PLATYPUS ATTACK

Vamitha P Velu

Cyber Security Analyst, EY

13-Dec-2020

Side Channel Attack

- Collects information about what a computing device does, when performing its cryptographic operation
- And uses the same information to reverse engineer the devices cryptography system
- Examples : Spectre, Meltdown, Tempest

Types of SCA

- Physical Side Channel Attack
- Software based Side Channel Attack

PLATYPUS Attack

- Power Leakage Attack : Targeting Your Protected User Secrets
- PLATYPUS attack can execute remotely via software
- Exploits the power consumption differences to steal secret data like cryptographic keys
- intel CPUs can leak data to adversary regardless of the OS

PLATYPUS Attack(Contd...)

- An attacker can monitor the power consumption changes by exploiting Intel's RAPL (Running Average Power Limit) interface.
- RAPL apparently serves as a power meter allowing the user to monitor the power consumption in the CPU via software.
- *powercap* framework of the Linux kernel allowed unprivileged access to the RAPL interface

HOW ?

- Messages are encrypted with cryptographic keys and returns the encrypted message
- The Energy/power consumed to perform the encryption are stored

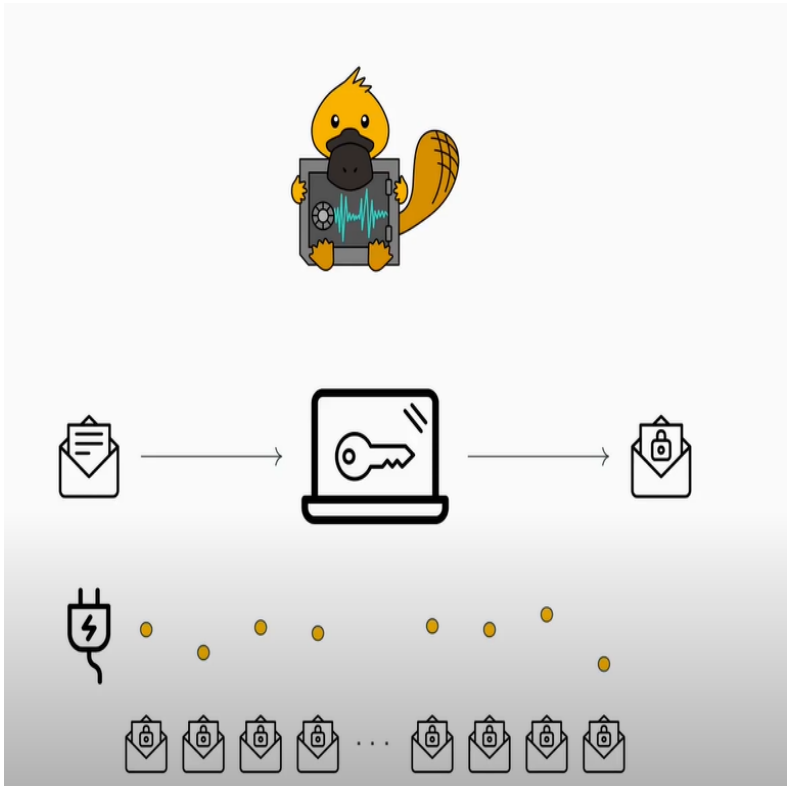

FIGURE – Power Consumed during Encryption

HOW ?

- */sysfs/class/powercap* framework
- *intel-rapl, intel-rapl :0, intel-rapl :0 :0, intel-rapl :0 :1*
- Details of the power consumed
- Difference in the hamming weights
- `https://www.kernel.org/doc/html/latest/power/powercap/powercap.html`
- `https://platypusattack.com/platypus.pdf`

Model

- Recording the Power Consumption
- Generating the keys
- Comparisons of the Round key and Recovery Key

Model- Recording the Power

- Records millions of encryption with different input messages
- Even For multiple days
- And store the obtained values

Model-Generating Keys

- The Key values are generated by splitting each part of keys
- Each part can have value from 0 - 255
- Provided to the model to obtain the power consumed for each key part

Model- Comparison

- The taken value (Round key) and the recovered value are compared
- To predict the energy consumption of the taken value
- Tries out each value to get equal or approximate value of the power consumed

Model

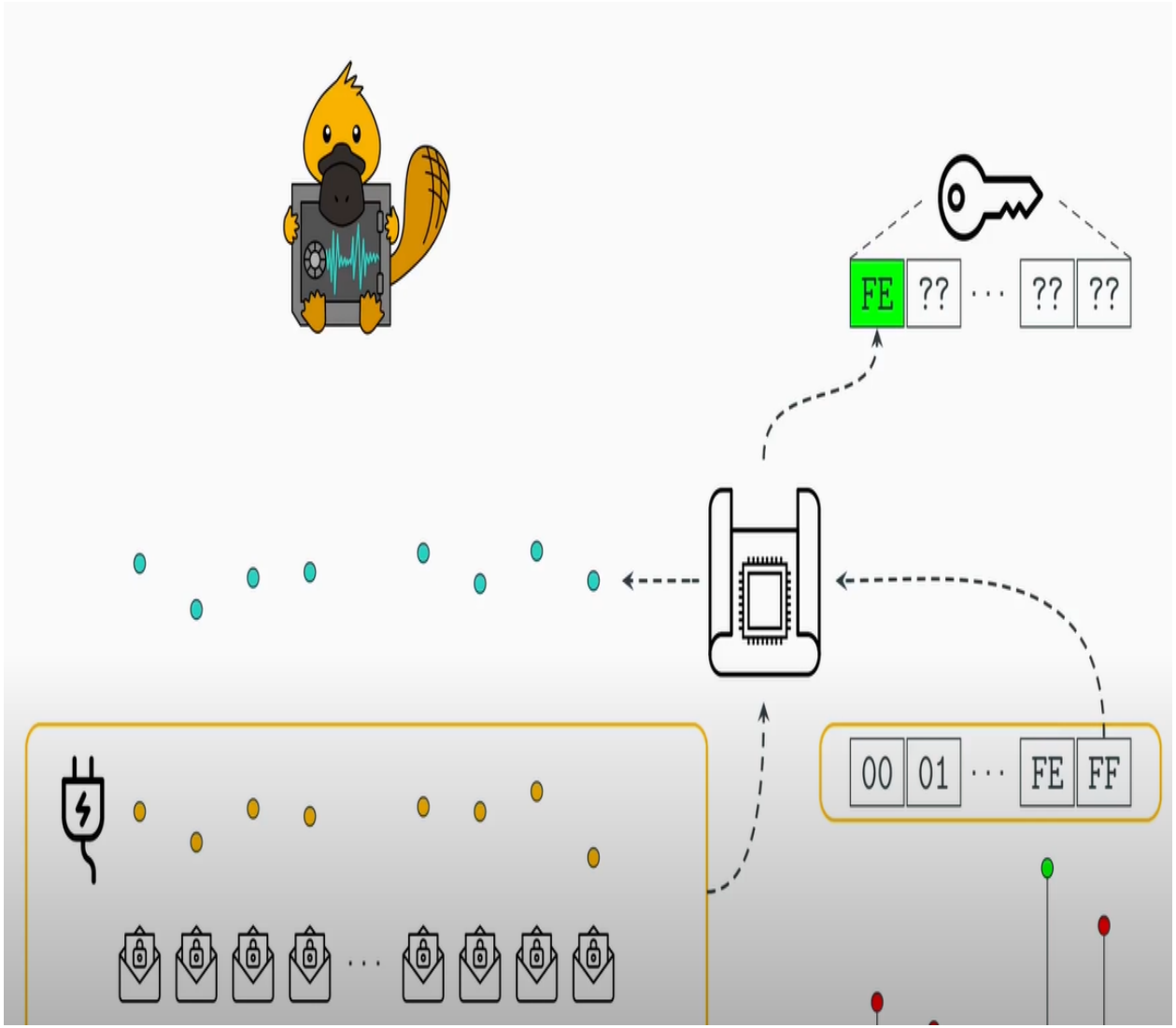

FIGURE – Platypus

CounterMeasures

- Platypus attack was reported to intel
- CVE 2020-8694 , CVE-2020-8695
- Patched with a microcode, denying the access to powercap interface

Question

- `https://dc0471.org/discord`
- Discord : `vamitha#5241`

Thank You

Thank You