Defending humans against killers


Daniel J. Bernstein (UIC, TU/e) and Tanja Lange (TU/e)
Defending humans against killers


Countermeasure: Eliminate the metadata.

Daniel J. Bernstein (UIC, TU/e) and Tanja Lange (TU/e)
Defending humans against killers


Countermeasure: Eliminate the metadata.

But do they also kill people based on content?

Daniel J. Bernstein (UIC, TU/e) and Tanja Lange (TU/e)
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.

Daniel J. Bernstein (UIC, TU/e) and Tanja Lange (TU/e)
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.

Daniel J. Bernstein (UIC, TU/e) and Tanja Lange (TU/e)
SRAM data on fast ARM → EM → key recovery
Arithmetic data on fast ARM → EM → key recovery

Daniel J. Bernstein (UIC, TU/e) and Tanja Lange (TU/e)