HP Atalla + HP Security Voltage

Data-Centric Security & Encryption Solutions
Brendan Rizzo / London, 24 June 2015
The waves of data are here...

**Data yesterday:**
- Known volumes
- Well defined
- Easy to control
- *(Thought to be) well-managed*

**Data in today’s enterprise:**
- Runaway volume and velocity growth
- Ill-defined variety
- Hard to control
- *(Almost) unmanageable*
HP Atalla & HP Security Voltage
Driving leadership in data-centric security
and protecting the world’s largest brands
HP Atalla – Data Security & Encryption Solutions

- **HP Atalla Network Security Processor (NSP)**
  Also known as Atalla Payments HSM – leading product in payments security

- **HP Enterprise Secure Key Manager (ESKM)**
  Creates, serves, and protects encryption keys for enterprises

- **HP Cloud Access Security protection platform**
  Adallom - Cloud Access Security Broker

- **HP Atalla Information Protection and Control (IPC)**
  Lifecycle security classification and protection for unstructured sensitive enterprise data

- **HP SecureMail**
  Encryption & key management for email

- **HP SecureData**
  Encryption & tokenization of structured data
HP Atalla

160+ million US card transactions protected daily
Leading payments HSM vendor serving Americas, APJ and EMEA card payments markets
70% of US card transactions touch HP Atalla

Hardcore
50 patents
Creative engineers delivering security inventions and driving HP’s security thinking

Rock-solid security
FIPS 140-2 validated Level 2 and level 3+
Our Enterprise Secure Key Managers (ESKM) and Network Security Processors (NSP) are built for the highest standards

Trusted name
$ Trillions
Atalla secures 1 in 3 card transactions, HP also processes billions of card transactions annually

...invented the security we often take for granted
Protecting data-at-rest
HP Enterprise Secure Key Manager 4.0

Video Introduction
HP Enterprise Secure Key Manager (ESKM) solves the problem

• Manage business-critical encryption keys

• Value Proposition
  o Manages encryption keys at enterprise scale
  o Separates keys from the data
  o Handles key backup, rotation, audit logging, etc.

• Quick Facts
  o Easily Deployed: 1U hardware appliance
  o Highly Available: deployed in clusters of 2-8 nodes
  o Scales for Modern Datacenters: 25K clients, 2 million keys
  o Highly Secure: FIPS 140-2 Level 2 validated appliance
  o Interoperable: supports industry-standard interface (KMIP)

http://www.snia.org/forums/SSIF/kmip/results
https://wiki.oasis-open.org/kmip/KnownKMIPImplementations
http://www.snia.org/forums/SSIF/kmip/results
ESKM 4.0 – Unified Key Management for the Enterprise

NonStop Volume Level Encryption

StoreEver ESL G3

BackBox® Virtual Tape

StoreEver MSL6480 MSL G3s

StoreFabric SAN Encryption

HP ProLiant Servers

HP Secure Encryption

Free Client SDK

ESKM 4.0 cluster

XP7 P9500 3PAR

Any OASIS KMIP Compliant Clients

HP Helion Atalla Cloud Encryption
Intelligence to Action: Data classification with HP Atalla Information Protection and Control (IPC)
#1 cause and concern of data loss – Human Error!
CompTIA report 2015

<table>
<thead>
<tr>
<th>Cause</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human error</td>
<td>52%</td>
</tr>
<tr>
<td>End-user failure to follow policies &amp; procedures</td>
<td>42%</td>
</tr>
<tr>
<td>General carelessness</td>
<td>42%</td>
</tr>
<tr>
<td>Failure to get up to speed on new threats</td>
<td>31%</td>
</tr>
<tr>
<td>Lack of expertise with website/applications</td>
<td>29%</td>
</tr>
<tr>
<td>IT staff failure to follow policies &amp; procedures</td>
<td>26%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Concerns</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human Error as the leading contributor to security breaches</td>
<td>52%</td>
</tr>
<tr>
<td>Human error - general staff</td>
<td>30%</td>
</tr>
<tr>
<td>Human error - IT staff</td>
<td>27%</td>
</tr>
</tbody>
</table>
Partnership with

secure islands

Video Introduction
Key Atalla IPC information protection elements

Injected at creation or initial access for protection at every stage in data lifecycle

Classification
Encryption
Permissions
Policy
Usage tracking

Integrate with ArcSight:
Identify propagation of sensitive information
Active monitoring for privileged information users and detect abnormal behavior
Key use cases/threat vectors

- **Internal exposure**: Exposure of sensitive data to unauthorized employees
- **IT admin/privileged user**: Exposure to privileged users/IT admins, whether server-side/client-side/ or cloud
- **External exposure (DLP)**: Threat of data exposure outside of the organization
- **Cyber threats**: Malware or other cyber attacks, threat of data theft/leak/loss
- **Secure collaboration**: Need to share sensitive data with people outside (or within) the organization
- **Compliance**: Compliance with industry/governmental regulatory directives
Cloud Access Security protection platform
Partnership with

Video Introduction
Cloud Access Security
Visibility, Governance and Protection

Visibility
Gain complete context into users, data devices, activities, access

Governance
Implement policies for access, activities and data sharing

Protection
Address risky activities, suspicious behaviors and threats

Integrates with multiple cloud applications
Works with any user, network, any device (managed & unmanaged)
Secures data at rest and data in motion
Choice of deployment architecture depending on use case

**API Integration for normal usage**

- Cloud apps
- Managed device
- API (data at rest)

- Scalable model
- Sits out of band (minimal performance impact)

**Smart Proxy for high-security use cases**

- Cloud apps
- SMARTProxy™ (data in motion)
- Unmanaged device
- “Home” device
- Monitors data in real time for more control and governance
Adallom & HP Solutions

HP Enterprise Services

Atalla IPC

ArcSight

Classify content
Manage permissions
Embed policy
Apply protection
HP Security Voltage
Voltage solves the industry’s biggest problem: making encryption and tokenization of data simple for even the most complex use cases.
HP SecureMail with HP Identity-based Encryption
Challenges with Traditional Technologies

- **Legacy PKI**: S/MIME, PGP, OpenPGP
  - Difficult to Use
  - Not business friendly / no ad-hoc
  - Incompatible (Gmail, Android)
  - High TCO

- **Proprietary Symmetric Key**
  - Data Loss Risk
    - Complex key management
    - Active code in messages / PDFs
    - High TCO

- **Proprietary Webmail**
  - Costs Rise w/ Use
    - Key and message stores to manage
    - e-discovery breaks, fines
    - Limited functionality
What is Identity-based Encryption (IBE)?

- IBE is a public-private key technology
  - Concept originally proposed by Adi Shamir in 1984
    - Eliminate the complexity of traditional PKI
  - DoD funded research at Stanford in 2000
    - Voltage formed in 2002
  - Extensive peer review and standardization
    - **IEEE 1363.3 – Standard** for Identity-Based Cryptographic Techniques using Pairings
    - RFCs: RFC 5091, RFC 5408, RFC 5409
IBE Public Key vs. RSA Public Key

**IBE Public Key:** Sender needs only this: bob@corp.com

- PKI that uses identities used to create asymmetric keys
- Eliminates need for certificates
- Strength of RSA Public Key (1024-bit)
- S/MIME message format with IBE wrapper

**RSA Public Key:** Sender must have this key and tie it to a certificate:

```
Public exponent=0x10001
Modulus=13506641086599522334960321627880596993888147560566702
  752448514385152651060485953383394028715057190944179820728
  216447155137368041970396419174304649658927425623934102086
  438320211037295872576235850964311056407350150818751067659
  462920556368552947521350085287941637732853390610975054433
  4999811150056977236890927563
```
HP IBE: Scalability & Disaster Recovery

Scales to Millions of Users
- No user key store
- No message store
- Load balanced servers

Disaster Recovery is Effortless
- One time backup of base key
- Fast recovery with no data loss
Value of HP SecureMail

• **Simple, Native User Experience – Just Like Regular Email**
  – Outlook, iPhone, iPad, Android, Blackberry, Web

• **HP Stateless Key Management Architecture**
  – No key or message store to manage
  – Low operational and infrastructure costs

• **Single HP IBE Solution for All Use Cases**
  – Internal and external protection and compliance
  – Single technology (HP IBE, 100% push, message format)

• **DLP, AV / AS, Archive, eDiscovery Support**
  – Full content scanning, filtering, and supervisory control

• **Outlook, Exchange, Windows AD Support**
  – Global Address List, Distribution Lists, Contacts
  – AD Authentication, AD Groups
Problems with Traditional Structured Data Protection

- Need to change data structures and applications
- Fully encrypted data is unusable until decrypted
- Key management can be a nightmare
HP Format-Preserving Encryption (FPE)

- Supports data of any format: name, address, dates, numbers, etc.
- Preserves referential integrity
- Only applications that need the original value need change
- Used for production protection and data masking
Mapping the Flow of Sensitive Data

Web Form → New Account Application

New Account Application → Mainframe Database

Mainframe Database → Fraud Detection

Fraud Detection → CC Processing

CC Processing → Hadoop Analytics

Customer Service Application → New Account Application
The Same Environment With HP SecureData

Web Form

New Account Application

Fraud Detection

Mainframe Database

CC Processing

Customer Service Application

Hadoop Analytics

HP SecureData

4040 1234 1234 9999
John Smith

4040 6763 0123 9999
Kelt Dqtp

4040 6763 0123 9999
Kelt Dqtp

4040 1234 1234 9999
John Smith

4040 6763 0123 9999
Kelt Dqtp

4040 6763 0123 9999
Kelt Dqtp
Data Protection with HP FPE and HP SST

- Guaranteed referential integrity or fully randomized output by policy
- Enables Data Protection and Data De-identification from one framework
  - Can be used to generate test data for QA, training, etc.

<table>
<thead>
<tr>
<th>Name</th>
<th>SS#</th>
<th>Credit Card #</th>
<th>Street Address</th>
<th>Customer ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>James Potter</td>
<td>385-12-1199</td>
<td>37123 456789 01001</td>
<td>1279 Farland Avenue</td>
<td>G8199143</td>
</tr>
<tr>
<td>Ryan Johnson</td>
<td>857-64-4190</td>
<td>5587 0806 2212 0139</td>
<td>111 Grant Street</td>
<td>S3626248</td>
</tr>
<tr>
<td>Carrie Young</td>
<td>761-58-6733</td>
<td>5348 9261 0695 2829</td>
<td>4513 Cambridge Court</td>
<td>B0191348</td>
</tr>
<tr>
<td>Brent Warner</td>
<td>604-41-6687</td>
<td>4929 4358 7398 4379</td>
<td>1984 Middleville Road</td>
<td>G8888767</td>
</tr>
<tr>
<td>Anna Berman</td>
<td>416-03-4226</td>
<td>4556 2525 1285 1830</td>
<td>2893 Hamilton Drive</td>
<td>S9298273</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>SS#</th>
<th>Credit Card #</th>
<th>Street Address</th>
<th>Customer ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kwfdv Cq vzgk</td>
<td>161-82-1292</td>
<td>37123 48BTIR 51001</td>
<td>2890 Ykzbpoi Clpppn</td>
<td>S7202483</td>
</tr>
<tr>
<td>Veks jounrfo</td>
<td>200-79-7127</td>
<td>5587 08MG KYUP 0139</td>
<td>406 Cmxtos Osalu</td>
<td>B0928254</td>
</tr>
<tr>
<td>Pdnme Wntob</td>
<td>095-52-8683</td>
<td>5348 92VK DEPD 2829</td>
<td>1498 Zeojtbxb Pqkag</td>
<td>G7265029</td>
</tr>
<tr>
<td>Eskfw Gzhqlv</td>
<td>178-17-8353</td>
<td>4929 43KF PPED 4379</td>
<td>8261 Saicbmeayqw Yotv</td>
<td>G3951257</td>
</tr>
<tr>
<td>Jsfk Tbluhm</td>
<td>525-25-2125</td>
<td>4556 25ZX LKRT 1830</td>
<td>8412 Wbbhalhs Ueyzg</td>
<td>B6625294</td>
</tr>
</tbody>
</table>
The use of standards based cryptography is essential
- Open standards are vendor agnostic and remove risks
- Non-standard and unpublished crypto has security and liability implications
- E.g. Organizations cannot claim safe harbor exceptions incase of a breach

**Format-Preserving Encryption (NIST SP800-38G)**
- HP Security Voltage invented the FFX mode of FPE standardized by NIST
- HP Security Voltage patents cover all modes of FFX
Use Case: HP SecureData for Test/Dev

- Fits within an overall Test Data Management / ETL flow
- Provides quick implementation, quick time-to-value
Use Case: Reducing PCI DSS Scope with Secure Stateless Tokenization

- Replaces token database with a smaller token mapping table
- Token values mapped using random numbers
- Lower costs
  - No database hardware, software, replication problems, etc.
HP SecureData

- **HP Stateless Key Management**
  - No key database to store or manage
  - High performance, unlimited scalability

- **Both encryption & tokenization technologies**
  - Customize solution to meet your exact requirements

- **Broad Platform Support**
  - On-premise / cloud / Big Data
  - Structured / Unstructured
  - Linux, Hadoop, Windows, AWS, IBM z/OS, HP NonStop, Teradata, etc.

- **Quick time-to-value**
  - Complete end-to-end protection within a common platform
  - Format-preservation dramatically reduces implementation effort
## Full coverage of data protection use cases

<table>
<thead>
<tr>
<th>Use Case</th>
<th>HP Atalla</th>
<th>HP Security Voltage</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PCI compliance/scope reduction</strong></td>
<td><strong>Atalla HSMs</strong>&lt;br&gt;PAYments applications, EMV, mobile, customizations and compliance in FIPS Level 3+ appliances</td>
<td><strong>HP SecureData</strong>&lt;br&gt;<strong>HP Secure Stateless Tokenization</strong> (SST)/ secure commerce solution with Page Integrated Encryption (PIE)</td>
</tr>
<tr>
<td><strong>Data de-identification and privacy</strong></td>
<td><strong>ESKM</strong>&lt;br&gt;Securing infrastructure &amp; cloud; KMIP enterprise key management</td>
<td><strong>HP SecureData</strong>&lt;br&gt;<strong>Format preserving Encryption</strong> (FPE) – Securing the data while enabling business processes</td>
</tr>
<tr>
<td><strong>Cloud &amp; Collaboration security</strong></td>
<td><strong>HP Atalla IPC</strong>&lt;br&gt;Automatic enterprise data classification&lt;br&gt;<strong>Cloud Access Security protection platform</strong> – visibility, governance and control for SaaS</td>
<td><strong>HP Secure Mail</strong> and <strong>HP SecureFile</strong> for email security without PKI complexity and for file protection using <strong>Identity Based Encryption</strong> (IBE)</td>
</tr>
</tbody>
</table>
We protect the world’s information

Banks’ data about your finances and accounts

Your Telco’s information about your account

Payments made to you

Your interactions with SaaS applications

Your credit rating information

Your email correspondence

Health records your care provider manages for you

Your private email to and from your smartphone

Your customers’ data.
Your organisational data.
Thank you.
voltage.com