Flash Memory Summit

The New TCG "Ruby" Standard

How did we get here, and what should we be doing with it?

Drew Tipton, CISSP

Technical Product Manager, Toshiba Memory America Inc.

Overview

- **Why should customers want this?**
  - Exposure Risk
  - Regulations/Statutes
- **History of TCG**
  - Development of Standards
  - What happened to the Enterprise specification?
  - How is Ruby different?

Customer Exposure?

- The 2018 Verizon Data Breach Investigations Report listed more than 53000 incidents and 2216 confirmed data breaches!

- 42% of data breaches were enterprises, 58% were small businesses

- 28% involved people internal to the company!

- 50% were carried out by "organized criminal groups"

- 12% were "state-affiliated"
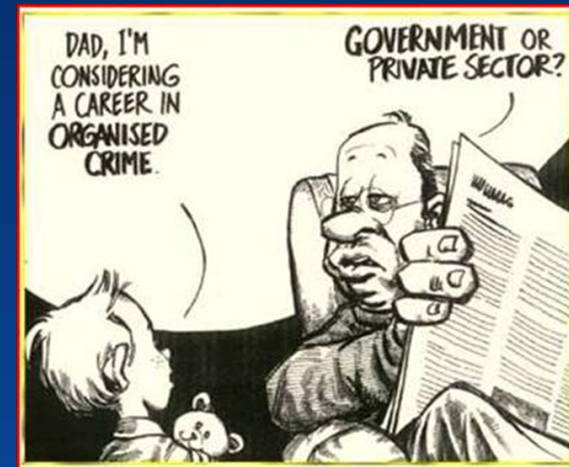
www.papermasters.com/organized-crime.html

Why Encrypt the Drives?

Physical loss of devices or storage media containing data costs approximately $2.8M per occurrence – not counting the losses in reputation, ongoing business, and other intangibles.[1]

One-in-four breaches in the financial sector was due to a lost or stolen device[1]

Drive encryption is now required by law or regulation in many areas[1]:

- Finance (Gramm-Leach-Bliley Act and Federal Financial Institutions Examination Council)
- Healthcare (HIPAA and HITECH (Health Information Technology for Economic and Clinical Health) Acts)
- EU GDPR (General Data Protection Regulation)

American Bar Association now recommends end-to-end data encryption stating that data loss "is not a matter of 'if' but 'when'." [1]

History of TCG

- The "Trusted Computing Group" was founded in 2003
    - 14 companies originally, now more than 75
    - Created "to develop, define, and promote open specifications for trusted computing and security technologies"
    - Not just Self-Encrypting Drives
        - The Trusted Platform Module (TPM)
        - All other security technologies, including Cloud, Networking, Mobile, and others

TCG Specifications

- Enterprise SSC (Security Subsystem Class) published in January 2009
    - Focused on server drives
- Opal SSC originally published in January 2009
    - Primarily targeted at Client/Boot drives
    - Contains requirements that an Enterprise or Datacenter Drive can't or won't meet.
    - Currently on V2.01 Rev 1.00 from August of 2015
    - Derivatives created (Opalite – simplified version and Pyrite – non-encrypted version)

Wait… What about the enterprise?

- But, the Enterprise SSC has been sparingly updated since introduction
  - V1.0 Rev 2 in Dec 2009
  - V1.0 Rev 3 in Jan 2011
  - V1.01 Rev 1 in Aug 2015
  - Primary changes have been editorial in nature and have not followed technology

What happened?

- The industry recognized that the Enterprise drive specification was not keeping up
    - Technology Changes (such as NVMe™)
    - No significant updates since original
- TCG "Ruby" is designed as an updated enterprise and datacenter specification – providing specifications for NVMe and other new technology drives.
- V1.00 Rev 1.19 recently completed public comment phase and should be ratified shortly.

NVMe is a trademark of NVM Express, Inc."

Now that we've got it… now what?

- The case for "Ruby"…
  - As we've mentioned, many customers are now facing requirements to encrypt drives
  - Delivering "Ruby"-complaint drives for customers improves flexibility and offers security improvements over the Enterprise SSC.

Toshiba and Ruby

- Toshiba is a leading member of TCG, and has been actively involved in creating the Ruby standard

- We are currently planning for all of our next-generation enterprise and datacenter drives to be Ruby-compliant

- As we have an extensive history with SEDs and TCG, we can work with you to enable your use model

- As a member of TCG, we can also work to make updates to Ruby to include your use model

Conclusions…?

- TCG Ruby is the logical evolution of TCG specifications for Enterprise and Datacenter use

- A single specification with optional features that covers every use model in the Enterprise and Datacenter

- Customers meet regulatory compliance (GDPR, HIPAA, HITECH, and others) more easily

- Toshiba is a strong proponent of Ruby, and can work with you to deliver your Self-Encrypting Drive use cases!

Please stop by <u>booth #307</u> to see the latest offerings and technology demonstrations from Toshiba Memory America