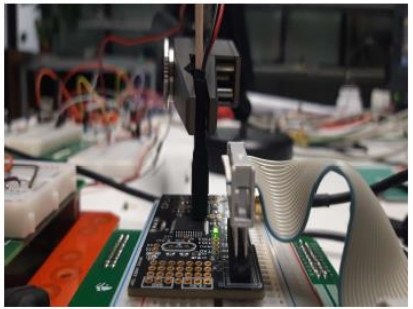
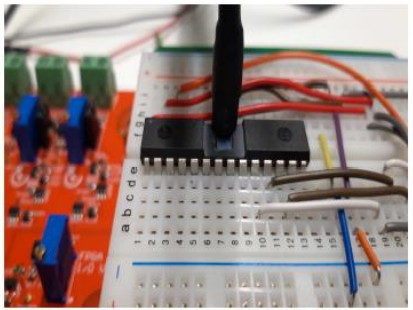
SiliconToaster: A Cheap and Programmable EM Injector for Extracting Secrets

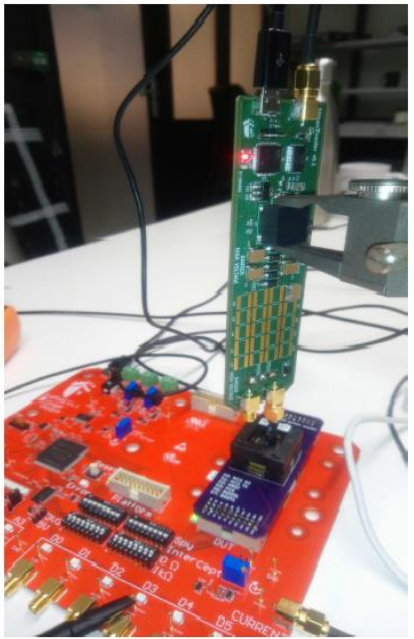
Karim Abdellatif and Olivier Hériveaux

Goals

- Building a home-made platform for injecting EM pulses
- Considering low cost components
- Platform validation





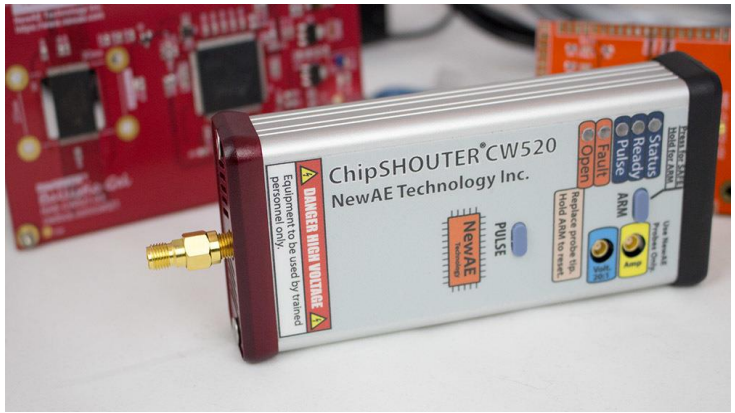


Agenda

- A short review of the state-of-the-art setups
- Presenting the design details of the SiliconToaster
- Application: Attacking the firmware protection of an IoT chip
- Conclusion

Previous Setups

Commercial Tools



ChipSHOUTER, $3300 USD (NewAe)

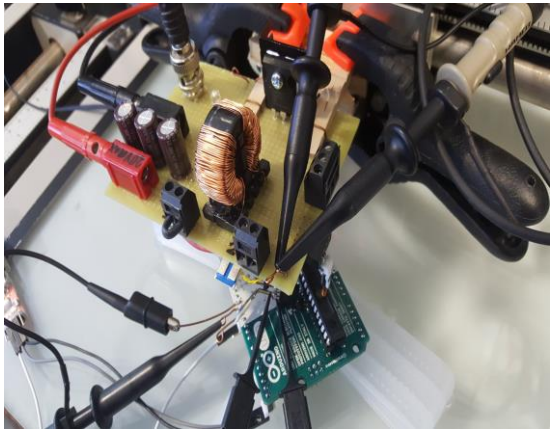
ChipSHOUTER: http://store.newae.com/chipshouter-kit/

Setups from Academia

Ordas et al. (FDTC 2015)

- **Commercial** pulse generator

Cui et al. (USENIX 2017)



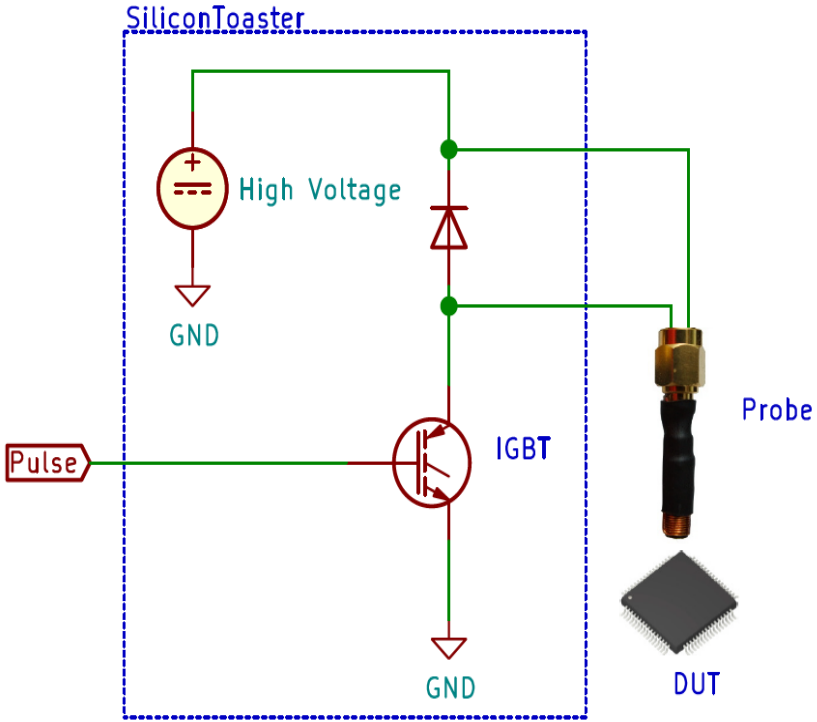
Balasch et al. (DCIS 2017)

- Hand-made pulse generator with **fixed voltage**
- **External power** supply to feed the pulse generator

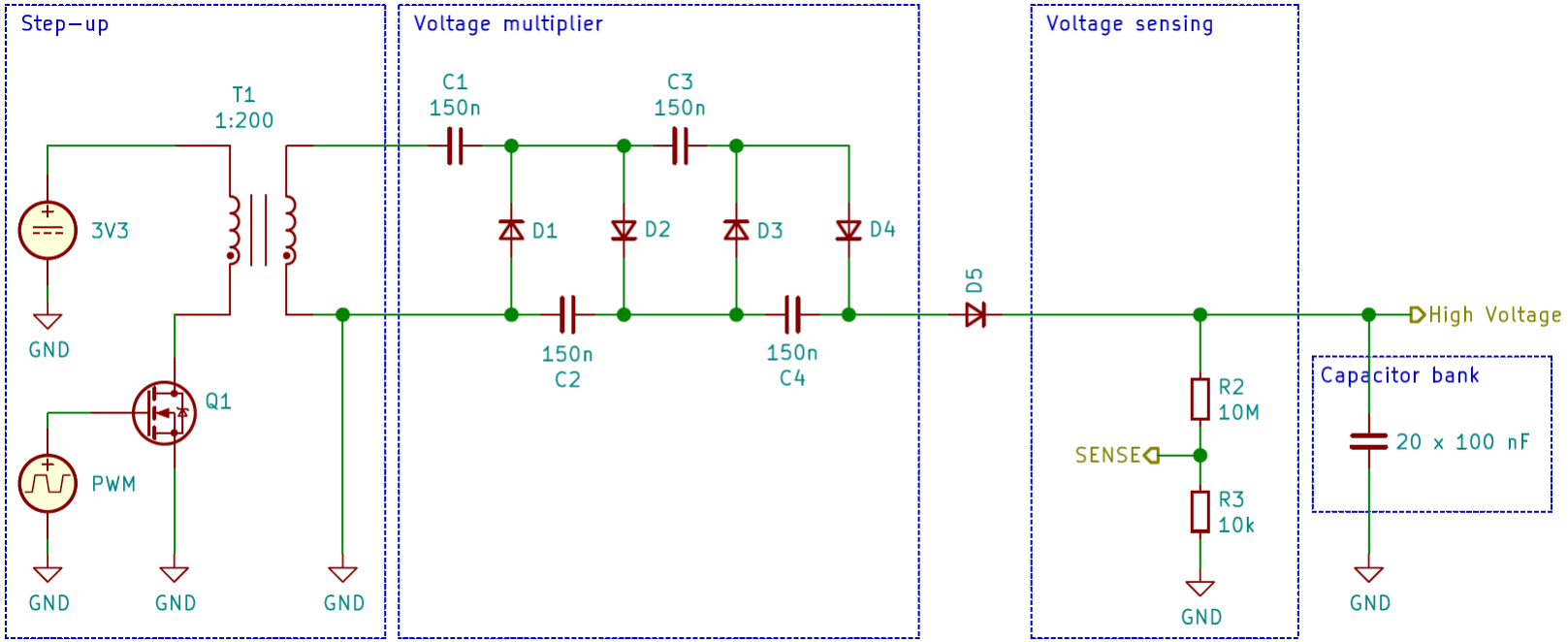
SiliconToaster

SiliconToaster

- Programmable high voltage generation up to 1.2KV
- High voltage switching circuit
- Probe fabrication

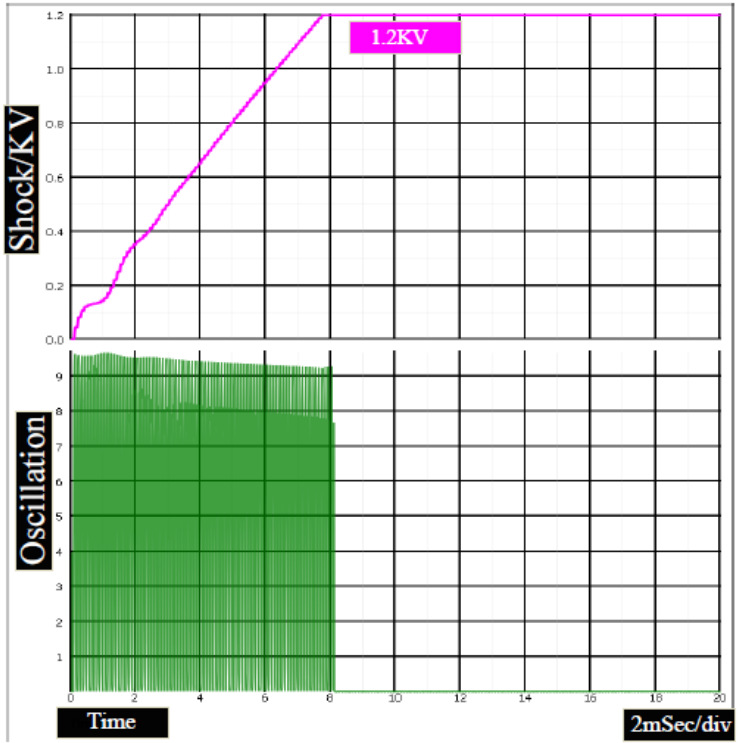


High Voltage Generator



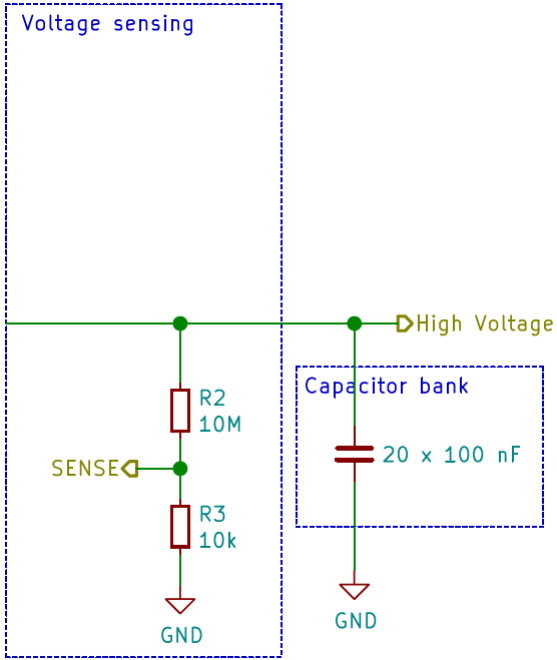
Programmable Voltage

- The generated high voltage depends on several parameters such as:
  - Number of pulses
  - Frequency of the input pulses
  - Pulse width
- With 8ms of pulses and frequency of 10KHZ, the output voltage is 1.2kV

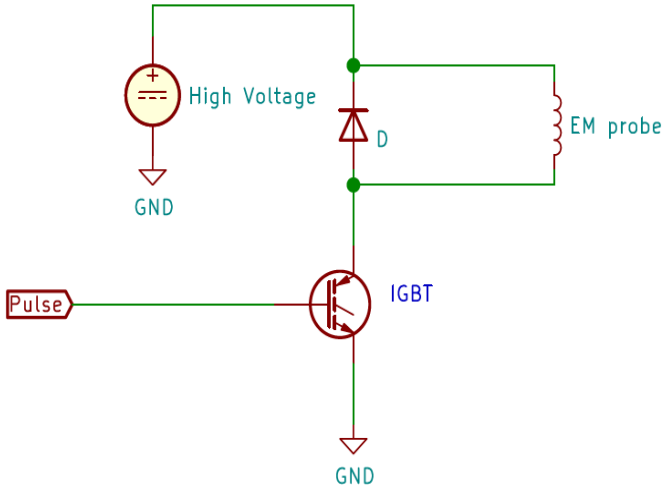


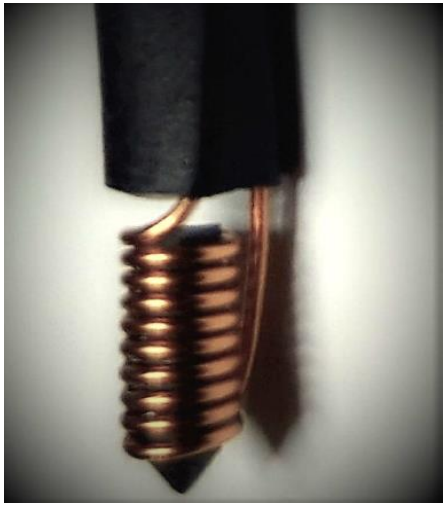
MCU-PWM

- The MCU changes the duty cycle of the input pulse to control the generated voltage
- PWM peripheral of STM32F2 [18] is used
- Another important feature is also using the analog-to-digital converter of the MCU.



High Voltage Switching circuit + Probe fabrication

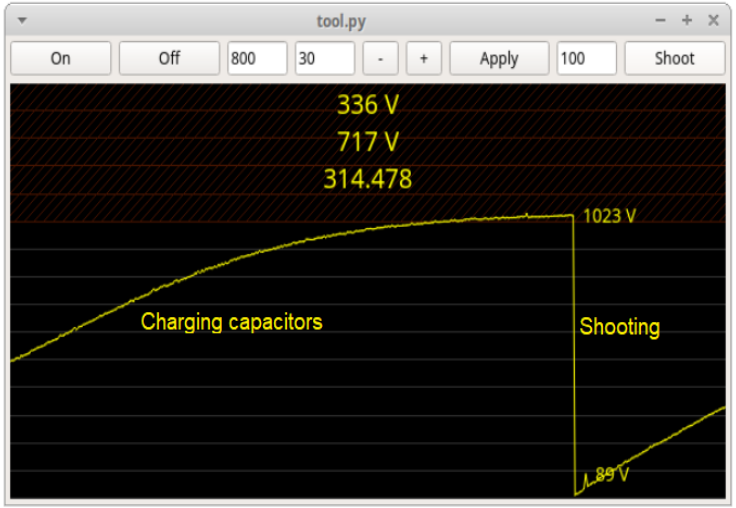


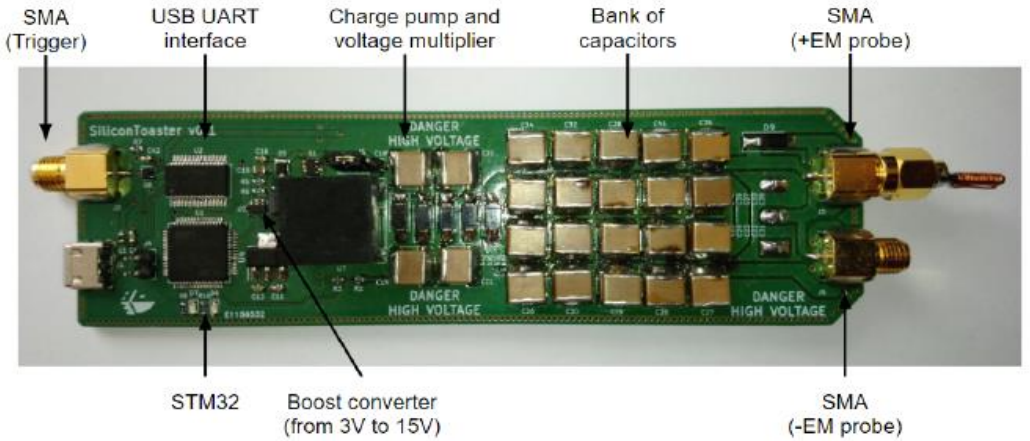


- IGBT: maximum ratings are 1.2kV collector-emitter voltage, 40A pulsed current and 20V gate-to-emitter voltage

- Fabricated from a flat coil of 6.6 mm diameter with 9 turns

Final Model + GUI





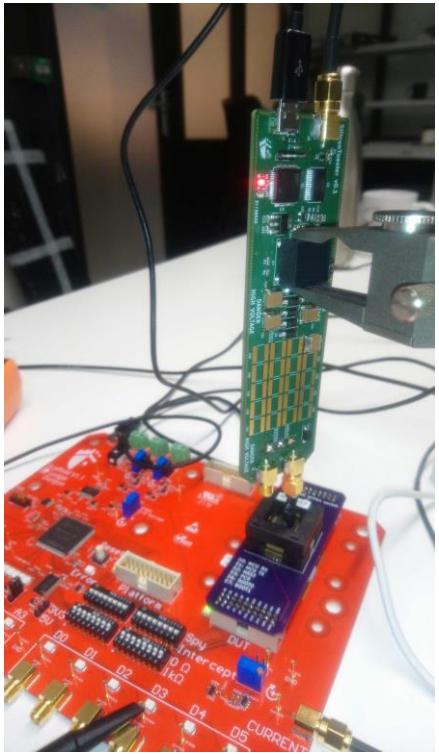
Application

Platform Validation

- **An IoT chip has three different configuration modes**
  - **A**: No security feature is activated
  - **B**: Bootloader is enabled, but commands used to read and write memory are disabled
  - **C**: All the security features for protect IP protection are enabled
- **The goal is to convert the configuration from C to A to dump the firmware**

Setup

- The DUT was placed in a custom board socket
- **SiliconToaster** is used for injecting EM pulses to bypass the security configuration modes
- **Scaffold** board is also used to communicate with the DUT

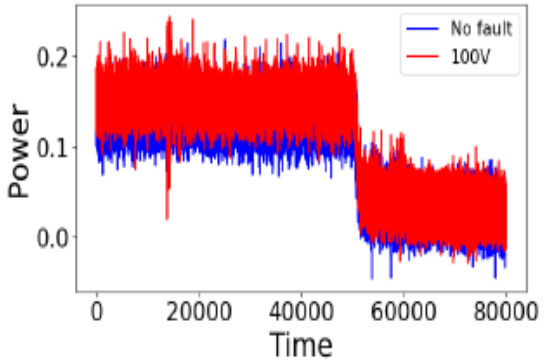


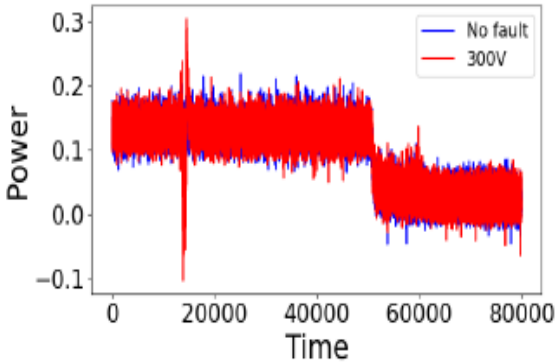
C configuration Attack

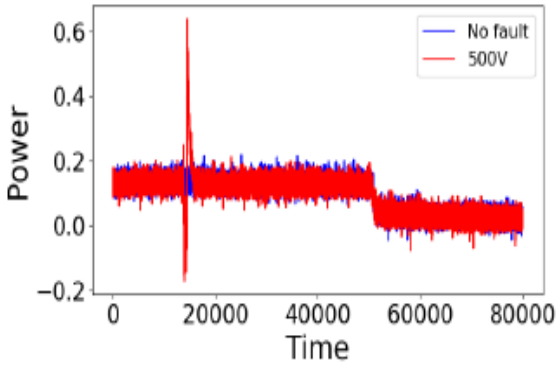
Algorithm 1: Attack sequence of C configuration

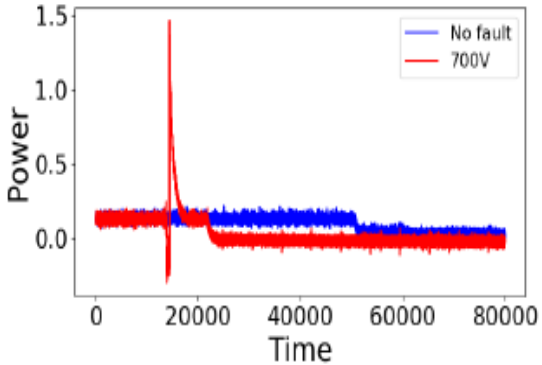
```
while True do
    Initialize-SiliconToaster(voltage, width, offset);
    uart.transmit(X, trigger=1);
    if (uart.receive=ACCEPT) then
        Go to B configuration attack;
```

Programmable EM Pulse

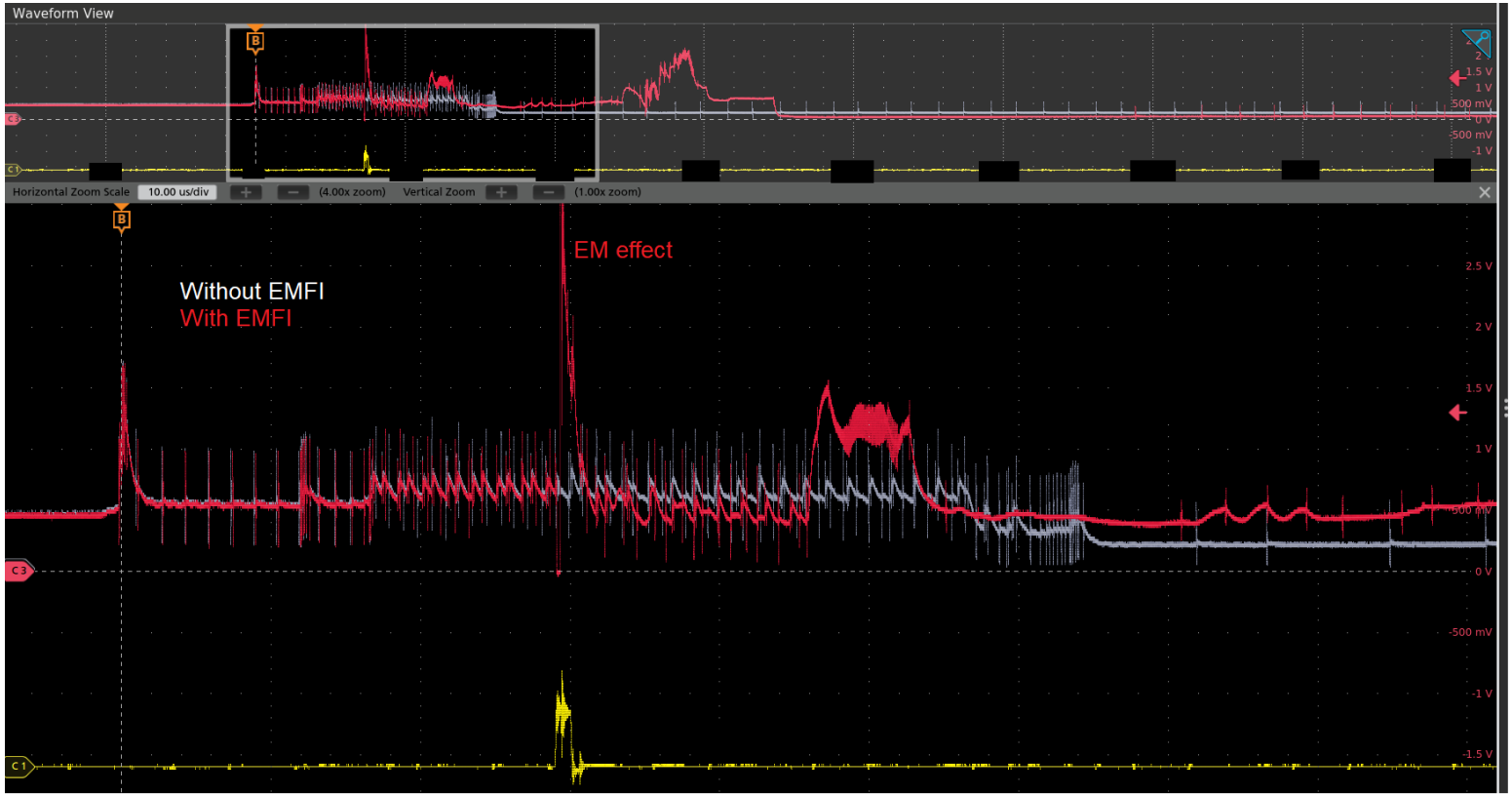








C Configuration Attack: 400V + Success= 60%

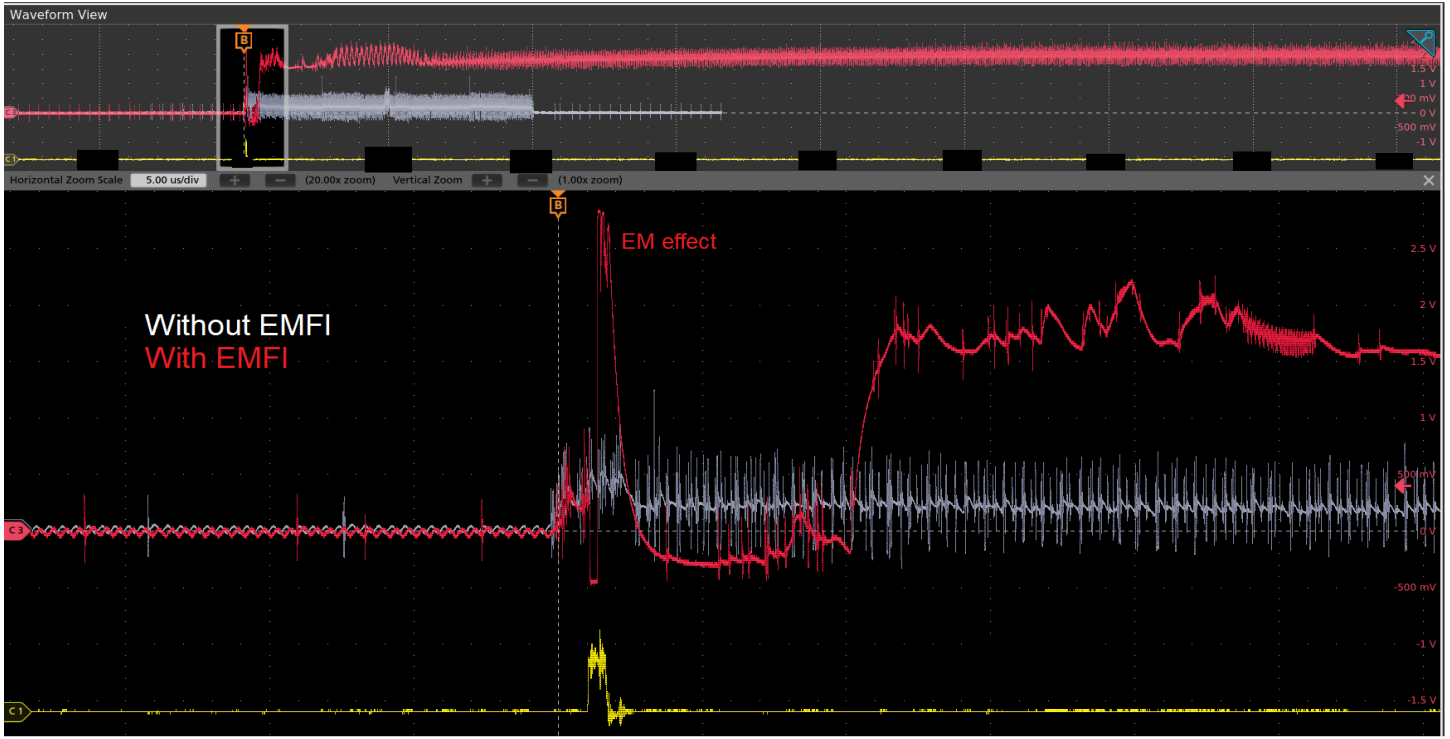


B configuration Attack

Algorithm 2: Attack sequence of B configuration

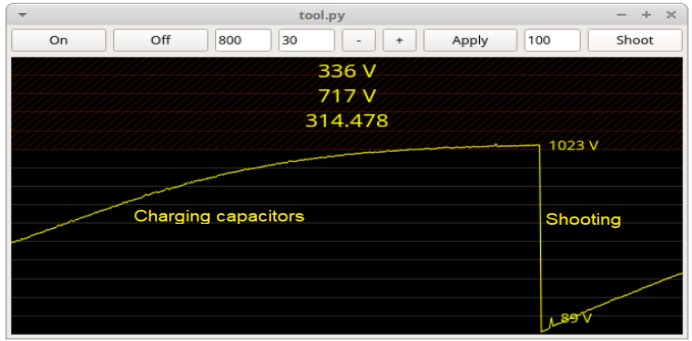
```
Initialize-SiliconToaster;
Read Memory Content (trigger=1, address, number of
  bytes);
if (uart.receive=ACCEPT) then
    Data=uart.receive(number of bytes);
else
    Data=None;
```

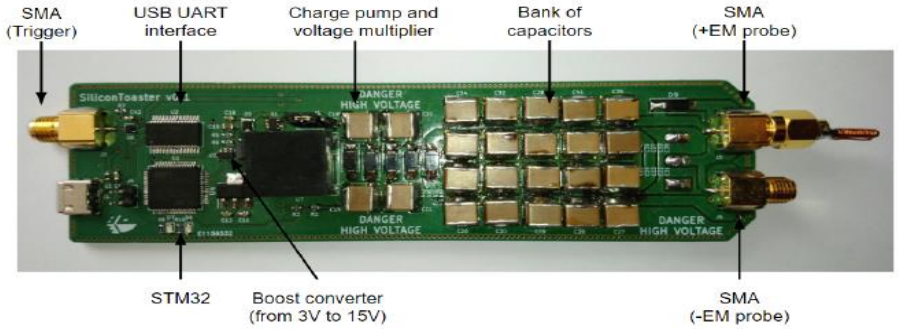
B configuration Attack: 400V + Success= 30%



Discussion

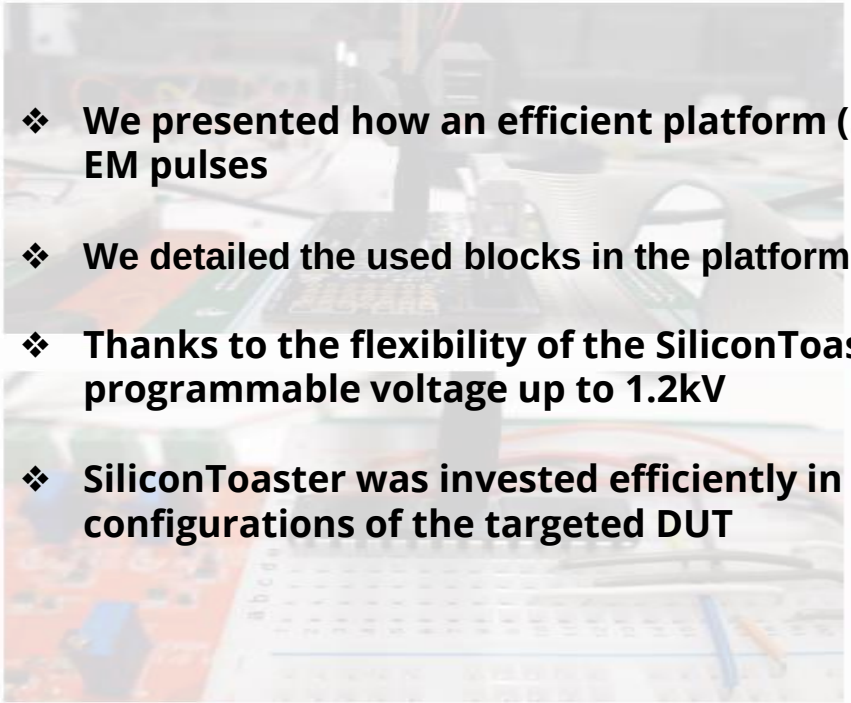
Design	EM voltage	Power supply	Visibility	Polarity
SiliconToaster	Programmable	USB-powered	GUI	Two SMA
USENIX 2017 + DCIS 2017	Fixed	External power supply	No	Another probe needed

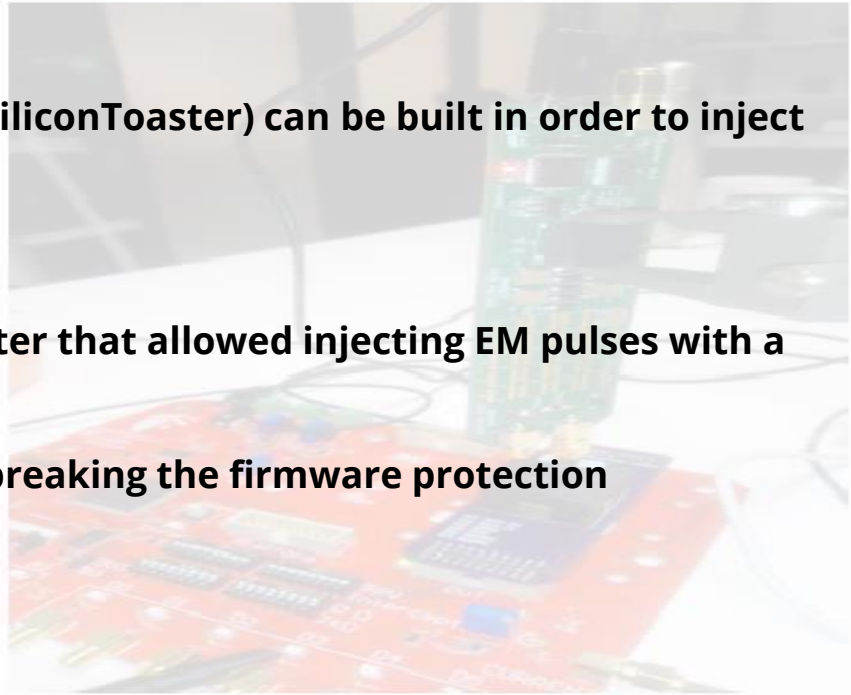




Conclusion

Conclusion





- We presented how an efficient platform (SiliconToaster) can be built in order to inject EM pulses
- We detailed the used blocks in the platform
- Thanks to the flexibility of the SiliconToaster that allowed injecting EM pulses with a programmable voltage up to 1.2kV
- SiliconToaster was invested efficiently in breaking the firmware protection configurations of the targeted DUT

Questions?