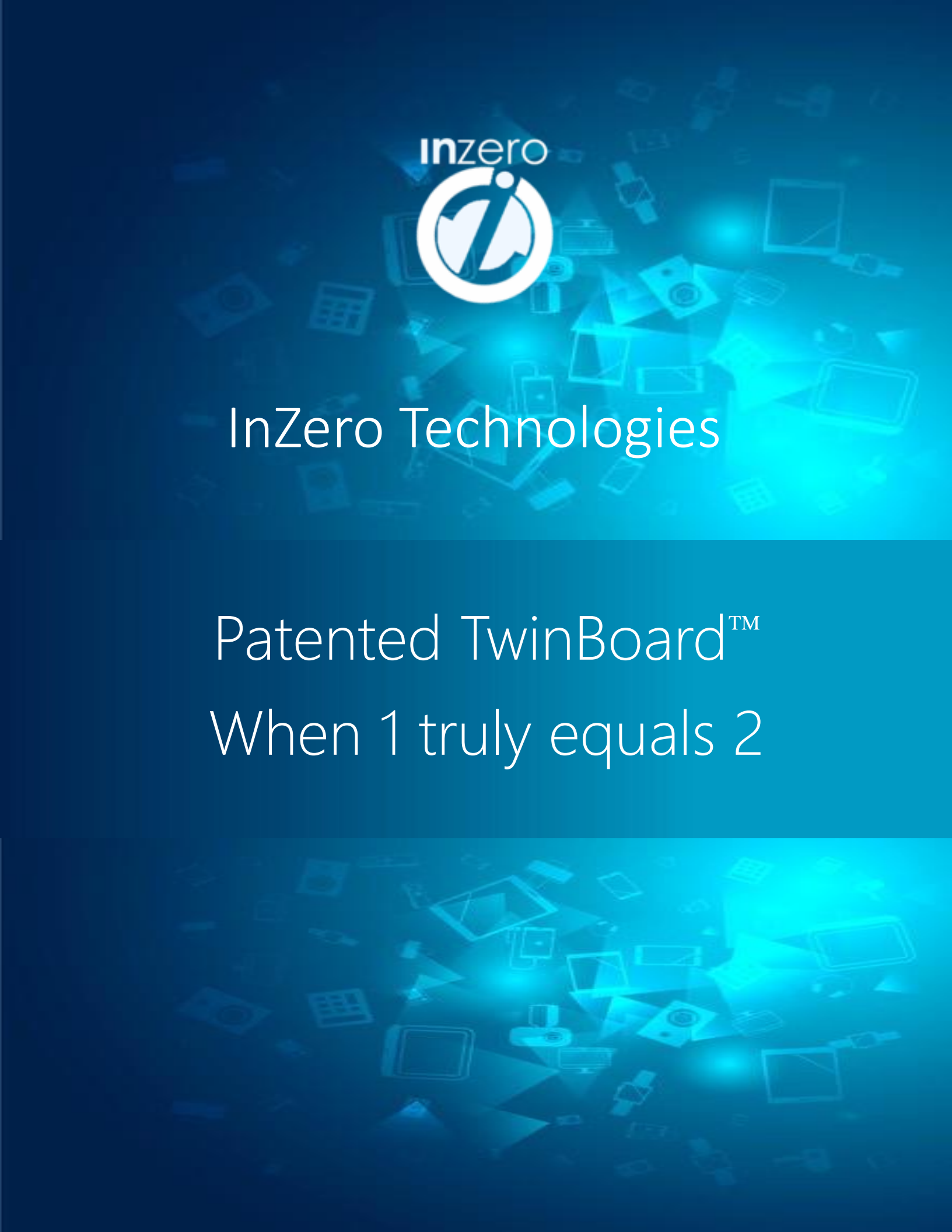


InZero Technologies

Patented TwinBoard™

When 1 truly equals 2

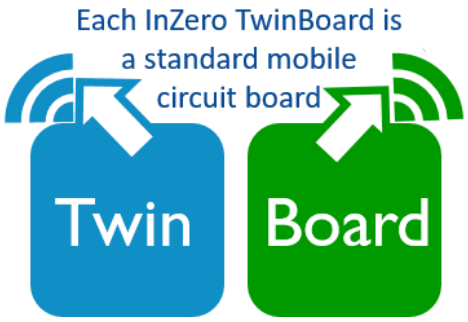
IN A NUTSHELL

InZero's TwinBoard is new, patented technology that combines the physical hardware of two smartphones or tablets into a single device. TwinBoard provides the full security of two separate devices yet allows instant switching between the two devices "inside", all with the touch, look and feel of a typical smartphone or tablet.

The key features are:

TWO STANDARD OTS CIRCUIT BOARDS

Each of the two circuit boards in TwinBoard is a typical, complete, fully-featured, off-the-shelf mobile circuit board. These are the same standard manufactured boards contained in common mobile devices. Thus, each board fully performs standard mobile operations, and can access separate Wi-Fi networks. These are isolated from each other, as if each was contained in its own mobile device case.

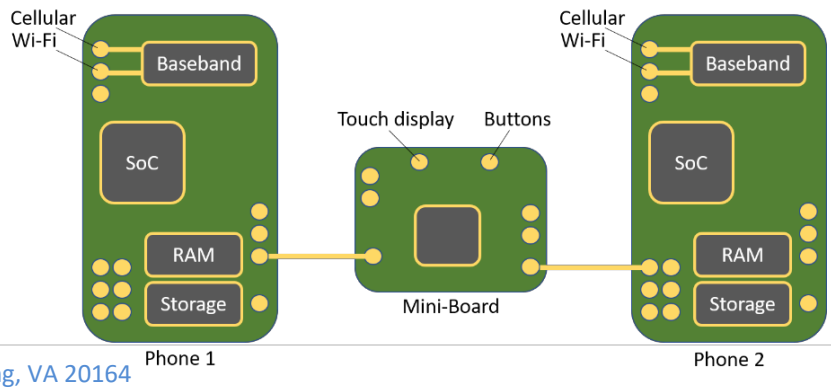


Indeed, the TwinBoard technology permits different circuit boards, therefore will allow different smartphone or tablet models to be included in the same TwinBoard device.

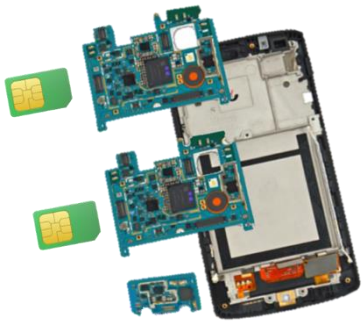
THE PROPRIETARY INZERO MINI-BOARD

TwinBoard also includes a mini-board that controls necessary shared functions between the circuit boards, and, if desired, can be used to provide for special functions. Specifically, this mini-board enables the user to quickly (perhaps a second) switch between the separate boards; controls battery power consumption so that it is only used for the active device; and if desired, can include additional user-preferred functions (whether for security, convenience or other reason) such as establishing a single Wi-Fi connection for the whole device.

Basic 2-in-1 Twinboard Design



MULTIPLE PHONE NUMBERS



TwinBoard permits up to four SIM cards, thereby enabling the device to possess up to four separate phone numbers with separate Wi-Fi connectivity. (It is unnecessary to use call-forwarding features.)

TYPICAL-SIZED CASE

InZero's special hardware design and configuration allows the TwinBoard circuit boards, mini-boards and SIM cards to be combined into a single smartphone or tablet casing that has the size, look, feel and weight of a standard device – this photo depicts the actual case for the first TwinBoard prototype.

THE KEY SECURITY DIFFERENTIATOR: ULTIMATE HARDWARE SEPARATION

Since the proliferation of mobile devices over the last decade, security cyber security development has created several cross-domain technologies to mitigate the risk of malware cross-contamination between domains. These include both multi-domain products such as containerization and virtualization, as well as separation of data access through authentication techniques and the like. However, currently used techniques still have readily exploitable attack surfaces to varying degrees that can be exploited to usurp complete device control, obtain Escalated Privileges and access all connected networks. The mini-board is purely limited to the specific shared functions (and any desired custom features).

INSTANT SWITCHING & INCOMING CALLS

InZero's TwinBoard does not require dual boot. Moreover, the TwinBoard smartphone will ring to signal an incoming call to the inactive circuit board SIM while the user is working in the other circuit board.

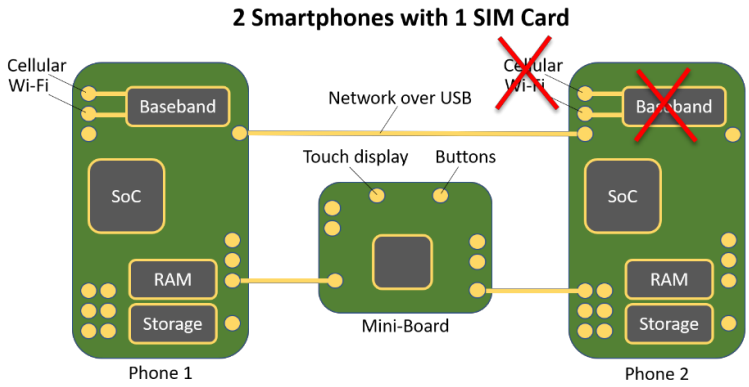
The Mini-Board Can Do Much More . . .

AN EXAMPLE, BASEBAND VULNERABILITY

Baseband vulnerabilities are fertile grounds for hackers, see, e.g., Exposing Mobile Device Exploits, CVE-2018-14318 Detail - Baseband Vulnerability. One industry observer advocates, "*What we need is phones that their baseband are separated from the system like old Nokia n900. SoC phones with an all-in-one system results in this mess*." (BleepingComputer).

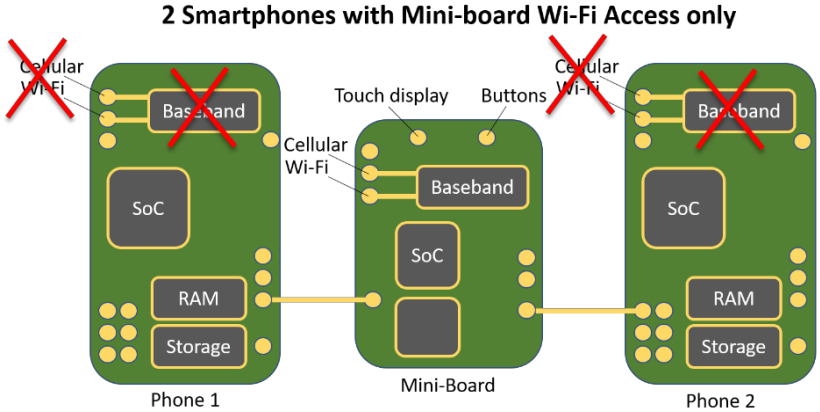
The custom capabilities of InZero's mini-board offers two solutions to the baseband vulnerability:

TWINBOARD SOLUTION 1: NETWORK OVER USB



In this solution, one of the TwinBoard smartphones is protected against a baseband vulnerability. This is accomplished by eliminating Wi-Fi access and connecting the smartphone to the organization's network via a USB connection to the other smartphone. In effect, the Wi-Fi connected smartphone serves to tether the disabled smartphone to the network. However, the Wi-Fi connected smartphone itself remains vulnerable to a baseband vulnerability.

TWINBOARD SOLUTION 2: MINI-BOARD BASEBAND CONNECTION



In this solution, each smartphone is protected against baseband vulnerability because direct Wi-Fi access is disabled. Instead, Wi-Fi access is added to the TwinBoard mini-board, with a single SIM card. The result is (1) each phone is protected against baseband vulnerability, while (2) any zero-day baseband attack is contained within the mini-board itself.

ANOTHER EXAMPLE: INZERO'S PATENTED TRUSTWALL

InZero TrustWall is a patented hardware-enforced endpoint OS firewall, that prevents outgoing traffic to unauthorized recipients. It can be implemented in single-CPU devices and be enforced at the SOC level, cannot be accessed by malware that typically overcomes software-based endpoint firewalls, DLP and the like. This can be also implemented in the InZero mini-board to control outgoing traffic of each of the mobile devices inside, controlled at the IT sysadmin level.

Many specific custom functions can be isolated in the InZero mini-board.

For Additional Security: Compatible with other InZero Technologies

TwinBoard is one of InZero's innovative cybersecurity mobile technologies founded on the belief that

When it comes to Cyber Security, Hardware can do what Software cannot.

Because both TwinBoard and InZero's additional cyber security technologies are OS agnostic, these are entirely compatible to mix-and-match as desired.

These patented and patent-pending technologies include:

- **Patented WorkPlay** – Creates multiple isolated and hardware-separated OS's (up to 3) from a single CPU, each having full resources (its own kernel, RAM, driver, storage), whereby one OS cannot access another OS, thus preventing potential cross-contamination *(developed, independently validated and installed in prototype devices)*
- **Patent-pending Bare-Metal Mobile Virtualization** – Uses different "types" of virtual machines (VMs) and direct peripheral hardware access to solve traditional, known power and performance problems of mobile hypervisors and strengthens bare-metal security *(developed for Xen hypervisor, with proprietary graphic acceleration code in development for further optimization)*
- **Patented TrustWall –** an isolated, hardware-enforced endpoint firewall comprising its own mini-OS or mini-VM, preventing outgoing traffic to unauthorized recipients (or enforcing other Sys Admin-determined security policy), even if the user OS is infected *(developed, tested, installed in a prototype device)*
- **Patent-pending Cloud Safe Passage –** InZero-created custom safe file exchange program, solving main problems of standard custom Content, Disarm & Reconstruction (CDR) technology, for cloud

implementation *(developed for commonly used file formats and tested; and Cloud Safe Passage implemented using Amazon Web Services for use by all user computers)*

- **Retrofit.** Except for TwinBoard, these Technologies may be remotely retrofitted to devices existing in the field, and as hardware-enforced technologies, are controlled by the Sys Admin.

InZero's TwinBoard Prototype

InZero has created a fully working TwinBoard prototype, adapted for a Motorola Nexus smartphone. This was developed by the InZero team to demonstrate and permit testing and evaluation of the TwinBoard technology capability. It is comparable to popular smartphones, for example, in comparison to a Samsung Galaxy 8.

Continuing Development

InZero's dedication to optimizing hardware-based cyber security continues as the company proceeds in further advancement of TwinBoard, our other patented and patent-pending technologies, and future innovations to come.

We welcome your questions and feedback at info@inzerosystems.com.

InZero Technologies, LLC