Policy-Based Networking Technology Development for Cybersecurity Applications

As communication and networking technologies advance, networks will become highly complex and heterogeneous, interconnecting different network domains, spanning countries and even continents. Since this path does not always guarantee confidentiality and ensure security, there is a need to provide user authentication and data protection in order to further facilitate critical mission operations, especially in the tactical and mission-critical net-centric networking environment.

The Autonomous Information Unit (AIU) technology[1] designed by JPL provides a fine-grain data access and user control in a net-centric system-testing environment that meets these objectives. In this research project we will explore new paths for utilizing cryptographic schemes and Linux security modules in order to ensure protection, authentication, confidentiality, and integrity of the data over a decentralized network of AIUs.

An AIU should be able to provide a mechanism to locate and join a decentralized network composed of previously deployed AIUs. With a potential combination of onion routing[3] and Karnin-Greene-Hellman secret sharing scheme[2] we can create a network traffic with the similar characteristics as the local data stored on AIUs based on the original paper; namely, we can make the network traffic unreadable unless a minimum number of AIUs are present in the network, thus making sure that a limited number of compromised AIUs will not reveal any critical data to the attackers. Optionally, we can create a portable live media that can turn any computer into an AIU; one possible implementation would be to modify the Lightweight Portable Security (LPS), which is a thin Linux distribution, developed by the Software Protection Initiative of the US Air Force Research Laboratory[4], that turns any Intel-based computer to a secure end-point (or a virtual "government-furnished equipment") capable of securely connecting to government networks using only a CD or USB flash stick, without leaving any trace on the machine (nothing to install).

Furthermore, an AIU should be able to act as a terminal that allows any user registered on the network to connect to their home directory using a decentralized directory server, even though the data is physically located on another AIU. To achieve that goal without loss of security, we can take advantage of Linux security modules such as the Security Enhanced Linux (SELinux), which is a policy based mandatory access control (MAC) mechanism developed by National Security Agency (NSA), that enables us to isolate an attacker in a single user or service without endangering all other users on all of the AIUs. SELinux supports targeted – based on user/service context – and/or Multi-Level Security (MLS) – based on classification and clearance level – policies. Additionally, SELinux provides a great audit logging structure that can be improvised to log erroneous data from every AIU (or just a set of them) from the network, thus enabling us to debug the infrastructure from only one AIU.

An AIU designed by JPL in the original paper provides a mechanism to establish trust among deployed AIUs based on recombining shared secrets, authentication and verify users with a username, X.509 certificate, enclave information, and classification level, all of which will be covered in the new model. AIU achieves data and network traffic protection through (1) splitting data into multiple information pieces using the Shamir's secret sharing algorithm, Karnin-Greene-Hellman scheme, and secure onion routing protocols, (2) encrypting each individual information piece using military-grade AES-256 encryption approved by Federal Information Processing Standard (FIPS) and restricting user access using Linux security modules, (3) randomizing the position of the encrypted data based on the unbiased and memory efficient in place Fisher-Yates shuffle method. Therefore, it becomes virtually impossible for attackers to compromise data since attackers need to obtain all distributed information as well as the encryption key and the random seeds to properly arrange the data.

The AIU technology can greatly enhance information assurance and security management in the bandwidth-limited and ad hoc net-centric environments. In addition, AIU technology can be applicable to general complex network domains and applications, where distributed user authentication and data protection are necessary. AIU achieves fine-grain data access and user control, reducing the security risk significantly, simplifying the complexity of various security operations, and providing the high information assurance across different network domains.

References:

[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.

[2] "On Secret Sharing Systems"; Karnin, E., Greene, J., Hellman, M.; IEEE Transactions on Information Theory, vol. it-29, no. 1, January 1983.

[3] "Tor: The Second-Generation Onion Router "; Dingledine , R., Mathewson , N., Syverson , P.; Proceedings of the 13th USENIX Security Symposium, August 2004.

[4] "Lightweight Portable Security"; Software Protection Initiative, US Air Force Research Laboratory; web: http://www.spi.dod.mil/lipose.htm