Security through Simplicity (StS): A resilient personal communicator

Paul.Gardner-Stephen@flinders.edu.au, +61 427 679 796

Cellular Phones are Untrustable

Smart-phones are extremely complex, with tightly integrated components running gigabytes of code on billions of transistors, making it practically *impossible to verify* such a device, and therefore *impossible to trust*.

Secure through Simplicity (StS) fixes this problem by making a device orders of magnitude simpler, creating a smart-phone that is *uniquely verifiable and trustable*.

Trustable code

StS has an operating system 10,000x smaller than normal smart-phones, allowing complete verification.

Only one program/app runs at any given time, and are fully isolated from one another, except through explicit user action, blocking any chance of cross-application information leakage, such as the Meltdown and Spectre bugs affecting almost every modern device.

Modular Design / Extensible

Industry-standard module slots allow creation and installation of a variety of specialised modules, such as Geiger counter / gamma sensor, or chemical detectors.

Trustable hardware

The StS hardware uses an improved version of the proven 6502 CPU architecture, used in NATO military systems as early as 1987[1], and is 100,000x simpler than modern mobile processors, allowing full verification.

The one un-trustable component that cannot be avoided is the cellular modem. StS neutralises this threat through isolation, including the ability to power-down or remove the device when performing sensitive activities. The cellular modem in normal phones has direct access to the microphone and storage: StS eliminates both.

Stand-alone secure networks

The StS device also includes a modular auxiliary radio system so that other radio communications channels can be used. With our peer-to-peer technologies, this allows a group of StS devices to form a fully stand-alone local network anywhere, preventing any opportunity for a hostile cellular network to even detect communications. *Satellite uplinks can be shared. A two-way Iridium satellite SMS module can also be built in, to give global communications from any point on the earth's surface.*

Remote wipe/locate capability

Either the cellular or auxiliary radio interfaces can be used to trigger authenticated remote wipe of a device.

Long battery life & integrated solar

The StS device incorporates an extreme capacity battery capable of supporting ~1,000 hours stand-by operation. It also includes a high-performance solar panel on the rear side allowing for potentially infinite battery endurance in the field. When discretion is required, it can look like a consumer device.

Simplicity reduces cost

Simplicity also greatly reduces development and integration effort. The hardware can be purchased at a price comparable to a high-end civilian smart-phone.

Encryption-at-Source

Normally, the cellular modem has direct access to the microphone, allowing cellular-based attacks to capture audio. With StS, this is impossible: Audio is encrypted by an FPGA (using any standard) before it gets to the modem. Completely secure voice (and in-call text exchange) over even hostile networks is the result.

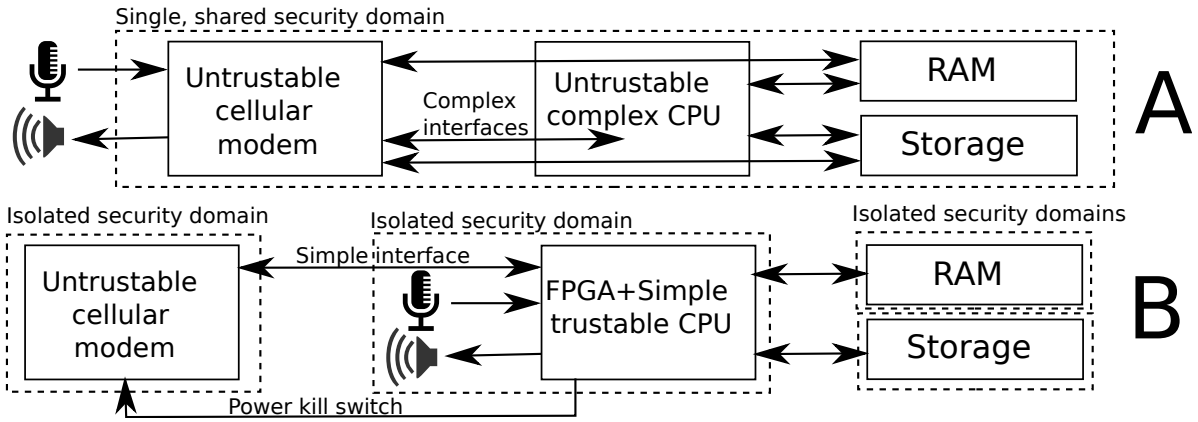

Figure 1: Comparison of existing insecure smart-phone architecture (A), and StS architecture (B).

1 AGARD-AG-160-VOL.18 „AGARD Advisory group for aerospace research and development, NATO 1987.