What Industry Standard Self-Encrypting Storage is, and why it is Essential

The Big Picture

Robert Thibadeau, Ph.D.

www.drivetrust.com

www.privust.com

A Talk with a New Book Behind It

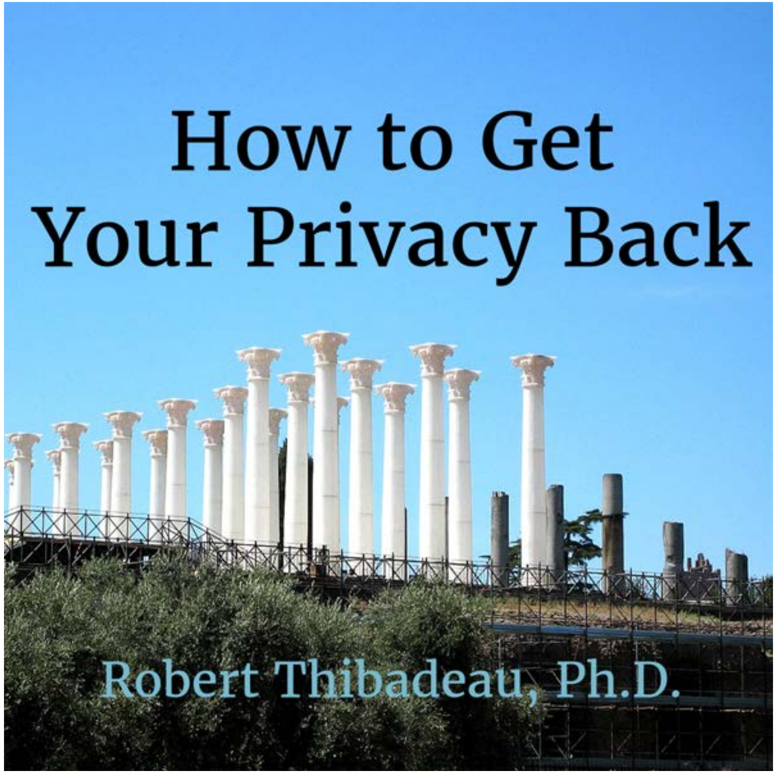
- History and Universal Defense for Self-Encrypting Drive Products
  - Popular Nonfiction : NO TECHNICAL KNOWLEDGE ASSUMED
  - In ~200 NonFiction Pages, 40 Diverse Chapters
  - All necessary detail for average person is in the book
  - Great Basic Education for Storage Sales, Marketing & {new} Managers and Engineers

The Book

Available NOW

On Amazon **Kindle**, **Paperback, Audible, iTunes,**

Search Title or my Name on Amazon Books

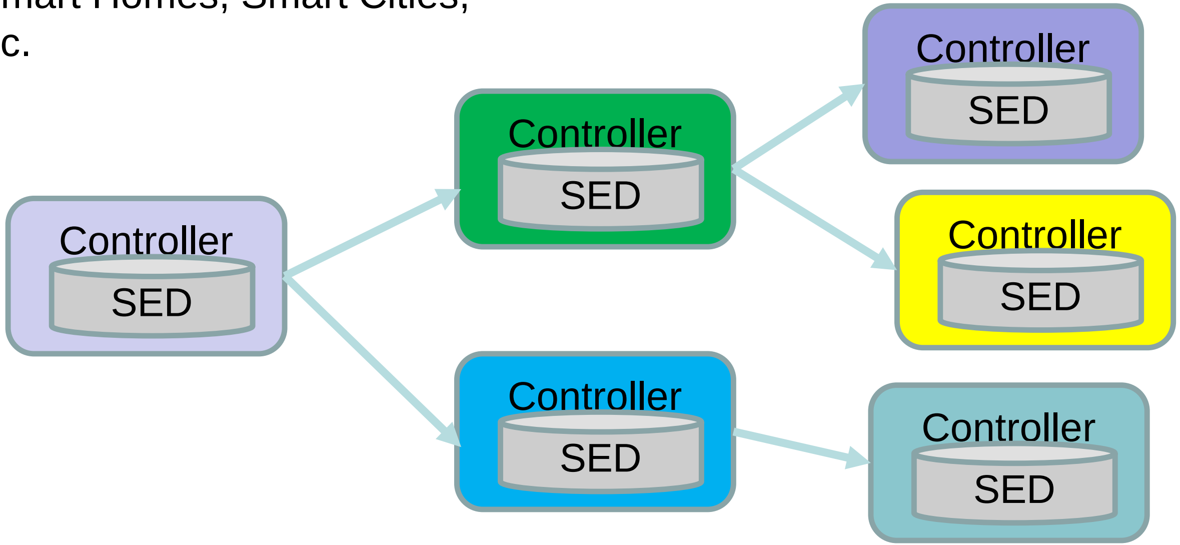


Agenda

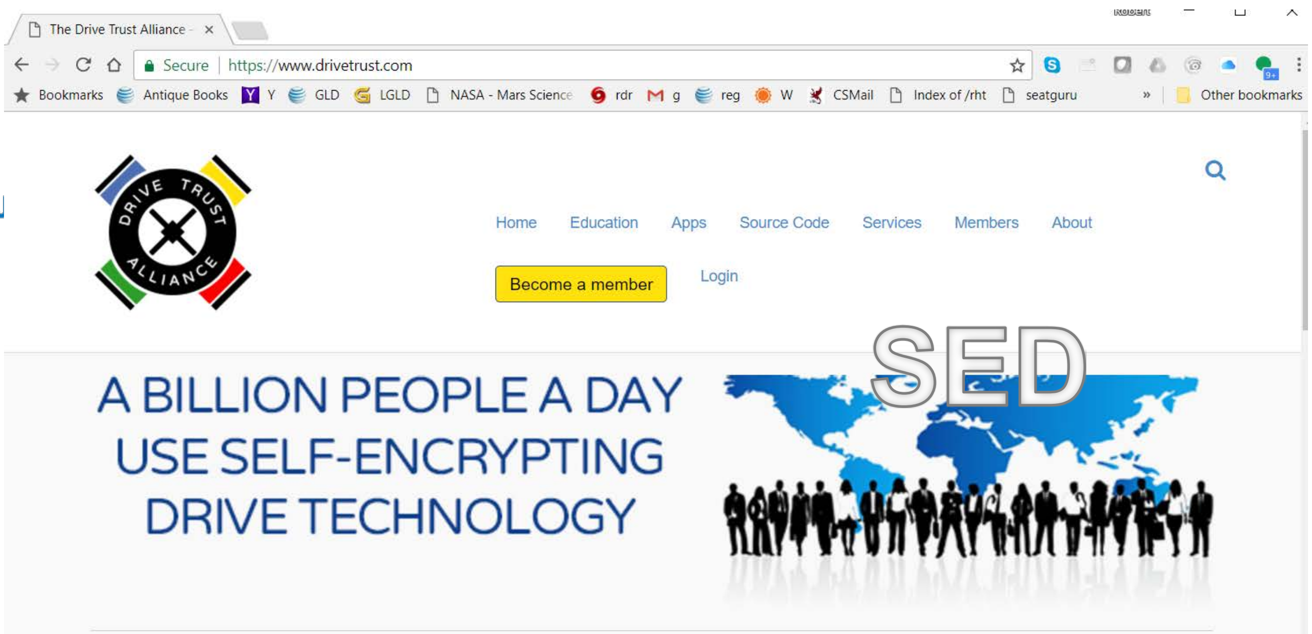
- Self-Encrypting Drive Overview
- The Book's Approach to the Average Person or Organization
- A few details in and not in the Book
  - Proposal for Apple/FBI Kerfuffle
    - How to Prevent Backdoors, but give FBI what it *should* want
    - REAL Backdoors – The Engineering Problem

Compute storage is a Supply Chain “thing” (or try “mess”)

This is what you find in Enterprise, Endpoints, Cars, Trucks, Planes, Smart Homes, Smart Cities, Robots, etc etc etc.



Self-Encrypting Drives (SEDs) Provide UNIFORM Privacy Assurances in Diverse Computing Environme



A BILLION PEOPLE A DAY USE SELF-ENCRYPTING DRIVE TECHNOLOGY

Every Non Volatile Memory Maker in World makes Industry Standard Self-Encrypting Drives

Intel, Western Digital, Seagate, Micron, Samsung, SK Hynix, Toshiba, San Disk, etc. etc. etc.

100% of Google, Amazon, eBay, Facebook, etc. etc., Cloud data centers use Self-Encrypting Drives

(Same use cases are for Automotive / IoT)

“How to Get Your Privacy Back” Chapter Organization

- 40+ Chapters including
  - Nutshell Courses in Computer Security and Cryptography
  - Apple/FBI Kerfuffle Solution
  - Better Alternative to the “AGREE” button blight
  - Bitcoin Privacy
  - Facebook and Social Media
  - GDPR – European Privacy and US Privacy Law
  - Why Self-Encrypting Drives (Hardware Encryption)
  - Automotive / IoT Privacy
  - The Power of Lies and Trump’s Method
  - Specific, Concrete, Predictions on How you are going to get your privacy back

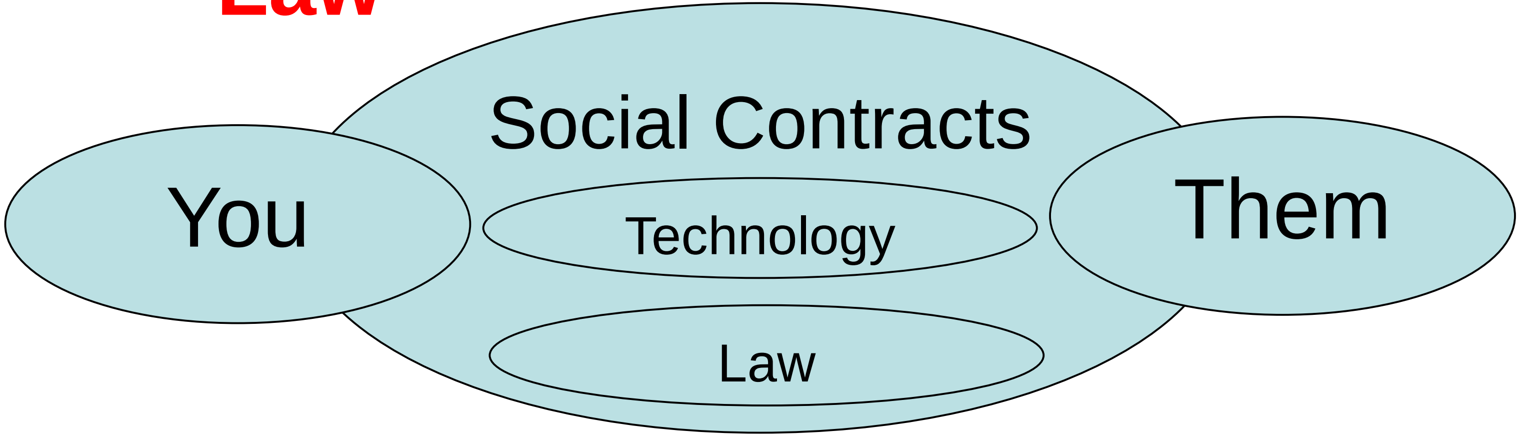
“How to Get Your Privacy Back”

Basic Themes

.

- How Privacy has been lost and but not lost forever
  - ***We cannot get your information back*** : We get ***control of your information back***

Universal Privacy Use Case: **Social Contracts** (from the Enlightenment), **Technology**, and **Law**



Backdoor Technology

- Keys including great passwords are Random Numbers (128 bit are great, 256 bit beyond any possibility of guessing)
- How to Build a Backdoor == How to make sure you didn’t.
- Why Hardware, storage device, Crypto with Random Number Generators is ESSENTIAL – You can’t trust people who just write code.

How to Make a Backdoor

simple to understand version

Terms

- K0, K1, K2 Apparently Random Numbers

User key → K0

BackDoor key → K1

Actual Encryption/Decryption key → K2

Software Processing Box (can lie)

Encryptor Box (cannot lie – e.g., public code, verifiable circuit)

Check(K) : checks the hash of a key against a stored hash of the key.

4 Use Cases

1. User access code known, Backdoor known
2. User access code not known, Backdoor known Universally
3. User access code not known, Backdoor known but always different
4. Pseudo Random Generators

XOR Key “Splitting” : key hiding

K0 – User, K1 – Backdoor, K2 – Encryption Key

XOR or $\oplus$ (Binary ADD without a Carry, or ADD mod 2)

Encryption $E(Data) = K2 \oplus Data$

Decryption $Data = K2 \oplus E(Data)$

$K = (K0 \oplus K1) \oplus K2$

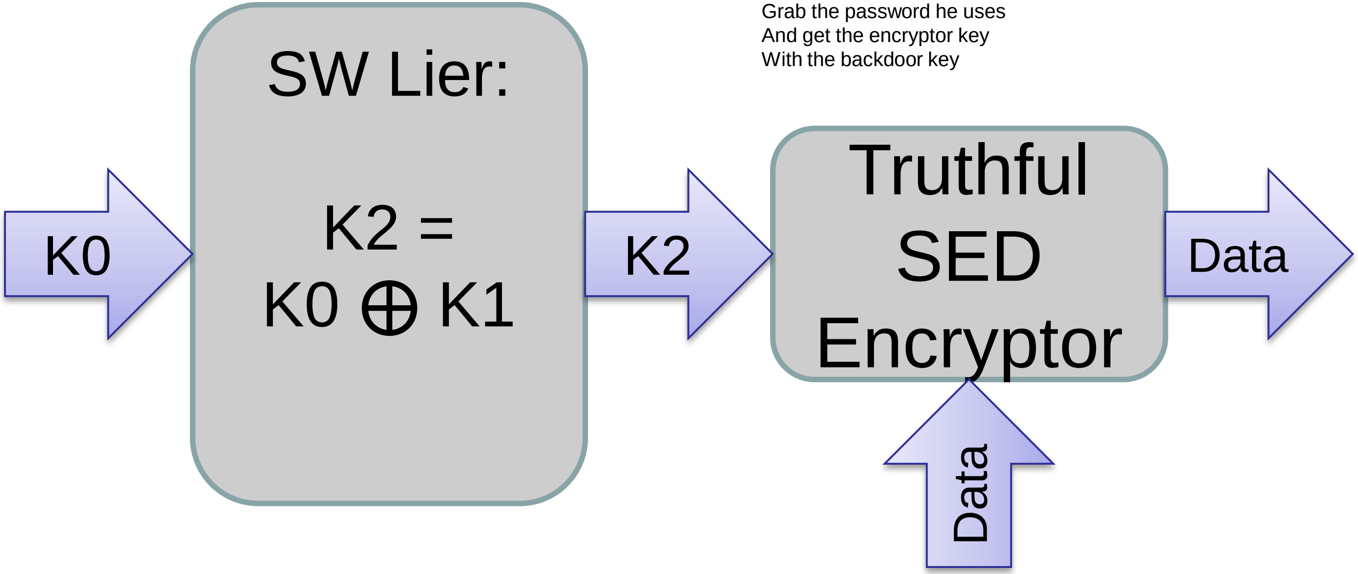
$K = K0 \oplus (K1 \oplus K2)$

$K = K1 \oplus (K0 \oplus K2)$

…

Use Case 1: K0-Known, K1-Known

You think K2 = PDKF(K0)
but it isn't.
Grab the password he uses
And get the encryptor key
With the backdoor key

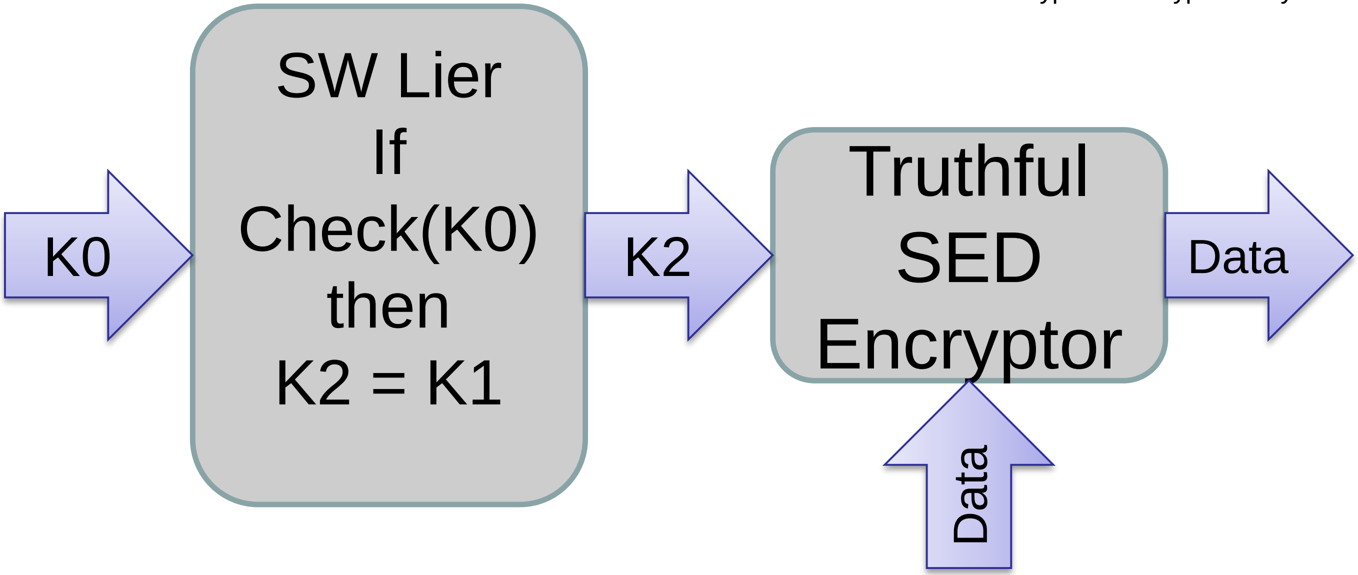


User key → K0
BackDoor key → K1
Actual Encryption/Decryption key → K2

Flash Memory Summit

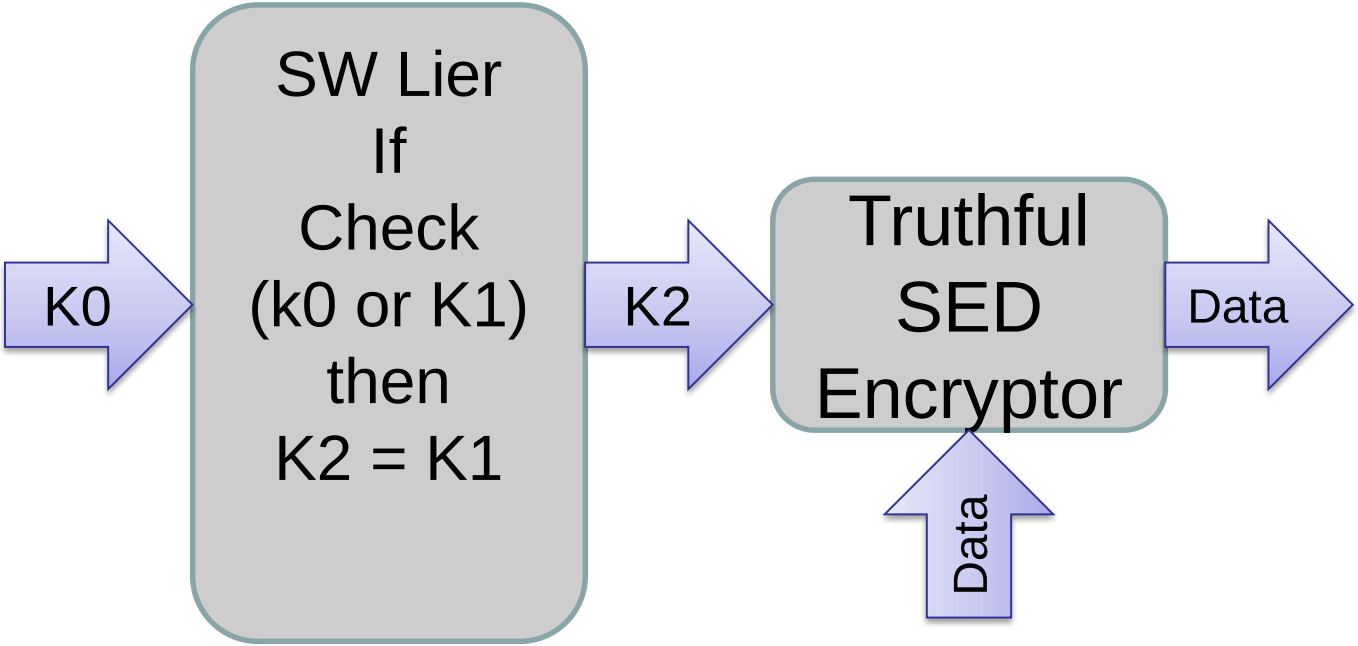
Use Case 2: K0-UnKnown, K1-Universal Backdoor

User key → K0
BackDoor key → K1
Actual Encryption/Decryption key → K2



You think K2 = PDKF(K0)
but it isn’t.
K2 is clear text and is the
Backdoor key

Use Case 1: K0-UnKnown, K1-Local Backdoor

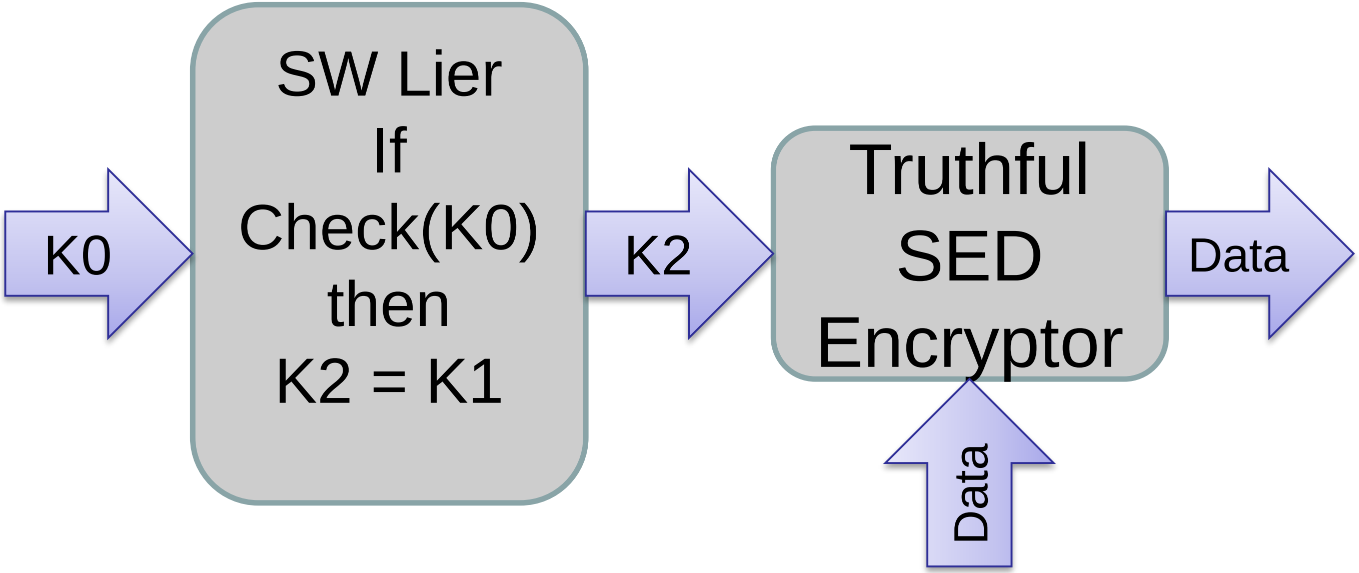


You think K2 = PDKF(K0)
but it isn't.
K2 is clear text and is the
Backdoor key
K2 can always be different

User key → K0
BackDoor key → K1
Actual Encryption/Decryption key → K2

“Accidental Backdoor”
K1 = rnd(0)
K1 = random(0)

User key → K0
BackDoor key → K1
Actual Encryption/Decryption key → K2



You think K2 = PDKF(K0)
but it isn’t.
K2 is clear text and is the
Backdoor key

Apple/FBI Kerfuffle

- Basic Problem – Can’t Crack good Crypto
- Proposed Solution
  - Multiple Passwords/Authorization Credentials (already deployed for TCG Opal and Enterprise) – Admin and User
  - *NEW* ***Licensed Privacy Assurance Providers*** (like Dentist Licenses, Bar Licenses)
    - All Confidentiality has a licensed assurance provider licensed to prevent privacy violations
    - Legal Warrant can get access, data, or key from LPAP
    - Technical Trick: Public Table on (Storage)Device associating encryption access with specific LPAP

“How to Get Your Privacy Back” Book At Conference

- Free Reminder Business Cards (around)
- Signed Copies $40 Cash (ask me)
- Free Store Inspection Copies / Free One Week Inspection Copies for Interoffice Mail in Company or Group