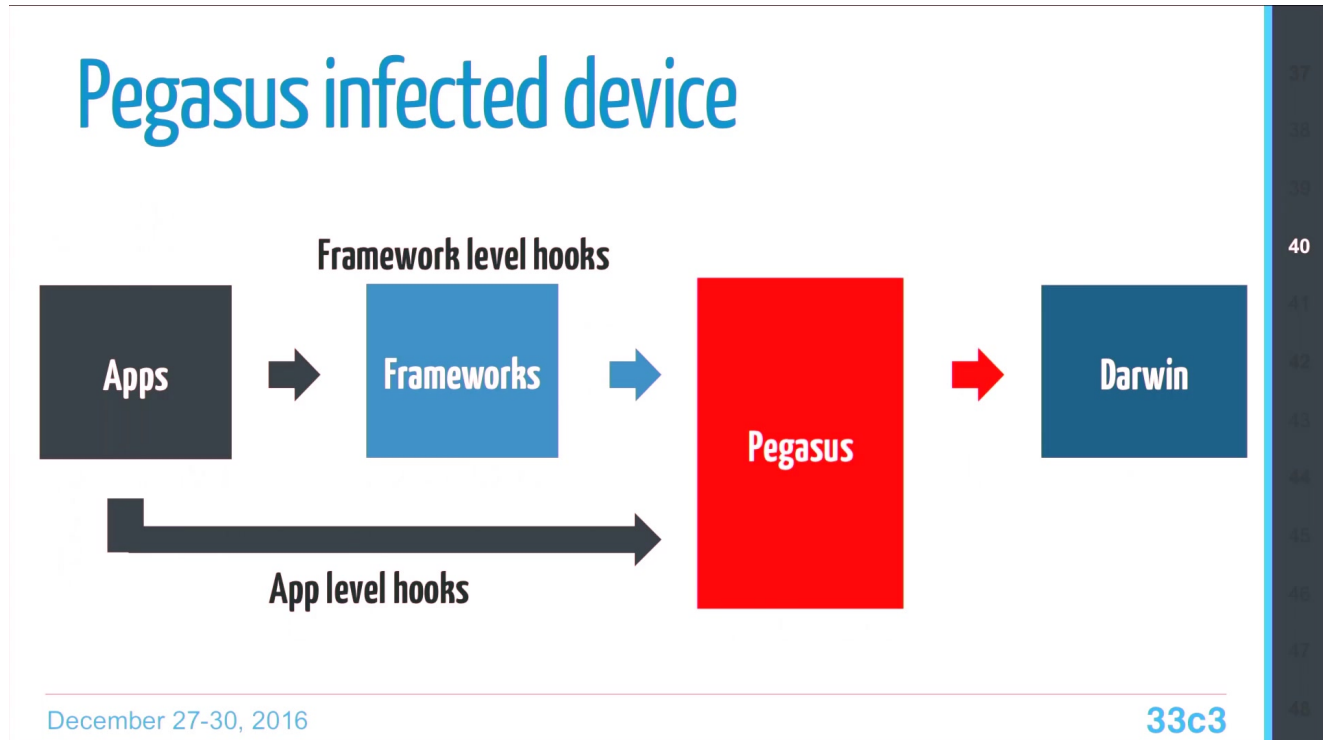


Pegasus internals

media.ccc.de/v/33c3-7901-pegasus_internals

Max Bazaliy



Max Bazaliy

Playlists: ['33c3' videos starting here](#) / [audio](#) / [related events](#)

- 29 min
- 2016-12-27
- 3055
- [Fahrplan](#)

This talk will take an in-depth look at the technical capabilities and vulnerabilities used by Pegasus. We will focus on Pegasus's features and the exploit chain Pegasus used called Trident. Attendees will learn about Pegasus's use of 0-days, obfuscation, encryption, function hooking, and its ability to go unnoticed. We will present our detailed technical analysis that covers each payload stage of Pegasus including its exploit chain and the various 0-day vulnerabilities that the toolkit was using to jailbreak a device. After this talk attendees will have learned all of the technical details about Pegasus and Trident and how the vulnerabilities we found were patched.

Download

Video

- [MP4](#)
- [WebM](#)

[Download 1080p](#)

[eng-deu 205 MB](#)

[Download 576p](#)

[eng-deu 78 MB](#)

These files contain multiple languages.

This Talk was translated into multiple languages. The files available for download contain all languages as separate audio-tracks. Most desktop video players allow you to choose between them.

Please look for "audio tracks" in your desktop video player.

Subtitles

[eng](#)

[fin](#)

[Help us to improve these subtitles!](#)

Audio

[Download mp3](#)

[eng 26 MB](#)

[Download opus](#)

[eng 22 MB](#)

Related

HAJJ 2 DAY 1 16:42

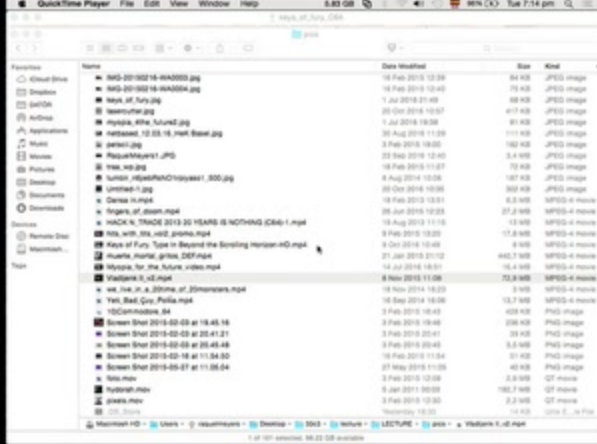
NEXT TALK

16:45
in 3 min

A Story of Discrimination and
Unfairness

Aylin Caliskan

@MarietjeSchaake: At #33C3 and have an opinion about politics and EU legislation? L

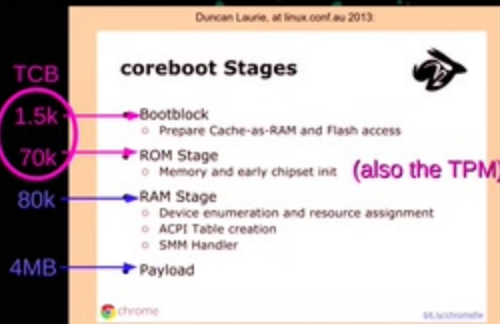


Austria



HSM Intrusion Detection

- Mesh: Continuity testing a printed maze trace on case inside
- RF Interference: Continuously measuring RF characteristics of wire stuffed into case chaotically
- Ultrasonic: Continuously measuring ultrasonic propagation inside potting material
- Triboluminescence: Photodiodes detecting mechanical disturbance of clear potting material loaded with "friction-glow"/"smash-glow" crystals



Show what the data would mean for your experience



@LISACROST

Imperfect Automation

- In two cases: minor technical faults
- In one case: perfectly working aircraft
- Pilots didn't know how to react properly
- Lack of training? That, too
- Awareness, Information, CRM





Unpair: MasterCard ID

- MasterCard ID is printed on the card
- However, each transaction contains the following:

```
{"amount": -0.11,  
"cardId": "bb484ca2-a674-4f1c-afd1-896a30fe6d15",  
"linkId": "0123456789-372287",  
"merchantCity": "DUESSELDORF",  
"merchantCountry": "D"}
```

MasterCard ID is part of every MasterCard transaction!



3303
EM ROF SKROW

High-precision geolocation on drones

"As part of the GILGAMESH (PREDATOR-based active geolocation) effort (...) for operational use on unmanned aerial vehicle (UAV) flights." (Snowden Archive)

Leak more documents!



10

Tags

Security