DATA STORAGE SECURITY SUMMIT

01010011 01001110 01001001 01000001

SEPTEMBER 22, 2016
SANTA CLARA, CA

SNIA

Panel Discussion:

Data Security Versus Recovery (think: Apple/FBI): Is There a Win/Win?

Moderator:

Michael Willett, VP Mktg-Drive Trust Alliance

Panelists:

Chris Bross, CTO – DriveSavers

Thomas Rivera- Sr. Tech. Assoc. – Hitachi

Robert Thibadeau, CEO – Drive Trust Alliance

Session Description

The recent **impasse between Apple and the FBI** made flash security part of the daily news. The FBI wanted to look at the data in a dead terrorist's cell phone and demanded that Apple unlock the encryption. Apple refused.

This **Panel will explore the tension between security and data recovery, search for any win/win trade-offs and alternatives, and hopefully elevate the discourse** above the irrational, often hysterical, level heard today.

Panel Participants

Chairperson/Moderator:

Michael Willett, VP Marketing, Drive Trust Alliance

Panelists:

Chris Bross, Chief Technology Officer, DriveSavers

Thomas Rivera, Senior Technical Associate, Hitachi

Bob Thibadeau, Chairman/CEO, Drive Trust Alliance

Background

- **Strong data security** is essential to private, personal, or business operation and communication
- **Data recovery** is legitimate and proper in selected contexts and under proper protocols
- U.S. Congress is drafting legislation that may not equally recognize the full pro/con;
  possible outcome being draft legislation to **require encryption "back doors"** [1]
  Draft: "Covered entities that receive a court order for information or data for the investigation or prosecution of specified serious crimes must provide it to the government in an intelligible format or provide the technical assistance necessary to do so."
- Is there a **win/win** strategy going forward?
  - **WHY should flash industry care? IoT is flash memory. Security/Recovery balance will affect acceptance.**
  - **History:**
    In the 70s/80s, the U.S. restricted crypto export to 40-bit keys.
    The mistaken belief was that the U.S. was the sole source of good crypto (false).
    U.S. businesses (including IBM) , eventually convinced the govt to lift that restriction.
    Now, we can export strong encryption products, with a one-time review.
  - **Points:**
    >>> Security and Recovery: mutually justified requirements, with proper controls

    >>> Legislation needs to be examined methodically for its impact; even practicality

1: http://www.feinstein.senate.gov/public/index.cfm/press-releases?ID=EA927EA1-E098-4E62-8E61-DF55CBAC1649

Opening Panel Questions…

- **Chris Bross:** **How badly does a phone have to be physically destroyed to be forensically unrecoverable for data?**

- **Thomas Rivera:** **Do you think that “back doors” can be securely designed into cryptographic systems?**

- **Bob Thibadeau:** **Given the tremendous increase in IoT (embedded) systems with memory in the future, how important will strong encryption (eg, self-encrypting storage) be in these scenarios?**

Advanced Mobile Device Forensics

DATA STORAGE SECURITY SUMMIT

Presented by:

Chris Bross

Chief Technology Officer

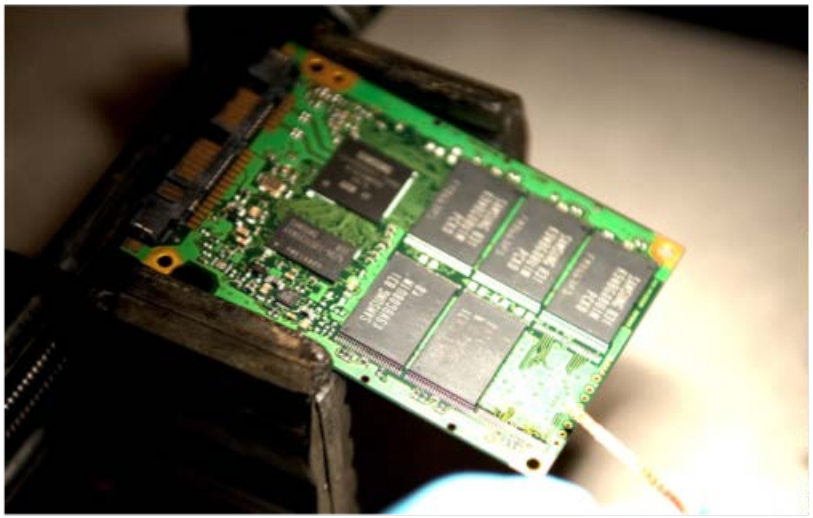
Apple Recent Security News

- iOS Security presentation at BlackHat conference
- New Apple iOS10 with new features just released
- New APFS Apple file system with more encryption

Advanced Forensic Service Labs & Tools

Advanced Data Recovery Lab Techniques

- Jailbreak or Rootkit
- Passcode unlock tools
- JTAG
- ISP
- Serial Port Access
- Chip-off
- NAND Decoding



Bob Thibadeau Charts

FBI/Apple Kerfuffle: Proposed Legislation

Drive Trust Alliance

www.drivetrust.com

www.drivetrust.com

Flash SSDs
iPhones, iPads, Android
All of Google etc.
All Printers

Protecting "USER" Data

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."

READ MORE

Encryption Central Management

Encryption Object ID

Device Owner

Name – Authentication
Create/Delete/Modify Self and Encryption Object, Administrator(s)

Administrator(s)

Name – Authentication
Create/Delete/Modify Self and More than One User
Create/Delete/Modify Media Encryption Key (MEK)

Users

Name – Authentication – Key Encryption Keys (KEK)
Create/Delete/Modify Self

Encryption Object

Data
Verify and Apply User KEKs → Derive and Use MEK

Characteristics of Proposed Legislation

- Extend HPAA/HITECH Regulation that Requires Encryption Central Management for Data at Rest to areas other than Medical Patient Data.

- **Encryption Law**: Owned assets that contain data that is encrypted must have that encryption under central management. The central management must retain sole custody of at least one valid user credential (KEK). Central management can be provided by any entity that is licensed to provide it.

- **Examples**:
  - All US and Local Government Entities must apply the Encryption Law
  - A law generally promotes but does not decree the use of central management for Private Company assets and Family assets

Sample Questions

- Are there alternatives to “back doors” to provide for authorized data recovery?
- What should be the direction, if any, for legislation in this area?
- What does history tell us about government attempts to limit cryptographic security?
- Do we have the known facts straight about the Apple versus FBI confrontation?

Thank you!

www.drivetrust.com

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