Telecommunications and Information Exchange Between Systems

ISO/IEC JTC 1/SC 6

Document Number:	N13856
Date:	2009-02-09
Replaces:	
Document Type:	Liaison Organization Contribution
Document Title:	Liaison statement from JTC 1 SGSN to JTC 1/SC 6/WG 7 on USN Security
Document Source:	JTC 1 SGSN Sydney meeting
Project Number:	
Document Status:	As per the JTC 1 SGSN Sydney Resolution 1, this document is forwarded to JTC 1/SC 6/WG 7.
Action ID:	FYI
Due Date:	
No. of Pages:	6

ISO/IEC JTC1/SC6 Secretariat Ms. Jooran Lee, KSA (on behalf of KATS)
Korea Technology Center #701-7 Yeoksam-dong, Gangnam-gu, Seoul, 135-513, Republic of Korea ;
Telephone: +82 2 6009 4808 ; Facsimile: +82 2 6009 4819 ; Email : jooran@kisi.or.kr

ISO/IEC JTC 1

Study Group on Sensor Networks

Document Number:	SGSN N064
Date:	2009-02-06
Replace:	
Document Type:	Outgoing Liaison Statement
Document Title:	Liaison statement from JTC 1 SGSN to JTC 1/SC 6/WG 7 on USN Security
Document Source:	JTC 1 SGSN Sydney meeting
Document Status:	
Action ID:	As per the JTC 1 SGSN Sydney Resolution 1, this Liaison Statement is submitted to JTC 1/SC 6/WG 7.
Due Date;	
No. of Pages:	2

SGSN Convenor: Dr. Yongjin Kim, Modacom Co., Ltd (Email: cap@modacom.co.kr)
SGSN Secretary: Ms. Jooran Lee, Korean Standards Association (Email: jooran@kisi.or.kr)

JTC 1 SGSN N064

Liaison statement from JTC 1 SGSN to JTC 1/SC 6/WG 7 on USN Security

JTC1 SGSN thanks SC6/WG7 for sending liaison statement (6N13793). In response, SGSN would like to collaborate with SC6/WG7 on 6N13661, “Security framework for USN”, and any other issues regarding sensor networks security.

SGSN has already realized the importance of sensor network security. Therefore, security of sensor network applications and services is addressed in SGSN Technical Document Section 7.15 which is attached with this liaison statement.

We would like to be kept informed of the development of this work.

Attachment

7.15 Security of Sensor Network Applications and Services

Considering security we distinguish between communication and application security. Communication services standards are domain independent which means standards from other application areas may be used. Application security services, however, depend on political, cultural, organizational, and ethical issues and are therefore specific to each domain.

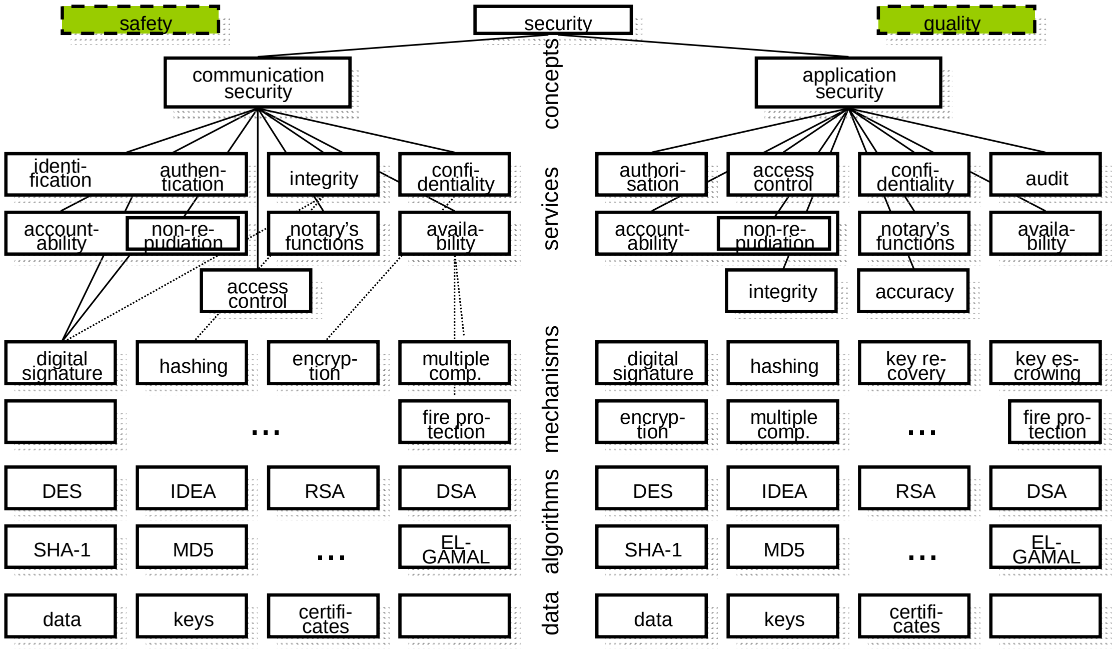

Figure 오류! 지정한 스타일은 사용되지 않습니다.-1. Layered security model.

Security is of extreme importance for many of the proposed applications of sensor networks. IP sensor nodes or even non-IP sensor nodes may be connected to global open networks, for example, the IP-based Internet. They could be victims of crackers and must be protected properly against cracking attacks. That is, there are various security issues such as device protection against system cracking and additionally authentication, information confidentiality and integrity, authorization and privacy protection. A tiny sensor node cannot provide all such security features because it has lots of system limitations such as low power, narrow bandwidth, small memory, low computational power, etc.

Because of sensor networks' unique properties, most notably limited resources and physical exposure of sensor nodes, sensor networks require a new type of security protocols. These protocols are tailored to the underlying system architecture, patterns of network traffic, and specific security requirements so that security related resource consumption is minimized. Physical exposure of nodes, as well as the threat that their cryptographic secrets are potentially available to an adversary, demands that security protocols in sensor networks protect the integrity of the network even if cryptographic secrets are compromised.

Therefore, network-provided security capabilities could be a solution for sensor node protection and other security requirements. That is, a security proxy at an edge network device could provide such security services to sensor networks. Other alternatives also are possible.

Some generic security services to be met by Sensor Networks relies on

- Confidentiality

  It is at risk while data is being generated, transferred or stored. A classical threat is the illegal capturing of personal information e.g., by intruding on the communication channels. This can be avoided by *encrypted* communication protocols at the different levels of communication and encrypted storage.

- Authenticity including non-repudiation

  This is threatened by hampering the data at the front-end, e.g., mobile terminals, the end-user's application or at the Health server. If altered the information cannot be attributed to the sender or the authorship of the information is being denied. Reliable safeguards are offered by "Message Authenticity Codes (MAC)"**.**

- Data Integrity

  It is at risk during transmission or during storage. In this case an intruder changes the data. Countermeasures consist in adding redundancy codes, the so called "Message Integrity Codes (MIC)" to the data.

- Accountability

  This means that the users can rely on the information provided. It implies that all actions are traceable. This requires ethical standards and legal regulations.

The availability of data is another neccessity. On top of that a set of control mechanism has to ensure that the organization's security policy is being met.

7.15.1 Security technology

The security technologies of sensor networks mainly focus on distributed key management, security route protocols (such as DSDV, DSR, and SEAD), node cooperation and selfishness, malicious power consumption, and intrusion detection model.

7.15.2 Security management

Referring to standard IEC 17799, security management of sensor networks also meets following requirements: easy deployment and application, reducing manual operation, maximum battery life, using existed security technology of encryption and authentication, using existing security standards.

7.15.3 Security evaluation

It is helpful for the system owner to perform security evaluation to ensure the security of sensor network activities, before selecting the specific devices, analyzing security requirements, constructing, rebuilding and running sensor networks, connecting to Internet.