WHITE PAPER

Dual Roots of Trust: A Better Way to Protect Your Digital Assets

V 1.0

LEN VEIL

rivetz

sales@rivetz.com

CONTENTS

A LOOK BACK

In the early days of the cell phone industry, it was easy for bad actors to clone your phone's identity and run up all sorts of charges on your phone number. Early carriers required their users to set up a PIN in order to use their devices, to combat that fraud.

The Subscriber Identity Module (you may have heard of the SIM card) came out of the European Telecommunications Standards Institute's efforts to combat that fraud. The SIM held the identity of the device and device owner in a way that couldn't be intercepted by the bad guys.

Over the past two decades, the SIM has undergone many changes, but fundamentally serves the same purpose: a protected environment in which to store important information and execute some limited, sensitive transactions.

Perhaps not surprisingly, the rise of the Internet brought with it similar fraud and attacks on identity and access to computers. Innovative industry leaders banded together to fight that fraud and formed organizations such as the Trusted Computing Group (TCG). The TCG developed specifications that have become the standard for securing devices, data and identity, including the Trusted Platform Module (TPM) for personal computers, laptops and other similar devices.

Global Platform, another industry organization, developed the standards for the Trusted Execution Environment (TEE), which is a vault of sorts that lives inside the hardware of a mobile phone, tablet and other related devices. The TEE is isolated from the normal operating system of the device, and so can execute code that can't be seen by that OS. It is also rooted in the hardware to guarantee a secure execution environment.

Together, these technologies brought Strong Machine Identity, Boot Integrity and Attestation, as well as Protected Storage and Protected Execution to a whole new class of platforms. Today, more than 1 billion cellular devices are TEE-enabled.

Nice history lesson – but what does this have to do with keeping my cryptocurrency safe or dual roots or whatever it was you were talking about?

> “The Trusted Execution Environment (TEE) is a vault of sorts that lives inside the hardware of a mobile phone, tablet and other related devices.”

Clearly, this demonstrates why I became an engineer and not a novelist. The concept of strong machine identity and secure enclaves was originally mass commercialized on the handset with the SIM because those technologies were needed to prevent substantial fraud. SIM came out of the cellular industry. TPMs were created to address issues within traditional IT environments, protecting sensitive keys from compromise and ensuring the computing environments were in a known condition before they

▶ were used. Concepts such as attestation were automated and associated with key usage.

Rivetz ends up combing two core security technologies that had their roots (pun intended) in different worlds for different reasons.

Carriers use the SIM to protect their network information. Consumers and enterprises use the handset OS environment, potentially with some TEE capabilities, to protect their assets. While this is a significant leap forward in the protection of digital information, using only one or the other leaves our digital assets vulnerable to imperfect hardware or software implementations – and nevermind the fact that humans are still involved in the process and we know how well that often turns out.

Having only a single domain in charge of security is akin to having only one lock on the door. The lock might be the best on the market. But what if it's not installed correctly? What happens if you forget to lock the door? What happens if you lose your key and wallet and your address is right there on your driver's license?

Obviously, the digital environment is a bit more complex than a lock and a door. And as the complexity of our systems increase, those designing our digital security need to implement ways to distribute the security in a way that takes more than just one means of attack or failure.

MEET THE DUAL ROOTS OF TRUST

The Evolving Attack Surface

Once upon a time, we went to work and used the computers given to us. As technology got more mobile, companies gave their employees computers and mobile phones to take home or on business trips. As smartphones became ubiquitous, people stopped wanting to carry two phones. They could use these smartphones to access email, surf the Internet, play games that simulated flinging birds – what more could one want?

No, not two smartphones. Just one.

▶ People began using their personal devices for work anyway, and employers gave in, setting up BYOD (Bring Your Own Device) policies and causing their IT departments to seek therapy, probably.
We now log into work environments across a multitude of devices, all of which have different levels of security. Admit it – you've signed into work email from public wi-fi at least once. The bad guys now have many different ways to acquire your credentials and use them to compromise your company's data. Nevermind your own financial data, crypto wallets and social media accounts.

Despite the best efforts of security professionals, there are more ways than ever for criminals to access your information, steal your identity, or otherwise wreak havoc on your personal and business assets. Even the secure enclaves mentioned above – the SIM and the TEE – aren't completely immune. Some of the vulnerabilities specific to each may be more difficult to exploit than others, but they exist.

As the value of the asset that could be compromised increases, so does the desire to find a way to get at it.

“Admit it – you've signed into work email from public wi-fi at least once. The bad guys now have many different ways to acquire your credentials and use them to compromise your company's data.”

Distributed Assets

We've established that having a single point of failure isn't the best way to manage your assets (or anything else, for that matter). Even if the single point is difficult to break into, you might not notice it right away if you leave your phone at the office or drop it at a concert.

▶ The longer it's out of your control, the bigger the chance someone can get into things they shouldn't.

The solution? Distributing those assets across two or more secure locations.

> “If we make sure your private keys aren't stored in one single spot, then someone who's targeted you has a much harder job getting his hands on them.”

If we make sure your private keys aren't stored in one single spot, then someone who's targeted you has a much harder job getting his hands on them. In fact, even if this person manages to get one of your devices, you can use another device to revoke all access from it.

Further, if you layer in the ability to guarantee the integrity of our devices and secure enclaves, you can provide evidence that our sensitive information was always protected. In the end, this provides for a higher-quality transaction for all involved.

DUAL ROOTS OF TRUST – WHAT'S THAT?

What is a “root of trust,” anyway?

A root of trust is a set of unconditionally trusted functions that consistently perform a set of security-specific operations in an expected and repeatable manner and are immune to software attack and ideally most hardware attacks. Simply put, roots of trust can examine the device and compare the results to a known and trusted condition – that it hadn't been tampered with from what is trusted.

A modern smartphone with a SIM

▶ and a secure enclave (such as a TEE) is a system that has those dual roots of trust. Distributing your private keys or other secrets across those two domains, even in one device, provides a much stronger level of security.

The solution we are working on does just that, with the key to unlocking the secrets being mathematically split between the two roots.

INDEPENDENT CONTROL PLANES

One of the reasons splitting the key between these two roots works is because – despite the fact that they're in the same device – the two roots are under the control of different entities. The carrier is in control of the SIM. The TEE remains under control of the device manufacturer of the device. Through a special application given permission to perform activities inside the TEE, the user can remain in control of the secrets within.

EXAMPLE USE CASES

Dual Roots of Trust has an unlimited number of use cases. A unique aspect of dual roots is the ability to provably control an application on a device when that device's location or possession is unknown.

> “A unique aspect of dual roots is the ability to provably control an application on a device when that device's location or possession is unknown”

For example, if a user were to lose a device used to sign into a platform with enterprise access credentials, the enterprise could disable the use of those credentials on that specific lost device, without requiring the

- user to change their credentials on other devices.

If a security flaw were found in an application, that application could be temporarily disabled until the problem were resolved.

Parents could remotely enable or disable their children's cryptocurrency wallets or messaging apps; employers could assert control over employee wallets.

ANDROID FOR NOW, BUT MORE TO COME

Secure enclaves are in a variety of platforms using a variety of technologies. You may have heard of SGX, which is in Intel devices, for example. Dual roots of trust can be implemented in many different configurations; the primary requirement is that the platform have two or more independent roots of trust.

CONCLUSION

We need a way to distribute sensitive cryptographic assets so they are protected in a provable way and parts are under control of two or more independent entities. We start with roots of trust that already exist on mobile platforms.

The SIM and the TEE are two of the most ubiquitous secure enclaves and are not controlled by the same entity – one is guarded by the carrier, the other by the manufacturer. If we start with these two, we solve for a wide swath of the market and can move to others in time.

As our mobile devices have become more important to our everyday lives and contain so much of our personal and vulnerable data, we need better ways to protect them. Dual Roots of Trust is the next step in keeping our assets safe.

ABOUT THE AUTHOR

Len Veil
VP, Strategic Business Development

Len is an entrepreneur in the fintech and trusted computing markets. After nearly a decade designing supercomputers, Len managed complex system development at Microsoft, and mixed signal chip design at Fujitsu. In 1996, emboldened with a passion for consumer cybersecurity, Len co-founded N*Able Technologies, and deployed embedded security systems with PC OEMs. After his company was acquired by Wave Systems Corp., Len led the effort to develop the Embassy Trust System and developed one of the industry's first implementations of the Trusted Platform Module. A technical contributor to the Trusted Computing Group set of specifications, Len enjoys applying his systems architecture and business development skills in growing companies.

ABOUT RIVETZ

Rivetz is delivering a new solution, the Rivetz Network, to simplify and enhance a user's digital experience. It's a new paradigm that moves trust from the servers to the powerful devices we use to access digital services. With its combination of blockchain technology and the hardware-based trusted computing capabilities already built into millions of devices, Rivetz verifies the intent of every transaction.

Rivetz bridges today's obsolete username/password model to a future where security is built in. Equipping developers with the technical solutions, foundations, protocols and distributed key management, Rivetz security seamlessly integrates with any blockchain, cloud or IoT project.