INTRINSEC

BitLocker downgrade attacks

Cassius Garat · github.com/garatc

INTRINSEC

What is BitLocker?

- Windows full volume encryption
- Threat model:
  - Attacker with physical access
- Preboot auth options:
  - None (default)
  - PIN
  - Startup Key (USB flash drive, e.g. Yubico)
  - PIN + Startup Key

Everyone's favorite sight

INTRINSEC

What is BitLocker?

VMK unlocks the **FVEK**, which decrypts the disk

VMK can be protected by several things, including magic and fairies (TPM & PCRs)

INTRINSEC

Why target BitLocker? My story as a pentester

- Locked-down Windows kiosk behind Citrix
- Goal: break out & reach the internal Active Directory
- Broke out of Citrix because it is Citrix, but still some annoying restrictions

INTRINSEC

Why target BitLocker? My story as a pentester

- Device encryption without PIN on a thin client
- Neodyme's article on BitPixie had just dropped a few weeks before
- Built my own exploit/downgrade attack from the article and witnessed the mighty powers of BitPixie:
  - Full read/write on the unlocked disk → Privilege escalation (e.g., replacement of SYSTEM binary)
  - Renamed the EDR's protected folders → EDR failed to load on next boot
  - (Data exfiltration)

Further reading: `neodyme.io/en/blog/bitlocker_screwed_without_a_screwdriver`

INTRINSEC

What protects the disk before Windows starts

SECURE BOOT

Only boot code signed by a trusted Microsoft certificate (1st or 3rd party). Two major Microsoft db certificates in the wild: PCA 2011 and PCA 2023

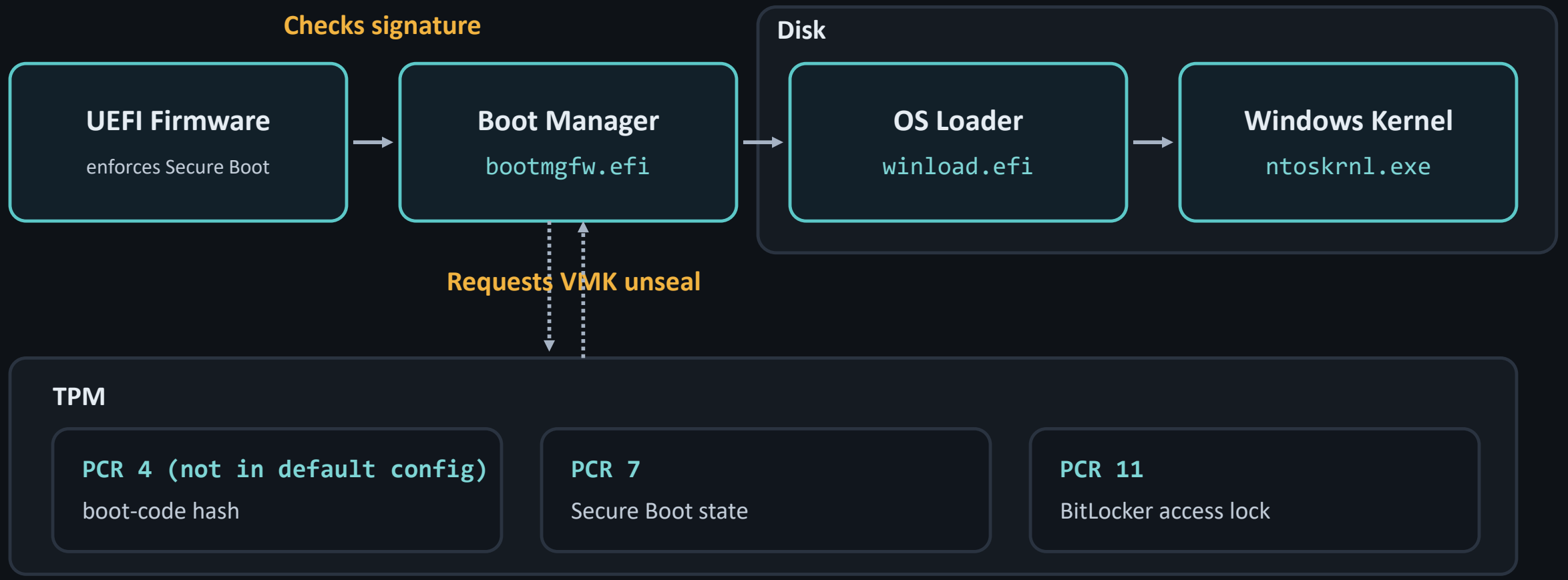
TPM (Trusted Platform Module)

Releases sealed keys only in an expected boot state. Can be on a separate chip (dTPM) or integrated to the CPU (fTPM)

PCR (Platform Configuration Register)

A TPM slot that records a hash of each boot stage

THE CHAIN OF TRUST



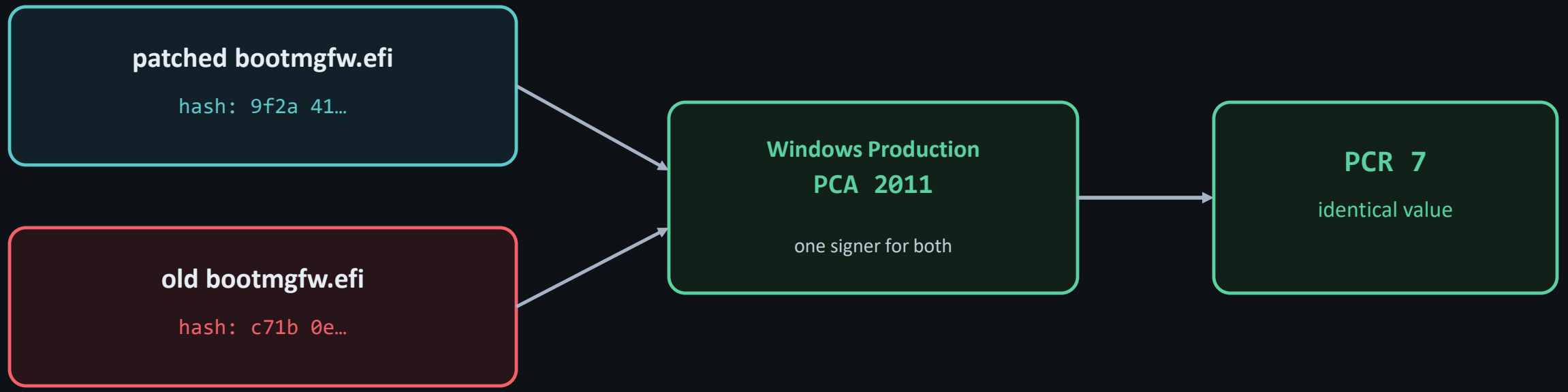
If a stage changes, its recorded value changes. BitLocker checks these values before unlocking the disk.

Boot the machine the way it expects, and the TPM unseals the VMK

SECURE BOOT ONLY CHECKS THE SIGNER

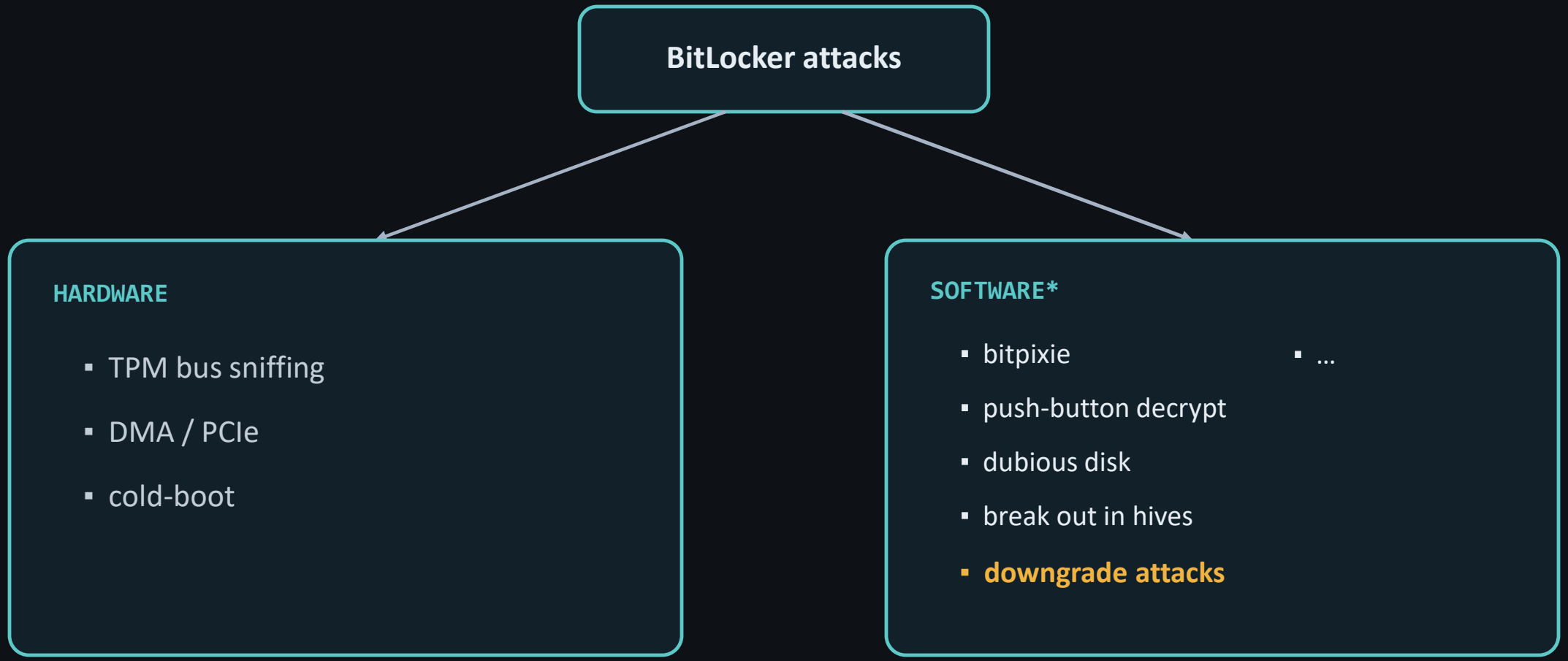
INTRINSEC

A bit of foreshadowing…



Different binaries, same certificate → same PCR 7

TWO CATEGORIES OF ATTACK



*Reference list: github.com/Wack0/bitlocker-attacks

INTRINSEC

Hardware attacks

- **Depends whether targeting dTPM or fTPM**
- **TPM bus sniffing** *(because Microsoft hates parameter encryption)*
- **DMA / PCIe**
- **Cold-boot**
- **…**

Bus-sniffing can take only about 15 minutes with little risk to the device *(except when I am doing it)*

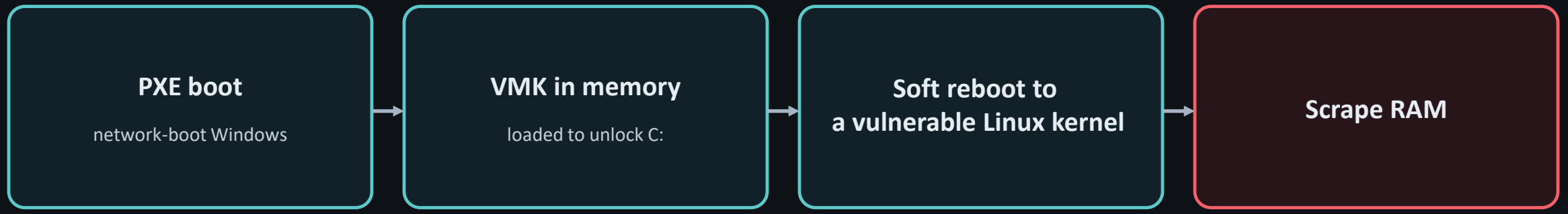
INTRINSEC

Software attacks

- Logical attacks targeting a variety of components: bootmgfw.efi, winload.efi, WinRE, …
- No equipment needed (besides a USB key or Ethernet cable…)
- Some attacks have prerequisites, e.g. USB or PXE boot
- Using a public PoC, not a lot of expertise needed to run (unlike hardware)

BITPIXIE (CVE-2023-21563)

Rairii



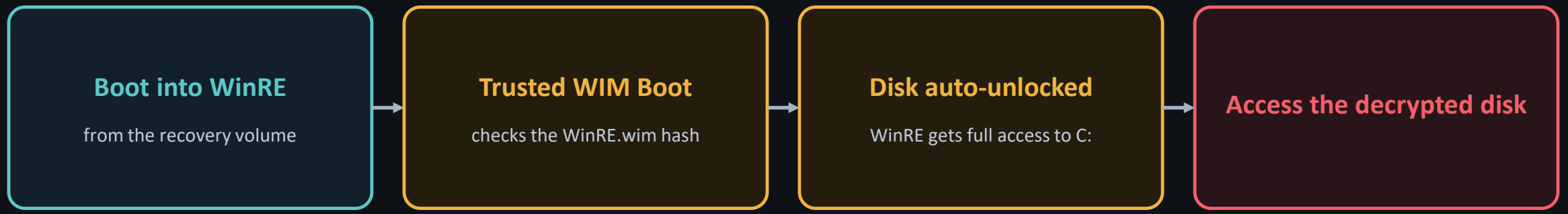
BitPixie abuses the fact that the VMK is not properly wiped from memory after an error (flaw in the boot manager)

✓ PATCHED

Further reading: neodyme.io/en/blog/bitlocker_screwed_without_a_screwdriver

BITUNLOCKER (CVE-2025-48804 and others)

Microsoft STORM (Leviev & Ben Simon)



BitUnlocker abuses a parsing flaw in the boot manager, which enables booting our own modified WinRE environment.

✓ PATCHED

Further reading: techcommunity.microsoft.com/blog/microsoft-security-blog/bitunlocker-leveraging-windows-recovery-to-extract-bitlocker-secrets/4442806

INTRINSEC

Downgrade attacks

- Re-enable the vulnerability on a device **by serving an older, vulnerable boot manager signed by the same PCA as the device's boot manager**

`BitPixie (CVE-2023-21563)`	→ **Public BitPixie downgrade attack on several repos including mine (although I procrastinated a bit)**
`BitUnlocker (CVE-2025-48804)`	→ **Public BitUnlocker downgrade attack on my repo**

MEASURED BOOT DOESN'T CATCH THE DOWNGRADE

Secure Boot accepts it: the signature is still valid (same certificate)

PCR 4

records the binary itself

OFF BY DEFAULT

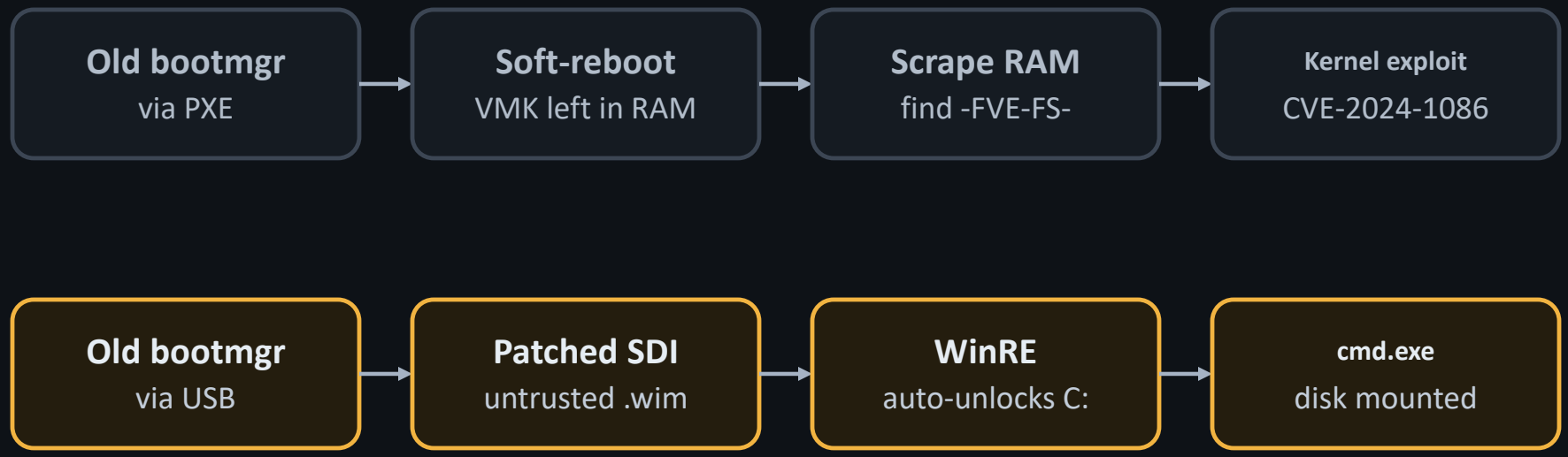
PCR 7

records the signing certificate

UNCHANGED

the TPM releases the key anyway → BitLocker bypassed

BITUNLOCKER VS BITPIXIE



BitUnlocker:

- Requires no external OS (although BitPixie doesn't need Linux *per se*, it's more stable this way)
- Doesn't rely on PXE

INTRINSEC

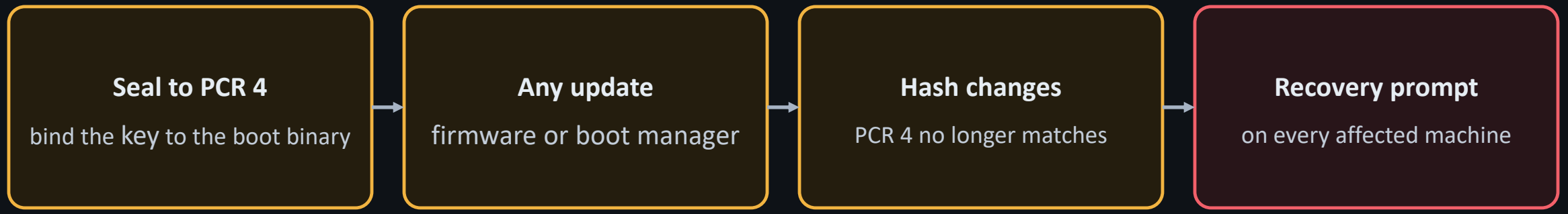
Demo

- Target: fully patched Windows 11
- Boot manager signed by PCA 2011
- Default TPM-only: PCR 7 + 11


Boot Manager
Boot normally
Windows Boot Manager
EFI VMware Virtual NVME Namespace (NSID 1)
EFI VMware Virtual SATA CDROM Drive (1.0)
EFI Network
Enter setup
Reset the system
Shut down the system
Continue to boot using the default boot order.
↑↓=Move Highlight
<Enter>=Select Entry

INTRINSEC

Re-enabling PCR 4 would break things



Microsoft tried this in 2024: recovery screens everywhere, enraged users… it was pulled within a month

Further reading: `neodyme.io/en/blog/bitlocker_why_no_fix`

CERTIFICATE ROLLOUT IN 2026

- PCA 2011 is expiring in 2026
- New PCA 2023 ships in new Windows 11 installs by default
- Once the 2023 certificate is everywhere, firmware rejects the old binaries, and the BitUnlocker downgrade stops working

→ … until we craft a downgrade attack targeting 2023-signed boot files

→ and companies are rolling out quite slowly in practice as 2011-signed devices will still boot

INTRINSEC

A lot of recent BitLocker bugs

- Wave of new BitLocker vulnerabilities
- More boot-path bugs → more downgrade candidates

INTRINSEC

Where downgrades are hard

BOOTMGFW.EFI

Old version still boots current Windows

WINLOAD.EFI

Harder: old loader can't boot a modern kernel

WINRE

Recovery image is integrity-checked so it cannot be replaced with an older one

INTRINSEC

Is your own machine exposed?

Check from an elevated prompt:

```
manage-bde -protectors -get c:
```

Exactly `7, 11` → seal trusts only Secure Boot

```
mountvol s: /s
sigcheck s:\EFI\Microsoft\Boot\bootmgfw.efi
```

`PCA 2011` signer → old binaries still trusted

7, 11 and PCA 2011 → vulnerable

INTRINSEC

REVISE mitigation (KB5025885) & SVN

PCA ROLLOUT

Rolls the Secure Boot certificate: distrust PCA 2011, enroll Windows UEFI CA 2023, ship a 2023-signed boot manager

SVN (SECURE VERSION NUMBER)

A version number baked into the boot manager and locked in firmware. Anything below the current number is refused

- **Has to be installed manually**

Further reading: `support.microsoft.com/en-us/topic/how-to-manage-the-windows-boot-manager-revocations-for-secure-boot-changes-associated-with-cve-2023-24932-41a975df-beb2-40c1-99a3-b3ff139f832d`

Mitigations summary

- Enable PIN but know that:
  - It doesn’t stop an insider with knowledge of their own PIN
  - It may also be guessed, especially when derived by GPO from the hostname
- Enable PCR 4 if you don’t mind recovery screens and complaints from your users (BitLocker legacy configuration)
- Roll out PCA 2011 and migrate towards PCA 2023
- Apply KB5025885 if you can

INTRINSEC

github.com/garatc/BitUnlocker