TEE: THE BEST TRADE-OFF BETWEEN SECURITY, PERFORMANCE AND COST

THIERNO BARRY, PHD

Huawei Mobile Security Team, UK

WHO AM I IN A NUTSHELL ?

>> Curriculum

- PhD in Security of Embedded Systems - Mines Saint-Etienne

>> Experiences

- Mobile Security team leader at Huawei R&D UK (since 2019)

Before that :

- Penetration tester / Principale TEE security evaluator at Thales ITSEF, Toulouse, FR
- Security researcher at CEA Grenoble
- Teaching assistant at INP Grenoble

AGENDA

>> Huawei's Mobile Security Architecture

>> Threat Modelling

>> Attack Types on Mobile Platforms

>> Mobile Devices Security Problems

>> TEE Industrial Use-Cases

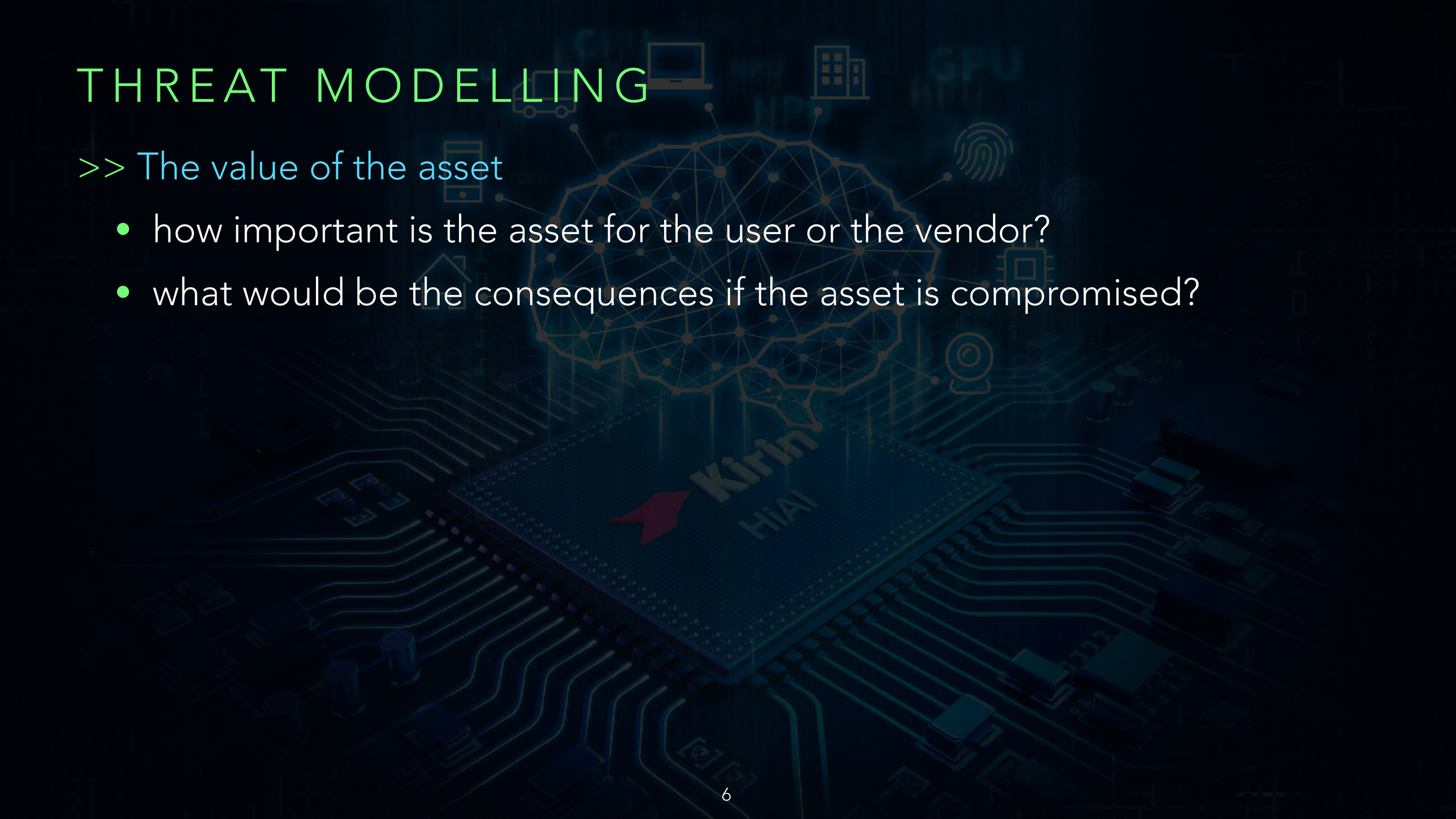
MOBILE SECURITY PROBLEM

HUAWEI'S MOBILE SECURITY ARCHITECTURE

THREAT MODELLING

>> The value of the asset

- how important is the asset for the user or the vendor?
- what would be the consequences if the asset is compromised?



THREAT MODELLING

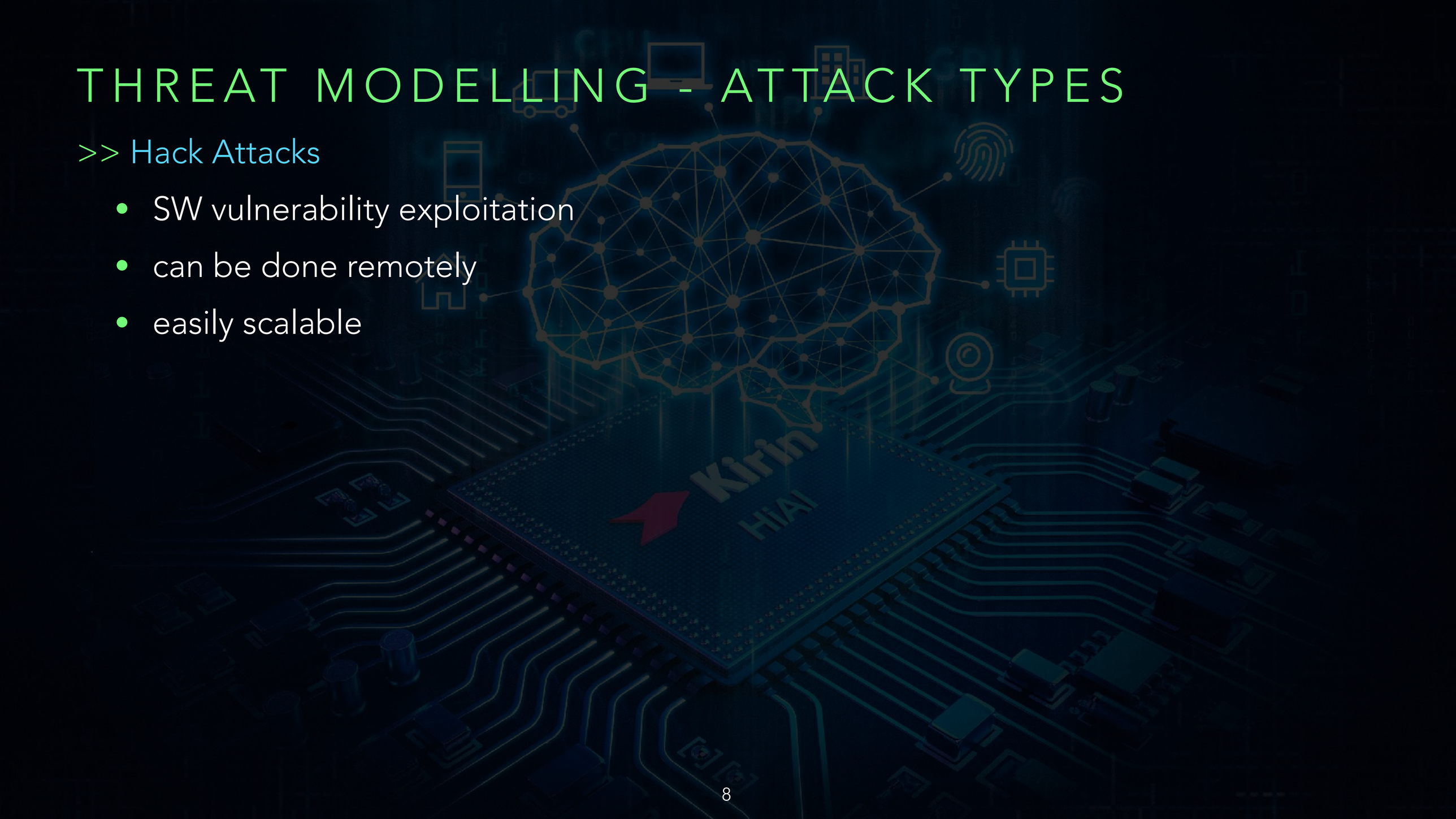
>> The value of the asset

- how important is the asset for the user or the vendor?
- what would be the consequences if the asset is compromised?

>> Attacker profile

- who might be interested into the asset?
- who has the required resources to compromise the asset?
- how long will it take for the identified attacker profile to compromise the asset?

THREAT MODELLING - ATTACK TYPES



>> Hack Attacks

- SW vulnerability exploitation
- can be done remotely
- easily scalable

THREAT MODELLING - ATTACK TYPES

>> Hack Attacks

- SW vulnerability exploitation
- can be done remotely
- easily scalable

>> Shack Attacks

- complex attacks
- may require proximity to the target

THREAT MODELLING - ATTACK TYPES

>> Hack Attacks

- SW vulnerability exploitation
- can be done remotely
- easily scalable

>> Shack Attacks

- complex attacks
- may require proximity to the target

>> Lab Attacks

- require physical access to the target
- use of expensive facilities
- highly skilled profiles

THREAT MODELLING - ATTACK TYPES

>> Hack Attacks

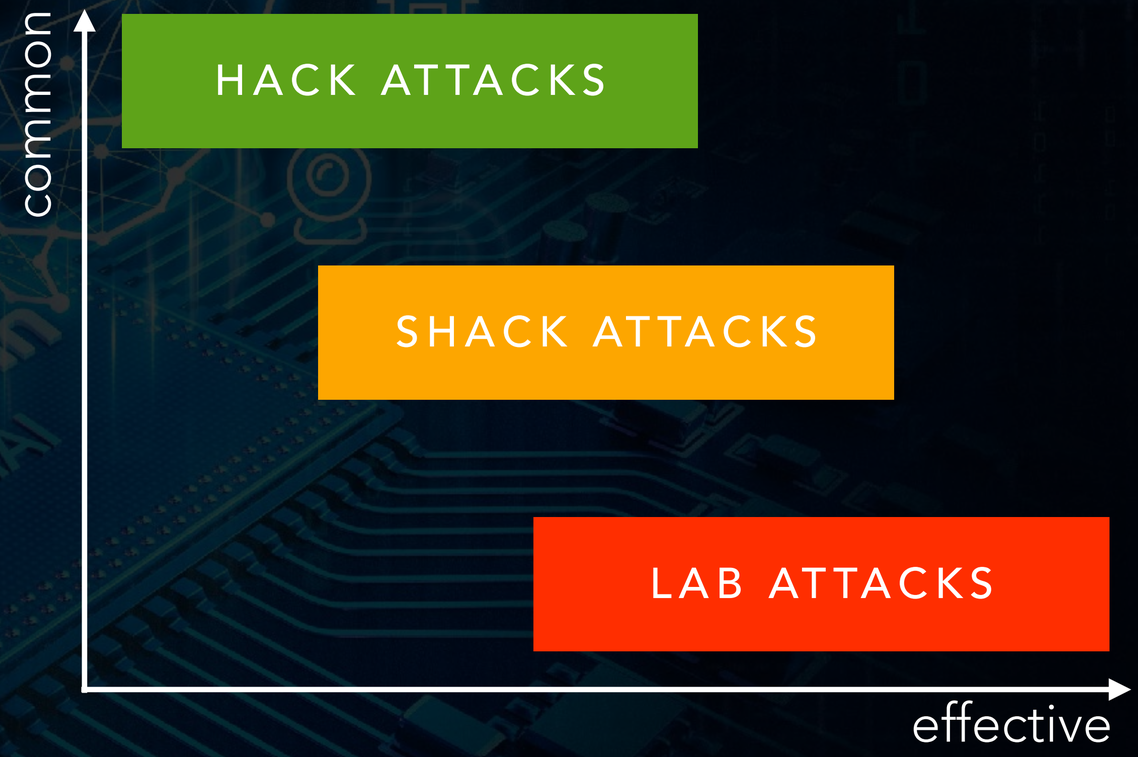
- SW vulnerability exploitation
- can be done remotely
- easily scalable

>> Shack Attacks

- complex attacks
- may require proximity to the target

>> Lab Attacks

- require physical access to the target
- use of expensive facilities
- highly skilled profiles



MOBILE DEVICES SECURITY PROBLEM

>> Android

Problems	Solutions
App Integrity	

MOBILE DEVICES SECURITY PROBLEM

>> Android

Problems	Solutions
App Integrity	App signing In-app/native Integrity check

MOBILE DEVICES SECURITY PROBLEM

>> Android

Problems	Solutions
App Integrity	App signing In-app/native Integrity check
Bypass the signature checking Replacing the key	

MOBILE DEVICES SECURITY PROBLEM

>> Android

Problems	Solutions
App Integrity	App signing In-app/native Integrity check
Bypass the signature checking Replacing the key	Remote Attestation + TLS

MOBILE DEVICES SECURITY PROBLEM

>> Android

Problems	Solutions
App Integrity	App signing In-app/native Integrity check
Bypass the signature checking Replacing the key	Remote Attestation + TLS
Proxy + MITM	Certificate Pinning + anti-replay

MOBILE DEVICES SECURITY PROBLEM

>> Android

Problems	Solutions
App Integrity	App signing In-app/native Integrity check
Bypass the signature checking Replacing the key	Remote Attestation + TLS
Proxy + MITM	Certificate Pinning + anti-replay
Rooting + Hooking	Enhanced root checking

MOBILE DEVICES SECURITY PROBLEM

>> Android

Problems	Solutions
App Integrity	App signing In-app/native Integrity check
Bypass the signature checking Replacing the key	Remote Attestation + TLS
Proxy + MITM	Certificate Pinning + anti-replay
Rooting + Hooking	Enhanced root checking
Bypass root checking	*Need to rely on something outside Android*

MOBILE DEVICES SECURITY PROBLEM

>> Linux Security Features

- Process Isolation
- Access Control Policies (UID, GUID) - Android Binder
- Efficient Memory Management
- ASLR
- SELinux
- Kernel Module Mangement

=> All this can be bypassed

=> Need for hardware-based solution

MOBILE DEVICES SECURITY PROBLEM

>> Hardware-based solution

	Pros	Cons

MOBILE DEVICES SECURITY PROBLEM

>> Hardware-based solution

	Pros	Cons
TPM	• separate HW • tamper-resistant	

MOBILE DEVICES SECURITY PROBLEM

>> Hardware-based solution

	Pros	Cons
TPM	• separate HW • tamper-resistant	• storage - - • cost ++ • dedicated for key storage and crypto operations • not thought for Mobile devices

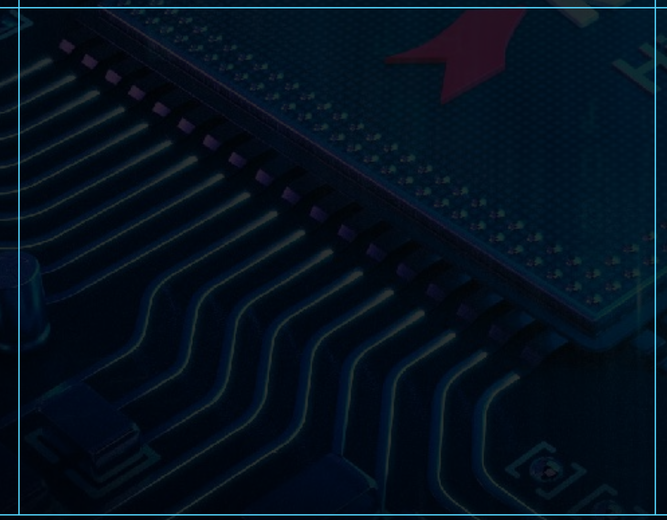
MOBILE DEVICES SECURITY PROBLEM

>> Hardware-based solution

	Pros	Cons
TPM	• separate HW • tamper-resistant	• storage - - • cost ++ • dedicated for key storage and crypto operations • not thought for Mobile devices
Secure Element	• separate HW • tamper-resistant	• cost ++ • resource - - • performance - -

MOBILE DEVICES SECURITY PROBLEM

>> Hardware-based solution

	Pros	Cons
Secure Co-Processor	• separate HW • tamper-resistant • performance ++	• storage - - • not for a general purpose usage => e.g: crypto accelerator
		

MOBILE DEVICES SECURITY PROBLEM

>> Hardware-based solution

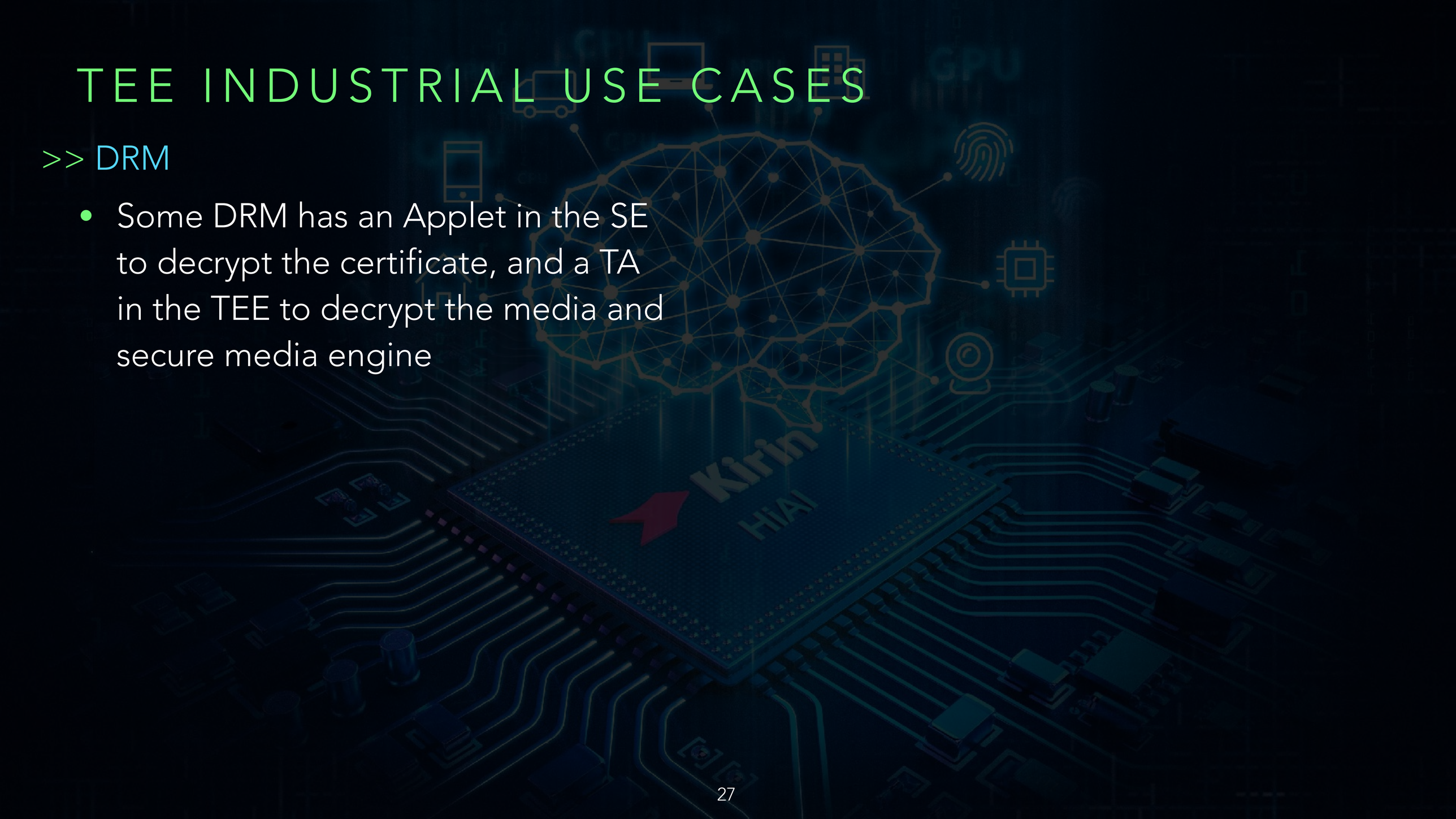
	Pros	Cons
Secure Co-Processor	• separate HW • tamper-resistant • performance ++	• storage - - • not for a general purpose usage => e.g: crypto accelerator
TEE	• cost - - • storage ++ • performance ++ • general purpose usage • security +/-	• not tamper-resistant • share some resources with the REE

TEE INDUSTRIAL USE CASES

TEE INDUSTRIAL USE CASES

>> DRM

- Some DRM has an Applet in the SE to decrypt the certificate, and a TA in the TEE to decrypt the media and secure media engine



TEE INDUSTRIAL USE CASES

>> DRM

- Some DRM has an Applet in the SE to decrypt the certificate, and a TA in the TEE to decrypt the media and secure media engine

>> Payment Applications

- The payment Applet in the SE, a proxy TA in the TEE and an Android App in the REE.

TEE INDUSTRIAL USE CASES

>> DRM

- Some DRM has an Applet in the SE to decrypt the certificate, and a TA in the TEE to decrypt the media and secure media engine

>> Payment Applications

- The payment Applet in the SE, a proxy TA in the TEE and an Android App in the REE.

>> Key management

- Android Key Store

TEE INDUSTRIAL USE CASES

>> DRM

- Some DRM has an Applet in the SE to decrypt the certificate, and a TA in the TEE to decrypt the media and secure media engine

>> Payment Applications

- The payment Applet in the SE, a proxy TA in the TEE and an Android App in the REE.

>> Key management

- Android Key Store

>> Device binding

- To tie assets to a device

TEE INDUSTRIAL USE CASES

>> DRM

- Some DRM has an Applet in the SE to decrypt the certificate, and a TA in the TEE to decrypt the media and secure media engine

>> Payment Applications

- The payment Applet in the SE, a proxy TA in the TEE and an Android App in the REE.

>> Key management

- Android Key Store

>> Device binding

- To tie assets to a device

>> Real-time Kernel Protection

- The integrity of the REE kernel is periodically checked by the TEE

TEE INDUSTRIAL USE CASES

>> DRM

- Some DRM has an Applet in the SE to decrypt the certificate, and a TA in the TEE to decrypt the media and secure media engine

>> Payment Applications

- The payment Applet in the SE, a proxy TA in the TEE and an Android App in the REE.

>> Key management

- Android Key Store

>> Device binding

- To tie assets to a device

>> Real-time Kernel Protection

- The integrity of the REE kernel is periodically checked by the TEE

>> Other services

- Device holder authentication
- SIM lock
- Root detection
- …


THANK YOU FOR YOU ATTENTION !