ICMC 2017

Development of cPPs for Full Disk Encryption

Garry McCracken CISSP, VP Technology
Abstract

Software Full Drive Encryption (FDE) -- Formerly known as Full Disk Encryption -- has been the prime choice for protecting the confidentiality of data at rest (DAR) on laptops for over a decade, but more and more Self-Encrypting Drives (SEDs) are becoming the obvious choice for FDE because of their advantages in performance, transparency and security.

The standard assurance approach for software FDE in the past has been FIPS 140-2 and Common Criteria EAL evaluations by third party accredited labs, but there are difficulties with this approach for software FDE, let alone SEDs.

To address these issues, International Technical Community (iTC) work groups were formed to create collaborative Protection Profiles (cPP) for FDE. This presentation provides an introduction to the set of cPPs for Full Drive Encryption (FDE) and explains how they relate to each other.
About WinMagic

Founded
1997

Headquarters
Toronto
Canada

Customers
84 Countries
8+ Million Active Licenses

- SecureDoc FDE 1998
- NSA RASP 2000
- NIST AES Validation 1 2002
- PBConnex 2010
- TCG OPAL 2009
- CC EAL4+ 2007
- FIPS 140-2 2006
- Lenovo 2010
- HP 2013
- Ivanti 2015
- Cloud 2016

SecureDoc Data Security
Architecture for Endpoint Encryption

Two Components to the Ideal FDE Solution.

**Key Management**
- Component (cPP AA + EM)
  - Authentication: PBConnex + MFA
  - Intelligent Key Management: SecureDoc Enterprise Server
  - Identity Management: AD/LDAP Integration + Sync

**Encryption**
- Component (cPP EE)
  - Hardware-based Crypto: OS-Agnostic Management
  - Native OS-based Crypto: Next-Level Integration
  - ISV Software-based Crypto: Leading Full Disk Encryption

- Trusted Computing Group: OPAL and Enterprise SEDs
- Microsoft: BitLocker
- Apple: FileVault 2
- WinMagic: SecureDoc FDE
Historical Approach for FDE: CC EAL

- Security Target – EAL (Evaluation Assurance Level)
- Unique to each product
- Difficult for customers to compare
- Evaluations time consuming
- Evaluations expensive
collaborative Protection Profiles (cPP) for FDE

- Technical Community (iTC) work groups formed with subject matter experts from the labs, academia, industry and governments
- No EAL level with cPPs
- All the “must have” security functions for FDE
- Practical
- Implementable
- Comparable
- First cPPs for FDE were completed in January 2015
Full Drive Encryption Protection Profiles
Full Drive Encryption cPPs

- cPP EE - Encryption Engine (V2.0 Sept 2016)
- cPP AA - Authorization Acquisition (V2.0 Sept 2016)
- cPP EM - Enterprise Management (in review*)

* The public comment period ends May 26, 2017: https://www.commoncriteriaportal.org/communities/fde.cfm
Describes the requirements for the Encryption Engine piece and details the necessary security requirements and assurance activities for the actual encryption/decryption of the data by the DEK.
Authorization Acquisition

Authorization Factors
- Hardware Key Storage
- Passwords
- External Token

Conditioning/Combining

Encryption Engine

BEV

Describes the requirements for the Authorization Acquisition piece and details the security requirements and assurance activities necessary to interact with a user and result in the availability of sending a Border Encryption Value (BEV) to the Encryption Engine.
NEW! Describes the requirements for the enterprise management (from a server) of the end point consisting of an AA and EE.
# FDE cPP Solutions

<table>
<thead>
<tr>
<th>cPP</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(AA + EM)</td>
<td>Host software provides the interface to a self-encrypting drive and Administrative software that allows enterprise management of the interface.</td>
</tr>
<tr>
<td>(AA + EM) + EE</td>
<td>A enterprise manageable software full drive encryption solution</td>
</tr>
<tr>
<td>AA + EE</td>
<td>A standalone solution without enterprise management (pure software or hybrid)</td>
</tr>
</tbody>
</table>
Applications for cPPs

- Who will use them?
- Who will want them?
Self-Encrypting Drive Manufacturers

- Trusted Computing Group - Opal Certification Program
  - Announced April 12, 2016
  - TCG-certified test suite (Test cases)
  - cPP EE (Security Evaluation)
Independent Software Vendor (ISV)

- Standalone
  - cPP AA + cPP EE SED
  - cPP AA + cPP EE SW
- Enterprise Managed
  - cPP AA + cPP EM for cPP EE SEDs and SW encryption
Endorsements

- cPP EE & cPP AA:
  - NIAP (United States)
  - CCCP (Canada)
  - AISEP (Australia & New Zealand)
  - CESG (United Kingdom)

- cPP EM – None (Not published yet)
Thank You!

For further information, please contact
garry.mccracken@winmagic.com