Personal Cloud
Self-Protecting Self-Encrypting Storage Devices

Robert Thibadeau, Ph.D.
Chairman & CEO
Drive Trust Alliance
Bright Plaza, Inc.

&

School of Computer Science
Carnegie Mellon University
Takeaways

• This talk: **Personal** non-volatile storage devices (in PCs, Pads, Phones, Cars, Homes, Businesses, etc etc etc) – NOT Enterprise data-center storage or Tutorial in TCG SEDs, see Willett’s SNIA Tutorial Later Today

• Self-Encrypting Drives **fantastically successful** in technology and availability, but not in Personal adoption (Coughlin Assoc., 2015, see references)

• **Drive Trust Alliance** in association with Tom Coughlin Assoc. has opened-sourced TCG Opal (and Enterprise) code for clients (not devices) to facilitate personal adoption.

• **New Other Open Source** models for Self-Protection, and Personal Monetization of Private Data (TCG Core, PDS, Homomorphic Encryption), from MIT.
Agenda

1. Security and Privacy
2. Security Evolution
3. OPM, etc.
4. SEDs & Object Storage
5. TCG Core SSDs
6. Personal Data System

Copyright © Bright Plaza, Inc., SNIA 2015
The Age of Uncontrolled Data Leakage

- Computer Forensics / Digital Evidence / Corporate Collections – Google, Yahoo, Microsoft, Amazon!
- NSA ANT Catalogue (USA)
- Ransomware (Russia)
- Sony (North Korea)
- OPM, US Office of Personnel Management hack (China)

All Phishing Initiated

- Somebody else gets paid (or worse) for YOUR stuff! Just because you are using the Internet.
Security and Privacy 101

• Security \( \sim \) Access Control

• Security should *SERVE UP Privacy*
  
  – Computer Security \( \sim \) IPAAAA: Integrity, *Privacy*, Authentication, Authorization, Audit, Availability
  
  – Computer Security \( \sim \) CIA: Confidentiality (*Privacy*), Integrity, Availability
• Core + Scripting
  – Core \(\sim\) Data Structures + Basic Operations
  – Scripting \(\sim\) Amazing Use Cases

• Security Providers or SPs: Admin, Locking, Clock, Forensic Logging, Crypto Services, Internal Controls and others.
What is an SED?

Drive Trust Alliance Definition

• The device uses built in hardware encryption circuits to write and read data in and out of NV storage.

• At least one Medium Encryption Key (MEK) is protected by at least one Key Encryption Key (KEK, usually a “password”).

• If one or more KEKs have not decrypted the MEK, the data that the MEK protects is not available.
  — i.e., you cannot reverse engineer a locked SED without a valid KEK input from outside of the self-protecting SED.
Self-Encrypting Storage
Personal Storage Landscape

• ~100% of all SSDs are Opal
  - Due to Data Sanitization Problem for Flash
• ~100% of all Enterprise Storage (SSD, HDD, etc) are TCG Enterprise
  - For fast safe and effective repurposing/disposal
• 100% of all Apple iOS devices are hardware self-encrypting storage for user data if password is set
• ~100% Western Digital USB HDD Drives are SEDs
• Much smaller number of Personal HDDs are Opal or SED
• BUT MS Bitlocker supports “eDrive” = Opal 2.0 Drives of all kinds
• 100% Opal Drive also supports the SATA Security Password as a KEK in addition to TCG Opal Commands.
• NVMe and other Personal storage devices are being handled by the TCG Storage Workgroup right now.
Drive Trust Alliance (DTA)

• Sole purpose to facilitate adoption of Personal SEDs... to the mutual benefit of ...  
  – Device Makers  
  – ISVs  
  – IT  
  – Individual Use

A rising tide lifts all ships

• GPL Open Source for TCG Opal (and Enterprise) Clients (PCs, Pads, Phones, Cars, IoT, etc.), Windows, MAC, Linux

• Educational Services, Open Source Custom Software services
DTA Details

- DTA Web Site: www.drivetrust.com
  Full Service Web Site Opening is Oct 15
Today 9-24-2015
Announcing First Sponsor of DTA!

Copyright © Bright Plaza, Inc., SNIA 2015
SP-SED Rule 1

• When we talk about Cloud things, every Personal Device is actually “in the cloud” so...

Look in the Clouds for What should be in Personal Storage Devices
TCG SED Ranges

• Every partition (range of LBAs) can have a separate KEK and MEK and can be locked and unlocked independently.
• TCG Enterprise Drives use Ranges for VMs
• Bitlocker eDrive – 4 Ranges
• US Gov’t uses DTA Open Source for Creating Resilient PCs using Ranges
• Personal: BYOD and Ransomware Protection Containers!
Personal Data Storage (PDS)

- All data you want to protect can be permitted to be queried under your control
- Classic example: You can ask if you are over 21 but not what your birthday is or how old you are, although that is what is in your PDS
- History: Pentland Started as cloud initiative, failed (distrusted), now Personal device initiative.
- MIT Media Lab, **OpenPDS** open source offered by the Kerberos Consortium at MIT
Homomorphic Encryption

- How can you do computing operations on encrypted data without ever decrypting the data?
- PDS: Ask questions without any possibility of getting at the data.
Homomorphic Encryption

• Idea around since early 80s, no idea how to do it until 1999ish

• General Solution was discovered but it is computationally infeasible (like Bitcoin 😊)

• Only in last few years (2011 or so) breakthrough in speed of computation
  – Divide and conquer (CryptDB, full SQL, from MIT)
  – Practical for SP-SEDs
HE Cloud Model and SP-SED Model

SED pRange
- Private Container
- ONLY ENCRYPTED DATA
- Nothing Plain Text
- Can only accept Authorized Queries (PDS Style)

Personal Client Has Keys

ONLY ENCRYPTED DATA
Nothing Plain Text
Can only accept Authorized Queries (PDS Style)
Solution for Homomorphic Encryption
Examples – Several copies of Data

MULTIPLE ENCRYPTION SCHEMES

SEARCH

Alice

{ ALICE, BOB, EVE }

ENCRIPT

IbAZ6

Tz73b

4zLE9

ENCRIPT

ENCRIPT

ENCRIPT

ENCRIPT

ADDITION

\[ B^2 \times B^3 = B^5 \]

ENCRIPT: RAISE B TO THIS POWER

ENCRIPT: RAISE B TO THIS POWER

DECRIPT: TAKE LOG BASE B

2 + 3 = 5

MULTIPLICATION

\[ 2A \times 3B = 6AB \]

ENCRIPT: MULTIPLY BY A

ENCRIPT: MULTIPLY BY B

DECRIPT: DIVIDE BY AB

2 \times 3 = 6

Copyright © Bright Plaza, Inc., SNIA 2015
SP-SED Rule 2

• Like the Internet cloud: **If anybody can make money off an SP-SED, then people get really smart really fast...**

---

**SP-SEDs Should Charge $$ for Access to the Private Data They Protect**

• **The TCG Core Spec was written with this in mind.** PDS and Homomorphic Encryption provide a conceptual path that could be done with the TCG Core Spec.
Challenges to You

• The TCG Core was designed to provide services that are essentially identical to what Apple did with the App Store but in Self-Protecting Storage devices. It was largely operational by 2002, but storage device Execs didn’t grasp how quickly a revolution could occur (Steve Jobs proved them wrong—several times over).

• No kidding, every Personal Storage Device should let the owner of the device make money off his private data on it. It’s up to you in this audience.
Good References

• TCG Storage Workgroup, Core, Opal, and Enterprise Specifications, [www.trustedcomputinggroup.org](http://www.trustedcomputinggroup.org)
• Drive Trust Alliance, [www.drivetrust.com](http://www.drivetrust.com)
• Personal Data Service (Open PDS), [http://openpds.media.mit.edu/](http://openpds.media.mit.edu/)