User Authentication and the Crypto Module

Electronically authenticating a user rather than relying on human verification is one of the most significant technology challenges of today for network and mobile security access. Even though robust encryption technology has been widely adopted to protect user data, encryption is simply bypassed. Adversaries hack the more vulnerable PIN or password authentication systems. Nearly every element of the Critical Infrastructure from telecommunications, medical, government, banking, retail, and transportation has been effectively circumvented by weak electronic user authentication. A recent study by the Chertoff Group stated, "It's hard to find any major cyber attack over the past decade where identity – generally a compromised password – did not provide the vector of attack."[i]

Robust electronic user authentication and encryption must be part of a fully integrated solution to prevent data breaches. The recent high-profile data breaches from the Democratic National Committee (DNC), Target, Yahoo, Verizon, OPM, IRS, JP Morgan Chase, Home Depot, Sony Pictures, are identical attacks – the passwords are compromised. Once the adversaries have access, they move throughout the enterprise escalating privileges to seize private and sensitive data. Verizon's annual Data Breach Investigations Report (DBIR)[ii] has also helped to emphasize this point. The 2016 DBIR found that "63 percent of confirmed data breaches involve using weak, default or stolen passwords." No other attack vector comes close[2].

An ambitious yet achievable goal is to elevate user authentication to the same level as robust encryption for protecting data. Doing this, we believe, requires several simple fundamental principles:

1. The authentication system should store, process, and match user electronic information **locally**, not at a remote central database containing all the user's data. A large cache of authentication data is also a large target. Moreover, the data path and hardware components from the user to the server must also be protected.
2. User authentication and key generation should be **cryptographically bound**. A PIN or biometric match should not simply result in a binary "Yes" or "No" in the authentication mechanism. Rather, a successful user authentication match (executed locally), results in the generation of a key split variable. This authentication key variable is then cryptographically combined with a locally stored *private key* split and a third *public key* split sent from the device. To unlock private / sensitive / classified data or applications all three keys must be cryptographically combined. Now, the hacker must attack the individual user AND they must gain access to the cryptographic hardware each time the user authenticates and unlocks their device.

3. The authentication must be **executed in separate trusted hardware**. Simply storing keys and sensitive authentication data in trusted memory like a smartcard / SD card, SIM, USB drive is not sufficient for strong authentication since the vulnerable commercial device unwraps and processes the data. Hardware-based storage and processing must be separated from the general-purpose processor and control to be secure. Unfortunately, most commercial based mobile, network, and IoT devices have NOT evolved with isolated trusted hardware modules. In this void, broad pervasive user authentication attacks have mushroomed.

   Conventional system integrators and U.S. Government entities have taken a traditional approach, developing purpose-built custom hardware platforms like SPE PED[iii] and Boeing Black[iv], respectively. These custom devices meet the fundamental security principles outlined above for robust user authentication, but widespread adoption never occurred. One reason may have been the high cost; 8 to 10 times more expensive then a commercial smartphone. The "secure" phone has very limited functionality beyond the specified secure processes.[v] It cannot be used in an untrusted mode for personal use and cannot be easily updated. The design approaches of the U.S. Government and OEM smartphone vendors have not resulted in a product that meets user needs and expectations.

A Different Path

Figure 2 Comparison of a Full Custom Design Secure smartphone & functional block diagram to a Commercial smartphone tethered to a Tocreo NFC Cryptographic Module.

Conventional thinking in designing and developing a secure smartphone asserts that you place all the security within the device as depicted by the Boeing Black phone Fig 2 Left. It follows then that the hardware (red blocks), trusted firmware (yellow blocks) and trusted paths (red lines) are “baked into” custom security components throughout the design. The red circle around the functional block diagram show the extent of the trust anchor required in the phone. A custom user authentication storage and matching process is very typical with a tailored architecture making it challenging to integrate or scale with legacy authentication systems.

Fig. 2 Right depicts a new security approach. In this architecture, an off-the-shelf smartphone is tethered to a custom Crypto Module through a standard Near Field Communication (NFC) interface. The Tocreo Crypto Module (TCM) with an isolated crypto processor, trusted memory & data bus, and display is now capable of STORING, PROCESSING, and DISPLAYING trusted operations. Tethered at the baseband layer, below the smartphone Operating System, the trusted components and trust anchor are very minimal (denoted by the yellow circled functional blocks).

Rather than placing the security inside the smartphone, a standalone crypto module executes the trusted isolated security processing. Now, with the addition of a Crypto Module interconnected (via the NFC interface) to a true commercial based smartphone the once insurmountable challenge of protecting user authentication process, key generation, and encryption is not only attainable, but also very cost efficient.

---

[i] https://www.chertoffgroup.com/news-events/white-papers/641-chertoff-group-white-paper-highlights-the-need-for-strong-authentication-in-cyberspace

[ii] http://news.verizonenterprise.com/2016/04/2016-verizon-dbir-report-security/

[iii] https://gdmissionsystems.com/cyber/products/secure-voice/sectera-edge

[iv] https://en.wikipedia.org/wiki/Boeing_Black

[v] http://mashable.com/2017/01/27/trump-boeing-black/#aYLknwLm_8qu