US Executive Order: Strengthening Information Security with Key Encryption for Data at Rest
US Executive Order:
Strengthening Information Security
with Key Encryption for Data at Rest

The webinar will start momentarily.
US Executive Order: Strengthening Information Security with Key Encryption for Data at Rest

Manish Upasani, Product Manager | @manishupasani
Mark Azadpour, Sr. WW Security Workload Product Manager | Computeseecurity@hpe.com
Agenda

- Introduction
- Federal Mandate
- Data Encryption & Key Management
- Q&A
Secure Technology Alliance

The Secure Technology Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption and widespread application of secure solutions. We provide, in a collaborative, member-driven environment, education and information on how smart cards, embedded chip technology, and related hardware and software can be adopted across all markets in the United States.

What We Do

Bring together stakeholders to effectively collaborate on promoting secure solutions technology and addressing industry challenges

- Publish white papers, webinars, workshops, newsletters, position papers and web content
- Create conferences and events that focus on specific markets and technology
- Offer education programs, training and industry certifications
- Provide networking opportunities for professionals to share ideas and knowledge
- Produce strong industry communications through public relations, web resources and social media

Our Focus
- Access Control
- Authentication
- Healthcare
- Identity Management
- Internet of Things
- Mobile
- Payments
- Transportation

Member Benefits
- Certification
- Council Participation
- Education
- Industry Outreach
- Networking
- Technology Trends

Secure Technology Alliance
Speaker – Manish Upasani
Introducing Your Speaker

Product Manager at UTIMACO

- Key Management & HSM Portfolio
- 15+ years industry experience
- 10+ years UTIMACO product experience
- Certifications
  - CISSP
  - TOGAF Certified
  - CTGA UT
  - CCSK-Plus
  - CEH
  - ECSA/LPT
  - ETA-CPP
Speaker – Mark Azadpour
Introducing Your Speaker

Workload Security Product Manager at Hewlett Packard Enterprise

- 20+ years of experience
- Focused on security from user perspective
- Zero trust focused
- CPU assisted security products
- Data at rest, Data in motion & ISV ecosystem execution
- PMP certified
- Security Clearance
Introducing
UTIMACO
We Protect...

- People and digital identities **against terrorism and cyber crime**
- Digital economy and digital transformation processes **against theft, abuse and manipulation**
- Financial transactions, data in motion and IoT devices **against theft and sabotage** – in the cloud and on premise
- Data and ideas
- Investments

With proven, future-proof technology, products and solutions that meet regulation and compliance standards
Introducing HPE
HPE is Your Partner in This Fast Pace Change Environment

HPE ADVANCING THE WAY PEOPLE LIVE AND WORK

BY ENGINEERING EXPERIENCES THAT UNLOCK YOUR FULL POTENTIAL
Growing Risk for Cybersecurity Attacks
Mega Trend: Jaw-Dropping Cyber Attacks and Insider Threats

250,000 MSFT Exchange servers fallen victim to the data breach on Mar 9

Snowden leaked thousands of US classified docs to journalists

Data breach at VW vendor impacted 3.3 million people in North America

A bug in Joe Biden’s campaign app gave anyone access to millions of voter files

CNA Financial paid $40M ransom after cyber attack

37,000 students across 50 schools in London unable to access email

Colonial Pipeline attack led to Biden declaring a state of emergency & oil company paid $5M

McDonald’s affected by a data breach which exposed private information of customers and employees in South Korea and Taiwan

Acer hit by $50M ransomware attack

37,000 students across 50 schools in London unable to access email

Colonial Pipeline attack led to Biden declaring a state of emergency & oil company paid $5M

McDonald’s affected by a data breach which exposed private information of customers and employees in South Korea and Taiwan

Acer hit by $50M ransomware attack
Executive Order
The Latest U.S. Government Reaction
Within 180 days of the date of this order, agencies shall adopt multi-factor authentication and encryption for data at rest and in transit, to the maximum extent consistent with Federal records laws and other applicable laws.
Why Information Security may Impact Every Aspect of Your Business

1. Executive Order
2. Legal Force
3. Government
4. Business
Why Security Affects Every Business

- Bad Press & Social Media
- Regulatory Bodies (e.g. PCI, HIPPA, SOX, FIPS, …)
How Does the Cybersecurity E.O. Affect You?

The Implementation is in Your Organization...
Threats and Risks

Disrupting the Adversary Ecosystem

Educate Users / Use Counter Intelligence
Stop Adversary Access
Find and Remove Adversary
Research
Infiltration
Discovery
Monetization
Exfiltration
Capturing
Plan to Mitigate Damage
Secure the Important Asset

Secure Technology Alliance

Hewlett Packard Enterprise

utimaco
Disrupting the Adversary Ecosystem

Threats and Risks

Disrupting the Adversary Ecosystem

Educate Users / Use Counter Intelligence

Stop Adversary Access

Find and Remove Adversary

Plan to Mitigate Damage

Secure the Important Assets

Hewlett Packard Enterprise

World’s most secure industry-standard server portfolio provides an enhanced holistic, 360-degree view to security: Begins in manufacturing supply chain & concludes with a safeguarded, end-of-life decommissioning

Secure encryption keys with consistent policy and controls – at rest, in use, and in motion

Root of Trust for your Enterprise

Trusted Security Partner

Secure Technology Alliance
Is Cryptography the Answer to all Cybersecurity Threats?
Data and Information Being Threatened at Different Levels

Typical Data at Rest Ecosystem

- Files & Folders
- Databases
- Operating Systems
- Virtual Storage
- Physical Storage

Is Cryptography the Answer to all Cybersecurity Threats?
Is Cryptography the Answer to all Cybersecurity Threats?
Data and Information Being Threatened at Different Levels

Typical Data at Rest Ecosystem

A Bare Metal Server...

- Can be stolen by employees or intruders
- Can fall into the wrong hands
- What happens if the data is not properly migrated?
- Is it safe against physical attacks?

Physical Storage
Is Cryptography the Answer to all Cybersecurity Threats?
Data and Information Being Threatened at Different Levels

Typical Data at Rest Ecosystem

- Can be stolen by the VMWare admin
- Can be compromised by hypervisor level attacks
- Is it safe against Ransomware attacks?

Virtual Storage
Physical Storage
Is Cryptography the Answer to all Cybersecurity Threats?

Data and Information Being Threatened at Different Levels

The Operating System...

- Can be attacked at the application level
- What happens if the OS Admin is rogue
- Is it safe against logical attacks?

Typical Data at Rest Ecosystem

Operating Systems

Virtual Storage

Physical Storage
Is Cryptography the Answer to all Cybersecurity Threats?
Data and Information Being Threatened at Different Levels

Typical Data at Rest Ecosystem

- Databases
- Operating Systems
- Virtual Storage
- Physical Storage

The Database...
- SQL injection
- Disgruntled database admin
- Unsecured database dump
Is Cryptography the Answer to all Cybersecurity Threats?
Data and Information Being Threatened at Different Levels

Typical Data at Rest Ecosystem

- Files & Folders
- Databases
- Operating Systems
- Virtual Storage
- Physical Storage

Files and Folders...
- What if the admin misuse the files?
- Are the email files secured properly?
- Are they secured against ransomware?
- Are the files and folders backed up?
Why Hardware-Based Security is Critical for Enterprise

Security is Only as Strong as the Layer Below the Point of Attack

- Ransomware, man in the middle, user error, worms
- Malware, data theft, theft of hard drives
- DOS, DDOS, user error, worms
- Ransomware, malicious insider, malware, phishing, SQL injection, theft, trojan horse, user error, water-holing, zero day attack

Why Hardware-Based Security is Critical for Enterprise

Establish a chain of trust up the boot stack, all the way to the application

- HPE Protection
- Secure Supply Chain
- Applications
- Platform
- Operating System
- Processor Attestation
- Silicon Root of Trust
- BIOS/Firmware
- TPM, SED Drives, Storage Controllers

- Processor authenticates itself using cryptographic attestation
- Continual attestation during runtime
- Boot with an immutable (unchangeable) source in silicon
- Firmware rollback protection

- Counterfeit materials, malware, tampering, data theft
- Root kit, boot kit, booting into alternate OS, phlashing
- Malware, firmware, unvalidated firmware updates, theft of data (w/EPYC)

Attack types
Is Cryptography the Answer to all Cybersecurity Threats?

Now encryption is an easy solution to protect confidential data

- Well-proven **defense against breaches** – highly effective, often mandated as a **must-have investment**

- **Simple** to implement: AES keys, standardized, now embedded, **but...**
Key management is hard if not done right!

- **Maintain centralized controls:**
  Lose access to keys = lose access to the data

- **Social engineering policy:**
  Who manages the keys?
  What authorization is required for applications?

- **Audit and prove of compliance:**
  Regulatory mandates expect evidence of protection
Key Manager
What to Look for...

Secure
- Meet NIST standards, validated to FIPS 140-2 Level 2, Common Criteria
- Encrypted keys in transit and at rest
- Certificate-based authentication and built-in CA

Manageable
- Configuration and keys replicated across cluster automatically
- Hands-off administration, automated backups and audit logging
- Deploy as a Virtual Machine

Available
- Active-Active cluster
- Automatic key replication, client failover
- Highly redundant hardware

Interoperable
- Support for OASIS KMIP (Key Management Interoperability Protocol)
- No vendor lock-in
- Custom integrations using SDK

Scalable
- Geographically separated clusters across datacenters
- Support for thousands of clients, and millions of keys

Interoperable KMIP
Best in Class Integrations
Secure FIPS 140-2 L2 CC EAL 2+
Key Manager Integrations
Data-at-Rest Key Management

Management Console

Authentication and Authorization Sources
- Active Directory

SIEM
Management Console

Business Applications, Data Stores and Processes

- Servers
  - HPE ProLiant
- Disk and Tape
  - 3PAR, X7, StoreEver, StoreOnce
- Web / Cloud
  - HPE Hybrid / OpenStack
- Big Data
  - Vertica, Zettaset
- HPE Nonstop Applications and Databases
- 3rd Party Applications
- Mainframe Applications and Databases
- Enterprise Applications
- 3rd Party SaaS Gateways
- Production Databases

HPE Portfolio
KMIP Compliant Partner Ecosystem

HPE Portfolio
KMIP Compliant Partner Ecosystem
Securing the Keys at Different Levels

Securing the Access to Data and Information at Different Levels

Data at Rest in HPE & External Ecosystem

- Files & Folders
- Databases
- Operating Systems
- Virtual Storage
- Physical Storage

Centralized Secure Key Manager
Securing Keys for Data at Rest
Securing the Keys at Different Levels
Securing the Access to Data and Information at Different Levels

Data at Rest Ecosystem
- Files & Folders
- Databases
- Operating Systems
- Virtual Storage
- Physical Storage

Centralized Secure Key Manager
Securing Keys for Data at Rest

Backup Solution
- Tape Storage Solution
- Data Protection Systems
Security Protection and Security by Design

1. Trusted Supply Chain
   Uncompromised and trusted supply chain, acts as your first line of defense

2. Automated Security
   Defend against malicious code with early detection and automated recovery

3. End of Life
   Retire old infrastructure with simple, safeguard removal of passwords, configuration settings, and data
### DNA of an Ideal Key Management System

<table>
<thead>
<tr>
<th>Centralized Key Management</th>
<th>Key Availability</th>
<th>Scalability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Streamline key management <strong>processes</strong>, reduce costs and the risk of human errors.</td>
<td>Multiple paths to request keys as a failover mechanism should a failure occur – <strong>Resiliency</strong> is vital.</td>
<td>Expect the number of keys in use and in archive to grow to millions. <strong>Scalability</strong> is key!</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Disaster Recovery</th>
<th>Ease of Use</th>
<th>Raising the Bar</th>
</tr>
</thead>
<tbody>
<tr>
<td>Be able to recover the key management system in the event of a complete failure is critical.</td>
<td>The ability to <strong>group keys, assign roles and policies to these groups</strong> is the only way to manage the high volume of keys.</td>
<td><strong>HSM</strong> as the preferred method of performing localized key management tasks, protecting the keys and the core operating functions</td>
</tr>
</tbody>
</table>

Deleting a key renders data useless or as good as deleted
White paper: Strengthening Information Security with Strong Key Management

Brochure: Enhanced Protection for Data at Rest
https://bit.ly/3CQ7fS1

Contact us
hsm@utimaco.com
computeSecurity@hpe.com
Q & A

Q: What are the benefits of using the utimaco software?

A: The benefits include:

- Out-of-the-box software
- Secure
- Easy to deploy and manage
- Unprecedented capacity
- Different security levels
- Single pane of glass
- Streamlining data and processes
- Portfolio Support

For more information, visit:


Free 60 Days Trial
Thank you for your attention!