Continuous Authentication in Internet of Things

Technology #17905

Applications

The Inventors propose a novel continuous authentication protocol for the Internet of Things (IoT) based on secret sharing schemes. This protocol provides secure and efficient authentication for frequent message transmission in short session time intervals. IoT applications can involve environment monitoring, e-health, electric vehicle and the smart house, in which appliances and services that provide notifications, security, energy-saving, automation, telecommunication, computers and entertainment are integrated into a single ecosystem with a shared user interface.

Problem Addressed

By connecting sensors, smart devices and everyday physical objects with the Internet, IoT provides a new form of communications for people and devices, which makes the virtual information world integrated seamlessly with the real world. As many of these applications are related to a user’s daily life, privacy and security aspects are very important. Unfortunately, the nature of the complex and heterogenous structure of IoT makes the security issues very challenging. In addition, most nodes are resource-limited, which makes the feature of lightweight necessary for IoT security mechanisms. The Inventors propose a lightweight protocol that satisfies all security requirements, via a novel secret sharing scheme, whereby the secret is used as an authenticator and the shares are used as authenticator tokens.

Technology

The Inventors employ secret sharing and time-bound concepts to build this continuous authentication protocol. They use the Shamir secret sharing scheme whereby shares of secret s are generated and distributed to n shareholders, from which t out of n shareholders can reconstruct the secret. They use the (t, n) scheme not to secure the secret by distributing its shares to n entities, but rather to authenticate the Claimer (secret and shares generator) to the recipient (Verifier) in a pre-defined time frame. This way, the Verifier will be able to link the received share to its original secret, thus authenticating the Claimer without performing costly public/private key operations.

In addition, the Inventors’ protocol employs time-bound concepts in which each share is tied with a time such that the share can only be revealed when the time it ties to is reached. This approach enables the realization of the ‘continuity’ in authentication as each time-bound share reveals a portion of the shared secret (authenticator) which enables the Verifier to authenticate the Claimer at any point in time during the session time-frame.

Advantages

- Security evaluation of the protocol shows that it fulfils the stated security requirements and addresses all IoT threat and attacks
- Lightweight, thus addressing the resource-constrained IoT endpoints
- Protocol does not require costly key cryptography operations, allow fast and efficient

continuous authentication

Categories For This Invention:

Computer Sciences & Information Technology
Cyber Security

Intellectual Property:

System and method for continuous authentication in internet of things
US Patent Pending
2016-0352732

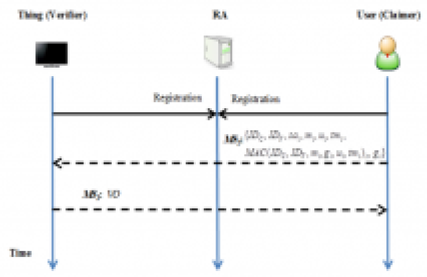
Inventors:

Kamal Youcef-Toumi
Omaimah Bamasag

Publications:

Towards Continuous Authentication in Internet of Things Based on Secret Sharing Scheme
Proceedings of the WESS'15: Workshop on Embedded Systems Security
2015

Image Gallery:


Thing (Verifier)
RA
User (Claimer)
Registration
Registration
Time