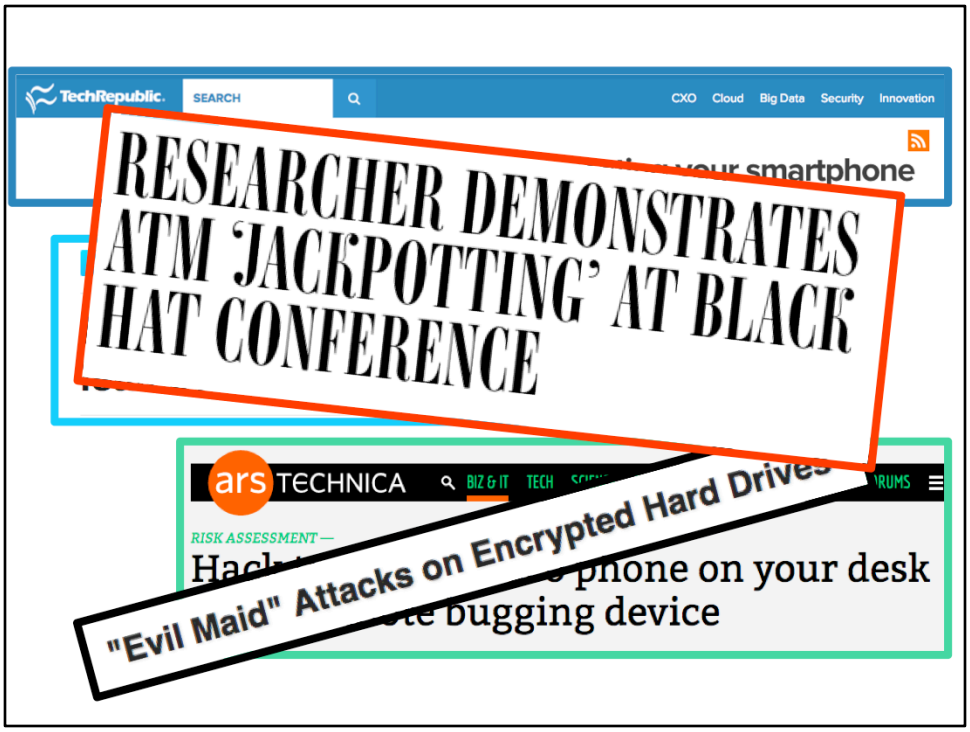
You Can Be a Hardware Hacker, Too!

Jennie Kam

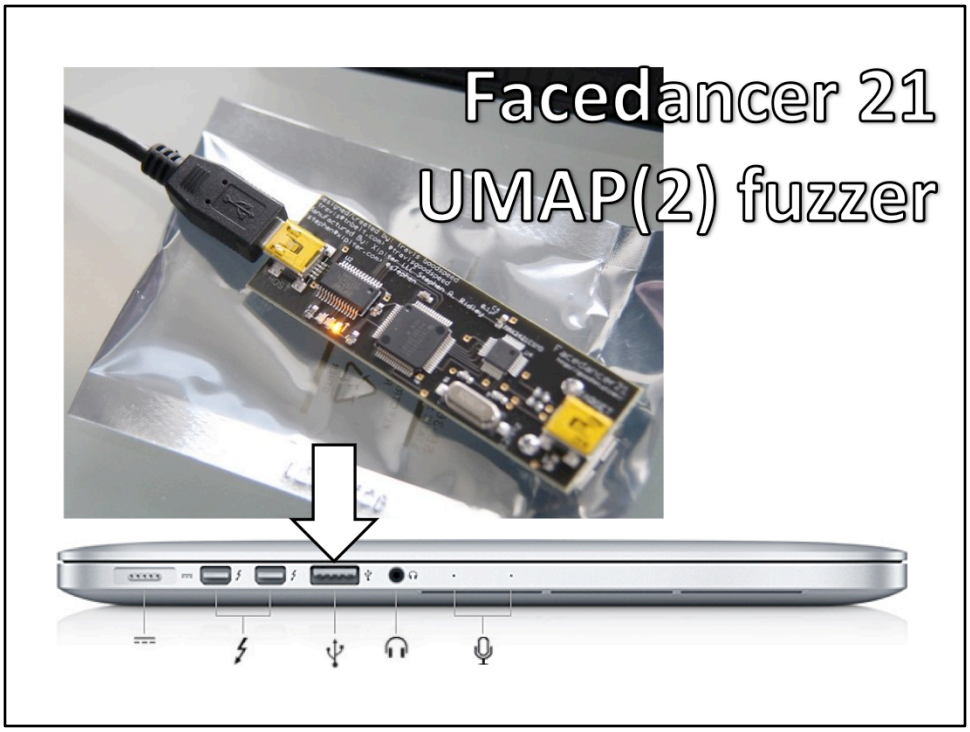
 @TXJennieK

I've had many software folks tell me that hardware is magic, which it's not, it's just electrons. Before Kali Linux evolved, I couldn't conduct a port scan, attack a web app with cross site scripting, or crack passwords. I'd like to invite anyone who doesn't consider themselves a hardware person to dabble in this community with these beginner friendly tools and a few seeds of knowledge.

Addressing the next common excuse: Because hardware hacking requires physical access, many feel this craft is meaningless when one can just unplug the device and POOF! Instant denial of service.



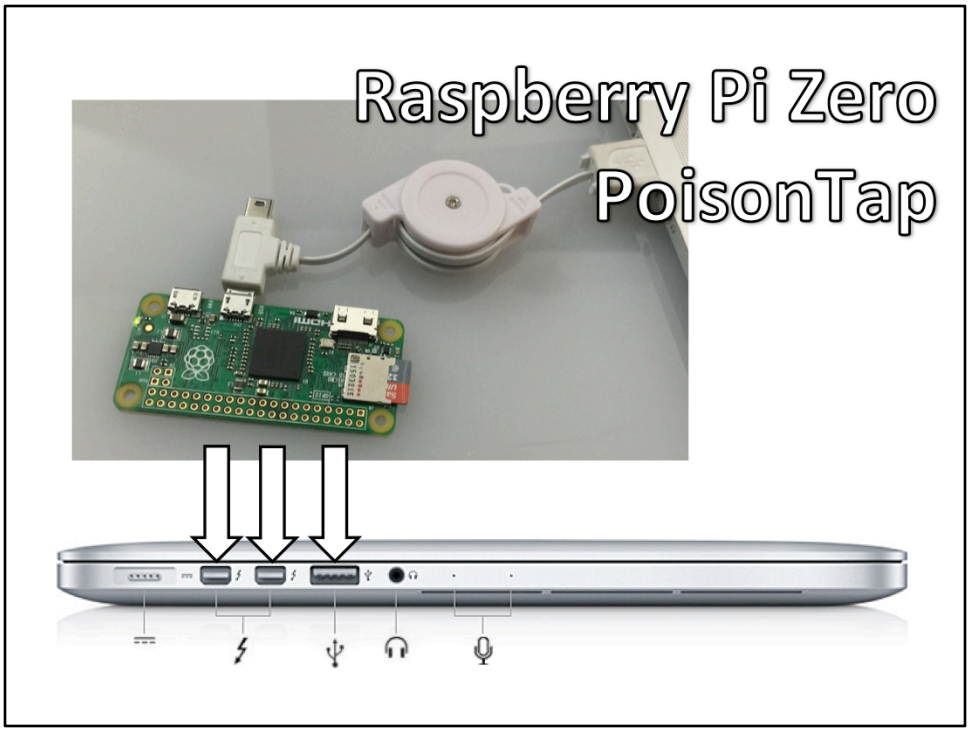
Guess what? Sometimes the end game isn't a denial of service. I'm sure the companies featured in these headlines would have loved researchers to stop after pulling the plug – but the attackers wanted unsigned code execution, remote listening capabilities, encrypted data, or cash.



Onto the tools! These first two can be used to conduct “pluggable” attacks – where one just needs temporary, possibly quick, access to a target.

Let's start with the familiar and easily accessible- the USB port. There's a tool called a Facedancer that enables python programmers to emulate USB devices. Not a programmer? An open source fuzzing framework called UMAP(2) will give you a good jump on finding USB traffic your test device can’t handle. Everything’s a tradeoff though – while the accompanying software makes this a good starting point, it’ll run you close to $75.

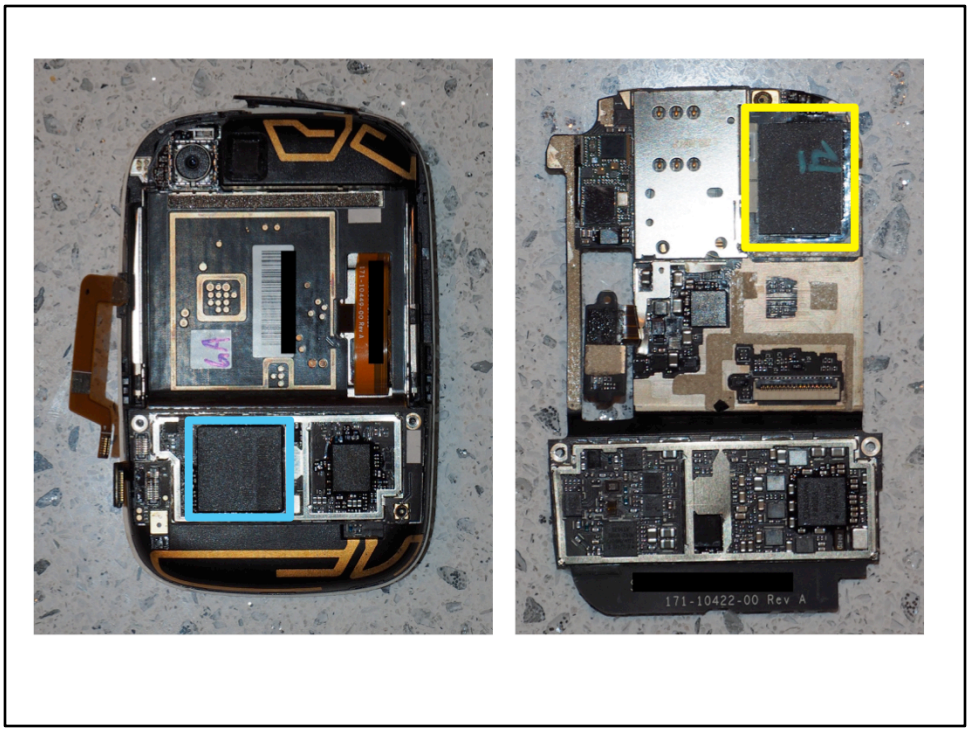
Travis Goodspeed Facedancer 21: http://goodfet.sourceforge.net/hardware/facedancer21/
Andy Davis UMAP: https://github.com/nccgroup/umap
Binyamin Sharet UMAP2+Kitty: https://github.com/nccgroup/umap2



Along the same lines, for the JavaScript crowd, we have a Raspberry Pi Zero at the super low cost of $5 and a project dubbed PoisonTap that emulates a USB or thunderbolt Ethernet device. This malicious Ethernet device hijacks all network traffic from your target computer and leave behind a few remote back doors as a bonus! While this tool is cheaper in money, it may cost you more in time due to the smaller community documenting it.

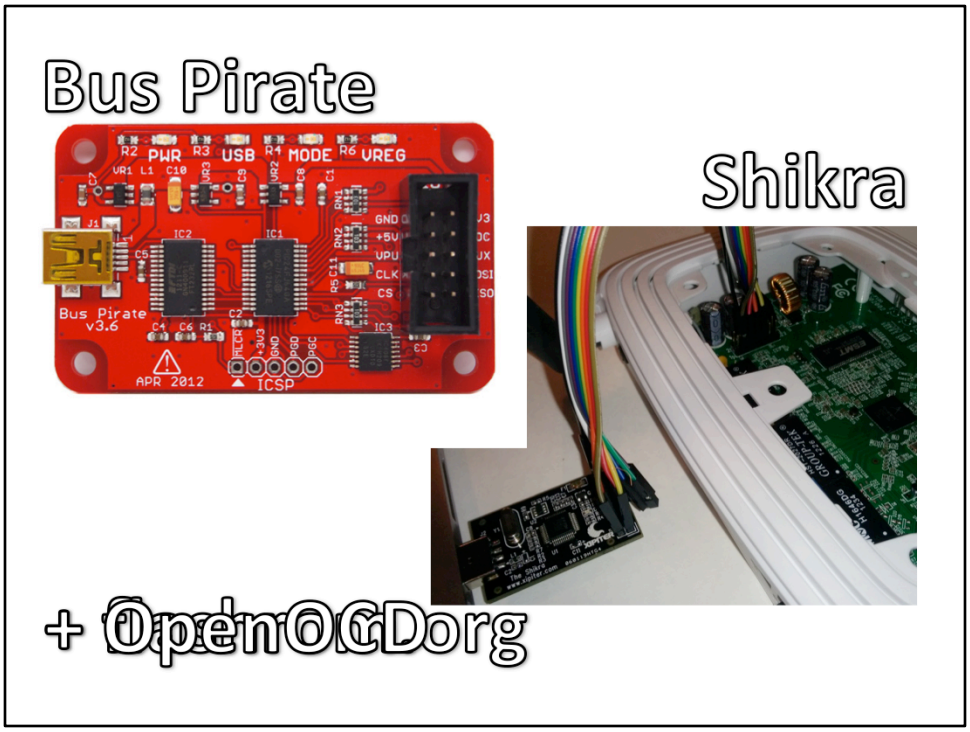
Raspberry Pi Zero: https://www.raspberrypi.org/products/pi-zero/
Samy Kamkar PoisonTap: https://samy.pl/poisontap/

So let's get a taste of how to start hacking printed circuit boards, or PCBs, found inside your everyday electronics. We're going to use this HP Veer, a credit card sized smartphone from 2011.



I used an eyeglasses screwdriver set – the phillips on the 4 screws and the flathead for leverage in popping off plastic parts and pulling back thin metal shielding called cans. Of course, I'm not in the business of putting things back together. If you are, you may want to consider gentler methods and tools of teardown.

Next use your favorite search engine on all the text you can read from the IC chips (plastic, black rectangles) and you're likely to turn up a processor, highlighted in blue, and some flash memory for firmware highlighted in yellow.

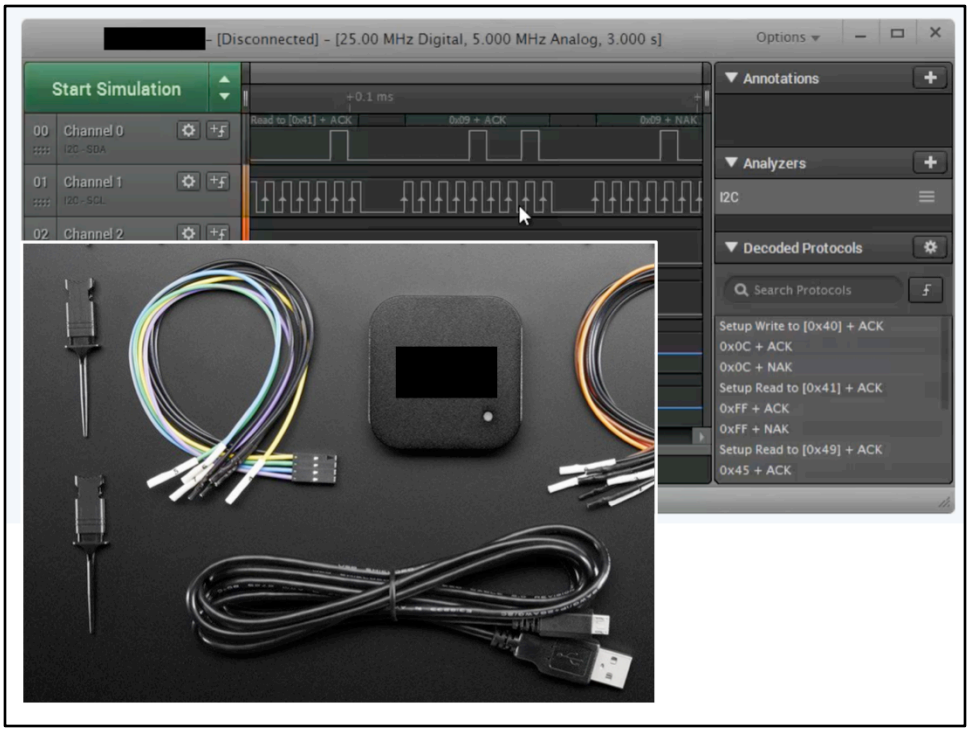


Once you've found the flash look nearby for any labeled debugging pins. Here's where the Bus Pirate or Shikra will come in handy. These tools can be paired with the flashrom project to read the binaries from a variety of chips. The recovered binaries are then ready for your favorite disassembler or friend who specializes in reverse engineering.

Depending on your target, you may also encounter hardware crypto accelerators or other ICs that could be sharing interesting secrets. The ICs typically speak a form of serial communication. Lucky for us, the Bus Pirate and Shikra enable us to speak and monitor these protocols as well.

Another program to use with these tools is OpenOCD or open on-chip debugging that allows you to halt CPU execution, and read registers or memory as you step through a program. You might use this once you've caused a crash and need more information about the state of the processor. Or, you could use it to confirm code flow you've discovered through reverse engineering.

Dangerous Prototypes Bus Pirate: http://dangerousprototypes.com/docs/Bus_Pirate
Xipiter Shikra: https://int3.cc/products/the-shikra
Xipiter Shikra Getting started: http://www.xipiter.com/musings/using-the-shikra-to-attack-embedded-systems-getting-started



With a little extra money, you can up your game and get closer to the electrons in action. There are a number of USB logic analyzers for less than $200 which will show you what a bunch of signals on the board are doing at the same time. For instance, if you have a few processors (main, wi-fi, crypto acceleration) and want to know the order in which they boot, this would be your tool.

That's NOT all folks!

Let's continue the conversation:

@TXJennieK

github.com/TXJennieK

Happy hacking, y'all.