Overcoming Data Security Challenges in Testing Environments

Jeff Kalibjian
DXC Technology Company
22nd Test Instrumentation Workshop
Tuscany Suites and Casino
Las Vegas, NV
May 16, 2018

DXC.technology

Today’s Discussion

- Data security value proposition in testing (and otherwise!)
- The state of data security
- Important security certification standards
- Best encryption practices and solution selection criteria
- Encryption implementation in testing environments

Data Security Value Proposition in Testing Environments

- Test data has great value and hence is a target for compromise
  - Collecting it costs money
  - End product diagnostic significance
  - National security significance
- Layered security concept
  - Use encryption as yet another security layer
  - If perimeter defenses fail, encrypted data wont be usable (*if encryption paradigm implemented robustly!)*
- Central issues
  - Flexibility of testing environment to support key management and audit operations
  - Security evaluated products and environments
  - Data security approach: disk/file/database/application
  - Hardware/software HSM and Key Managers

Encryption Background: Sep 16, 1999

- Clinton Administration greatly reduces complexity for selling products (world-wide) leveraging strong encryption technologies:
  - Any encryption commodity or software of any key length may be exported under license exception (i.e., without a license), after a technical review, to individuals, commercial firms, and other non-government end users in any country except for the seven state supporters of terrorism.
  - Any retail encryption commodities and software of any key length may be exported under license exception, after a technical review, to any end user in any country, except for the seven state supporters of terrorism.
  - Streamlined post-export reporting will provide government with an understanding of where strong encryption is being exported, while also reflecting industry business models and distribution channels.
- This helped facilitate widespread use of cryptographic technologies to better protect sensitive data----enabling creation of ever more capable data security products

State of Encryption Use

- Over 43% of the companies had an overall encryption strategy; another 44% had deployed a limited strategy
  - Key inflection year: 2011
  - Biggest commercial users: Finance(60%) and healthcare (55%)
  - Biggest threats to organization sensitive data: Employee mistakes (47%), system malfunction (31%), hackers (30%)
  - HSM use 2012/2017: 26%/41%
  - HSM own vs. rent (cloud): 47% vs. 36%
  - HSM use: TLS (43%), Application (41%), Database (37%),
  - % of IT security spending spent on encryption 2014/2017: 15.7%/12.3%
  - Protecting data in the cloud: Encryption before cloud –keys not managed by cloud provider (47%), encryption in cloud-keys managed by cloud provider (38%), encryption in cloud-keys not managed by cloud provider (21%),

From: Ponemon Institute LLC Global Encryption Trends Study April 2018 Sponsored by Thales eSecurity

Motivations and Challenges: Data Security

- **Motivations:**
  - Protect information against identified threats (54%)
  - Protect organization IP (52%)
  - Protect customer PII (50%)
  - Comply with governance mandates (49%)
- Other considerations
  - Demonstrated cost benefit in the per capita cost of a data breach
  - Used to protect sensitive or classified data (Public Sector)
- **Challenges:**
  - Finding the sensitive data! (67%)
  - Initial deployment of solution (44%)
  - Categorizing the data once its identified (34%)
  - Key Management (29%)

From: Ponemon Institute LLC Global Encryption Trends Study April 2018 Sponsored by Thales eSecurity

Product Security Certification Standards: NIST FIPS 140-2

- The NIST Federal Information Processing Standard (FIPS) 140-2 is a hardware specification that is used to evaluate hardware that protects cryptographic keys and performs sensitive cryptographic operations on data at rest and in motion.
  - **Level 1**—No specific hardware physical security is required. Instead, it primarily revolves around the use of approved NIST cryptographic algorithms, for example, Advanced Encryption Standard (AES) and Triple DES
  - **Level 2**—In addition to Level 1 specifications, requirements involve hardware fixtures on the computing platform that can show evidence of tampering. Examples of such fixtures would be pick-resistant locks or covers, coatings, or seals
  - **Level 3**—In addition to Levels 1 and 2 measures, Level 3 includes tamper detection and response circuitry to prevent any cryptographic keying material from being lost to an adversary.
  - **Level 4**—In addition to Levels 1, 2, and 3 measures, Level 4 includes protection against a key compromise from environmental attacks, for example, temperature and voltage changes. Additionally, the system must be completely, formally modelled.

Product Security Certification Standards: ISO Common Criteria

- Common Criteria (CC) is an International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) standard and is recognized internationally by 25 countries.
  - countries have signed a memorandum stating that a Common Criteria evaluation done in one country to a particular Evaluation Assurance Levels (EAL) will be recognized as if that evaluation was done in their country.
- The CC includes specifying a Security Target (ST) document that defines the security functionality and assurance methodologies used to verify that those functionalities are actually achieved. The desired EAL level being pursued dictates the rigor of how those assurances are verified.
  - The ST document also defines the Target of Evaluation (TOE)—which is the product or subset of product for which the methodology will be performed
  - A Protection Profile (PP) is a ST that is written in a general way for a particular product type—for example, firewall products or intrusion prevention products

Product Security Certification Standards: ISO Common Criteria

- The Common Criteria seven Evaluation Assurance Levels are:
  - **EAL1—functionally tested**—Evaluation of TOE includes testing against the specification with respect to the documentation.
  - **EAL2—structurally tested**—Design and test information is evaluated.
  - **EAL3—methodically tested and checked**—There is a thorough evaluation of the TOE.
  - **EAL4 —methodically designed/tested/reviewed**—This is the highest level a “retrofit” can achieve on an existing product line.
  - **EAL5—semi-formally designed and tested**—Rigorous commercial development techniques, planned at design time, are used.
  - **EAL6—semi-formally verified design and tested**—Development techniques are consistent with a TOE that is in a high-threat environment.
  - **EAL7—formally verified design and tested**—Rigorous formal evaluation techniques require TOE to have very tight and well-defined security behaviors

Environment Security Certifications: FedRAMP

- Federal Risk and Authorization Management Program
  - Uniform approach to assessment, authorization, and continuous monitoring for cloud products and services
    - FedRAMP Low: 125 controls
    - FedRAMP Moderate: 325 controls
    - FedRAMP High: 421 controls
- Guiding NIST documents: SP 500-292, SP 800-34 rev. 1, SP 800-37 rev. 1, SP 800-39, SP 800-53 rev. 4, SP 800-53a rev 4, SP 800-60 rev 1 vol. 1, SP 800-60 rev 1 vol 2, SP 800-61 rev 2, SP 800-86, SP 800-92, SP 800-94, SP 800-115, SP 800-122, SP 800-128, FIPS 140-2, FIPS 199, FIPS 200, FIPS 201,

Product Evaluation Recommendations

- It is very desirable to deploy security evaluated products and leverage them in environments adhering to NIST risk management and technical system and network security guidelines

Encryption Element Certification Desirability

Product	FIPS 140-2	Common Criteria
HSM	Must: Level 2 and above	Desirable: EAL 3 or above
Key Manager	Must: Level 2 and above	Desirable: EAL 3 or above
Software Application/Agent	Must: Level 1	Desirable: EAL 3 or above

Environment	Comment
FedRAMP Moderate	Desirable
FedRAMP	Most desirable

Encryption Best Practices

- There are basically four encryption approaches used to protect enterprise server and database data at rest
  - **Disk Encryption**. Encryption employed by the disk itself provides the least amount of data security to the organization. This is because when the disk spins up and the proper authentication/password information is presented, the entire content of the disk is available for decrypted use by the host operating system (OS) and any higher layer application with no further protections on the data except what the operating system might offer.
  - **File Encryption**. Encryption used on files provides a fair amount of data security to the organization employing it. Typically in this mode of operation, there are two types of encryption technology: agents and agentless.
  - **Database Encryption**. Database encryption can almost be considered a subset of application encryption. Basically in database encryption very specific subsets of the data in the database can be encrypted utilizing the native encryption capabilities of the database. This implies that even when the DBA is in the database that data can still be protected from compromise by the DBA.
  - **Application Encryption**. At the application level, very specific subsets of data can be encrypted. This granular control affords data in the enterprise to have the most protection as data is essentially encrypted to the very last moment until it is required by the application.

Encryption Best Practices Implications

- **Exposure of data**
  - Disk Encryption: most exposure. As soon as password input entire disk at risk
  - File Encryption: better exposure risk. Only information in file is at risk when it is decrypted
  - Database Encryption: even better exposure risk. Only specific information in a row or column at risk when decrypted
  - Application Encryption: similar to database. Only specific element of interest is decrypted when required by the application
- **Impact to applications (do they need to be changed to implement encryption)**
  - Disk Encryption: no
  - File Encryption: no
  - Database Encryption: yes
  - Application Encryption: yes

Some Guiding Principles in Solution Selection

- Data protected as soon as possible
- Minimize attack surface of key storage
- Key material separated from encrypted data in storage
- Cross platform integration and policy enforcement
- Minimize amount of time encrypted data items must be unencrypted
- FIPS 140-2 Level 2 evaluation
- Common Criteria evaluation EAL 3+ also desirable
- Facilitate centralized policy definition (e.g. for crypto algorithms, modes, key size, etc.)
- Transparent use for data to be stored in cloud
- Choose solution with long track record and vendor with significant market experience
- Make sure solution can meet all required governance mandates and additional organization requirements
- Should minimize modifications required for application(s) that will use the encryption solution

Some Guiding Principles in Solution Selection (cont.)

- Solution should implement a robust audit framework
- Encryption solution should not preclude testing framework from being established to validate encryption solution functionality
- Solution should manage encryption for both structured and unstructured data
- Solution should not preclude phased deployment
- Solution should interoperate with encryption back-up solutions
- Solution should seamlessly be leveraged in both testing and production environments
- Solution should minimally impact organization business processes
- Should be capable of leveraging a physical HSM and/or key management system

Encryption Implementation in Testing Environments

- Important: Flexible key management/HSM architectures in products that can leverage cloud environments:

Preference I	Application level encryptions with FIPS 140-2 and CC evaluated products
Preference IA	Database level encryption with FIPS 140-2 and CC evaluated products
Preference II	File level encryption with FIPS 140-2 and CC evaluated products
Preference III	Disk level encryption with FIPS 140-2 and CC evaluated products

Promising Transformative Technologies

- **Homomorphic encryption**
  - Data transformation operations can be performed on already encrypted data
  - This yet further reduces the time sensitive data may be exposed when data transformation needs to take place. Essentially when transforming the data, there would be no exposure at all, because the data would not have to be decrypted
- Key concepts
  - Partially homomorphic – limited transformation operations
  - Fully homomorphic – unlimited transformation operations
  - Malleable – alteration of ciphertext without having to see the original unencrypted ciphertext

Wrapping Up

- Application level encryption is the best way to protect data in testing environments
  - Unfortunately, organizations may not be able to implement an application encryption strategy if their commercially procured data analysis tools do not support application encryption.
  - In such circumstances the next most optimal approach would be to proceed deploying a file based encryption solution.
- Unfortunately, a third encryption option, self-encrypting disks, provide little practical data security once the disk has spun up and the password has been entered to decrypt the disk. This is because after the disk has been decrypted, only the host operating system access control protections are available to mediate access to the data on the disk
- All encryption solutions (whether application, file or disk based) should be minimally FIPS 140-2 Level 2 evaluated and preferably also have undergone Common Criteria evaluation at a level of EAL of 3 or higher
- Homomorphic encryption has intriguing implications, most notably not requiring encrypted data to be decrypted to apply data transformation operations. However, there are still challenges with this technology, most notably its malleability.

.

Questions

Thank you

Jeff.Kalibjian@dxc.com