The Dog Ate My Encryption Keys 2.0

Lessons to learn about failures of hard drive encryption.

CRYPTO PARTY

Who?

- **Whitehat Hacker, over 7 years performing penetration tests.**
- **Author of exploits, rootkits & offensive security testing tools.**
- **Electronics & Radio enthusiast.**
- **Security & Privacy Advocate.**
- **Volunteer at CryptoParty London.**
- **I like LOLCATS.**

FDE? WDE? What is that?

- **Full Disk Encryption / Whole Disk Encryption.**
- **Hardware based (Flagstone)**
- **Software based (PGP-WDE, TrueCrypt, FileVault2 etc.)**
- **We will focus on a completely open-source software solution.**
- **Linux - Device Mapper (DM) Crypt & Linux Unified Key Setup (LUKS)**
- **Allows to encrypt an entire block device or partition. Can encrypt an entire Linux system! Used by Android, focus on laptop use.**

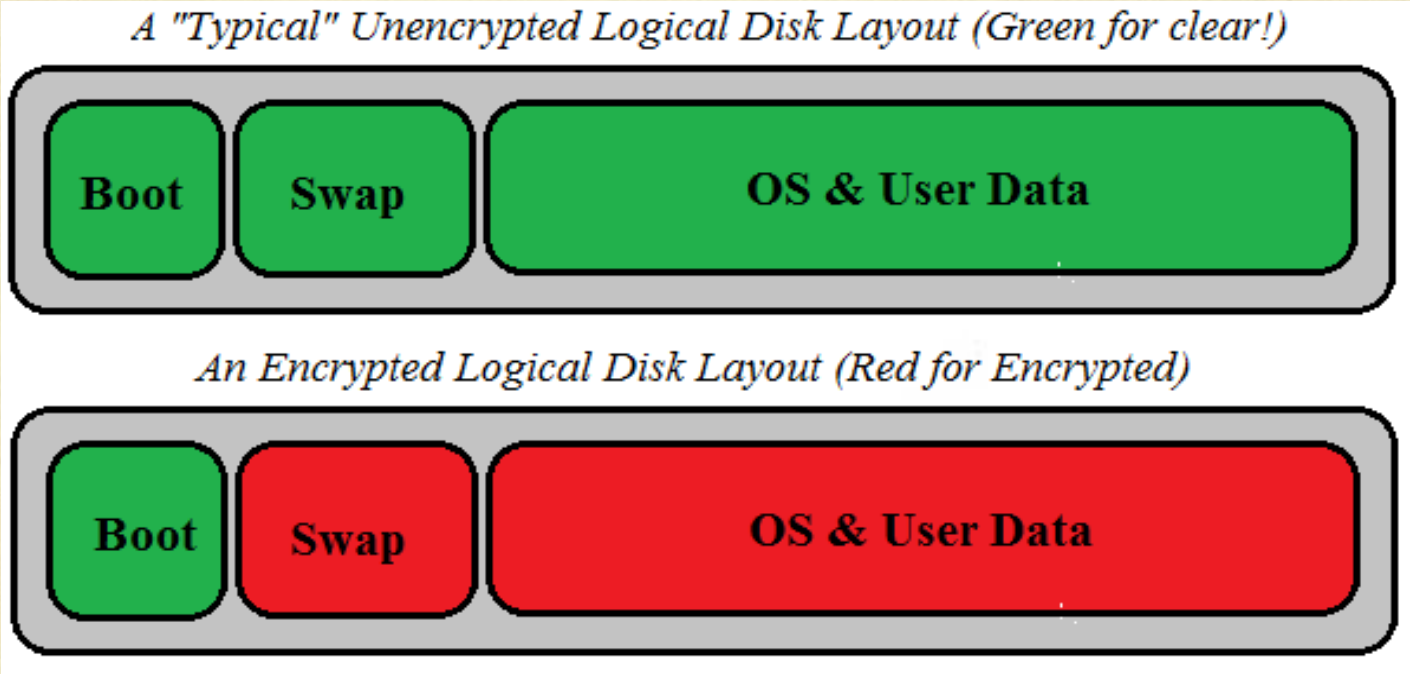
What can WDE protect against?

- **On The Spot Data Inspection (E.G. border security).**
- **Lost & Stolen Devices, hinder sensitive information falling into the wrong hands.**
- **Intended to protect your data from prying eyes when computer is powered off.**
- ***WDE is not infallible!***
- **Strong computer security hygiene and operational security (OPSEC) practices should also be used.**

How does it work?

- **Typical Computer Boot Strap Process. Newer systems use UEFI instead of a BIOS.**
- **The Boot Loader or the Operating System is usually responsible for decrypting an encrypted drive.**
- **With DM-crypt it is the Operating System – the Linux Kernel - which is responsible for decrypting and accessing the drive.**

Logical Disk Layout



- **Both layouts have an unencrypted “boot” partition. This is where the code that prompts for key file or pass-phrases is stored.**
- **Current open-source tools do not support encrypting this partition. You can & should encrypt everything else.**

DM-Crypt & LUKS

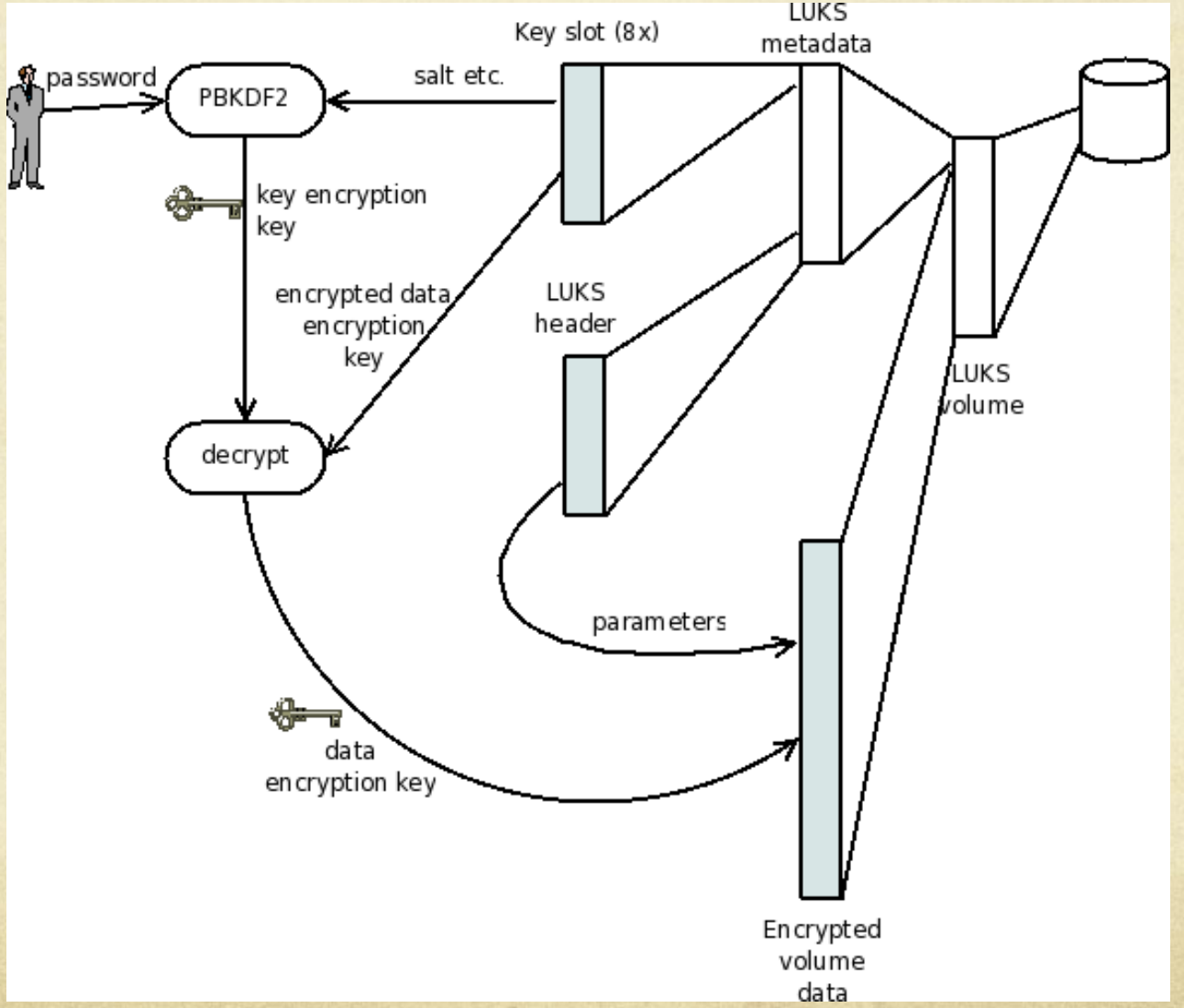


Image from online Redhat tutorial

Pass-Phrase & Key files

- **A secure pass-phrase should be chosen for WDE solutions.**
- **A software token or “key file” can be used instead of a pass-phrase.**
- **Key file can be stored on a USB drive so that the data cannot be decrypted without the USB drive.**
- **The key file can also be protected with a pass-phrase using a Gnu Privacy Guard (GPG) private key or OpenSSL.**
- **Attacker would need the key file, the key file pass phrase & the hard disk to access your data!**

Encryption Setup & Watermarking

- **Linux DM-Crypt & LUKS supports a range of different encryption algorithms, schemes and IV generation selection options.**
- **A number of helpful tutorials exist on-line. I am not a cryptographer, read discussions online!**
- **AES-XTS-ESSIV:SHA256 is believed to offer high levels of security, unless you encrypt large amounts of data (1TB or more).**
- **Review all the options available to you and ensure you pick a setup appropriate for your needs and security level.**
- **Water-marking is an attack to identify if a specific file exists on disk. AES-CBC-PLAIN is potentially vulnerable.**

Setting it up!

- **Ubuntu Community Pages (Beginner)**
- **https://help.ubuntu.com/community/EncryptedFilesystemHowto**
- **Arch Linux Wiki (Intermediate)**
- **https://wiki.archlinux.org/index.php/Dm-crypt_with_LUKS**
- **Gentoo Wiki Article (Advanced)**
- **http://en.gentoo-wiki.com/wiki/DM-Crypt_with_LUKS**

The De-Facto Best Practice

- **Use a GPG or OpenSSL protected key-file stored on removable media.**
- **Key-file protected using the “Diceware” pass-phrase method.**
- **Good candidate for key file storage is a CD-R.**
- **The damn dog ate my encryption keys!**

Evil Maid Attack

- **Evil Maid attacks shown to be used by an intelligence agency to access nuclear secrets from Syria in London Hotel.**
- **One of the most effective known attacks against WDE.**
- **Software WDE requires computer to execute or boot something first.**

"*Remember the evil maid attack: if an attacker gets hold of your computer temporarily, he can bypass your encryption software*" - Bruce Schneier

Mossad hacked Syrian laptop to steal nuke plant secrets • The Register - Google Chrome

Mossad hacked Syrian

www.theregister.co.uk/2009/11/06/mossad_syria_trojan_hack/

Access Control –... BBC News - How... ▶ sinergy the fo... 'I've Got Nothing... Home | IMLI STR...

Mossad hacked Syrian laptop to steal nuke plant secrets

Evil Maid attack led to air raid

By John Leyden, 6th November 2009 Follow 1,847 followers

27

Vendor Landscape: Small to Mid-range Storage Arrays

Mossad reportedly used a Trojan to hack into a Syrian official's laptop while he stayed in a London hotel.

The information extracted was used to plan a bombing raid at a suspected nuclear reactor facility in Syria, Israeli newspaper *Haaretz* reports.

The air raid on the partly-constructed Syrian nuclear facility in September 2007 took place a year after the unnamed Syrian official left his unattended laptop in his room in a hotel in Kensington, London. The government

RELATED STORIES

Schneier: Teens and treaties - our cyber-war saviors

Israeli air raid vs Iran nukes boardgame out in time for Xmas

MOST READ MOST CO

TUPPERWARE FOUND ON MC Saturn

Microsoft investors push for E defenestration: report

500 MEELLION PCs still run W How did we get here?

Ubuntu 13.10: Meet the Linu a bizarre Britney Spears fixat

GTA V Online hits speed bum delay before you can rough u hooker

SPOTLIGHT

The NSA's hiring - and they want a CIVIL LIBERTIES officer

UK.gov zombie under Chann

DMA attack

- **DMA allows device bus, drivers & kernel mode to access physical memory normally restricted to user by the MMU.**
- **IEEE 1394 (Firewire) most widely known for this attack, public tools available to dump entire system memory or bypass screen lock. Other vectors exist.**
- **Commercial packages available aimed at Government & Law enforcement clients.**
- **This can be used to recover cryptographic key material from system memory!**

Usage

1. Go to your Target System

2. Start FinFireWire

3. Plug in FireWire Adapter & Cable

4. Select a Target

5. Wait until System is unlocked

Product Components

FinFireWire - Tactical Unit

· Complete Tactical System

Point-and-Click User Interface

· Easy-to-use User Interface

Connection Adapter Cards

· PCMCIA and ExpressCard Adapter for Target Systems without FireWire port

Universal FinWire CableSet

· 4 pin to 4 pin
· 4 pin to 6 pin
· 6 pin to 6 pin

GAMMAGROUP

GAMMA INTERNATIONAL
United Kingdom

Tel: +44 - 1264 - 332 411
Fax: +44 - 1264 - 332 422

info@gammagroup.com

Cold Boot Attack

- **When a machine is cold-booted, powered off then on rapidly, cryptographic key material may still be present in RAM.**
- **Cooling the RAM can extend the window of opportunity for an attacker to recover the memory contents.**
- **Effective against full disk encryption solutions and demonstrated publicly numerous times.**
- **In 2007 CERT assisted the FBI and Secret Service to perform this attack against Max Butler. Max was found to be running “Carders Market” and without this attack much evidence against him would have been lost.**

Bootkits

- **Bootkits are a form of “backdoor” that replace the boot loader or infect kernel memory from firmware.**
- **BIOS, UEFI & PCI network cards infection methods have all been demonstrated publicly.**
- **“Stoned” bootkit can be used to recover encryption pass-phrases.**
- **Extremely difficult to defend against, security tools do not widely exist for identifying threats at this low-level.**

Hardware Key Logger!

- **A simple USB or PS/2 keyboard logger might be all that is needed!**
- **These can be configured to send keys over wireless technology so they do not need to be recovered from target!**

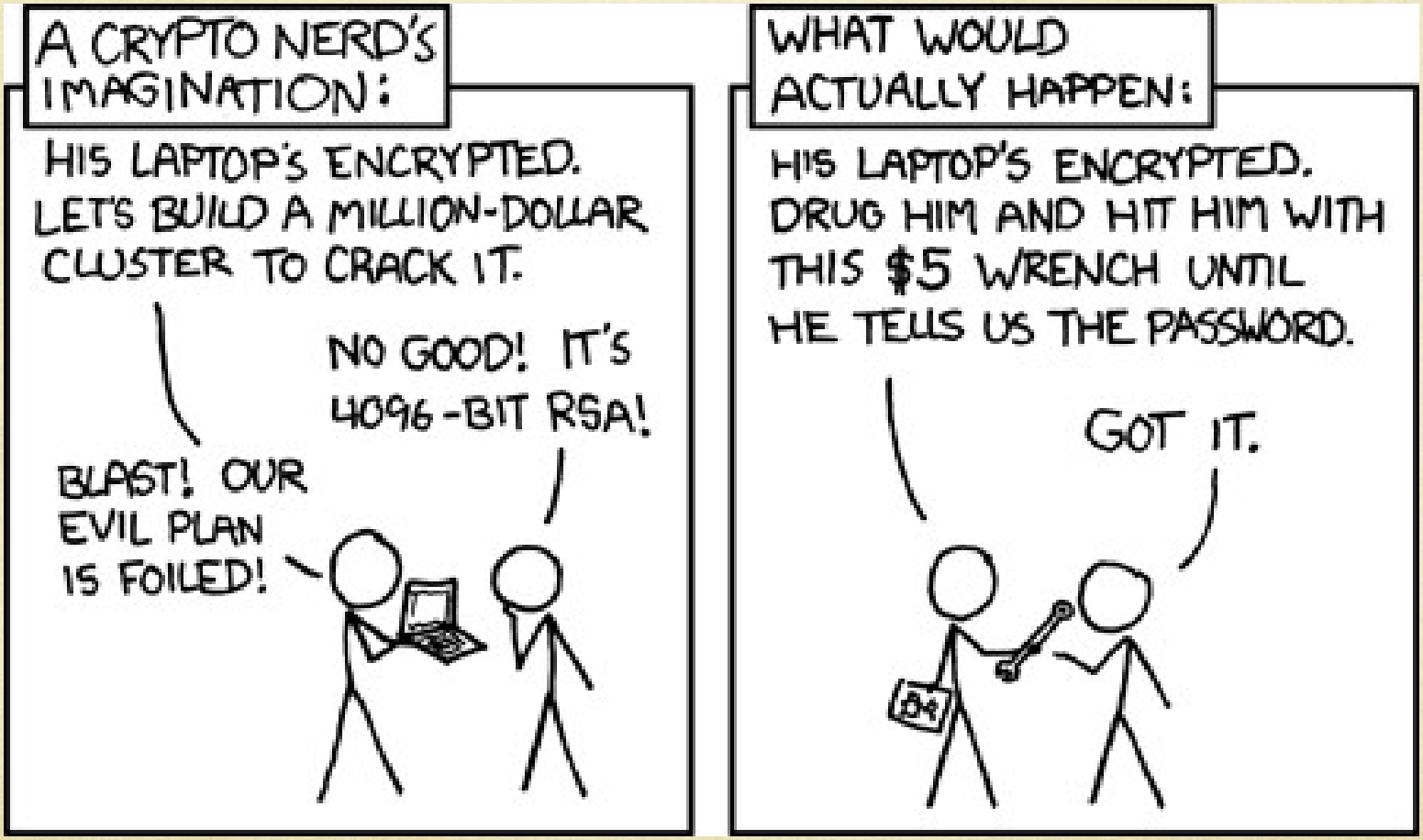
Offline Brute-Force Attacks

- **PBKDF2 implements key stretching, pass-phrases and key files create a “derived key”. This increases the time required for a brute force attack.**
- **PBKDF2 is used by LUKS.**
- **The biggest weakness in any computer system is the person operating it.**
- **Individual profiling can expose common traits or hobbies that can assist in password guessing attacks.**
- **Password re-use, WDE passwords should be unique and not used elsewhere under any circumstances.**

Diceware

- **Diceware is a method for constructing a pass-phrase from a pad or dictionary using dice rolls as a hardware random number generator.**
- **I tested with a number of different length pass-phrases to see results, best practice recommends seven or more.**
- **I Assumed no cryptographic weakness attacks & the stop condition is successful decryption of data.**
- **Seven words gave 90.474896 bits of entropy.**
- **This means one in 1720618914350498293236105216 possible outcomes.**
- **Here is a pass-phrase “warebayvetmaybenumbmesonnora”**
- **Attacker requires the following time at 100000000000000 (1e15) guesses/second to exhaust all possible pass-phrases.**
- **199145707 days, 16:18:24.982422**
- **You can make adjustments to improve the scheme!**

$5 Wrench Attack



Fighting Back.

- **Don’t leave your machine locked and unattended! Even when just going to a hotel bar!**
- **Add OS level integrity checks, an init or boot script that hash checks kernel and initrd after booting may alert to compromise.**
- **Disable hardware you do not need. Fill external ports with glue! Disable drivers you don’t need. Blacklist all DMA capable devices! (modules.d)**
- **THC secure delete can wipe memory! Do it on boot up & cron!**
- **Double Encrypt! Use WDE and another encrypted container for data! Encrypt additional files inside with OpenSSL or GPG.**

Snowden Revelations!

- **We need more transparency to understand the damage done to existing cryptography solutions.**
- **Closed-source solutions cannot be trusted.**
- **Open-Source gives more insight, if standards are intentional weak we must know how!**

“The Internet has become essential to our lives, and it has been subverted into a gigantic surveillance platform. The solutions have to be political. The best advice for the average person is to agitate for political change.” – Bruce Schneier

Questions?

Remember, encryption can provide privacy but not secrecy.

hackerfantastic @ riseup . net

GPG: 9027AB55
C491 A58D 2C47 97A6 DF74 7EE6 2764 E8E1 9027 AB55