V-KEY
STRONGER WITH V-OS

Article

HOW DO WE DETERMINE THE EFFECTIVENESS OF MOBILE APPS' SECURITY SYSTEMS?

With the spate of remote working regime due to Coronavirus pandemic, the reliance and growth for video conferencing platform has been exponentially escalated. Zoom, one of the more widely and popularly used platform, was reported to have 500,000 hacked accounts being sold on the Dark Web. Zoom credentials stolen includes email address, passwords, Zoom host keys, among others. These type of attacks are not unique to Zoom.

In 2019, a white-hat hacker successfully accessed Tchap, the French government's secure, encrypted messaging app that was restricted to certain government officials. Meanwhile, banks and digital forensics experts have been reporting a new type of malware that targets mobile banking apps, obtains financial data, and covertly performs operations on these apps.

A few factors contribute to this widespread lack of security. The most commonly used protective measures—code obfuscation, app shielding, and even sophisticated white-box cryptography—can only slow down a cyberattack, not prevent it.

MOST MOBILE APPS TODAY ARE NOWHERE NEAR AS SECURE AS WE WOULD LIKE THEM TO BE.

Businesses also need to consider user experience and scalability alongside security. You could make the code almost undecipherable for cybercriminals, but that would significantly slow an app down, too. You could use hardware to physically protect data, but that would limit operations to a specific location or device and have an impact on user experience.

The problem with settling for the status quo is that you can possibly compromise secret keys and user data. This is compounded in the banking and government sectors. A successful hack could result in the theft of millions of dollars, state secrets, or comprehensive information on citizens

As a result, additional mobile app security solutions have emerged, ranging from mobile ID software to biometric verification. But with the erosion of customers' trust in IT security, the same problem plagues these security solutions: how do we know we can actually rely on them? What vulnerabilities in these systems will expose our data?

And, more fundamentally, do these security solutions actually do what they claim to do?

What certification does - and doesn’t - achieve for security products

That’s why many IT security companies undergo rigorous evaluation to get their solutions certified.

But ask any cybersecurity insider and they’ll tell you to take these certifications with a grain of salt. After all, these badges only serve to guarantee that a product does what it’s designed to do. That means they hold varying weight for products with different designs, functions, and objectives.

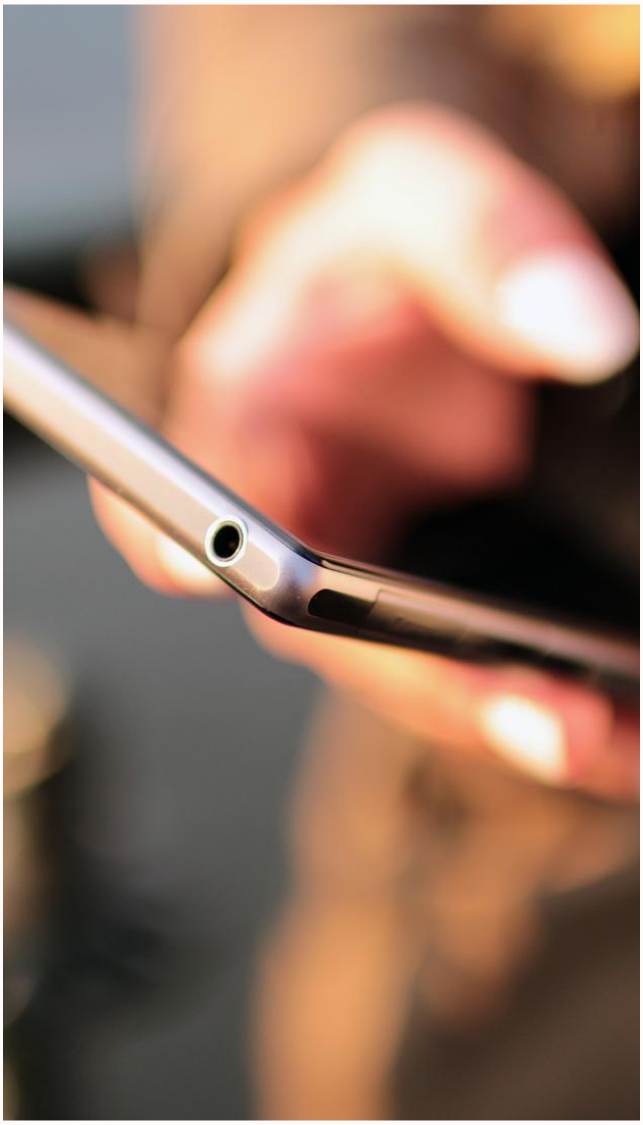
Herein is another conundrum for consumers - if they can’t take certifications at face value, then what guarantee of security can they have?

"The key is to analyze what exactly was tested and certified," according to Er Chiang Kai, Chief Technology Officer of V-Key. "You also need to look at the scope of the certification. Gaining certification for one security product does not mean the entire suite of security solutions is certified, too, unless the former serves as the design foundation and basic infrastructure of the entire suite."

That’s what V-Key did when it obtained EAL3+ certification for its V-OS product in July 2020.

> “The more complex the product, the more requirements and steps necessary to validate its security. Not many complex IT solutions make it to or past level three,” said Er Chiang Kai, CTO of V-Key.

What is EAL?
An Evaluation Assurance Level (EAL) is a category ranking given to an IT system or product following a Common Criteria security evaluation, which is an international standard. The category is reflected in a numerical rating (i.e., EAL 1, EAL 2, and so forth). A higher rating doesn’t necessarily mean a product is more secure, but rather that it underwent a deeper and more rigorous level of evaluation.



Protecting mobile apps through a virtual secure element

V-OS is a patented virtual secure element that can be embedded within a native iOS or Android mobile app. Think of it as a secure sandbox that "creates a safe operating environment where data can be stored and cryptographic processes can be executed in isolation from the rest of the mobile app".

In other words, even if cybercriminals can reverse-engineer a mobile app's code and get into the system, they can't break or access the box. They can't get their hands on confidential data stored within V-OS.

V-Key's other security products, including but not limited to a smart token, biometric EKYC (electronic Know-Your-Customer), and cloud identity solutions, are built on V-OS. That means by obtaining EAL 3+ certification for V-OS, V-Key has shown that its entire suite of security products can be trusted.

Er Chiang Kai highlighted that this is the first virtual secure element in the world to accomplish such a feat.

In addition, V-Key achieved FIPS (Federal Information Processing Standard) 140-2 Level 1 certification – a security standard issued by the U.S. government – for V-OS in 2016. The company is now aiming for a higher level for FIPS140-2 certification.

Bottom line: it's all about trust

Government agencies, as well as banks like UOB and DBS, use V-OS to secure their mobile applications. With the V-OS' EAL3+ and FIPS 140-2 certifications, these and other V-Key clients can guarantee their customers that their apps' security systems work the way they're intended to.

That goes a long way in establishing trust, especially in today's climate where cybercrime is rampant.

"By having a common criteria certification, we give our customers the assurance that our product has been well-evaluated and has all the protections that are expected by the customer when they use it," added Er Chiang Kai in the press release. "We want to give customers a product they can trust."

And in the end, thats really what certifications help achieve.

GLOBALPLATFORM® The Standard for Managing Applications on Secure Chip Technology
FIPS VALIDATED 140-2
Common Criteria
fido™ ALLIANCE MEMBER
SG:D ACCREDITED

V-KEY
STRONGER WITH V-OS

V-OS Virtual Secure Element | V-OS App Protection | V-OS Smart Token
V-OS Face Biometrics EKYC | V-OS Messaging | V-OS Cloud
SECURING THE GLOBAL DIGITAL EXPERIENCE

info@v-key.com v-key.com +65 6850 5155