Publication: Network Asia Online
Date: 13 July 2017
Headline: Why mobile hardware security is fundamentally broken

Why mobile hardware security is fundamentally broken

The mobile device sits squarely in the center of the modern person's life, in a manner like no other tool before it. The mobile phone's ubiquity means that users have access to information, financial management tools, and communication tools, for personal and professional uses, often on the same device.

This is precisely why security for a mobile device is so crucial. As a nexus for so much important and sensitive data – which forms a user's digital identity – mobile devices should be as protected as your most personal physical documents.

This is why security features have been some of the most lauded elements to launch on mobile devices recently. And, with device manufacturers touting these hardware security features, it might be easy to assume that all their personal data is safe.

This assumption is incorrect. This is the case even on some of the most advanced mobile devices available today.

Recent exploits show that our devices are not as secure as we are led to believe. For instance, hacker Jan Krissler published a high-profile hack of Samsung's Galaxy S8 iris scanning feature, using a consumer grade camera and contact lenses. In Singapore, ethical hackers from the Whitehat Society at the Singapore Management University (SMU) showed that it was possible to take over a user's device using only their phone number, and then use the device's camera and audio equipment to spy on the user.

Even the smartcard chip, which provides tamper-proof security for phones and cumbersome hardware tokens, offers practically no protection against misuse. Smartcard chips don't authenticate the user, and are unable to decipher the intent of the person using it, be it for the owner or a person with malicious goals.

High-profile exploits against smartcards in recent years have often involved some form of hardware hack. For instance, before they were apprehended in 2011, a criminal group in Belgium succeeded in compromising at least 40 PIN-enabled EMV cards. Programming hobbyist chips called FUN cards, which validate any pin that is entered, were soldered onto each EMV card's original smart chip. The 2015 paper that revealed their technique was widely covered in the press.

In 2016, a demonstration at the 2016 Black Hat security conference showed that attackers could use a tiny Raspberry Pi computer to skim credit card information off from EMV cards at the terminal.

Architecturally, at their core, mobile operating systems and mobile apps cannot be trusted. Relying solely on hardware for security is becoming increasingly insufficient. In many cases, it's only a matter of time before attackers can access devices.

What are the alternatives? It is tempting to say that we need more advanced hardware, or more robust processes to put in between users and services. Yet, after two-factor authentication, where do we stop? Three, or perhaps more?

Ultimately, this approach leads to more expensive products and services that are difficult and inconvenient to use. Yet the costs to businesses are not merely in terms of the time and material costs of deploying hardware, but also the missed opportunity to provide value to customers who have come to expect better user experiences.

Publication: Network Asia Online
Date: 13 July 2017
Headline: Why mobile hardware security is fundamentally broken

This is why, in a study conducted by Asian Banker Research (2017), close to 80% of the leading banks in Asia Pacific listed enhancing digital and mobile experience and cybersecurity preparedness as the top technology investment priorities going forward.

Those priorities precisely capture the solution that enterprises need for the future. To provide truly resilient security—one that is scalable, trustworthy, and convenient—companies need to go further in developing mobile experiences that are as secure as they are convenient. In other words, product design needs to be one that is led by both security and convenience as a fundamental philosophy.

Organizations, especially in a rapidly evolving security landscape, must continually pursue better and more innovative methods to secure sensitive customer data. Instead of relying on stagnant hardware solutions that are now faced with ever-diminishing effectiveness, solutions must be sought elsewhere.

Benjamin Mah is the Co-founder & CEO of V-Key