ClkScrew
Aaron Zhang
Outline

• Introduction to DVFS and background information.
• What makes CLKSCREW unique?
• Challenges to CLKSCREW
• Attacks and Results
• Conclusion
Voltage + Frequency = Energy Usage
HARDWARE

DVFS
(Dynamic Voltage and Frequency Scaling)

SOFTWARE
Outline

• Introduction to DVFS and background information.
• What makes CLKSCREW unique?
• Challenges to CLKSCREW
• Attacks and Results
• Conclusion
Less time for number to go through Flip-Flop
TRUSTZONE

NON-TRUSTZONE

DVFS
Steps

1. Clear Residual States
2. Profile for Anchor
3. Pre-fault Delaying
4. Deliver the fault.
Outline

• Introduction to DVFS and background information.
• What makes CLKSCREW unique?
• Challenges to CLKSCREW
• Attacks and Results
• Conclusion
Do phones allow for overclocking/under-volting?
How do you make sure the flip-flops do not damage the injected code?
Attacker Code

CPU CORE 1

Victim Thread

CPU CORE 2
How do you get the timing precise enough?

How do we make sure the attack occurs where we want it to occur?
Outline

• Introduction to DVFS and background information.
• What makes CLKSCREW unique?
• Challenges to CLKSCREW
• Attacks and Results
• Conclusion
Inferring AES Keys

- TRUSTZONE
  - AES Decryption
- NON-TRUSTZONE
  - Attacking Code

DVFS
Loading Apps into Trust Zone

TRUSTZONE

Attacker’s App

DVFS

NON-TRUSTZONE

Attacking Code
Each App has 4 Signatures

One signature takes 270 Million clock cycles to validate.

In order for CLKSCREW to corrupt data it needs to change just 65 thousand clock cycles within the entire process
\[
\frac{65000}{1080000000000} = 0.00000601\% 
\]
Cache Profiling

- Pick a memory address of the area of interest
- Run dummy instructions and time the amount it takes for these instructions to be removed
- Patterns for removing will tell you the pattern of the actual code.

Timing Anchor

- Track duration of consecutive cache instructions
Figure 14: Histogram of observed faults and where the faults occur. The intended faulted position is 141.
Outline

• Introduction to DVFS and background information.
• What makes CLKSCREW unique?
• Challenges to CLKSCREW
• Attacks and Results
• Conclusion
Defenses
Hardware Limits regarding Voltage and Frequency

• Make it unable for users to overclock and under-volt their phones
• Difficulties include having to remake hardware chips from scratch and having every phone and chipmaker adhere to regulation.
Separate DVFS for Trustzone

• Create a separate DVFS for Trustzone itself
• Separate DVFS’ for cores on the same chip can cause massive overhead.
Randomization

• Randomize clock cycles so that attackers do not know what to expect.
• Useless when run-time time-anchors are used.
Conclusions

• CLKSCREW is a side-channel attack that utilizes voltage and frequency of devices to induce faults.

• Exploiting faults that cannot be easily changed.