Low-Cost Side Channel Attacks on Smartphones and Embedded Devices using Software Defined Radios

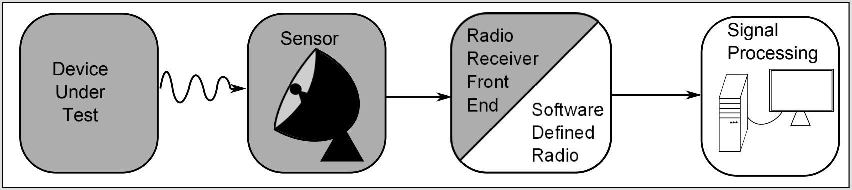
Gabriel Goller

2015/11/5

Giesecke & Devrient

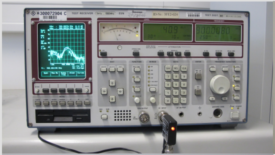
Creating Confidence.

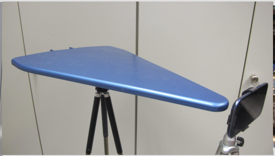
Introduction

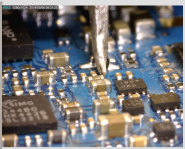


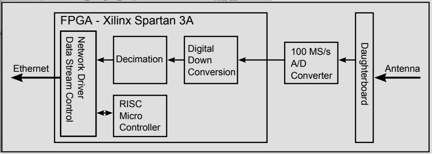
Capture the electromagnetic emanations of a device with state of the art radio equipment to use them for a side channel attack.

Experimental Setup - Hardware



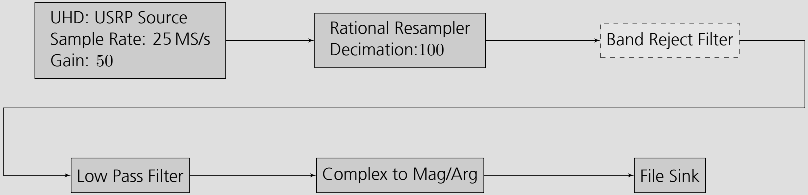






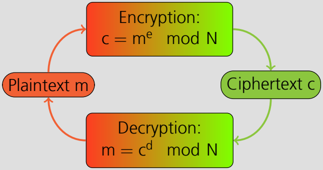
- 2 Antennas: Log-P and Bi-Quad
- ESN test receiver with preamplifier
- High-end setup using USRP N210 connected to IF of ESN
- DVB-T stick as low-cost alternative

Experimental Setup - Software



- GNURadio to process and record data
- Octave for offline post-processing

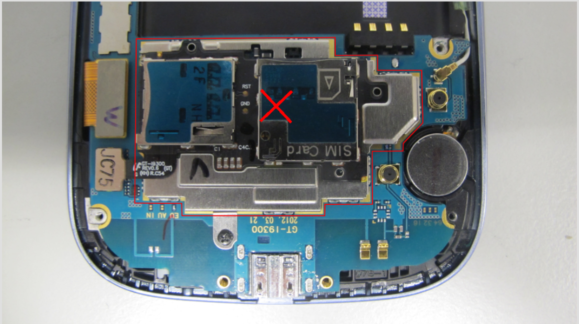
Device under Test - Software




```
function square-and-multiply(c, d, N)
    result = 1
    for each bit(d)
            from (number_of_bits(d) - 1)
            downto 0
        result = square(result) mod N
        if bit(d) == 1
            result = (c * result) mod N
        end if
    end for
    return result
end function
```

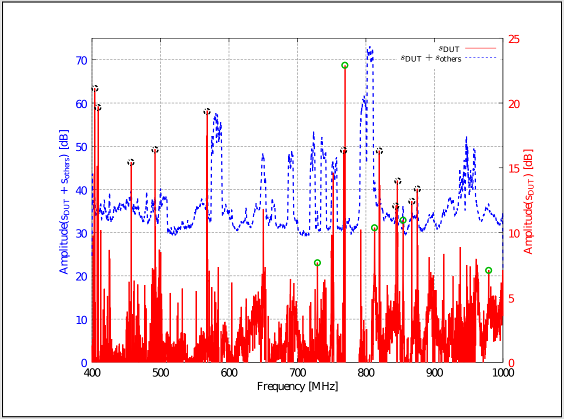
- Simple Square & Multiply Algorithm implemented in C using functions provided by OpenSSL.

Devices under Test - Hardware



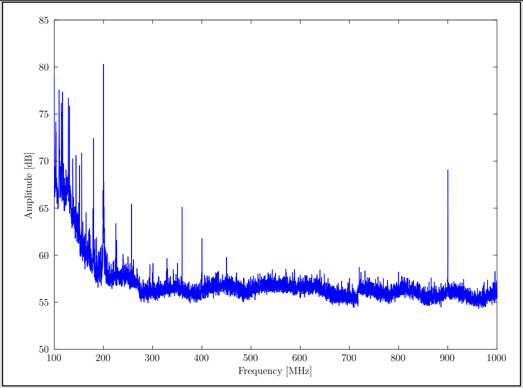
- CPUs based on ARM architecture
- Android (BeagleBone Black, smartphones) and Linux (Raspi)
- Removal of all shieldings and housings for tests

Finding Emanations



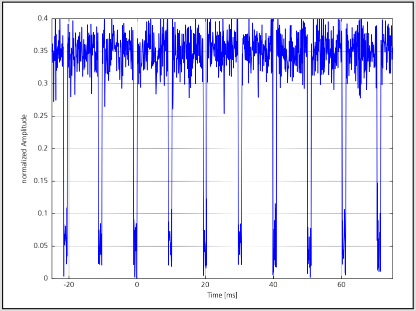
- Measurements using Frequency Sweep

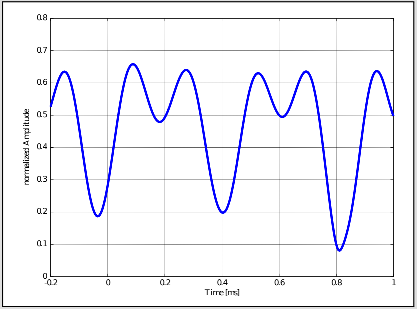
Finding Emanations II



- Measurements using Nearfield Probe
- Educated Guessing

CPU Dependent



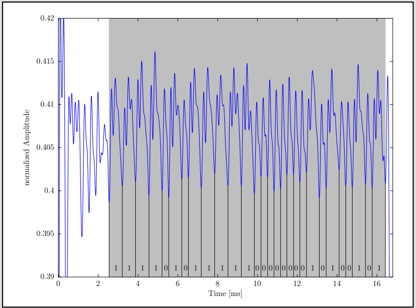


- A signal which correlates with the program flow can be found when the clock frequency of the CPU is set to a fixed value.
- No SPA possible.

Post-Processing of Signals

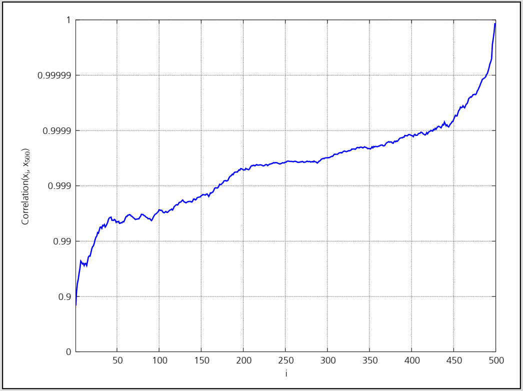
Steps:

- Record signal with multiple S&M executions with same secret key d
- Extract each trace t where algorithm is executed (automated)
- Compute $y(t) = \text{mean}(t_1(t), t_2(t), t_3(t), \ldots)$



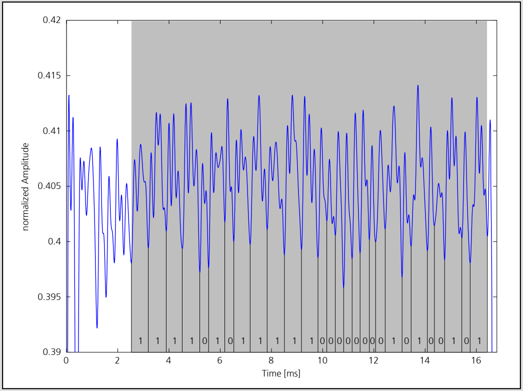
Automated averaging of multiple signal blocks makes it possible to extract key of S&M algorithm.

Evaluation - Number of Traces



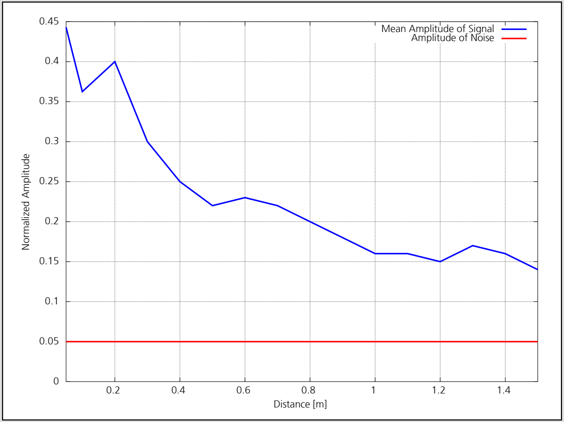
- $y(i) = \text{corr}[\text{mean}(t_1, t_2, \ldots, t_{500}), \text{mean}(t_1, t_2, \ldots, t_i)]$
- ~ 170 traces should be sufficient to reconstruct key

Evaluation - Number of Traces



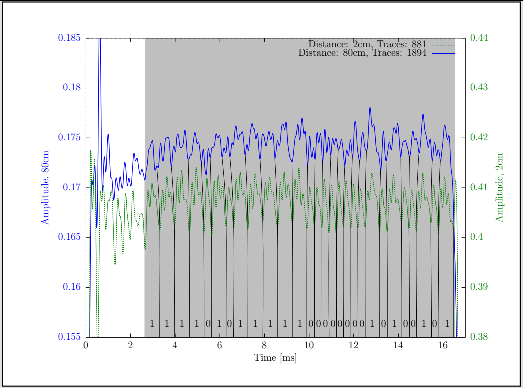
- $y(i) = \mathrm{corr}[\mathrm{mean}(t_1, t_2, \ldots, t_{500}), \mathrm{mean}(t_1, t_2, \ldots, t_i)]$
- ~ 170 traces are sufficient to reconstruct key

Evaluation - Distance & Shielding



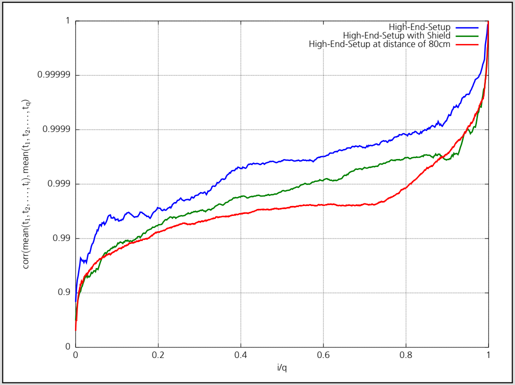
- Signal measurable up to a distance of 1.5 m.

Evaluation - Distance & Shielding



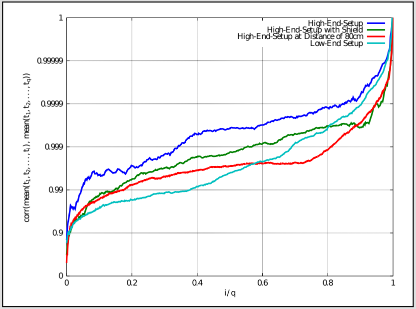
- Successful attack at distance of 80 cm using 1894 traces.
- Reaffixing shielding plate results in similar effects.

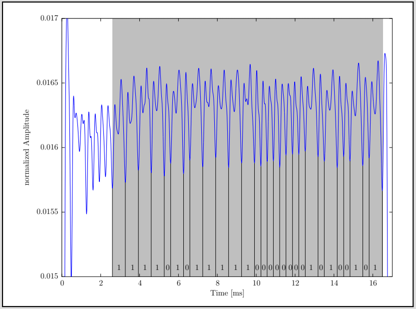
Number of Traces II



- Shielding: Correlation of 0.999 with 276 traces ($\approx$ factor 1.6)
- Distance: Correlation of 0.999 with 1530 traces ($\approx$ factor 9)

Evaluation - Lowcost Setup





- Reduced costs to under 30 €
- Signal-to-noise ratio decreased from 13.94 dB to 11.82 dB
- Correlation of 0.999 with 346 traces ($\approx$ factor 2)

Evaluation - Miscellaneous

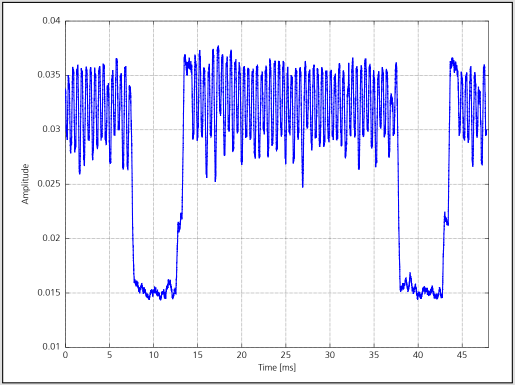
Device	OS	CPU Frequency	Attack possible?	Remove Shielding?	Orientation
DUT 1 SBC	Android	1000 MHz	Yes	No	→
DUT 2 SBC	Linux	900 MHz	Yes	No	→
DUT 3 Smartphone	Android	900 MHz	Yes	Yes	→
DUT 4 Smartphone	Android	1000 MHz	Yes	No	↗
DUT 5 Smartphone	Android	1000 MHz	Yes	Yes	↑

- 5 different devices were tested, all with the same results.
- The smartphone also emits signals when disassembled.

Near Field Sensors

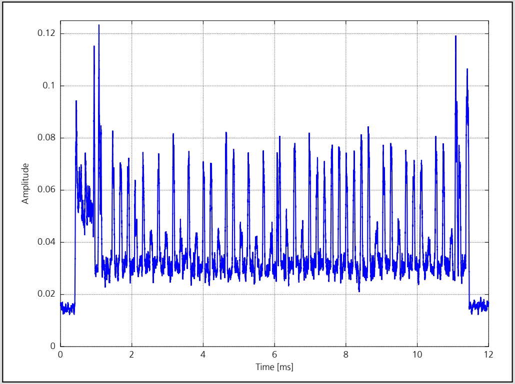
- Wideband signals emanated at frequencies near 35MHz

Signal



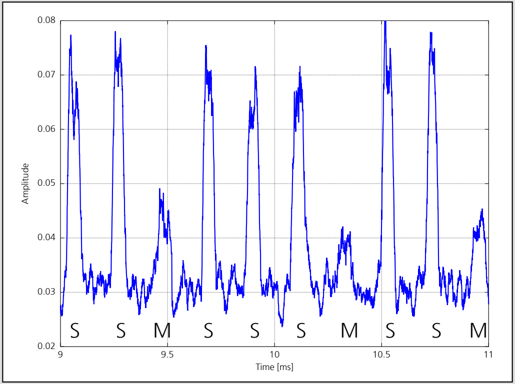
- Different signals are emanated depending on the CPU clock frequency.

SPA - CPU Clock Frequency 1400 MHz



- Visual inspection

SPA - CPU Clock Frequency 1400 MHz



- Visual Inspection

SPA - CPU Clock Speed

CPU Clock	Signal?	SPA?
1400 MHz	Yes	Yes
1300 MHz	Yes	Yes
1200 MHz	Yes	Yes
1100 MHz	Yes	Yes
1000 MHz	Yes	Yes
900 MHz	Yes	Yes
800 MHz	Yes	Yes

Frequency	Signal?	SPA?
700 MHz	Yes	Yes
600 MHz	Yes	Yes
500 MHz	Yes	Yes
400 MHz	Yes	No
300 MHz	Yes	No
200 MHz	No	No

- At most CPU frequencies, the key could be extracted directly by visual inspection.
- Rule of thumb:
  "The higher the CPU clock speed, the better the signal"

Summary

- SCA on embedded devices and smartphones are feasible using standard radio equipment.
- The experimental setup can be built for less than 30 €.
- A private key can be extracted with only 170 traces.
- Attack was successfully conducted on multiple devices.
- An even cheaper attack can be mounted from a closer distance using a near field probe.

Demo - Lowcost Far Field Setup

```
function square-and-multiply(c, d, N)
    result = 1
    for each bit(d)
             from (number_of_bits(d) - 1)
             downto 0
        result = square(result) mod N
        if bit(d) == 1
        result = (c * result) mod N
        end if
        sleep()
    end for
    return result
end function
```

Demo - SCA with Near Field Setup

```
function square-and-multiply(c, d, N)
    result = 1
    for each bit(d)
            from (number_of_bits(d) - 1)
            downto 0
        result = square(result) mod N
        if bit(d) == 1
        result = (c * result) mod N
        end if
    end for
    return result
end function
```