25C3: Nothing to hide

Full-Disk-Encryption Crash-Course
– Everything to hide –

Jürgen Pabel, CISSP
Akkaya Consulting GmbH

Introducing myself

- I studied Computer Science at Georgia Tech and Information Assurance at Norwich University
- I work as an IT-Security consultant at Akkaya Consulting GmbH in Cologne (Köln), Germany
- I like to play Rugby, but my ambitious playing days are over

„Okay, what are we looking at and why are we looking at it?“ - MST3K

- What: Full-Disk-Encryption
  - Hardware solutions (some quick notes)
  - Software solutions
- Why: Data stored on mobile devices is exposed to unauthorized physical access (loss/theft).

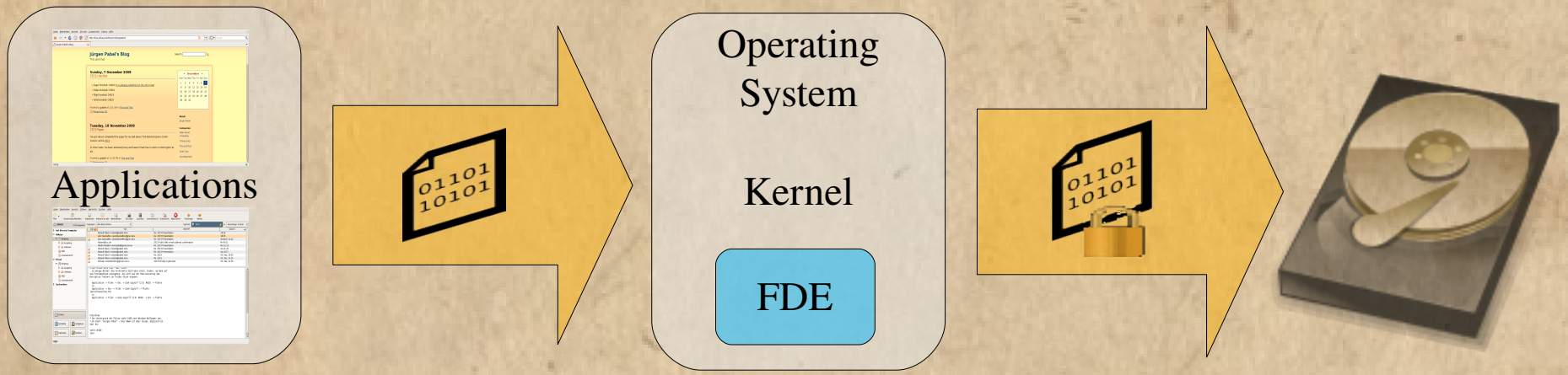
Full-Disk-Encryption

- Encrypts (almost) every bit on your disk ...
  - ... through hardware (these are the quick notes)
    - USB/Firewire HDD with cryptographic controller (fingerprint/PIN authentication, ...)
    - HDD provides cryptographic controller (ATA security)
  - ... through software
    - Operating system component, works transparently
    - Neglible every-day performance impact (depends mostly on CPU)

Architecture: Pre-Boot-Authentication

- Loaded by BIOS from unencrypted storage
  - Linux: boot partition with init-RamDisk (/boot)
  - Windows: (proprietary) pre-boot environment
- Reads in the cryptographic key for encrypted disks
  - Password, smart-card, ...
- Loads operating system from disk
  - Linux: filesystem on encrypted device is mounted
  - Windows: interrupt 13h is hooked (NTLDR uses int 13h)

Architecture: Encryption driver



- Linux: Device-mapper, device driver hooking, ...
- Windows: Lower-level filter driver
  - Key handoff from int 13h function (used for NTLDR)

Architecture: Initial encryption

- Linux
  - Device-mapper: Only new filesystems can be created on encrypted device
  - Device driver hooking: Available as proprietary software (with support for in-place encryption)
- Windows
  - Lower-level filter driver: In-place („on-the-fly“) encryption is a standard feature

Solutions (1/2)

- Windows: Commercial software
  - CE-Infosys CompuSec (also available for Linux)
  - CheckPoint FDE (also available for Linux & OSX)
  - PGP WDE
  - Safenet ProtectDrive
  - Secude FinallySecure
  - Utimaco Safeguard Easy/Enterprise
  - Windows Vista BitLocker

Solutions (2/2)

- Windows: Open-Source Software
  - TrueCrypt
  - DiskCryptor
- Linux
  - Device encrypted filesystems (LUKS/dm-crypt)
  - Cryptographic filesystems[1]
  - Stacked filesystems[1]

[1]Only mentioned for completeness, not relevant to focus of presentation

Risks

- Weak passwords
  - About 6 bits of entropy per password character, but cryptographic keys are usually 128 or 256 bit
- Cold-boot attacks
  - Requires powered-on computer system
- Coercion

Oddities

- TPM support != TPM support
  - Cryptographic key storage
  - Binding operating system to TPM chip
- Multi-disk support (not RAID)
  - Works great ...
  - ... except for when disks fail or new disks are installed
    - Decrypt all remaining (working) drives
    - Uninstall & reinstall software
    - Encrypt all drives

TrueCrypt

- Unique cryptographic features
- Multi-Platform compatible
- Unsuitable for most enterprise environments
  - No key management (preconfigurable recovery key, ...)
  - No user management (multiple users for PBA)
  - Very technical and somewhat confusing user interface

DiskCryptor

- Project created by russian developers
  - Still in development phase: current version is 0.4
  - DiskCryptor aims to be TrueCrypt compatible[1]
- Unsuitable for most enterprise environments
  - No key management (preconfigurable recovery key, ...)
  - No user management (multiple users for PBA)
- No installer application

[1]This will (unfortunately) change with version 0.5

DiskCryptor+AC

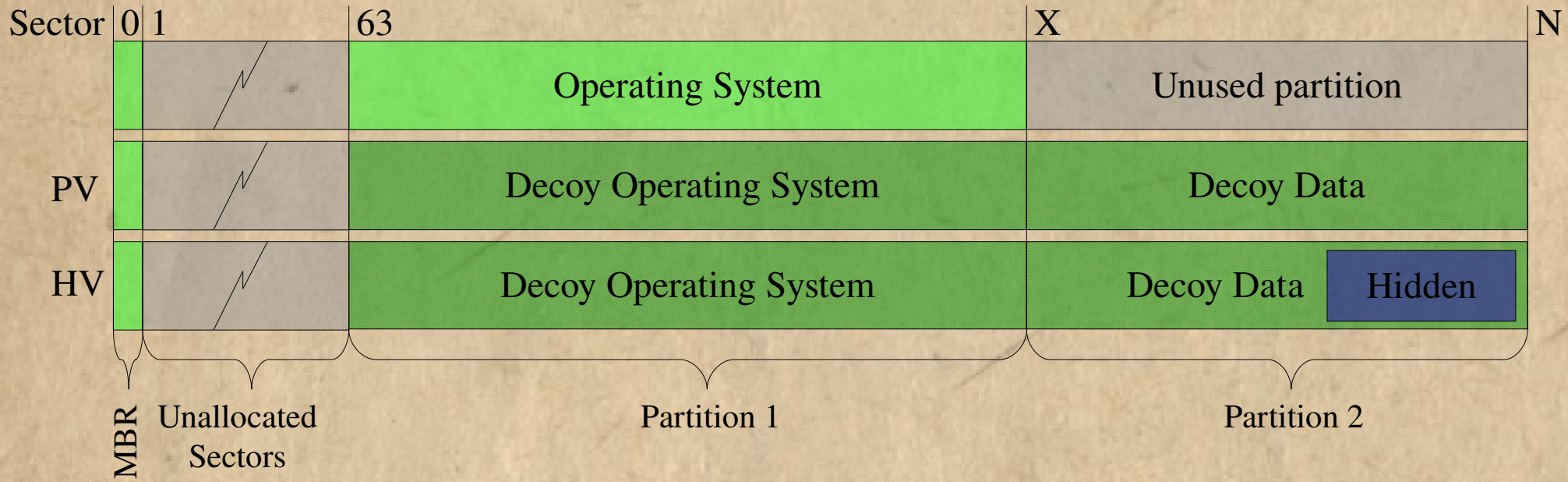
- Based on DiskCryptor
  - Includes an installer (and uninstaller) application
    - Installs software
    - Prompts user for drive selection for encryption
    - Prompts user for encryption password
  - Added user manuals (English and German)
- Future releases will remain TrueCrypt compatible (will fork under new name)

TrueCrypt: Volume layout

- Volume header
  - In-place encrypted system partition volume (512 bytes)
    - Header is encrypted: magic string („TRUE“), header version, ...
  - All other volumes
    - Volume header + hidden header & reserved area (128 Kb)
- Volume backup header (128 Kb)
  - Encryption key is derived from different salt value
  - Ommitted for in-place encrypted system partition

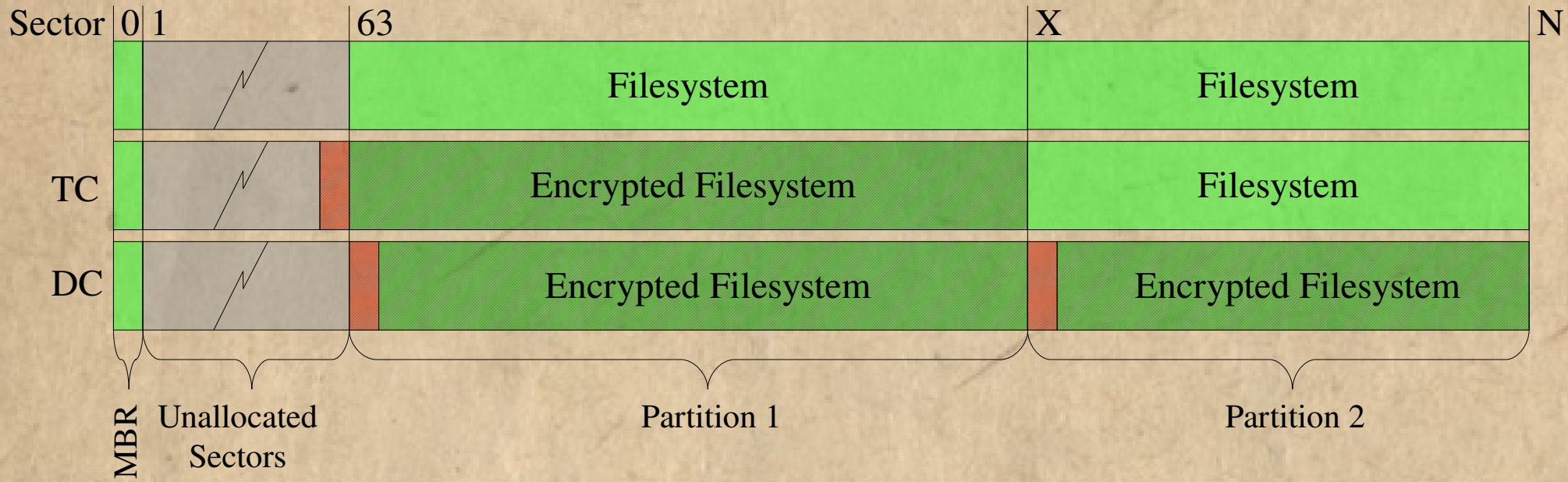
TrueCrypt: Hidden volume

- Decoy volumes: Partition 1 (encrypted): Operating system
  Partition 2 (encrypted): Data
- Hidden volume: Partition 2 (encrypted): Operating system/Data
  (TrueCrypt driver emulates hidden volume as a disk partition when running the hidden OS)



TrueCrypt: In-place encryption

- TrueCrypt:
  1. Volume header is prepended (marked in red)
  2. Sectors are encrypted in-place
- DiskCryptor:
  1. Filesystem is shrunk
  2. Volume header is inserted (marked in red)
  3. Sectors are relocated & encrypted



Open-Source feature wishlist

- TrueCrypt compatible user and key management
  - TrueCrypt volume specifications are key agnostic ...
  - ... user and key management data must reside elsewhere
- Pre-Boot-Authentication environment
  - Storage implementations
    - Unallocated or „hidden“ sectors (Host-Protected-Area)
    - Unencrypted file on otherwise fully encrypted filesystem
  - Cryptographic key storage (TPM, HSM, Network, ...)
- Protection against cold-boot attacks

Full-Disk-Encryption Crash-Course

- Workshop: tomorrow from 19:00 to 20:00 in A03
- Thank you for your attention

Q & A

Full-Disk-Encryption Crash-Course

The typewriter font used on the title slide is the „Last words“ font by Johan Holmdahl (http://www.free-typewriter-fonts.com).