Security Framework for RFID-based Applications in Smart Home Environment

Divyan M. Konidala*, Daeyoung Kim**, Chan Yeob Yeun***
and Byoungcheon Lee****

Abstract—The concept of Smart-Homes is becoming more and more popular. It is anticipated that Radio Frequency IDentification (RFID) technology will play a major role in such environments. We can find many previously proposed schemes that focus solely on: authentication between the RFID tags and readers, and user privacy protection from malicious readers. There has also been much talk of a very popular RFID application: a refrigerator/bookshelf that can scan and list out the details of its items on its display screen. Realizing such an application is not as straight forward as it seems to be, especially in securely deploying such RFID-based applications in a smart home environment. Therefore this paper describes some of the RFID-based applications that are applicable to smart home environments. We then identify their related privacy and security threats and security requirements and also propose a secure approach, where RFID-tagged consumer items, RFID-reader enabled appliances (e.g., refrigerators), and RFID-based applications would securely interact among one another. At the moment our approach is just a conceptual idea, but it sheds light on very important security issues related to RFID-based applications that are beneficial for consumers.

Keywords—RFID, Smart Home, Home Network System, Home Server, Secure RFID-Based Applications, RFID Reader-Enabled Devices, RFID Tagged Consumer Items, EPCglobal Architecture Framework

1. INTRODUCTION

In this section we briefly introduce the concept of Radio Frequency IDentification (RFID) technology, its usefulness to businesses and consumers, and its related standards.

1.1 RFID Technology

RFID [8] technology is a means to efficiently and quickly auto-identify objects and assets. RFID offers businesses an automated supply chain management system [9]. With RFID tech-

※ This work was published as an abstract in the proceedings of 2007 Symposium on Cryptography and Information Security. This work was supported by the ICT Standardization program of the Republic of Korea's MKE (The Ministry of Knowledge Economy).
Manuscript received August 6, 2010; accepted August 31, 2010.

Corresponding Author: Divyan M. Konidala
* Dept. of Information and Communications Engineering, Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Republic of Korea (divyan@kaist.ac.kr)
** Department of Computer Science, KAIST, (kimd@kaist.ac.kr)
*** Computer Engineering (Sharjah Campus), Khalifa University of Science, Technology & Research (KUSTAR), Sharjah, UAE (cyeun@kustar.ac.ae)
**** Dept. of Information Security, Joongbu University, Chungnam, Republic of Korea (sultan@joongbu.ac.kr)

nology, businesses attach Passive-RFID-Tags to their products/items. These tags are low-cost electronic labels that are resource constrained *e.g.*, up to 512 bytes of memory and 3K gates. These tags contain tiny computer chips with very small antennas and are powered-up by an RF signal from an RFID Reader. The tag's tiny chip stores a unique Electronic Product Code (EPC) number [1] that uniquely identifies the item to which it is attached, and this EPC number is automatically transmitted (without requiring line-of-sight scanning) to readers within the RF range (up to 10m for ultra high frequency passive-tags).

Further information associated with the item/EPC number (*e.g.*, item description, manufacturing date, packaging, shipments, item arrival and departure details, *etc.*) is captured and stored on a network of servers and databases, called EPC-Information Services (EPC-IS) [1]. The unique EPC number is like a universal resource locator (URL) directing the RFID reader to the right EPC-IS on the EPC Network from where the reader can download and upload data about the item it scanned. Therefore, RFID and EPC-IS assist geographically distributed supply-chain stakeholders (*e.g.*, manufacturers, distributors, retailers, *etc.*) with instantaneous item identification, and `real-time' updating, querying, accessing and sharing of item information such as, shipping and receiving, track and trace, theft detection, precise item recall *etc*.

1.1.1 RFID Technology Standards

The ISO 18000: Part 1-4, 6 and 7 standards describe the use of RFID for item management. We also have the EPCglobal Inc. [1], leading the development of industry-driven standards for the EPC to support RFID in supply chain management. The ISO 18000 Part 6C standard is in fact the EPCglobal's standard: “Class-1 Generation-2 (C1G2) Ultra High Frequency (UHF) RFID Protocol for Communications at 860MHz - 960MHz” [3]. This standard is for low-cost, passive-backscatter, interrogator-talks-first, RFID systems operating in the 860 MHz - 960 MHz frequency range. It specifies the physical interactions (the signaling layer of the communication link) between readers and tags, and Reader and tag operating procedures and commands.

While C1G2 UHF tags are suitable to tag cases and pallets, there is an ongoing debate among the supply chain stakeholders and RFID tag manufacturers whether to use high-frequency (HF) 13.56 MHz tags or UHF 915 MHz tags for item-level tagging. The former has a shorter read range but tends to perform better on items that cause RF interference. Still, advances in tag design are showing that UHF tags can be resilient to RF interference at close range to the interrogator, [4] claims that from items to pallets, C1G2 UHF tags are all we need. However, EPCglobal will develop its own HF standard. The memory structure, security and simplified command set used with the UHF C1G2 would be incorporated in an HF air-interface protocol to make it more useable and interoperable.

1.2 RFID Technology for Consumers

Due to the above-mentioned advantages of RFID technology, very soon it will become economical to tag products at the item level. We can certainly see large-scale use of tags on consumer goods. This would further lead to development and deployment of electronic appliances and devices that are RFID-reader-tag-enabled; as a result we can realize one of the visions of ubiquitous computing: an “Internet of Objects”, where devices and objects dispersed through our surroundings, can talk to each other, providing real-time information about themselves, their locations, and ambient conditions around them. RFID technology will have a tremendous impact on our society, once it starts to assist people in their daily lives.

1.2.1 Mobile-RFID Technology

With Mobile-RFID (mRFID) technology handheld portable devices like the mobile/smart phones, apart from having the usual voice/data communicating features, also behave as mRFID-readers and mRFID-tags. As a result, mRFID brings the RFID technology closer to consumers rather than just constraining its usage to supply chain management. With mRFID technology users can efficiently perform two major tasks, namely: download and view information represented by RFID tags, and machine-to-machine identification and communication.

Just by bringing an mRFID near a tagged object, we can quickly and easily query that tag's EPC number and by utilizing 3G/4G/Wi-Fi networks we can reach the appropriate EPC-IS and download information represented by that EPC number and view this information via our mobile device's display screen. With mRFID we can authenticate ourselves to another reader in order to access a particular facility (building, home) or services. We can carry out micro payments at subway stations, buses, newspaper stands and gas stations by bringing our mobile device near an RFID reader. We can give out information about our mobile device's model no. and size of its display screen, in-order to download and view suitable multimedia content from a multimedia kiosk.

Near Field Communication (NFC) [6] is a short-range high-frequency wireless connectivity standard (ISO/IEC 18092), which enables the exchange of data between devices when they are touched or waved within four centimeters of each other. NFC is a combination of the already existing proximity-card standard (ISO/IEC 14443, contactless RFID card) and a reader into a single chip, operating at 13.56 MHz and transferring data at up to 424 Kbits/second.

1.2.2 RFID Technology for Smart Homes

With RFID-reader-tag-enabled devices and appliances, consumers can make use of the RFID tags attached to their purchased items in their homes. For example, a display screen on an RFID Reader-enabled refrigerator can list out the details of all the RFID tagged items inside the refrigerator, such as item name, ingredients, manufacturing date, expiry date, *etc.* This example is just one of the many RFID-based applications that would very soon become common in a Smart Home environment.

In order to make life easier in many ways, and more entertaining, a smart home environment offers a ubiquitous home network system, where different information gadgets, home appliances and other Internet-based applications communicate with each other. Smart homes exchange information and commands among these networked devices via wired and wireless communications. A Home Server or a Home Gateway operating inside this environment is considered as possibly serving as the brain of this home network system. A home server supports all networking needs in the home, *e.g.,* interacting with the home telephone, stereo system, air-conditioning system, kitchen appliances, lights, blinds, and other network-enabled devices. It also connects the home's local area network to the Internet, which allows the home network to communicate with the external world for sending messages and communicating with the residents of the home. This communication makes it possible to program the smart home from inside or outside the house. In this paper we explore the possibilities of deploying RFID-based applications in a smart home environment and specifically focus on various related security issues and propose a security framework.

1.3 Contributions of this Paper

The following are the contributions of this paper:

- Introduce some of the practical example scenarios pertaining to RFID-based applications in smart home environments. Based on these example scenarios we derived their corresponding security threats and necessary security requirements.
- Propose a security framework that alleviates these derived threats. Our framework is just an outline of possible solutions to the security threats. The framework is built from a set of concepts linked to existing cryptographic methods and primitives.
- We composed this paper based on the following two standards: (i) EPCglobal Architecture Framework [2], (ii) EPCglobal C1G2 UHF RFID Protocol [3]. In this paper we assume that all the items are tagged with EPCglobal C1G2 UHF tags.

2. SHOPPING TAGGED CONSUMER ITEMS

Scenario I: *Alice visits a department store and purchases items that have RFID tags attached to them. She wants to utilize the RFID tags attached to these purchased items in her smart home environment. But while carrying these items to her home, she might be snooped upon by a thief, Charlie, who has a powerful RFID reader, using which, from a distance is able to scan the RFID tagged items inside Alice's bag, to check if she is carrying any items that are worth stealing. On the other hand, Alice may be carrying an RFID tagged MP3 player with her at all times and this tag has a unique EPC number. If Charlie happens to be a stalker, he can track and trace Alice at different locations based on this unique EPC number. Therefore consumers carrying RFID tagged items have to be protected from both Information and Location privacy violation.*

2.1 Protecting Consumer Privacy

2.1.1 Killing the Tag

As per the EPCglobal C1G2 UHF RFID Protocol standard [3], the manufacturer of the items can embed C1G2 UHF Tags with a Kill Password. Whenever an RFID reader sends this kill password to the tag, the tag is killed and rendered permanently unusable and unreadable. Therefore, once a tagged item is purchased by Alice, the trustable clerk at the point-of-sale (cashier) can obtain the tag's kill password from the store's EPC-IS and kill the tag permanently. But with this approach Alice cannot make use of the tag capabilities at her smart home environment, *e.g.,* RFID enabled refrigerator or book shelf.

2.1.2 Locking the Tag

As per the EPCglobal C1G2 UHF RFID Protocol standard [3], the manufacturer of the items can also embed C1G2 UHF Tags with a unique 32-bit value Access Password. An RFID reader submits the access password to the tag and the tag verifies if this access password is the same as the one embedded within itself. If the access passwords tally, the tag allows the reader to perform on it, the mandatory commands such as Read, Write, and Lock. A tag's chip has four memory banks: Reserved, EPC, TID, and User. The Reserved memory bank is used to store the kill password and access password. The reserved memory bank is permanently locked by the manufacturer; as a result the access password can neither be read nor modified by any reader.

As mentioned above, most of the tags contain only its unique EPC number and all the data associated with that EPC number is stored with the EPC-IS. Access to the EPC-IS is secure, and restricted to only authorized supply chain stakeholders. Generally, the EPC memory bank is never locked, because the EPC number is used to retrieve the data associated with that item and also to retrieve its corresponding access password (from EPC-IS). The tag's access password is thus used for "reader to tag" authentication and also allows the reader to access the locked memory banks within the tag, permission to change the lock status of the memory banks (except the reserved memory bank), and write data into the tag, *etc*.

Based on the above-mentioned access password and locking features available with C1G2 UHF tags, we propose the following approach, where the tag need not be killed permanently in order to protect consumer privacy. Once a tagged item is purchased by Alice, the trustable clerk at the point-of-sale can retrieve the tag's access password from the store's EPC-IS and using this access password, the clerk can lock all the memory banks of the tag including the EPC memory bank. Alice can download and store the EPC numbers and their corresponding access passwords into her mobile/smart phone. This can be made possible via the mRFID-enabled mobile/smart phone communicating with the mRFID-module at the point-of-sale. With this proposed approach, Charlie, the potential thief can no longer get any information (including the EPC number) from the RFID tags that are in Alice’s possession, as all the memory banks of the tags are locked and Charlie does not have the access passwords.

Ari Juels [7] summarized many previously proposed security models for tag-reader mutual authentication, which allow the tag to respond to only authorized and genuine readers. But unlike these models, the main advantage of our proposed approach is that it does not require implementation of any special cryptographic functions/keys within the tag. There is also no need for the tag and the reader to synchronize security keys/hash values. Just by locking the EPC memory bank we protect consumer privacy.

3. Interacting with Smart Home Environments

Scenario II: *After purchasing the RFID tagged items from the store, the point-of-sale terminal allows Alice to download and store the EPC numbers and their corresponding access passwords into her mRFID-enabled mobile/smart phone. Alice uses her smartphone’s 3G/4G/Wi-FI network to establish an HTTPS (Hypertext Transfer Protocol Secure) connection [5] with her home server, in order to send the EPC numbers and their access passwords. Based on the EPC numbers, the home server identifies the appropriate EPC-IS and uses the access passwords as proof of purchase, downloads the related information (product description, size, weight, manufacturing date, expiry date, directions to use, ingredients, warranty certificate, etc.) associated with the EPC numbers. The EPC-IS must provide only the information, which is relevant to the consumer who purchased the items. Therefore, by the time Alice reaches her home with the purchased tagged items, the home server is ready with all the information about the items.*

3.1 Secure Communication between mRFID-Smartphones and Home Servers

Alice's mRFID-enabled smartphone can establish an HTTPS connection with the home server, before sending the EPC numbers and their corresponding access passwords as shown in Fig.1. Otherwise the communication channel between the smartphone and the home server can be easily compromised, and prone to man-in-the-middle attacks, replay attacks, data manipulation and corruption. An HTTPS communication uses cryptographic tunneling protocols to provide the intended confidentiality (preventing snooping and Packet sniffing), sender authentication (preventing identity spoofing), and message integrity (preventing message alteration) to achieve privacy. When properly chosen, implemented, and used, such techniques can provide secure communications over unsecured networks.

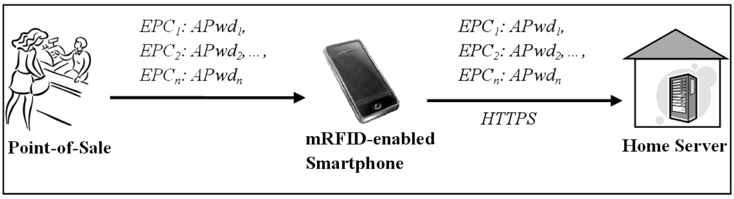

Fig. 1. Secure Communication between mRFID-Smartphones and Home Servers

3.2 Secure Communication between Home Servers and EPC-IS

After obtaining the EPC numbers from Alice's smartphone, the home server now needs to contact the appropriate EPC-IS to download the related information associated with the EPC numbers. As per the EPCglobal Architecture Specification [2], there exists an Object Naming Service (ONS), which can assist the home server in locating the EPC-IS. The ONS provides a global lookup service to translate an EPC number into one or more Internet Uniform Reference Locators (URLs) where further information on the item may be found. The Root ONS provides the initial point of contact for ONS lookups. In most cases, the Root ONS delegates the remainder of the lookup operation to a Local ONS, which is within the control of the enterprise. The home server establishes an HTTPS connection with the EPC-IS, before sending the EPC numbers and their corresponding access passwords as shown in Fig. 2.

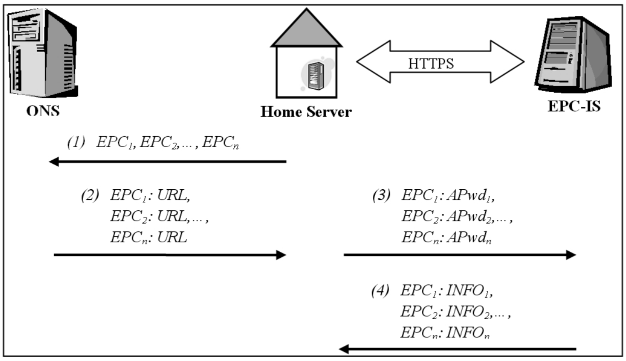

Fig. 2. Secure Communication between Home Servers and EPC-IS

The clerk at the point-of-sale gives away the access passwords to only those consumers who purchased the tagged items. The EPC-IS already has the list of EPC numbers and their corresponding access passwords, therefore when the home server sends the access passwords to the EPC-IS it proves that Alice/home server indeed purchased the tagged items.

***Scenario III**: Alice stores the tagged items in the RFID Reader-enabled refrigerator. The RFID reader in the refrigerator realizes that some of the tagged items are not responding with their EPC numbers, which means that these are newly added items and their memory banks are all locked. The RFID reader securely communicates with the home server to retrieve the access passwords and unlocks the tags' memory banks. Whenever Alice requests a listing of the items in the refrigerator, the RFID reader in the refrigerator collects all the EPC numbers from the tags and sends them to the home server. The home server retrieves the information associated with these EPC numbers and displays the same on the refrigerator's display screen.*

3.3 Secure Communication: RFID Reader-enabled Appliances & Home Servers

RFID Reader-enabled appliances (*e.g.,* refrigerator) must identify, authenticate and establish HTTPS connection with the home server. We should also consider threats in which a malicious powerful RFID reader positioned outside the smart home might impersonate a genuine RFID reader-enabled appliance inside the home. Therefore, whenever a new RFID reader-enabled appliance/device is brought into the house, the home server would need to generate a private key and a public-key certificate for that appliance. Alice would then configure the appliance with its private key and public-key certificate and also install the public-key certificate of the home server, in order for the appliance and the home server to successfully establish HTTPS communication. This approach is depicted in Fig. 3.

As mentioned in scenario III, the RFID reader in the refrigerator does not get any EPC numbers from the newly added items in the refrigerator as their memory banks are all locked. In such a situation, the RFID reader communicates with the home server and requests all the RFID tag access passwords that have been downloaded by the server (from EPC-IS) but not yet activated in the smart home. The home server then sends all those access passwords (which must be few

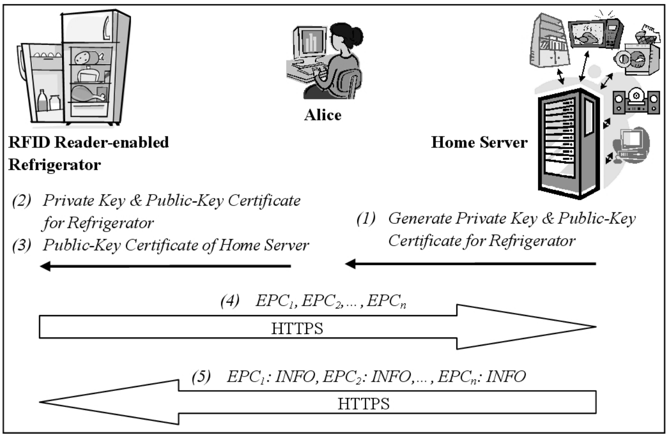
Alice
RFID Reader-enabled Refrigerator
Home Server
(2) Private Key & Public-Key Certificate for Refrigerator
(3) Public-Key Certificate of Home Server
(1) Generate Private Key & Public-Key Certificate for Refrigerator
(4) $EPC_1, EPC_2, \ldots, EPC_n$
HTTPS
(5) EPC_1: INFO, EPC_2: INFO,..., EPC_n: INFO
HTTPS

Fig. 3. RFID Reader-enabled Appliance Configuring Process

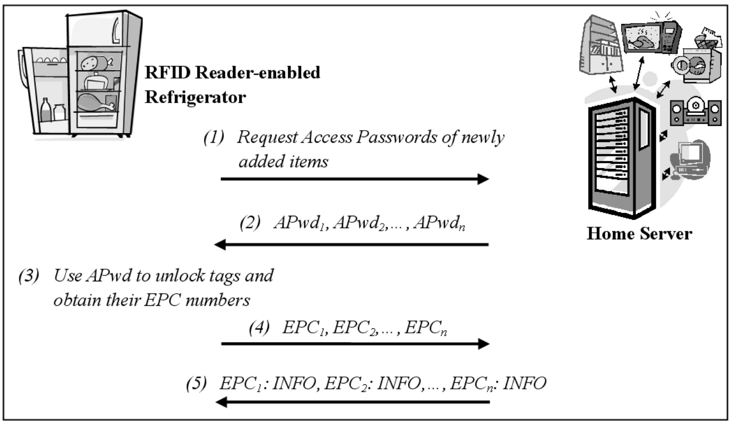
RFID Reader-enabled Refrigerator
(1) Request Access Passwords of newly added items
(2) $APwd_1, APwd_2, \ldots, APwd_n$
Home Server
(3) Use APwd to unlock tags and obtain their EPC numbers
(4) $EPC_1, EPC_2, \ldots, EPC_n$
(5) EPC_1: INFO, EPC_2: INFO, ..., EPC_n: INFO

Fig. 4. Unlocking RFID tags using an RFID Reader-enabled Device

in number) to the RFID reader in the refrigerator and the reader checks each of these passwords with every locked tag until a particular tag responds with its EPC number. With this approach a tag can be unlocked without knowing its EPC number initially. This approach can be easily understood by looking at the Fig. 4.

Scenario IV: *Alice has an RFID reader-enabled refrigerator, which stores many tagged items. All these tagged items emit their EPC number when queried by the RFID reader inside the refrigerator. But this poses a threat, where a malicious powerful RFID reader positioned outside the smart home, may be able to query the tagged items in the refrigerator and retrieve their EPC numbers. Then the malicious reader may communicate with the EPC-IS and retrieve information associated with these EPC numbers. This leads to privacy violation.*

3.4 Protecting Smart Home Residents' Privacy

To elliminate the above mentioned problem, we propose the following approach: Once the RFID reader in the refrigerator unlocks the tags, it can assign a different unique tag ID (pseudonym) and write this pseudo ID into the User memory bank of the tag. After which, with the exception of the user memory bank, the RFID reader must also lock all the other memory banks including the EPC memory bank. The reader notifies the home server of the new pseudo ID which maintains the reference between the EPC number and its new pseudo ID number. From then on whenever the RFID reader inside the refrigerator queries the tags in the refrigerator, they all respond with their new pseudo IDs which are completely different from their original EPC numbers. And only this new pseudo ID will be used in the smart home environment. Even if a malicious RFID reader gets these unique pseudo IDs he cannot obtain any information by sending pseudo IDs to the EPC-IS, as the EPC-IS will have no knowledge of these new pseudo IDs.

4. Conclusion

In this paper we considered various RFID-based application scenarios that are suitable for Smart Home environments. Based on these scenarios we identified some of the security and privacy threats. We identified the needs for protecting consumer privacy and proposed a "Locking the Tag" approach. We also proposed security measures to provide authentication, data confidentiality, and data integrity between the following communicating entities: the consumer's mobile RFID-enabled smartphone, home server, Electronic Product Code – Information Services and the RFID Reader-enabled household appliances and devices. We are confident that this conceptual idea can become a seed for further research and efficient modifications or improvements. Our future work includes practical implementation and thorough performance analyses.

REFERENCES

[1] *EPCglobal Inc.*, http://www.EPCglobalinc.org

[2] *EPCglobal Ratified Specification*, “The EPCglobal Architecture Framework,” 2009. http://www.epcglobalinc.org/standards/

[3] EPCglobal Ratified Standard, “EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860MHz - 960MHz Version 1.2.0,” 2008. http://www.epcglobalinc.org/standards/

[4] *Impinj RFID Technology Series Whitepaper*, “UHF Gen 2 for Item-Level Tagging,” REV 1.0 02-06, February 2006, http://www.impinj.com/files/MR_GP_ED_00003_ILT.pdf

[5] *Internet Engineering Task Force (IETF), Network Working Group, and E. Rescorla*, “HTTP Over TLS,” RFC2818, http://tools.ietf.org/html/rfc2818, 2000.

[6] *ISO/IEC 18092*, “Near Field Communication Interface and Protocol (NFCIP-1),” http://www.iso.org/iso/catalogue_detail.htm?csnumber=38578

[7] Juels, A. (2005), *RFID Security and Privacy: A Research Survey*, RSA Laboratories.

[8] Klaus, F., *RFID Handbook - Fundamentals and Applications in Contactless Smart Cards and Identification,*, 2nd Edition, John Wiley & Sons, 2003, ISBN-13: 978-0470844021.

[9] VeriSign, *The EPCglobal Network: Enhancing the Supply Chain*, White Paper 2005, http://www.verisign.com/stellent/groups/public/documents/white_paper/002109.pdf

Divyan M. Konidala

Divyan M. Konidala received the B.E. degree in Computer Science engineering from Bangalore University, India, in 2000 and the M.S. degree in the School of Engineering from the Information and Communications University [now merged with Korea Advanced Institute of Science and Technology (KAIST)], Korea, in 2004. He received the Ph.D. degree in Information and Communications Engineering, KAIST, Korea, in 2011. He was the graduate research assistant at the Auto-ID Labs Korea from 2006 to 2010. His research interests include: Secure and privacy-preserving (cryptographic) protocols for: RFID, mobile-RFID, ubiquitous computing applications, location-based services, and mobile payments. Light-weight cryptology, block/stream ciphers, and digital signatures. GS1 EPCglobal RFID Specification Development–UHF Gen 2.

Daeyoung Kim

Daeyoung Kim received the BS and MS degrees in Computer Science from the Pusan National University, Korea, in 1990 and 1992, respectively, and the PhD degree in Computer Engineering from the University of Florida in 2001. Since March 2009, he has been an Associate Professor with the Department of Computer Science, KAIST, Korea. He was an Associate Professor with the Department of Computer Science and Engineering, Information and Communications University, Korea from 2002 to 2009. From September 2001 to January 2002, he was a research assistant professor at the Arizona State University. He worked as a research staff member with ETRI, Korea, from January 1992 to August 1997. His research interests include sensor networks, real-time and embedded systems, and robotics. He is a director of Auto-ID Lab Korea of the Global USN National Research Laboratory.

Chan Yeob Yeun

Chan Yeob Yeun received his Master's degree in Information Security, and later obtained his PhD in the same subject from University of London. Since 2008, he serves in the position of Assistant Professor at the Khalifa University of Science, Technology & Research, Sharjah, UAE. Prior to his current position, he served as the Vice President of LG Electronics for developing the World First Mobile TV 3G handsets with CAS/DRM and taught Network Security at KAIST-ICC. He also served as the Wireless Security Team Leader of Toshiba TRL for researching and developing 4G and Ubiquitous Security. His primary areas of expertise lie in the area of Ubiquitous Network Security. Working closely with the students, he performs research and is a prolific author, having written 43 publications including Journals and Conferences, two Book Chapters and nine international patents compilations.

Byoungcheon Lee

Byoungcheon Lee received the BA and MS degrees in Physics, from the Seoul National University, Korea, in 1986 and 1988, respectively, and the PhD degree in the School of Engineering from the Information and Communications University, Korea, in 2002. From July 2003 to June 2004, he was a Postdoctoral Research Fellow, at ISI, QUT, Australia. Since 2002, he has been an Assistant professor with the Department of Information Security at the Joongbu University, Korea. Prior to his current position, he served as a Researcher at the LG Cable Research Center (1988-1994) and LG Corporate Institute of Technology (1994-1998). His research interest includes all aspects of cryptology and information security. His major research areas are cryptographic protocols and digital signature variants. Currently he is working on secret signature and secure key issuing problems in ID-based cryptography.