A Usable Interface for Location-based Access Control and Over-the-Air Keying
Technology #14407

Applications

This technology facilitates the dissemination of data among mobile devices with cryptographic protections. It has applications in the aviation, auto, trucking and taxicab industries, as well as satellite and mobile communications. Specifically, one application of this technology is for unmanned aerial vehicles (UAVs) to broadcast video surveillance data to selectively chosen mobile receivers on the ground for commercial, civilian and military use.

Problem Addressed

Modern cryptography offers numerous schemes for the protection of various types of data, at-rest and in-transit, across a broad set of applications. Some major impediments to the adoption and use of cryptographic protections in applications is the lack of easy-to-use interface and resource-laden key management that could allow users to enact desired protections through intuitive means. Furthermore, it is desirable for operators to employ cryptographic protections to control the conditions (such as location) under which receivers can access communication data.

Technology

The inventors have developed a map-based graphical user interface that allows an operator to specify access control rules for broadcasting content to subscribers in mobile settings by defining geographic regions on the map and associating individual receivers with these regions, among other conditions. The interface allows the operator to define and save different access control rules for different types of missions, and to automatically enforce a particular set of rules during the mission.

Once such access rules are defined using the intuitive user interface described above, they are enforced via cryptographic means. A recently developed technology called Dynamic Group Keying (DGK) allows one to change the data encryption key at any time and to securely and efficiently distribute the new key to authorized receivers. The distribution of keys to the receivers is accomplished using an Over-The-Air Keying (OTAK) protocol. Only authorized receivers possess the correct key, meaning no other receivers can decrypt the data feed. The monitoring and rekeying may occur in parallel with the broadcast, and the rekeying can be made completely transparent to the subscribers unless the subscriber's access status has changed.

Advantages

- Simple and intuitive user interface
- Technology allows for specified access rules in mobile settings based on the publishers' and subscribers' identities, locations, time, and other conditions
Categories For This Invention:
Computer Sciences & Information Technology
Cyber Security
Lincoln Laboratory

Intellectual Property:
Location based access control of material transportation vehicle resources
Issued US Patent
9,152,147

Inventors:
Roger Khazan
Daniil Utin
Adam Petcher

Publications:
A Usable Interface for Location-based Access Control and Over-the-Air Keying in Tactical Environments
Military Communications Conference (MILCOM)
Nov. 2011, pp. 1480-1486

External Links:
Lincoln Laboratory
http://www.ll.mit.edu/

Image Gallery: