc. Workshop Interconnecting Smart Objects with the Internet*, Internet Architecture Board, Mar. 2011; [www.iab.org/about/workshops/smartobjects](http://www.iab.org/about/workshops/smartobjects).
5. R. Roman et al., "Key Management Systems for Sensor Networks in the Context of the Internet of Things," *Computers & Electrical Eng.*, Mar. 2011, pp. 147-159.
6. H. Akram and M. Hoffmann, "Support for Identity Management in Ambient Environments—The Hydra Approach," *Proc. IEEE Int'l Conf. Advances in Human-Oriented and Personalized Mechanisms, Technologies, and Services (I-CENTRIC 08)*, IEEE CS Press, 2008, pp. 371-377.
7. A. Sarma and J. Girão, "Identities in the Future Internet of Things," *Wireless Personal Comm.*, Mar. 2009, pp. 353-363.
8. E. Rekleitis, P. Rizomiliotis, and S. Gritzalis, "A Holistic Approach to RFID Security and Privacy," *Proc. 1st Int'l Workshop Security of the Internet of Things (SecIoT 10)*, Network Information and Computer Security Laboratory, 2010; [www.nics.uma.es/seciot10/files/pdf/rekleitis\\_seciot10\\_paper.pdf](http://www.nics.uma.es/seciot10/files/pdf/rekleitis_seciot10_paper.pdf).
9. J. Sen, "Privacy Preservation Technologies in Internet of Things," *Proc. Int'l Conf. Emerging Trends in Mathematics, Technology, and Management*, 2011; <http://arxiv.org/ftp/arxiv/papers/1012/1012.2177.pdf>.
10. G. Broenink et al., "The Privacy Coach: Supporting Customer Privacy in the Internet of Things," *Proc. Workshop What Can the Internet of Things Do for the Citizen? (CIOT 2010)*; Radboud Univ., May 2010; <http://dare.ubn.ru.nl/bitstream/2066/83839/1/83839.pdf>.
11. S. Radomirovic, "Towards a Model for Security and Privacy in the Internet of Things," *Proc. 1st Int'l Workshop Security of the Internet of Things (SecIoT 10)*, Network Information and Computer Security Laboratory, 2010; [www.nics.uma.es/seciot10/files/pdf/radomirovic\\_seciot10\\_paper.pdf](http://www.nics.uma.es/seciot10/files/pdf/radomirovic_seciot10_paper.pdf).

**Rodrigo Roman** is a researcher at the University of Malaga, Spain. His research interests include Internet of Things security, sensor network security, and security architectures. Roman received a PhD in computer science from the University of Malaga. He is a member of IEEE. Contact him at [roman@lcc.uma.es](mailto:roman@lcc.uma.es).

**Pablo Najera** is a doctoral candidate in computer engineering at the University of Malaga. His research interests include personal area network security, RFID security, and integration of security technologies. Najera received an MS in computer science engineering from the University of Malaga. Contact him at [najera@lcc.uma.es](mailto:najera@lcc.uma.es).

**Javier Lopez** is a full professor in the Department of Computer Science at the University of Malaga and head of the Network, Information, and Computer Security Laboratory. His research interests include security services, the protection of critical information infrastructures, and computer communications security. Lopez received a PhD in computer science from the University of Malaga. He is a member of IEEE and the ACM. Contact him at [jl@lcc.uma.es](mailto:jl@lcc.uma.es).

# Call for Articles

## IEEE Pervasive Computing

seeks accessible, useful papers on the latest peer-reviewed developments in pervasive, mobile, and ubiquitous computing. Topics include hardware technology, software infrastructure, real-world sensing and interaction, human-computer interaction, and systems considerations, including deployment, scalability, security, and privacy.

### Author guidelines:

[www.computer.org/mc/pervasive/author.htm](http://www.computer.org/mc/pervasive/author.htm)

Further details:  
[pervasive@computer.org](mailto:pervasive@computer.org)  
[www.computer.org/pervasive](http://www.computer.org/pervasive)



Selected CS articles and columns are available for free at <http://ComputingNow.computer.org>.