Storage as an IoT Device Roundtable

Walt Hubis, CISSP
Tom Coughlin
Participants

**Monty A. Forehand**  
Product Security Officer and Technologist  
Seagate Technology

**Robert Thibadeau**  
Chairman and CEO  
Drive Trust Alliance

**Michael Willett**  
VP Marketing  
Drive Trust Alliance

**Walt Hubis, CISSP**  
Hubis Technical Associates
The Fog and the Cloud
Source: Fog Computing: Bringing Cloud Capabilities Down to Earth, Cisco Blog, August 2015

Fog Computing...
a system-level architecture
to extend
Compute
Network
Storage
capability of cloud to the edge of the IoT network

© 2016 Coughlin Associates
Storage devices for IoT

© Coughlin Associates, 2016
Storage Devices and Security

- Primarily Direct Attach
  - FC/FCoE – limited connectivity
  - 1 to 100 devices
- Block Oriented
- Client Systems and Arrays
  - Dedicated controllers
- Security
  - Data encryption - at rest
    - Secure Erase
  - Authentication - symmetric
IoT Devices

- Primarily network attach
  - Unlimited connectivity
  - 1 to $10^6$ devices – or more!
- Stream, KV pair oriented
- Huge number of architectures
- Security
  - Encryption – at rest and in flight
  - Authentication - PKI
  - Non-repudiation
  - Process Isolation
New Interface Architectures

- NVMe over fabric
  - iWARP and RDMA
  - Complex security

- Kinetic drives
  - Ethernet Interface
  - Key-Value
  - Transition to fully networked drives
At the Open Compute Summit WDLabs was showing an 8.0 TB Helium Sealed HDD with 1 GB DRAM and an ARM-based Microprocessor capable of general computing tasks and Ethernet connectivity that was called a Micro-Server.
What is a Self-Encrypting Drive (SED)?

Trusted Computing Group
SED Management Interface

AES Hardware Circuitry
- Encrypt Everything Written
- Decrypt Everythong Read

Authentication Key
Encryption Key
~100% of all new, office and enterprise quality, Solid State Drives (SSDs) are TCG Opal SEDs
Due to the Data Sanitization Problem for Flash (Traditional erasure techniques fail)

~100% of all Enterprise Storage (SSD, HDD, etc) are TCG Enterprise SEDs
eg, All of Google’s Storage of your data and data they have on you
Fast, safe, and effective cryptographic repurposing and disposal of storage devices; protect against data leakage

100% of all Apple iOS devices are hardware SEDs for user data
when iPhone or iPad password is set, that is the KEK (Key Encrypting Key)

~100% Western Digital USB Hard Disk Drives (HDDs) are SEDs
In case you lose your USB storage device

~100% of ALL Office-Class Printers and Copiers in the world use SEDs
To protect against theft of what people have printed/copied

>>> Much smaller number of Personal HDDs are TCG Opal or SED
But Microsoft Bitlocker supports “eDrive” which requires Opal 2.0 SEDs

100% TCG Opal Drives also support the SATA Security Password (Hard Disk Password)
No Software needed: already supported by BIOS/UEFI setup on nearly every laptop and PC in the world

Note: Newest fastest solid state drives, such as NVMe, are already commercially available as TCG SEDs.
Standardization details are currently being handled by the TCG Storage Workgroup.
“Perfect Storm”

- Business requirements
- Technical definition (TCG)
- Standardization (TCG, NIST, ISO)
- Product proliferation (multi-vendor)
- Legislative mandates (breach notification)
- Promotion (TCG, DTA)
- Best practices (SNIA)
A BILLION PEOPLE A DAY USE SELF-ENCRYPTING DRIVE TECHNOLOGY

There Should Be No Encryption Backdoors, Only Front Doors

"In two sentences: iPhones and iPads have always had front door central encryption management using international standards. The government needs to learn how to legally employ the solutions that companies have employed for over a decade."

Drive Trust Alliance on Apple/FBI Security Debate

Copyright Robert Thibadeau
rht@brightplaza.com
IoT and Self-Encrypting Drives

USB SED – MAC – iPhone

iPhone unlock-lock of TCG Opal USB drive on MAC
-- send encrypted drive to destination
-- unlock when you confirm the destination actually has it

iPhone location proximity
-- unlock TCG Opal USB drive using iPhone as the authentication token

Automotive SEDs
Automotive / Vehicular (land, sea, air, space)
-- Erase car / fleet vehicle of Privacy Sensitive Data when vehicle is repurposed

Privacy Sensitive Data 😊

Apple/FBI Kerfuffle
-- Encryption Central Management
Every Product is a Security Product

Monty A. Forehand
Product Security Officer & Technologist
Seagate Technology
Every Product is a Security Product

- The Things are coming in masses and most have vulnerabilities
- The Things connect to Things that connect to Things that store the data
- All the things are potential hacks to get to the data – the real value

* Ernst & Young: Global Information Security Survey - 2015
** Ernst & Young: Cybersecurity and the Internet of Things
Secure Products AND Product Security

Secure Products:
Increasing Security Policies, Capability, & Cyber Protections in All Products

Product Security:
Increasing Assurance All Products are Secure, Authentic, and Unaltered

The security of the “thing” is only as secure as the network in which it resides: this includes the people, processes and technologies involved in its development and delivery. *

* Ernst & Young: "Cybersecurity and The Internet of Things"
Organization & Governance

Executives and BoD

Corporate Risk Management

Product Security Office

Mobilization
- Processes
- Suppliers, Factories
- Products
- Customers
- Communications
- Training, Audits

Security Ops Center
- Security Inventory
- Threat Intelligence
- Incident Response
- Monitoring
- Fix Management
- Notifications

Product Security Engineering
- Penetration Test
- Forensics
- Threat Research
- Security Research
- Tech Alignment
- Tools (e.g. SIEM)

Policy, Standards & Certifications
- Product Certs
- Ecosystem Certs
- Clearances
- Standards
- Professional Certs
- Policies

Information Security and eSecurity Office

Physical & People Security Office

Technology, Products, Operations, Business, and Legal

* Ernst & Young: Cybersecurity and the Internet of Things
Broad Based Deployment with Standards

Open - Trusted Technology Provider Standard (O-TTPS)

Comprehensive Open Security Provider Standard:
- Technology Development Section
- Supply Chain Section
- Option for Certification

O-TTPS: Open Trusted Technology Provider Standard

- Supply Chain & 3rd Parties
- Development, Operations, & Products
- Customers & Markets
Thank you!

Download this presentation and others from SNIA’s Data Storage Security Summit at: http://www.snia.org/dss-summit