Flash Automotive Flash

Robert Thibadeau, Ph.D.
Bright Plaza, Inc. (www.drivetrust.com)
& CMU
rht@drivetrust.com
August 7, 2017

Agenda

(Note. Time Taken will Depend on YOU.
Ask Questions Anytime)

- Problem : No, we knew it was going to happen!
- Automotive Security and Privacy INSIDE Cars
- www.drivetrust.com/autoerase

France 1935 and 1995

- Digital Paper Street Maps of France
- Nobody cared about Privacy….
- Then WWII
- Then they DID!

Flash Memory Summit

Vehicular Privacy and Security

- **Highly Automated Vehicles (HAVs)**
  - Land: Cars, Trucks, Rail, etc.
  - Sea: Boats, Ships, Subs
  - Air: Planes, Airships, Drones
  - Space: Satellites, Space Ships

The same technical revolutions impact IoT

Notably similar: *Smart Homes / Smart Buildings / Smart Campuses, Smart Cities…even IT and Cloud Societies*

Flash Memory Summit

But…let's do cars today

Automated Vehicle received views:

1. Feasible
   - Aircraft Proven Already
   - Watercraft Proven Already
   - Train Proven Already
   - Cars/Trucks believed Proven in Principle
2. Necessary : Relieve Traffic Congestion, Safety
3. Inevitable : ~2020 time frame, ubiquitous

by 2035

Received Vision of the Future

We'll go **from buying cars** to **subscriptions to cars**.

Existential Example: Car/Truck Rental

Existential Changeover Example: Buy Software to Subscribe to Software (Microsoft, Cloud Computing)

But, your subscription says, for example,

- Type of car (Premium, Standard, Compact, Electric, Fuel Cell)
- Rights to call a car to you. (Every morning at 8AM, car is waiting at your house for you unless time changed or request cancelled, Every afternoon at 5PM, car is waiting where your morning pickup took you unless otherwise fetched.)
- Number of other people sharing car (0, 1, 2, 3?)

Results of Automated Vehicle Adoption

- More enjoyable travel experience
- Less congestion on roads (more efficient car utilization)
- Improved safety on roads
- Cost of ownership, one expense, tax advantage for civil result.
- Car Makers make more money!

Sept 2016
NHTSA HAV Guidelines

https://one.nhtsa.gov/nhtsa/av/pdf/Federal_Automated_Vehicles_Policy.pdf
Also with our comments at www.drivetrust.com/

Flash Memory Summit

THIS IS NOT A LEGAL DOCUMENT!

IMHO: It is a great framework out of which you can begin to think about technical and legal issues

- Automotive **Industry accepted nomenclature** and Concepts
- Long life … reasonably **good framework for tracking technology change** for the next 20 Years at least
- Check list for **areas of (safety) concern** as Vehicular Technology learns to speak to the world

And it is short and easy to read! Good for High School Classes

Two Components Splashed Together

- **6 Levels of HAVs** (from nearly no automation to full automation) from SAE
- **10 Areas of Safety Concern** (mapped to different levels) from NHTSA

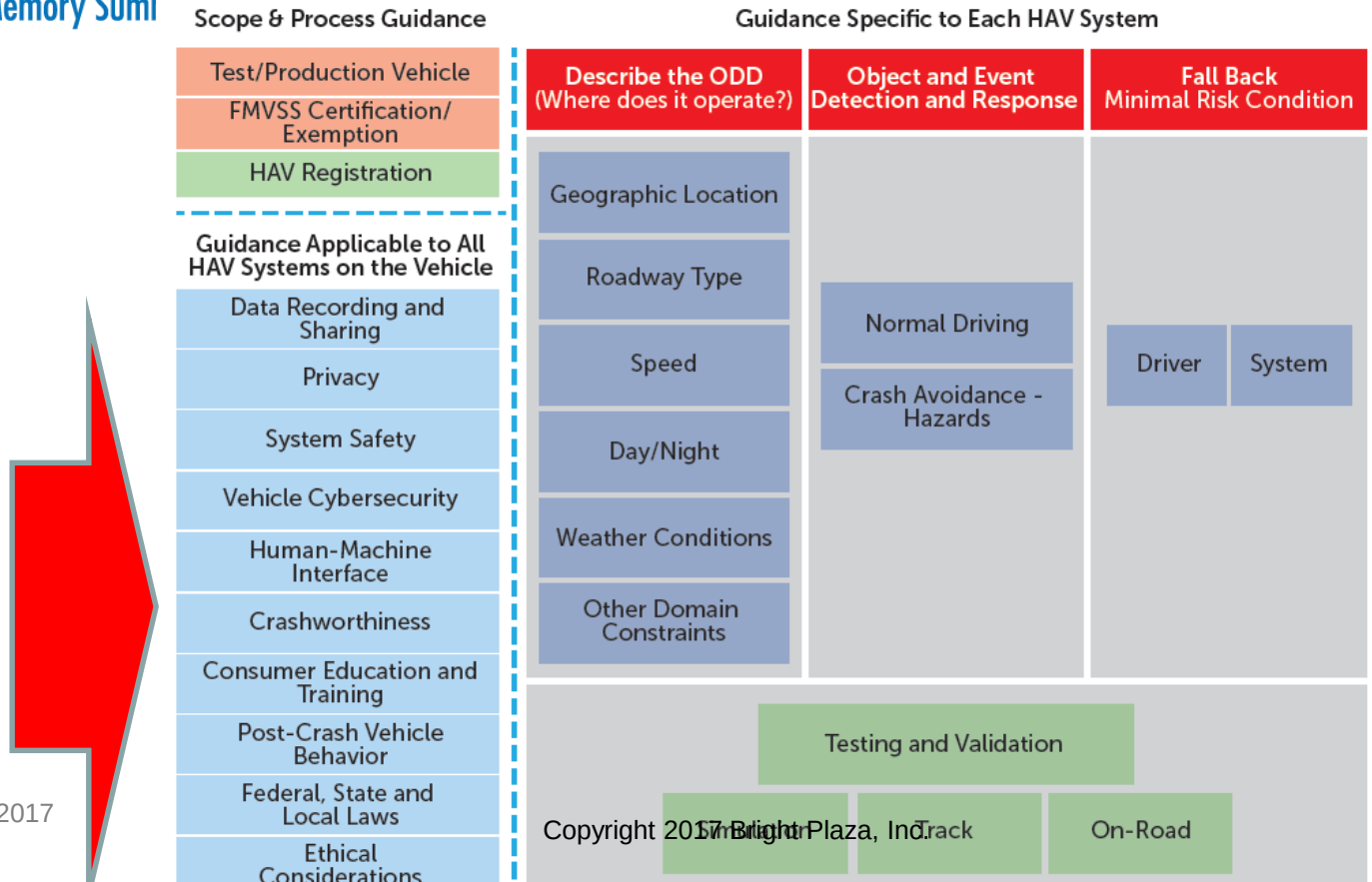
EOS (End of Story)

Comment Period Over on September 2016 Draft

6 HAV Levels

- At SAE Level 0, the human driver does everything;
- At SAE Level 1, an automated system on the vehicle can *sometimes assist* the human driver conduct *some parts of* the driving task;
- At SAE Level 2, an automated system on the vehicle can *actually conduct* some parts of the driving task, while the human continues to monitor the driving environment and performs the rest of the driving task;
- At SAE Level 3, an automated system can both actually conduct some parts of the driving task and monitor the driving environment *in some instances*, but the human driver must be ready to take back control when the automated system requests;
- At SAE Level 4, an automated system can conduct the driving task and monitor the driving environment, and the human need not take back control, but the automated system can operate only in certain environments and under certain conditions; and
- At SAE Level 5, the automated system can perform all driving tasks, under all conditions that a human driver could perform them.

10 Areas of 'Safety' Concern



4 Data Communications Systems

Inside Car

Car to ‘Road’

Car to Car

Car to Cloud

Privacy

Flash Memory Summit

4 Privacy Invations

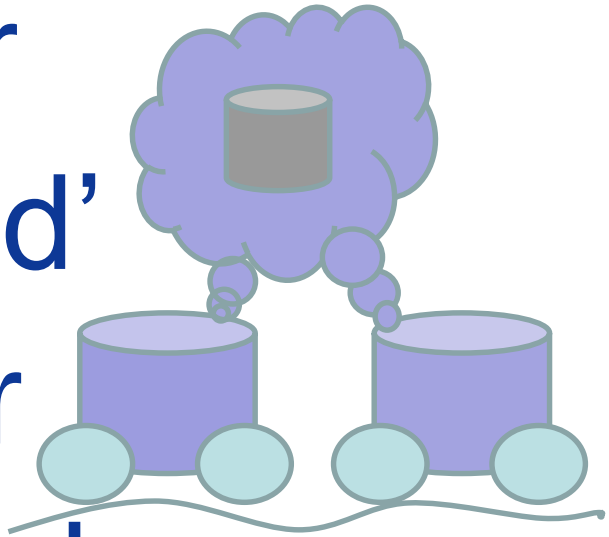
“Invation” = Invasion Invitations

Inside Car

Car to ‘Road’

Car to Car

Car to Cloud



Where's the Data? Inside CAR

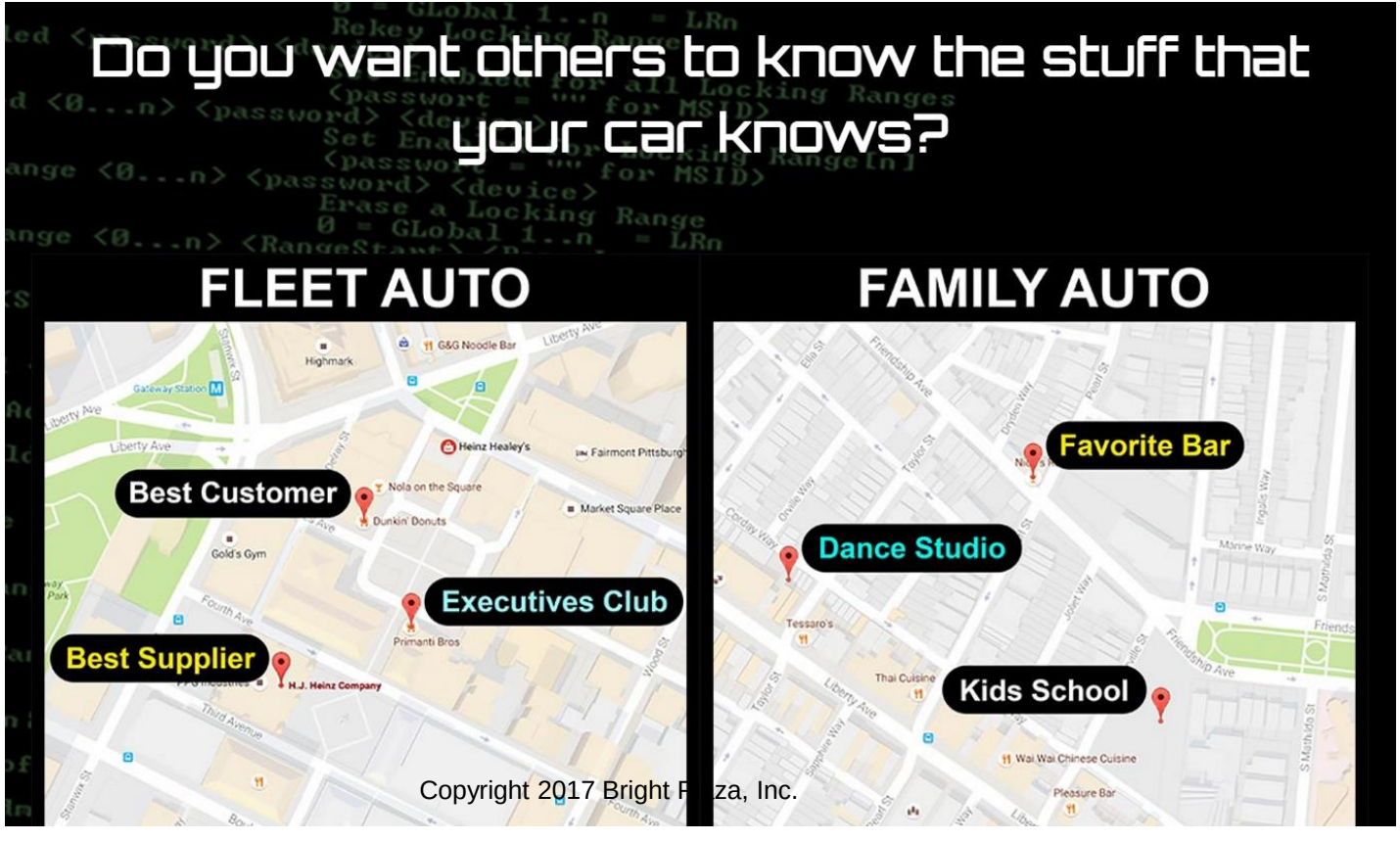
ADAS (Advanced Driver Assist System)
- GPS (Locations)
- Infotainment
- Human Interactions
- Automated Vehicle Systems (e.g., Cars ahead, Behind, Beside, MPG, EV History)
- Video – Audio Recording

Trackers (Insurance)
Engine (Mileage, Wear, Power)
Black Box (Law, Accidents, Insurance)
Smart Sensors (Raindrop, Predictive Road Slickness)
Network Logs

-  = Machine Learning / AI

GPS Memory…

from www.drivetrust.com/autoerase



Flash Memory Summit

Other Family Use Cases

- HAV 3+ that can Listen to your voice can listen to passenger voices, so must recognize who is talking (your 13 year old screaming “STOP!”)
- Do you really want the person who buys your car to be able to find out what happened in the back seat, and who it happened with, for the last 10 years?

What's in the Cloud
WOW!

- ***All Cars today*** have Cryptographic Certificates (X.509) that **ID the car** and **ID the manufacturer** (software updates).
- ***Plaintext Data in the Cloud*** needs to be enough to provide network applications, with real-time and historical data:
  - Advertisements (upsells, like Ludicrous Mode)
  - App Stores (upsells)
  - Manufacturer Monitoring (to improve your experience…)
  - Legal Records (Insurance Proof)
- **Car Restore Functionality**
  - New Car gets old car's brains about you, your family or you, your company

Flash Memory Summit

Thibadeau's HAV Laws

- A Car is a **Supersized Smart Phone that carries you**, instead of you carrying it.
  - HAV Privacy is vastly more an issue than a lawyer writing a privacy policy. (See www.drivetrust.com Privacy comments on NTSHA HAV Guidelines 2016)
- When **cars can listen and understand** (people, roads, cars, and the cloud), ***and then act***, **privacy sensitive information becomes supersized too**.

Family and Corporation Privacy Technology

- **Your car 'key' should unlock your user data and all the current passenger user data.** Like the iPhone – Hardware Encryption Locked/Unlocked
- **Your car web site should let you sell or repurpose your car by cryptographically erasing** all current user/passenger knowledge.
- **In a car Crash, even removing the flash memory and trying to read it won't work.**
- **Your car web site should let you download your last car's knowledge** from your old car while preserving the privacy of that knowledge.

Privacy of this sort is already coming from the car buyers!

- June 28, FTC/NHTSA Privacy Workshop
- DTA AutoErase gives exactly **the privacy people want**

PROVEN by the National Automobile Dealer Association (NADA): YouTube Video https://youtu.be/lelTwCSJBaM, June 28,2017, NHTSA/FTC Privacy Workshop, Washington DC.

DTA Comments on NHTSA Privacy Policy

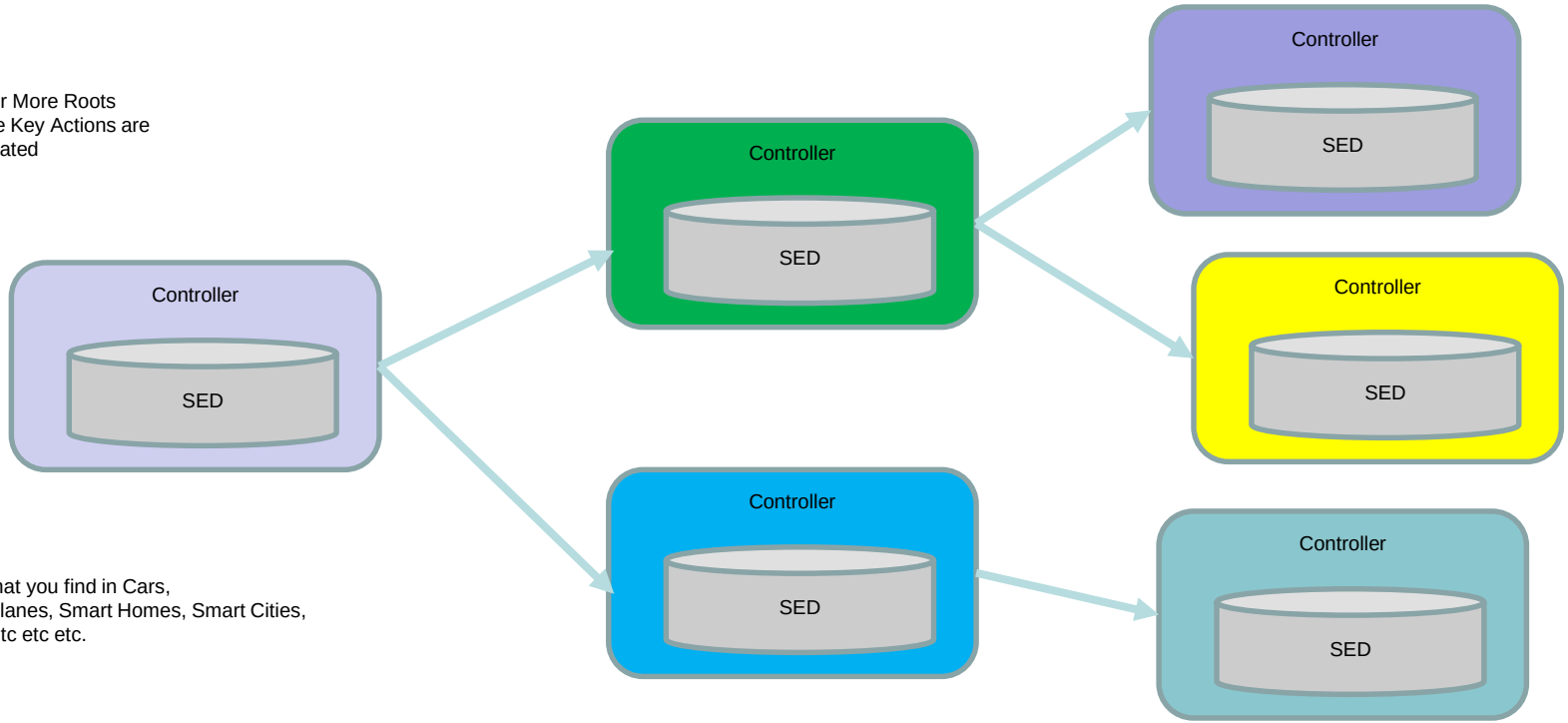
Repurposing a Vehicle – When a vehicle is repurposed, all individual or organizational data about owners, drivers and passengers should be cryptographically erased, like the iPhone.

Multiple Drivers – In a vehicle with multiple drivers, only the personal information of the person driving, and the people riding, should have their data cryptographically unlocked for reading and writing, like the iPhone.

Central Management Privacy Assurance – A remote, cloud privacy manager is essential This way the HAV can be proven to have been protected even if it is stolen or otherwise lost, like the iPhone.

Car compute storage is a Supply Chain thing (try “mess”)

One or More Roots
Where Key Actions are
Originated



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

Supply Chain Assurance Proposed Requirement

- Self-Encrypting Drives (Non-Volatile Storage Devices) should be required for Supply Chain Assurance.
  - Industry Standard Interface to Device Required (Trusted Computing Group, Storage Workgroup, Opal, Enterprise, or other approved Standard.
  - Encryption in Industry Standard Self-Protecting Hardware simplifies assurance immensely
  - Allows law enforcement a known device where privacy sensitive data is protected
  - Already all Smart phones…but proprietary interfaces

Security 101 in One Sentence

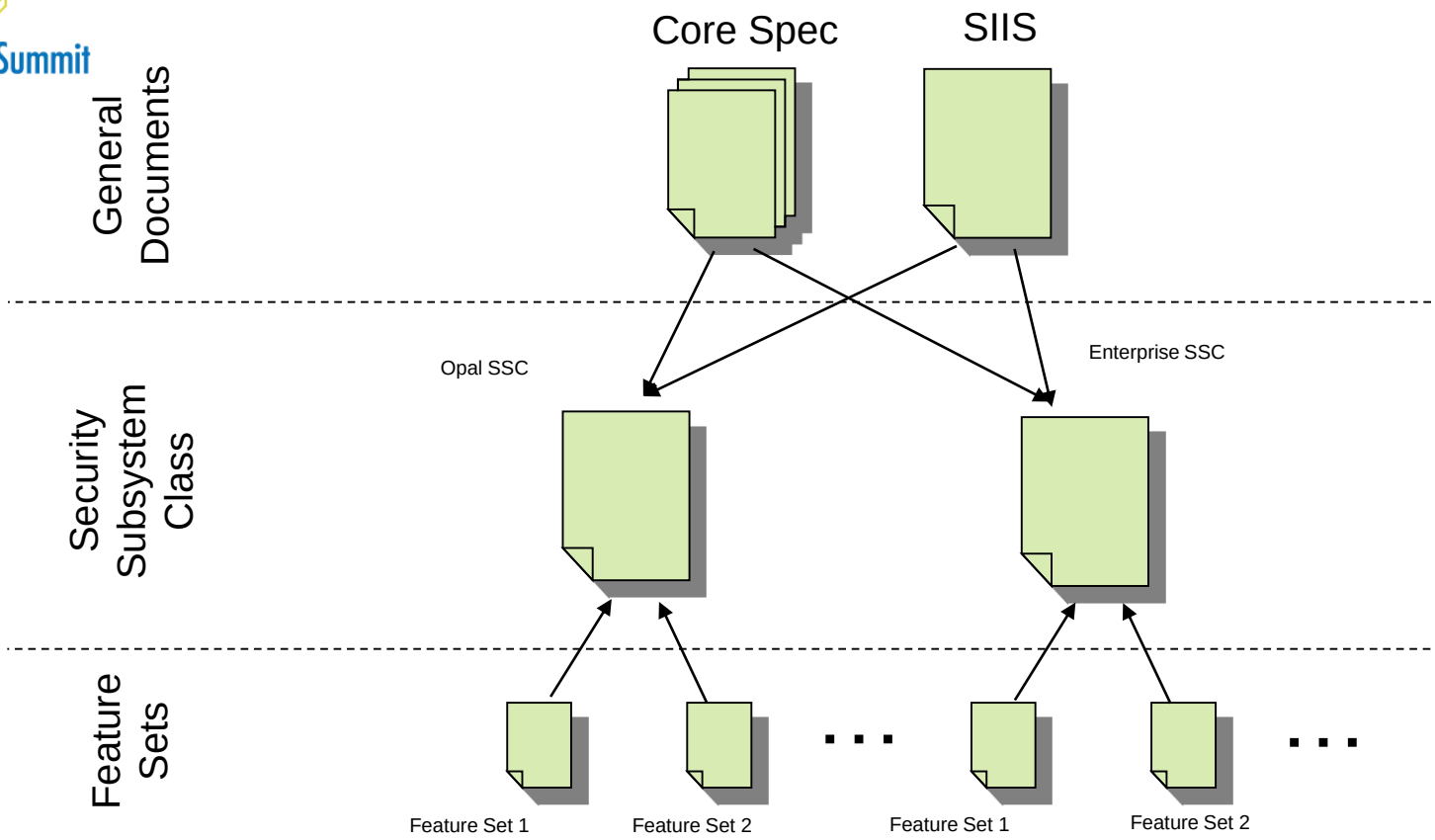
- Computer Security is all about *Access Control*

DriveTrust.com
Please Sign Up with a Login

- Self-Encrypting Drives
  - 1 Billion People a Day Use these, and Don’t know it. LG makes these (in LG Android phones).
- Definition
  - MEK : One or More Media Encryption Key
  - KEK : One or More Key Encryption Keys (to hide the MEK and authorize Encryption/Decryption)
- Use Cases

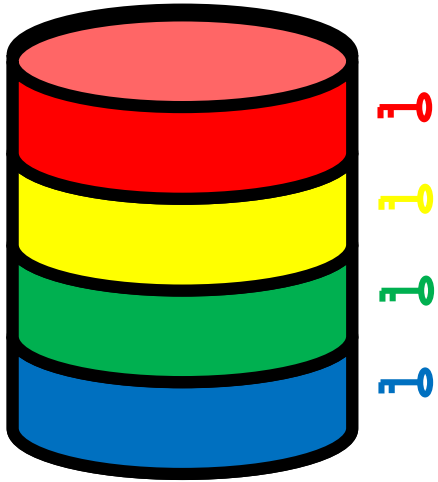
Trusted Computing Group
SWG Documents Overview
www.trustedcomputinggroup.org

- **Core Specification**
  - Overall architecture for the storage work group specification. It is not a device specification per se, but rather a description of the underlying constructs to be used in the device specifications.
- **Storage Interface Interactions Specification (SIIS)**
  - Describes the interactions of the TCG SWG specification with the underlying storage interface protocols, such as ATA, SCSI, USB, etc.
- **Security Subsystem Class (SSC)**
  - These are device specifications. They consist primarily of subsets of the functionality contained in the Core Spec.
  - Currently we have **Opal SSC** and Enterprise SSC.
- **Feature Sets**
  - These are documents that define extensions to the basic functionality of SSCs.
    - These were created to allow for simple extensions to be added to the SSC at a faster pace. Additionally, it allows for features that only appeal to a subset of the market to be standardized.


Core Spec
SIIS
General Documents
Opal SSC
Enterprise SSC
Security Subsystem Class
Feature Sets
Feature Set 1
Feature Set 2
Feature Set 1
Feature Set 2

The Locking Table

- The **Locking Table** controls the locking and encryption of the SED's media in both Enterprise SSC and Opal SSC
- The entire host-addressable space can be locked and encrypted with a single key (Full Disc Encryption - FDE), or…
- The media can be divided into multiple Logical Block Address (LBA) ranges, each encrypted with its own key (Full Volume Encryption – FVE)



Enterprise's Access Control Model

The Locking SP in Enterprise has two types of Authorities:

BandMasters

- Each BandMaster has complete control over exactly one LBA Range (password for unlocking, start/end LBA, locking configuration)

EraseMaster

- The EraseMaster authority can be used to crypto-erase any LBA Range and restore that range to its initial default configuration

In Enterprise's Locking SP, all access control settings are **fixed** and **static**

SED Use in Cloud

- 100% of all of Google uses SEDs
- SEDs are married to the storage racks
  - No user interaction required
  - Data cannot escape the data center

SED Use in Automotive

- SEDs are married to the cars and trucks
  - No user interaction required
  - Data cannot escape the car even in a CRASH

A Car is a **Supersized Smart Phone that carries you**, instead of you carrying it.

...and all that implies...

Thank You!

rht@drivetrust.com/autoerase