Policy-Based Networking Technology Development for Cybersecurity Applications

In Cryptography, key management refers to the protocols devised to ensure safe generation, exchange, storage, use, and if required, replacement of the keys used in a cryptosystem. Since each cryptographic algorithm may have unique requirements regarding keys, many different key management protocols exist. Some protocols may be as simple as using pre-shared keys while others may require a well thought infrastructure, such as the public key infrastructures involved in HTTPS connections.

The problem is that many of these schemes fall short when deployed in extreme situations such as a tactical combat environment where soldiers need to access certain confidential data, but the data link may be slow, unreliable, or even unavailable, thus making the infrastructure unreachable.

A solution for this problem is to design a cryptosystem that distributes the data between multiple parties such that accessing the data would depend on the presence of all the parties rather than a key. Using this scheme, soldiers can each take a piece of the data and access it once all of them are present. This protocol is currently implemented by researchers at JPL and deployed in form of the Autonomous Information Unit (AIU) technology [1].

A remarkable feature of this protocol is that it ensures that an adversary can gain no knowledge about the data even if all but one of the pieces are compromised. On the other hand, an undesirable outcome is that it effectively renders the data impossible to recover once a single piece is lost or stolen.

In this project, my first goal is to improve this system to allow accessing the data if at least K of the N soldiers are present, thus making the protocol more fault tolerant. So far my main approach to finding a solution for this problem has been to explore alternative options that satisfy the objectives. The Journal of Cryptology, in particular, has been a very good resource for such options. However, due to lack of proper technical documentation about the current implementation in particular, identifying the details of the protocol has been challenging so far.

In the following weeks I hope to finish this phase of the project and start the next phase in which I will work on designing a decentralized architecture similar to the mesh topology.

[1] "Autonomous Information Unit for Fine-Grain Data Access Control and Information Protection in a Net-Centric System"; Chow, E., Woo, S., James, M., Paloulian, G.; California Institute of Technology and NASA's Jet Propulsion Laboratory. April 2012.