Side Channel attacks

Indra

What is

- A side-channel attack is an attack that uses information gained from the implementation of a computer system, rather than weaknesses in the implemented algorithm itself
- Use information from monitoring systems on the computer or external tools to reconstruct data
- Leaves no trace

How

- Power usage for different components
- EMF radiation emitted by a computer screen
- Acoustics attacks

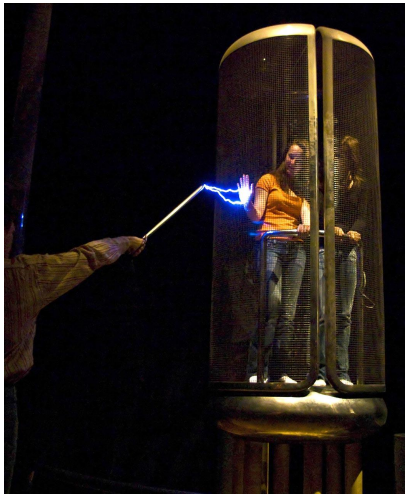
Tempest

Screens emit EMF radiations that can be recorded hundreds of meters away

Use radiation to view screen in real time

Use a faraday cage to prevent

Wavelength of the radiation is larger than the holes



Platypus

- **P**ower **L**eakage **A**ttacks: **T**argeting **Y**our **P**rotected **U**ser **S**ecrets (for short)
- Side Channel attack that monitors a CPU power consumption
- Uses Intel's **R**unning **A**verage **P**ower **L**imit (RAPL)
- Measurements for RAPL interface can be obtained by unprivileged users using a linux driver
- The driver allows malicious applications installed on the targeted system to access power consumption data and correlate it to data being processed.
- A mathematical model is used to break a key into parts and plug in a value into each part where the power consumption of the value matches the power consumption of the individual part.

Last tidbits for Platypus

- Platypus can’t target specific application, but targeted application always work with the same data (cryptographic keys)
- The time complexity for Platypus varies greatly: seconds - hundreds of hours
- KASLR broken in 20 seconds
- AES-NI encryption key 26 hours to 277 hours in a real world environment
- RSA private key 100 minutes
- These were done through SGX which is designed to protect data when the system has been compromised

General Mitigations

- Tricky cause of the various attacks
- Faraday cage
- Swapping out compromised components
- Using low powered cpu

References

- PLATYPUS: Hackers Can Obtain Crypto Keys by Monitoring CPU Power Consumption. (2020, November 10). Retrieved from https://www.securityweek.com/platypus-hackers-can-obtain-crypto-keys-monitoring-cpu-power-consumption
- https://www.csoonline.com/article/3388647/what-is-a-side-channel-attack-how-these-end-runs-around-encryption-put-everyone-at-risk.html
-