Oral: **Multi-Factor Authentication for More Resilient Storage in Wireless Networks**

Scott Bell, Eugene Vasserman, Dan Andresen

Kansas State University

Modern military units derive great tactical advantage from secure real-time sharing of data such as maps, images and orders among soldiers. However, distributing this information in real time within a combat situation creates significant risk: when using a mobile communication network, the adversary may capture one or more mobile devices and use them to gain access to data stored locally on the device, or shared data stored in the network, endangering the entire unit. While such devices are generally tamper-resistant and require a login, these measures are insufficient to stop a well-funded and motivated attacker.

This work presents a protocol that significantly reduces the adversary's window of opportunity for such attacks. This is achieved by never storing files locally on a device but rather fetching them from the network as needed. Files are first encrypted, then fragmented using m of n erasure coding and distributed across n mobile devices. Distributing file fragments rather than entire files prevents an adversary from reconstructing the original file unless at least m devices have been compromised. Revocable multi-factor authentication is incorporated to reduce the adversary's ability to gain access to the mobile network using a captured device.

Users are authenticated using a PIN (as is standard to access a mobile device) and a wireless token which is worn by the user. The token is embedded with a secret key that is used to sign challenges from the mobile device to uniquely identify the user. This challenge-response is performed periodically to provide fresh proof that the token and device remain in proximity to one another. A fresh signed response from the token, along with a signature from the device, provides authentication for file fragment requests sent to other mobile devices within the wireless network.

Each device responding to file fragment requests is able to verify the signatures of both the user (token) and device making the request using locally stored public keys. This allows devices within the network to revoke access to specific users and/or devices who may be compromised. At the same time, it allows users the flexibility to switch devices as needed – tokens are not permanently paired with devices. Thus, a user is required to possess both a personal token and a mobile device, each with an unrevoked key, in order to make successful file fragment requests across the wireless network.

We analyze the costs and benefits of this design using simulations and a prototype implementation on real-world mobile devices. Results show that the added computational overhead, response-time delay, and battery consumption are acceptable even when using purely software-based operations. Incorporating inexpensive hardware acceleration can further reduce these costs. Simulations indicate the probability of data loss is significantly reduced in this design as opposed to current systems, which only employ a user secret (password or PIN).