
Fully Sovereign,
Fully Open
Mobile Devices

Fully Sovereign, Fully Open Mobile Devices

Dr. Paul Gardner-Stephen,
Flinders University,
Serval Project &
MEGA Museum of Electronic Games & Art.

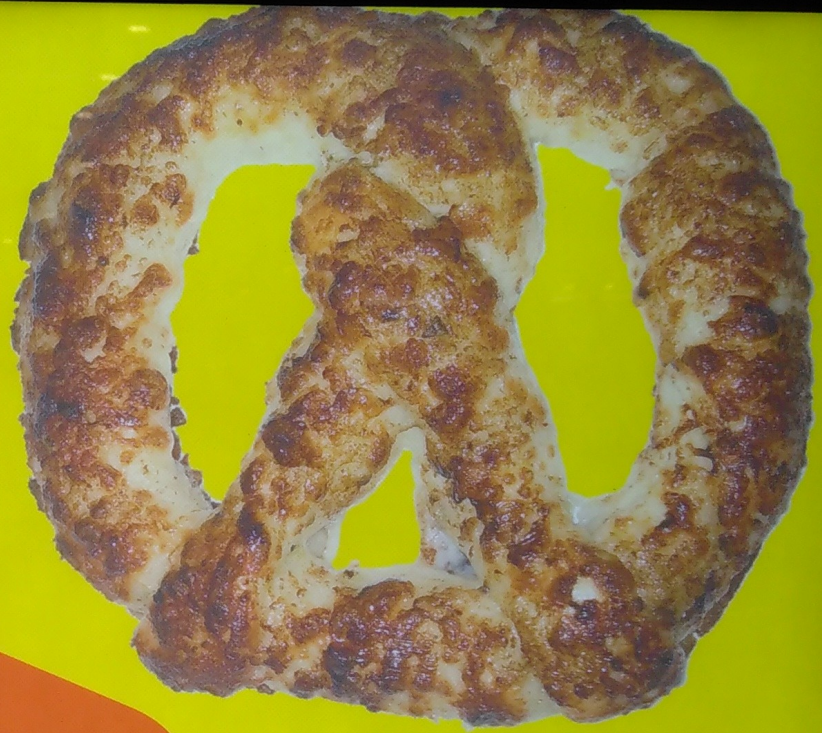
Paul.gardner-stephen@flinders.edu.au
+49 1521 58 205 33 while in .DE

MEGA65

An Apology

- We had intended to present this talk using our prototype device, but time got away
- See previous prototype making calls at LCA 2019: https://youtu.be/KuNB4ocZDXA
- Or come grab me during the camp to play with the current prototype

Try our NEW



VEGEMITE & CHEESE PRETZEL

Outline

- The rise and fall (and rise?) of Digital Sovereignty
- Making mobile devices easier to make and maintain
- Sandboxing untrustable/complex components
- Using digital sovereignty to make new kinds of mobile devices
- Making mobile packet radio-based devices that use “unlicensed” spectrum for infrastructure sovereignty

What is Digital Sovereignty

The ability for all persons who wish to, to create, modify and share digital artefacts of their choosing (whether hardware or software) and the means to re-produce them, without hindrance.

Me – last week

- Permission-less innovation
- Permission-less re-purposing
- Permission-less capability maintenance

By Analogy to “Normal” Sovereignty

- Wikipedia definition of sovereignty:

  Sovereignty is the full right and power of a governing body over itself, without any interference from outside sources or bodies.

- From which we derive:

  Digital Sovereignty is the full right and power over a digital artefact, without any interference from outside sources or bodies.

- Right != Power

Digital Sovereignty lags Physical Sovereignty

Buckets
(and many other things)

- Can use how vendor intended indefinitely.
- You can make your own*
- Can be re-purposed, e.g., cut eye-holes and use as a rain hat.
- Can be innovated, e.g., stick/bolt things on.

Smart-Phones

- Can hopefully use how vendor intended, hopefully, and only until they stop support.
- Really hard to make your own*
- Really hard to re-purpose (outside of the vendor-approved App sand-pit).
- Really hard to innovate on (teeny tiny undocumented circuits and super-complex software).

The rise and fall and rise of Digital Sovereignty

- In the early days of computers, there were few concentrations of outside power that acted to interfere with Digital Sovereignty
  - Digital Sovereignty was often encouraged, as it increased sales, e.g., in the Home Computer Era
- Growing size of digital economy led to rise of concentrations of interfering outside power
- Growing complexity of digital artefacts also undermines power to exercise digital sovereignty

The Rise of Planned Obsolescence

- Can be passive (lack of care) or active (make sure old products stop being (as) useful)
- “Greatest competitor is the products you have already sold”
- Vendor lock-in for maintenance leveraged to generate revenue
- User-driven maintenance/enhancement actively fought against
- Very naughty indeed

Complexity is the Enemy

- Sovereignty easy to exercise over simple digital artefacts, irrespective of permission
  - … and the opposite is true
- Huge effort may be required to exercise power of sovereignty, even when permission is granted
  - e.g., porting and maintaining an Android fork
  - e.g., designing and maintaining a mobile phone circuit design

The 2nd rise of Digital Sovereignty: Re-discovering Simplicity

- (Relative) simplicity is the cure for complexity and enabler of 2nd wave of Digital Sovereignty
- The question is how to make simple but still 21st century useful digital artefacts
- … and how to protect the future Digital Sovereignty of these systems

MEGA65

Mobile Phones are Hard to Make

- Teeny-tiny physical circuits
- Complex interfaces

… and that’s the easy part!

Mobile Phones are Hard to Make

- Teeny-tiny physical circuits
- Complex interfaces

  … and that’s the easy part!
- The software is so complex to port to new hardware, let alone to maintain.
  - … just ask FairPhone or Purism

MEGA65

Making Digitally Sovereign Mobile Phones is Even Harder

- Modern processors are untrustable
- No open 3G/4G modems
  - Even if you find one, it will be obsolete before you finish!
- Need cellular networks
  - And I don’t just mean a BTS, but complete open cellular-like functionality

Maintaining Digitally Sovereign Mobile Phones Even Harder Still

- Keeping up with Android (or any other mobile OS) takes >1 person-year per year.
- Keeping up with available CPU/GPU/SoCs takes >1 person-year per year.
- Point: Even if you overcome barriers and make something, you can’t maintain it.

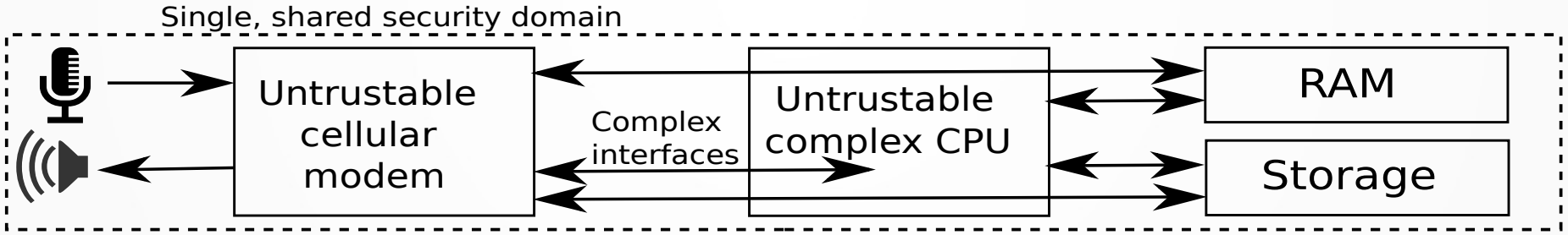
There are other open phone projects

- e.g., Librum5, WiPhone etc
- Varying degrees of open and capability
- More importantly, absolute Digital Sovereignty is traded-off for various (usually good and sensible) reasons
- We love the diversity the different projects bring, but our own goal is absolute Digital Sovereignty

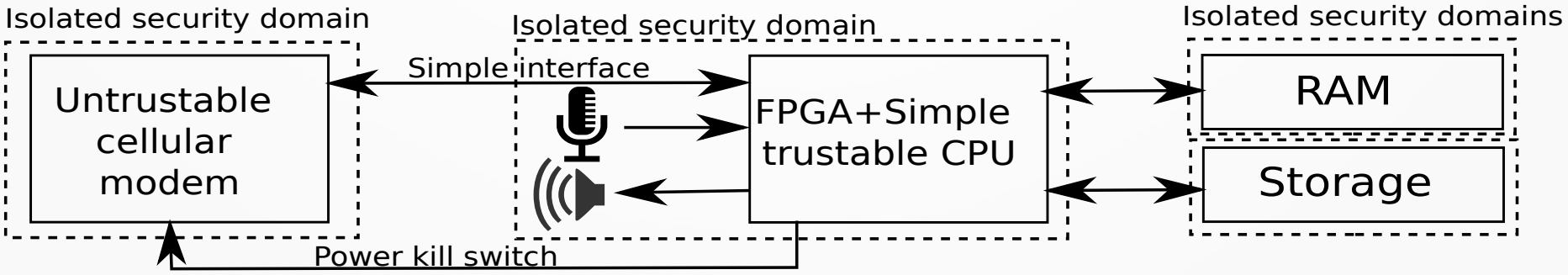
Reinventing Planned Obsolescence

- If you start obsolete, you can't get obsolete.
- Reduce features to minimise complexity
- Retain utility as much as possible
- Commodore 64, GEOS etc proved you can do a lot with a simple architecture
  - But can it do enough to really be useful?
  - Watch LCA talk to see telephone and slide presentation software with anti-aliased proportional text etc on the MEGAPhone.

System Architecture (3)

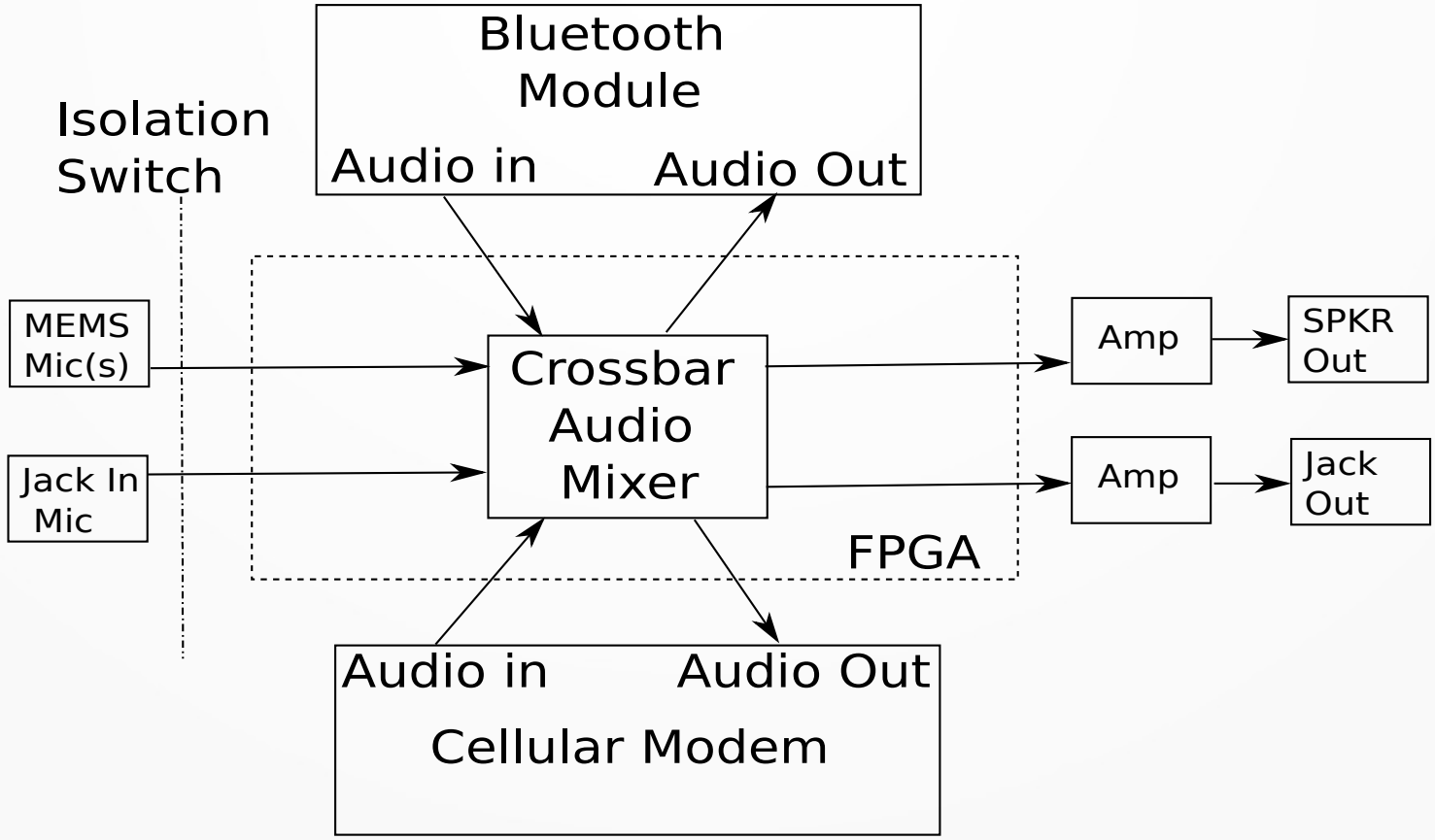


Typical Smart-Phone Architecture



Security Through Simplicity Architecture

Protected Audio Paths



Introducing The Little Brother

- Intel Management Engine is about opacity
  - But the idea of a simple and transparent management device has merit.
- Turn the idea on its head: open management processor controls the proprietary main processor.
- Divide and conquer
  - Re-use, e.g., Rpi Android port, industrial 4G cellular modems as subordinate components
- C64 derived management processor
  - Open processor. Open software
  - Implement core privacy functions directly, e.g,., microphone and telephony
  - Boot in <2 seconds! And plays games while the cellular modem boots!

Exercising Sovereignty over Untrustable Complex Components

- Use industry-standard miniPCIe cellular modems
  - loosely-coupled UART + PCM audio interface
- Use Raspberry Pi 3CM for “complex processor”
  - Android port maintenance becomes SEP
  - FPGA gen-locking video switch + peripheral simulation
- Both can be removed, replaced upgraded
- Device creation dramatically reduced
- Capability maintenance dramatically reduced

Exercising Digital Sovereignty over Mass Market-Oriented Products

- No need to limit ourselves to “normal” functions.
- Current prototype:
  - 2x miniPCIe form-factor expansion slots for 4G/5G/satellite/whatever
  - 4 microphones for experimenting with noise rejection
  - Full-size SIM/smart-card slot
  - 100 dB speaker with 2W amplifier
  - BT & WiFi
  - Joypad *plus* full-size C64 joystick port for 2-player fun…
  - 32Wh battery + provision for 7W solar panel on rear for Energy Sovereignty
  - Tri-band UHF packets radios for Infrastructure Sovereignty

Exercising Digital Sovereignty in Nearby Fields

- Realised we are creating a Digitally Sovereign Platform, not just a “phone”
- Field hospital patient monitor
  - Make pulse-oxy sensor expansion board
  - Write wiggly line software
- Open point-of-sales device
  - Use SIM/smart-card reader to read Giro/credit cards
- Field data collection device for disaster/humanitarian
  - Iridium satellite module expansion board
  - Adapt Serval Succinct Data software

Exercising Digital Sovereigny for Defeating Disibility Digital Divide

- Make phones with custom user interfaces for people living with disability
  - Customised for each person!
- Need to adapt only Little Brother, not Android
- Full source code + schematics can be given to user
- Allow continuous evolution according to user’s wishes
- Could be a great sustainable and ethical business ...

MEGA65

Packet-Radio Enabled Phones

- Theoretical possible with some existing phones
  - e.g., FairPhone2 has internal expansion connector
- Many problems remain with this approach
  - Energy / Small batteries
  - Effort to integrate with Android
  - Ongoing effort to maintain integration

Packet-Radio Enabled Phones

- Connect radios to Little Brother FPGA
  - Maintain communications when main processor is off
  - Perform communications from trustable portion of device
  - Full Digital Sovereignty to innovate on protocols etc
  - Could implement SDR in FPGA if desired

The MEGAPhone Prototype

- Artix 7 FPGA for Little Brother
  - Isolates all IO and communications devices from one another
  - All audio processing done here: Cellular modem has no direct connection to the microphone
- Power-cut switches for all sub-systems
- Proof-of-concept telephony software
- Tri-band LoRa radios on latest prototype
- Battery life ~10 hours with FPGA + screen on

“License Free” UHF Communications

- Not actually “license free”, but “liberally licensed”.
  - Think GPL etc: free to use, but some conditions applly
- ITU Guidelines for major global regions
- Europe and USA in different regions with no common useful band.
- National variations also!
- Europe particularly poorly served

“License Free” UHF Communications

- Three major bands:
  - 433-434 MHz
  - 868 MHz
  - 900ish* MHz
- No one band available everywhere
- Rules of use vary widely between jurisdictions
- Tri-band radio + GPS juristiction detection safest bet
  - But have radios fully Digitally Sovereign
  - i.e., don’t use a problematic authorisation database
- Digitally Sovereign phone hardware allows use of Digitally Sovereign radios

900ish MHz Band

- USA, Aus, NZ, Vanuatu etc: >5MHz >=1W EIRP
- But not the same 5MHz!
- No duty cycle restrictions in most countries
- 921MHz – 923MHz seems most common overlap
- 10s of kbits/second over several km possible
- Totally unavailable in Europe, AFAIK

433-434MHz

- Available in Europe with significant restrictions
- Recently became available in Australia, but with even worse restrictions
- Not available in the USA, AFAIK
- Poor bandwidth / distance trade-off due to restrictions
  - But can theoretically go a long way at very low effective data rates

868MHz

- Available in Europe, but not in many other places
- Very narrow band
- Highly congested

Licensed and Legacy Bands

- Citizen Band radio channels can be interesting
  - Not all jurisdictions allow digital modes
  - Duty-cycle limits may apply
  - But often 40+ (narrow) channels near 27MHz or 460MHz
  - Typically 5W EIRP power limit = 5 – 25km range

Licensed and Legacy Bands

- … or just license a frequency and use it!
- Digital Sovereignty makes it possible to use
- Price varies wildly based on jurisdiction, frequency, bandwidth, EIRP and phase of moon
- e.g., 5,000km^2 region of Australian Outback, 10W EIRP, a few MHz wide can be as little as ~ $100 per year

HF can be fun

- Modern HF radios include data modems
- Combine with encrypt-at-microphone + One Time Pad in MEGAphone and full Digital Sovereignty
- Can reproduce capability of SIGSALY from WW-II
  - Global reach, provable security

SDR and Dynamic Spectrum Use

- FPGAs are great for implementing SDR
- In-field re-purposing possible
  - e.g., gain frequency allocation during a disaster and use Digital Sovereignty to change software (or hardware) to use

UHF Communications Protocols

- An open area, due to historical lack of activity
- Low-bandwidth, intermittent connections favours Delay Tolerant Networking
  - Text Messaging, voice mail, file exchange etc
  - Web browsing, not so much
- Serval Rhizome is one option
  - Experimental support for several UHF and HF radios
  - Will port to MEGAphone's Little Brother

Conclusion

- Digital Sovereignty is important to reclaim, and is within reach.
- Remove barriers through simplicity
  - MEGAphone as proof-of-concept of what small poorly-resourced team can achieve in short time
- We want to make the MEGAphone useful
  - … and we could really do with your help on a bunch of fronts

MEGA65


THE COMMODORE C65 DEVELOPMENT SYSTEM
COPYRIGHT 1991 COMMODORE ELECTRONICS, LTD.
COPYRIGHT 1977 MICROSOFT
BASIC 10.0 V0.98.911001 ALL RIGHTS RESERVED
Thank you
for your interest!