# BootPwn

## Pwning Secure Boot by Experience.

Niek Timmers
niek@twentytwosecurity.com
@tieknimmers

Cristofaro Mune
c.mune@pulse-sec.com
@pulsoid

WELCOME EVERYBODY.

# The BootPwn Experience

- Broaden your understanding of, and experience with, Secure Boot
- Mostly done using an offensive perspective:
  - Taking the seat of an attacker
  - Identifying and exploiting Secure Boot vulnerabilities
- Getting your hands dirty during hands-on labs while having fun

# ! ( BootPwn )

- Not just a training… it’s an experience!
- Not focused on just software or hardware security
- Not focused too much on generic aspects of embedded security

# YOUR TRAINERS.

# Niek Timmers

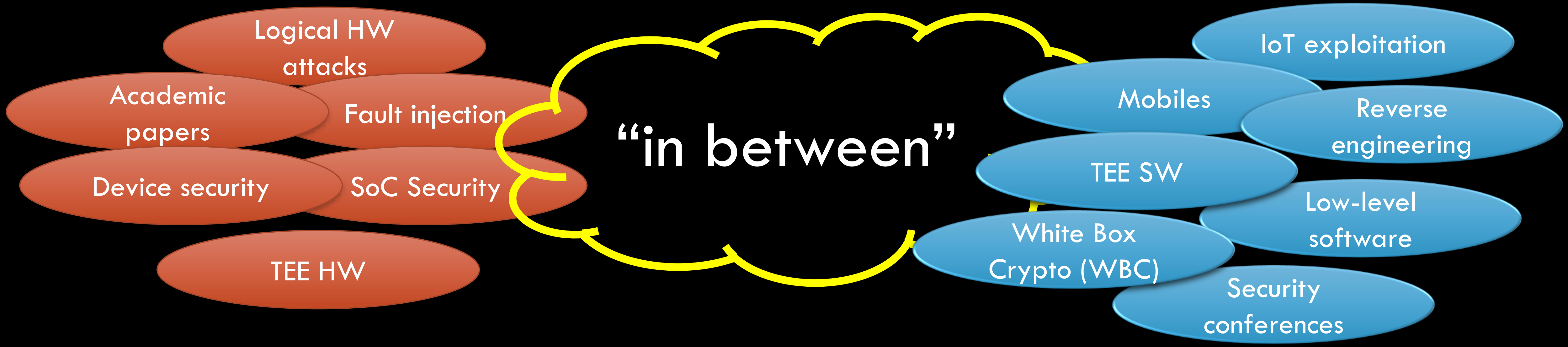
- Independent embedded security researcher, consultant and trainer
  - Professionally active for ~8 years at an advanced security test lab in the Netherlands
  - Since 1 year active independently at TwentyTwo Security

- I like to get my hands dirty with anything where device hardware is involved:
  - Reviewing and reversing low level software (e.g. bootloaders, kernels, …)
  - Analyzing hardware technologies (e.g. system-on-chips, security features, …)
  - Performing hardware attacks (e.g. fault injection, power analysis, …)

- Publications at both academic and hacker conferences
  - NULLCON, PoC, FDTC, escar, HITB, Black Hat, BlueHat, PoC||GTFO, …

# Cristofaro Mune

- Product Security Consultant (17 years in security)
- Multiple years of product security testing at an advanced lab
  - Lots of source code review, device testing, exploiting, fault injection…



# Secure boot research.

- We have been reviewing and testing Secure Boot implementations since 2010
- Since then, we have seen many flawed implementations…
- Presented on attacking and hardening secure boot repeatedly
  - Bypassing Secure Boot using Fault Injection @ BH EU 2016
  - Secure boot under attack: Simulation to enhance fault injection & defences @ BH EU 2018
  - Hardening Secure Boot for Hostile Environments @ BlueHatIL 2019
  - PEW PEW PEW: Designing Secure Boot Securely @ NULLCON 2019
  - More can be found on my personal website: https://niektimmers.com#research

# THE TRAINEES.

# Introductions

- What’s your name?
- Where are you from?
- What’s your role at your work?
- What’s your (technical) background?
- Why did you choose this BootPwn and what are your expectations?

*Feel free to skip any question…*

Enough you, enough us, let’s talk BootPwn

# The classroom.

- Use your trainers
  - Feel free to ask questions at any time
  - You can also contact us before and/or after the training
- Interact
  - Share, discuss and support your fellow trainees and trainers
- Practice, play and have fun…

*Don’t worry… ask for help!*

# The atmosphere.

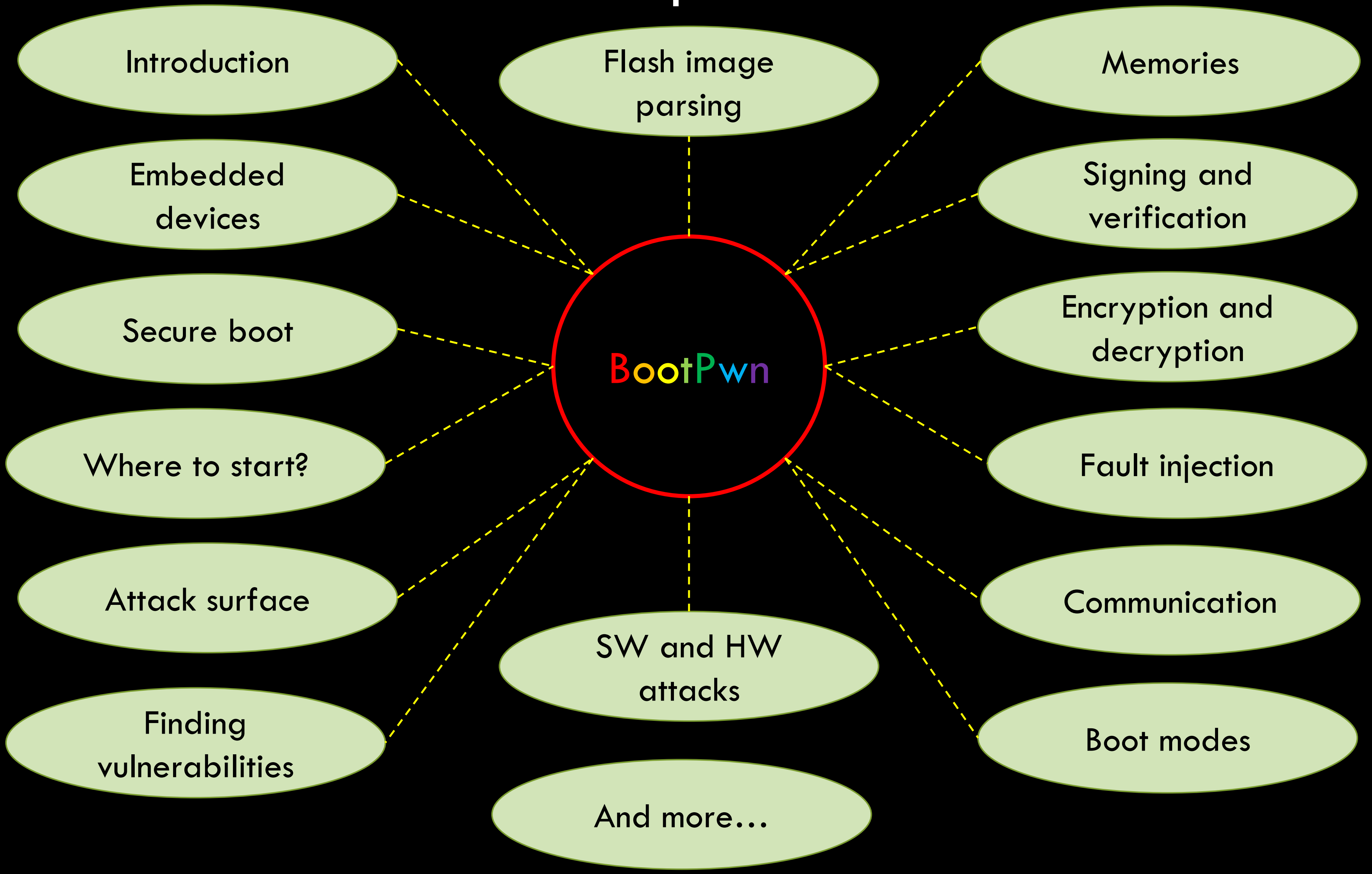
- Please no photos unless everybody in the frame gives consent
- Let’s make everybody feel at home; respect each other
- If all fails, please blame your trainer, not your fellow trainee

THIS EXPERIENCE.

# BootPwn – Goals

- Increase your understanding of Secure Boot while having fun
- Bypass Secure Boot with attacks beyond software exploitation
- Utilize your offensive understanding for defensive purposes

# Topics



BootPwn

Introduction

Embedded devices

Secure boot

Where to start?

Attack surface

Finding vulnerabilities

Flash image parsing

SW and HW attacks

And more…

Memories

Signing and verification

Encryption and decryption

Fault injection

Communication

Boot modes

# BootPwn – We will be…

- … giving you three intense days with more practice and less theory!
  - You won’t sit still.

- … giving you a gamified lab-focused experience!
  - Your progress is tracked using a CTFd-based website.

- … providing you an playful and friendly environment!
  - You will feel at home.

# BootPwn – We won't be…

- … turning you into a software, hardware or crypto security expert!
  - Concepts from these domains will be covered.
- … providing you any N-days for real products or devices!
  - You learn generic concepts that are applicable to real implementations.
- … making you 'push buttons and see magic' all day!
  - You will need to think before you move.

# THE SCHEDULE.

# BootPwn – Day 1 schedule

| Topic | Time | Duration | Lecture | Lab |
|---|---|---|---|---|
| BootPwn #01 | 09:00 AM | 2h 00m | X | X |
| Break | 11:00 AM | 0h 15m | | |
| BootPwn #02 | 11:15 AM | 1h 45m | X | X |
| Lunch | 01:00 PM | 1h 00m | | |
| BootPwn #03 | 02:00 PM | 2h 00m | X | X |
| Break | 04:00 PM | 0h 15m | | |
| BootPwn #04 | 04:15 PM | 1h 45m | X | X |

# BootPwn – Day 2 schedule

| Topic | Time | Duration | Lecture | Lab |
|---|---|---|---|---|
| BootPwn #05 | 09:00 AM | 2h 00m | X | X |
| Break | 11:00 AM | 0h 15m | | |
| BootPwn #06 | 11:15 AM | 1h 45m | X | X |
| Lunch | 01:00 PM | 1h 00m | | |
| BootPwn #07 | 02:00 PM | 2h 00m | X | X |
| Break | 04:00 PM | 0h 15m | | |
| BootPwn #08 | 04:15 PM | 1h 45m | X | X |

# BootPwn – Day 3 schedule

| Topic | Time | Duration | Lecture | Lab |
|---|---|---|---|---|
| BootPwn #09 | 09:00 AM | 2h 00m | X | X |
| Break | 11:00 AM | 0h 15m | | |
| BootPwn #10 | 11:15 AM | 1h 45m | X | X |
| Lunch | 01:00 PM | 1h 00m | | |
| BootPwn #11 | 02:00 PM | 2h 00m | X | X |
| Break | 04:00 PM | 0h 15m | | |
| BootPwn #12 | 04:15 PM | 1h 45m | X | X |

# ANY QUESTIONS?

Niek Timmers
niek@twentytwosecurity.com
@tieknimmers

Cristofaro Mune
c.mune@pulse-sec.com
@pulsoid