FrOSCon 2009

From PBA To Login

Improving The Full-Disk-Encryption Experience For Linux

Jürgen Pabel, CISSP
Akkaya Consulting GmbH

Introduction

- Jürgen Pabel
  - Consultant for IT-Security (CISSP)
  - Various Open-Source Activities
  - Rugby

- Akkaya Consulting GmbH
  - IT-Consulting http://www.akkaya.de/
  - Medical Software http://www.ac-stb.de/

Agenda

- Overview
  - Data-At-Rest Security For Linux
  - LUKS & dm-crypt
  - Implications of the LUKS design
- TokenTube: Integrating the PBA with PAM
  - Concepts, Components & Features
  - Debian/Ubuntu Integration
  - Live Demo
  - To-Dos

Data-At-Rest Security For Linux

- File encryption
  - GnuPG
- Cryptographic filesystems
  - EncFS
- Device encryption
  - loop-aes
  - dm-crypt
    - Cryptographic computation in kernel space
    - Key management not included

Linux Unified Key Setup (LUKS)

- Platform independent on-disk layout specification
  - Encryption cipher (& mode)
  - Digest of master key
  - 8 key slots

- Attack-resilient key management
  - Randomly chosen number of iterations on key
  - Anti-Forensic Information-Splitting

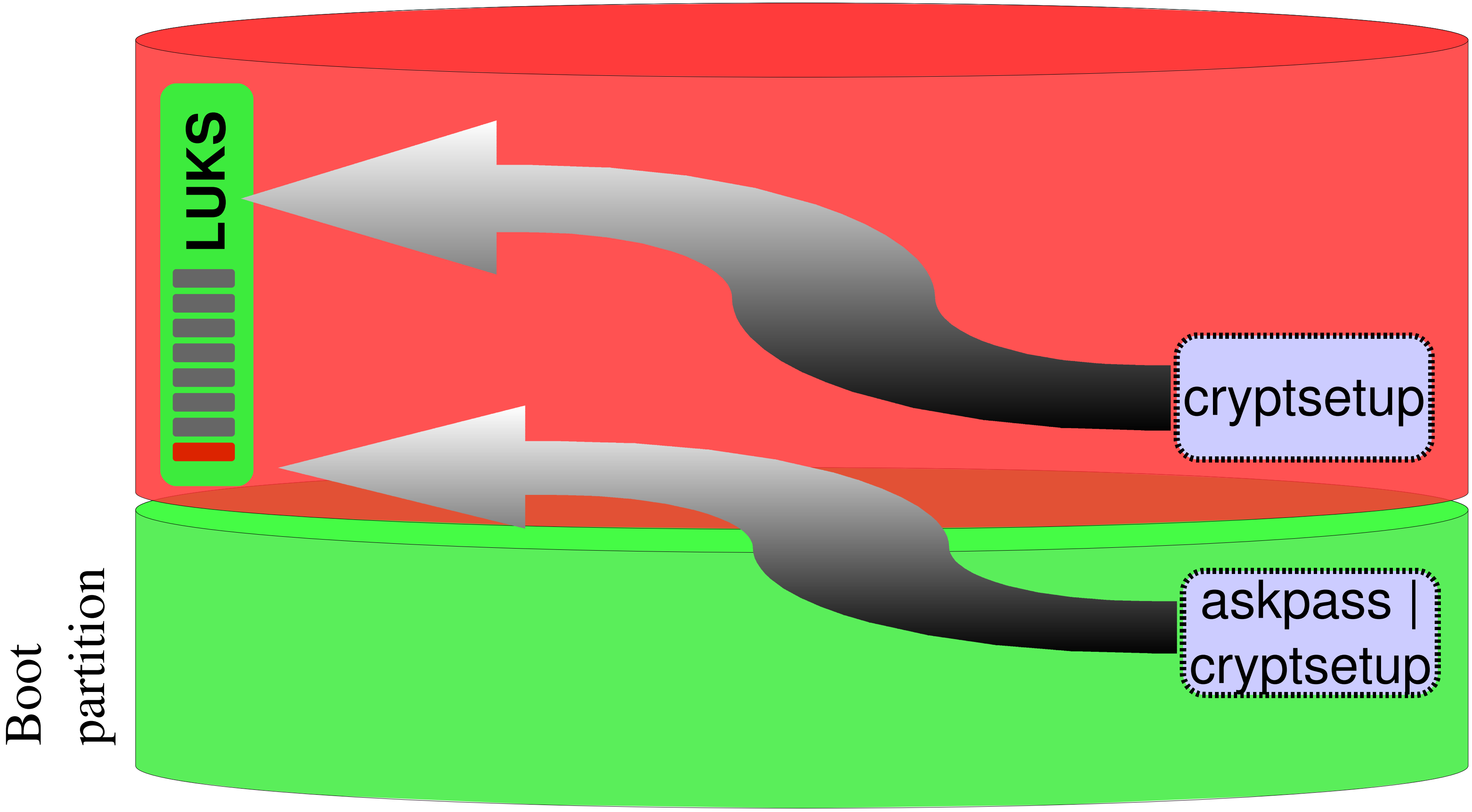
- LUKS tool: cryptsetup

LUKS/dm-crypt: System Startup

- Kernel startup
- Initramfs
  - Pre-Boot-Authentication
    - Debian/Ubuntu: askpass | cryptsetup
  - pivot_root

- System startup
  - *Some other magic happens here...*
  - Console/Desktop login

LUKS/dm-crypt Visualized



LUKS/dm-crypt: Status Quo

- The good
  - Ability to use a really strong encryption password
- The bad
  - Who actually uses truly strong passwords for encryption?
- The ugly
  - It actually impedes a wider deployment of LUKS/dm-crypt

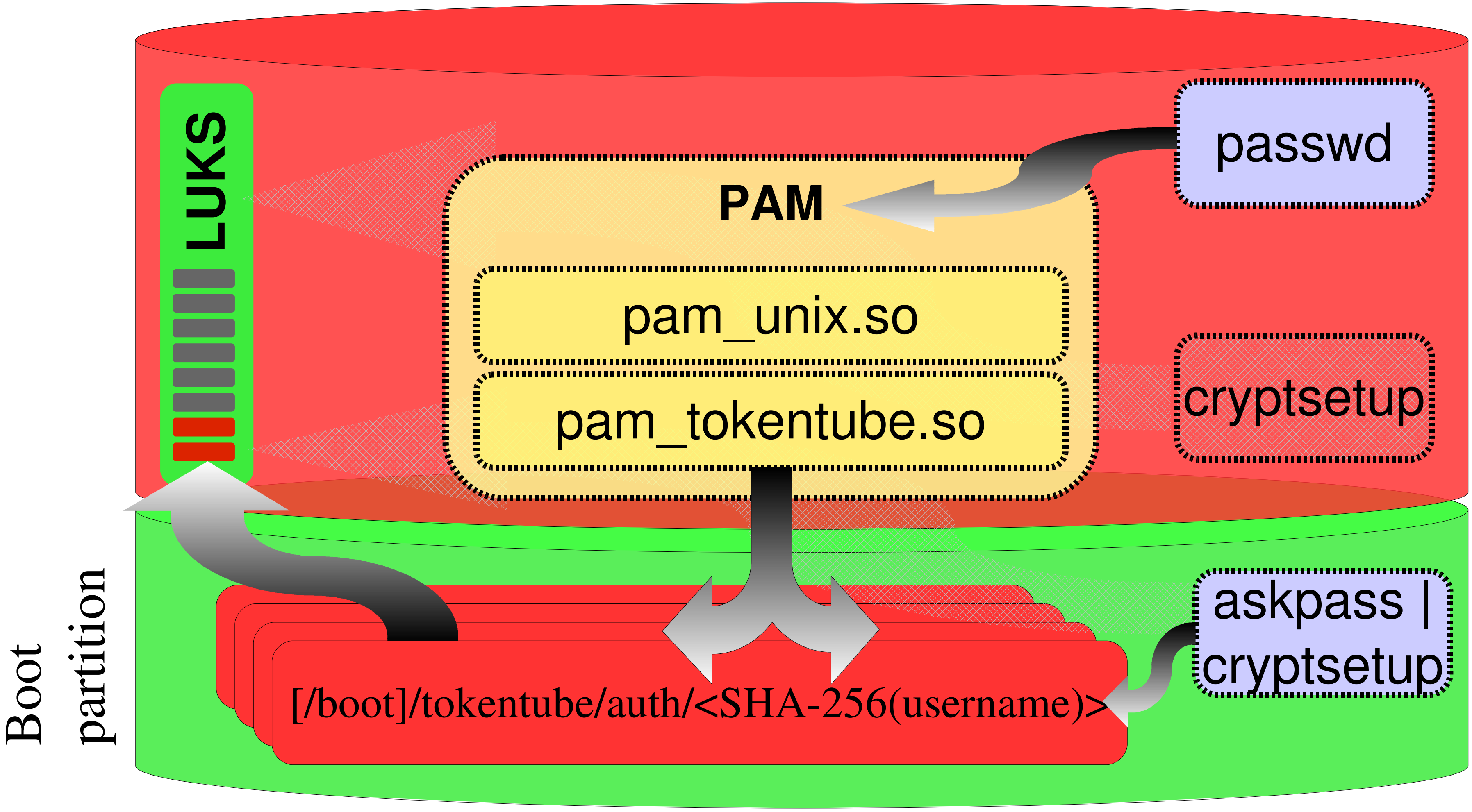
TokenTube

- Per-user authentication file in /boot/tokentube/auth/
  - Encrypted with user's login password
  - Contains the keyfile for unlocking a LUKS keyslot

- PAM module [sic]
  - Re-encrypts authentication file with user's new password

- PBA User Authenticator („askpass“)
  - Locate user's auth file on boot device
  - Decrypt user's auth file using login password
  - Print decrypted key to stdout (piped into cryptsetup)

TokenTube Visualized



Authentication Files

- Filesystem
  - /boot/tokentube/auth/
    - Filename ➛ SHA-256(username)
    - Encrypted with user's password

- Data structure
  - 32 bytes ➛ LUKS master key
  - 32 bytes ➛ SHA-256(UUID of device containing root filesystem)

Configuration Files

- Initramfs
  - /etc/tokentube/boot.conf
    - Contains name of boot device (/dev/disks/by-uuid/...)

- Filesystem
  - /boot/tokentube/askpass.conf
    - Language resources for prompts
    - Default username
    - Credential-caching daemon
  - /etc/tokentube/luks.key (optional)
    - TokenTube master key for LUKS

askpass (Debian/Ubuntu)

- Load configuration
  - Obtain boot device from initramfs (/etc/tokentube/boot.conf)
  - Read configuration file from boot device (e2fslibs)
- Prompt for username & password
  - Leave username empty for „native“ LUKS key
- Unlock TokenTube master key for LUKS
  - Load user's auth file from boot device (e2fslibs)
  - Decrypt key from auth file with user password
  - Print key to stdout (piped into cryptsetup)

Credential-Caching Daemon

- In a nutshell
  - Open a UNIX socket for communication
  - Receive user credentials from askpass for caching
  - Send user credentials to GDM/KDM greeter

- Security
  - Prevent swapping of memory pages (mlockall)
  - Prevent others from tracing it (PTRACE_TRACEME)
  - Identify the connecting process (SO_PEERCRED)
  - „Hide“ user credentials among random data in memory

Challenge-Response Recovery

- User experience
  - User enters C/R initiator string as username („#helpdesk“)
  - Randomly generated Challenge-Code is displayed
  - User enters Response-Code (provided by helpdesk)

- Perfect Forward Secrecy
  - $\mathtt{Key}_{\mathtt{file}} = \mathtt{Challenge} \oplus \mathtt{Response} \oplus \mathtt{Secret}$
  - $\mathtt{Secret} = \mathtt{MD5}(\mathtt{Key}_{\mathtt{luks}})^{\mathtt{n}}$ → n decrements per C/R
  - $\mathtt{Key}_{\mathtt{luks}} = \mathtt{AES}\texttt{decrypt}($„helpdesk.key“, $\mathtt{Key}_{\mathtt{file}})$

Debian/Ubuntu Integration

- Pre-Boot-Authentication
  - Enhanced version of „askpass“
- System
  - Update initramfs
    - TokenTube binaries
    - Configuration file with device name of boot device
  - Configure PAM integration (pam-auth-update)
- Debian-Installer
  - partman-crypto
  - user-setup

Live Demo

- Ubuntu 9.04
  - /dev/sda1 Encrypted root filesystem
  - /dev/sda5 Boot partition

- Presented functionality
  - Installation and configuration (if time permits)
  - Pre-Boot-Authentication
  - GNOME automatic user login
  - Change user password

To-Do List (1/2)

- TokenTube binary & library
  - Code clean-up
- PAM
  - Establish preferred PAM configuration directives
- GNOME / KDE Greeter
  - Correctly implement GDM conversation
  - Implement GDM conversation logic for GNOME >= 2.21
  - Implement KDE conversation

To-Do List (2/2)

- Pre-Boot-Authentication
  - Challenge-Response
  - Integration for non-Debian based distributions

- Helpdesk Frontends
  - Command line
  - Web application

URLs

- SourceForge (mailing list, issue tracker, ...)
  - http://sf.net/projects/tokentube/
- Ubuntu PPA
  - https://launchpad.net/~jpabel/+archive/ppa
- My Ramblings
  - http://blog.akkaya.de/jpabel/
  - http://twitter.com/juergenpabel/

From PBA To Login

Thank you for your attention.

Please ask questions!