Defending humans against killers

Attack: “We kill people based on metadata.” —April 2014, Michael Hayden (DIRNSA 1999–2005; DIRCIA 2006–2009)

Defending humans against killers

Attack: "We kill people based on metadata." —April 2014, Michael Hayden (DIRNSA 1999–2005; DIRCIA 2006–2009)

Countermeasure: Eliminate the metadata.

Defending humans against killers

Attack: "We kill people based on metadata." —April 2014, Michael Hayden (DIRNSA 1999–2005; DIRCIA 2006–2009)

Countermeasure: Eliminate the metadata.

But do they also kill people based on content?

Defending crypto libraries against side-channel attacks

Crypto libraries leak secrets through metadata.
e.g. 2012 CRI DEMA attack against smartphones
extracted secrets from timing of memory accesses.

Defending crypto libraries against side-channel attacks

Crypto libraries leak secrets through metadata.
e.g. 2012 CRI DEMA attack against smartphones
extracted secrets from timing of memory accesses.

Countermeasure: Eliminate the metadata.
No secret memory addresses, no secret branch conditions.
e.g. NaCl crypto library (Bernstein–Lange–Schwabe).

Defending crypto libraries against side-channel attacks

Crypto libraries leak secrets through metadata.
e.g. 2012 CRI DEMA attack against smartphones
extracted secrets from timing of memory accesses.

Countermeasure: Eliminate the metadata.
No secret memory addresses, no secret branch conditions.
e.g. NaCl crypto library (Bernstein–Lange–Schwabe).

Which secrets still leak via *data* being processed?
How can we defend crypto libraries against these leaks?

Defending crypto libraries against side-channel attacks

Crypto libraries leak secrets through metadata.
e.g. 2012 CRI DEMA attack against smartphones
extracted secrets from timing of memory accesses.

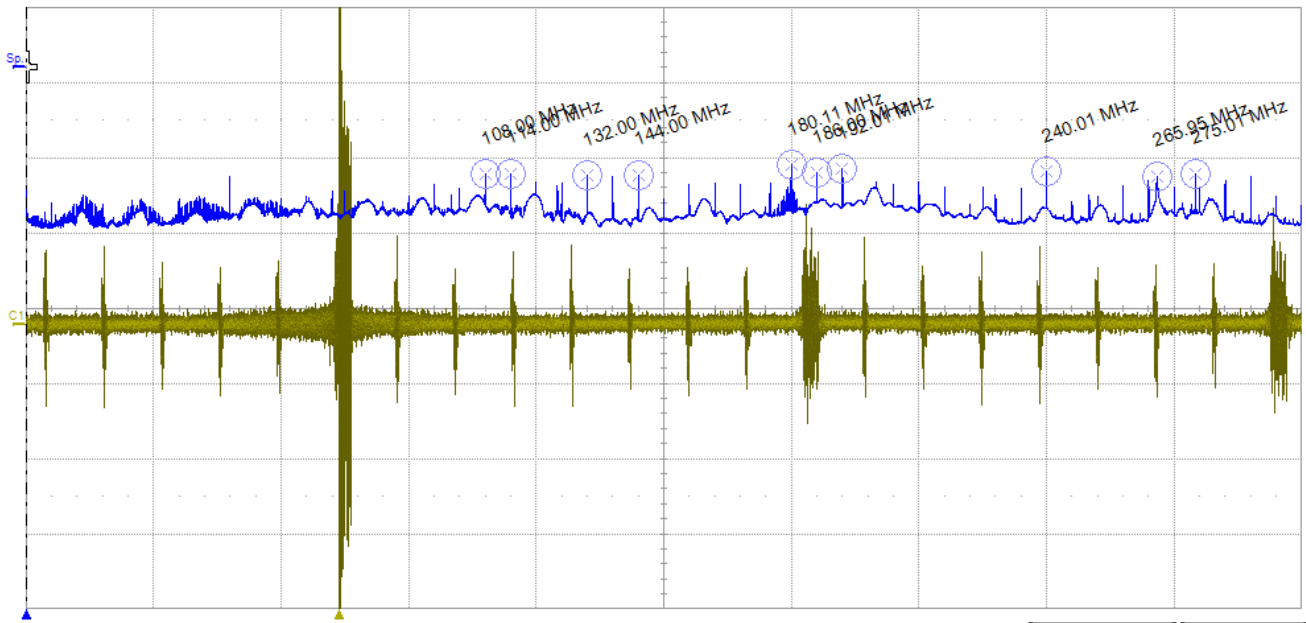
Countermeasure: Eliminate the metadata.
No secret memory addresses, no secret branch conditions.
e.g. NaCl crypto library (Bernstein–Lange–Schwabe).

Which secrets still leak via *data* being processed?
How can we defend crypto libraries against these leaks?

News (Bernstein–Bekkers–Lange): successful EM extraction of secrets from **constant-time software** running on **fast ARMs**.

SRAM data on fast ARM → EM → key recovery

SpecAn	Freq.	Amplitude
1	180.114 MHz	-64.98 dBm
2	192.005 MHz	-67.53 dBm
3	240.006 MHz	-69.56 dBm
4	186.004 MHz	-70.43 dBm
5	275.005 MHz	-70.67 dBm
6	114.002 MHz	-70.90 dBm
7	108.002 MHz	-71.08 dBm
8	144.004 MHz	-71.59 dBm
9	132.002 MHz	-72.24 dBm
10	265.947 MHz	-72.32 dBm



Arithmetic data on fast ARM → EM → key recovery