Putting the “Information” Back in Information Security

Rich Mogull
Securosis
But what about the information?
Security architectures over the next ten years will focus on information, mobility, ubiquitousness, transparency, collaboration, and openness.
Information-Centric Security
Data Breach Triangle

Exploit

Data

Egress
Pragmatic Data Security Cycle

Define

Discover

Secure

Monitor

Protect
The Pragmatic Philosophy

- Keep it simple
- Keep it practical
- Start small
- Grow iteratively
- Eat the elephant
- Document everything
The Two Sides of Data

Data Center

Productivity
Your Arsenal

DLP/CMP

DAM/ADMP

Encryption

Access Controls

IAM

VA and Pen Testing

Everything Else
DLP/CMP
ADMP (WAF + DAM)
ADMP (WAF + DAM)
Getting Started
Discover

1. Define sensitive data.
2. Find it.
3. Correlate back to users.
Techniques

- **DLP**
  - Network monitoring
  - Server/endpoint discovery
  - Some DB discovery

- **DAM**
  - DB only
  - Not all tools support

- **Network Tools**
  - WAF/UTM/IPS/etc.
  - Many now include RegEx monitoring
  - Extremely limited

- **eDiscovery/Classification**
  - Servers/storage
  - Limited analysis

- **FOSS**
  - Network and storage
  - Basic RegEx
  - Some file cracking

Thursday, June 3, 2010
Integrate with Infrastructure → Define Initial Policy → Baseline policies → Evaluate results

Tune policy
Expand policy scope
Add protection
Securosis
VA and Pen Testing

• Find vulnerabilities

• Focus on sensitive data stores.

• Use specialized tools for web apps and databases.

• Penetration test

• Validates risks.

• Determines information exposure.
What You Should Do

• Start with 1-3 data types.
• Use CMP/DLP to find them in storage and on endpoints.
• Use DAM/ADMP (or CMP) to find in databases.
• FOSS tools can help for basic data/PII, but not IP.
Secure

- Fix access controls.
- Remove unneeded data.
- Lock down access channels.
- Segregate network
- (Maybe) encrypt
The Three Laws of Encryption

- If Data Moves Physically or Virtually
- For Separation of Duties
- Mandated Encryption
Encryption Layers
Tokenization
Access Channels

Remote DB Access

Web Application Servers

Direct DB Access

Application Servers
Batch Jobs
Data Masking

Production

ID | Name | SSN
---|------|------
1  | Smith| 111-22-3333
2  | Jones| 444-55-6666
3  | Doe  | 777-88-9999

Development

ID | Name | SSN
---|------|------
1  | Johns| 123-45-6789
2  | George| 453-67-7356
3  | Blike| 245-12-7329

Thursday, June 3, 2010
Network Segregation
What You Should Do

- Remove/quarantine viral data.
- If you can’t map access controls to users, just lock it down and manage exceptions.
- Encrypt laptops, backup tapes, and portable media.
- Lock down application and database access channels.
- Begin data masking.
Monitor

- DLP/CMP for the network, storage, and endpoints.
- DAM/ADMP for databases.
- Egress filtering.
- Other tools may help, but give a false sense of security.
Content Analysis

Partial Document Matching

Exact File Matching

Database Fingerprinting

Categories

Statistical

Conceptual

Rules

\(^{(?:(?<Visa>4\d{3})|(?<Mastercard>5[1-5]\d{2})|(?<Discover>6011)|(?<DinersClub>(?:3[68]\d{2})|(?:30[0-5]\d))|(?<AmericanExpress>3[47]\d{2}))\[ -\]?)(?(DinersClub)(?:\d{6}\1\d{4})|(?(AmericanExpress)(?:\d{6}\1\d\5)))(?:\d{4}\1\d{4}\1\d{4})\)$
## Incident Management

<table>
<thead>
<tr>
<th>ID</th>
<th>Time</th>
<th>Policy</th>
<th>Channel/Location</th>
<th>Severity</th>
<th>User</th>
<th>Action</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1138</td>
<td>1625</td>
<td>PII</td>
<td>/SAN1/files/</td>
<td>1.2 M</td>
<td>rmogull</td>
<td>Quarantine</td>
<td>Open</td>
</tr>
<tr>
<td>1139</td>
<td>1632</td>
<td>HIPAA</td>
<td>IM</td>
<td>2</td>
<td>jsmith</td>
<td>Notified</td>
<td>Assigned</td>
</tr>
<tr>
<td>1140</td>
<td>1702</td>
<td>PII</td>
<td>Endpoint/HTTP</td>
<td>1</td>
<td>192.168.0.213</td>
<td>None</td>
<td>Closed</td>
</tr>
<tr>
<td>1141</td>
<td>1712</td>
<td>R&amp;D/Product X</td>
<td>USB</td>
<td>4</td>
<td>bgates</td>
<td>Notified</td>
<td>Assigned</td>
</tr>
<tr>
<td>1142</td>
<td>1730</td>
<td>Financials</td>
<td>//sjobs/C$</td>
<td>4</td>
<td>sjobs</td>
<td>Quarantine</td>
<td>Escalated</td>
</tr>
</tbody>
</table>
DB Auditing vs. Activity Monitoring

Native Auditing
- Single Platform
- Passive
- Locally stored (default)

DAM
- Cross platform
- Active alerting
- Secure repository
- All activity capable
- Additional features
Aggregation and Correlation

<table>
<thead>
<tr>
<th>System</th>
<th>Query Type</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Or1</td>
<td>Select</td>
<td></td>
</tr>
<tr>
<td>MS23</td>
<td>Update</td>
<td></td>
</tr>
</tbody>
</table>
Alternatives/Adjuncts

• **SIEM**
  - Many SIEM tools now include DAM support, or can pull (some of) audit logs.

• **Log Management**
  - Many also now include some database support

• **Triggers**
  - A bad option, but free and might be good enough under some circumstances
Network Security Monitoring

- Network monitoring for data security is now absolutely essential for financial services.
- Deep packet inspection and egress filtering.
- *Must* have proactive alerting, especially on transaction networks.
What You Should Do

- Focus network DLP/CMP on transaction areas first, since that’s where the worst losses occur.
- Use DAM on priority databases, then expand.
- Other logging/monitoring can help, but is not content specific, and won’t give great results.
- Monitor sensitive data on endpoints with DLP, especially portable storage transfers.
Protect

- Secure web applications.
- Validate encryption.
- Use DLP/CMP for network communications and endpoints.
- Set DAM policies for proactive alerting.
Web Application Security

- Secure SLDC
- Monitoring
- Static Analysis
- WAF
- Dynamic Analysis
- Penetration Testing
- Vulnerability Scanning
WebAppSec Priorities

- Vulnerability Assessment to find
- Web Application Firewall to shield
- Fix the code
CMP Deployment Modes

- **Passive**
  - Monitoring only

- **Bridge**
  - Block, but some data leaks

- **Proxy**
  - Full blocking
  - Often requires integration
Endpoint Options

- DLP/CMP for content-based blocking.
- Portable device control or encryption for gross protection.
- Monitor/Shadow files with CMP or PDC.
Defining Process

Open
- Violation detected, appears in queue
- Handler confirms incident and severity
- Escalation

Investigate
- Business unit notified
- Incident evaluated
- Protective actions taken, user notified/placemarker left

Close
- Notify employee manager and HR as needed
- Perform required employee education
- Close incident
Egress Filtering

- Segregate sensitive networks/transactions paths
- Lock channels with firewall/UTM
- Filter content with DLP
- Application control/next gen firewalls
- Hide behind a VPN
What You Should Do

- WAFs offer the quickest protection for web applications.
- DLP/CMP for network monitoring and blocking.
- You may use existing email and network tools to protect PII, but it will be more difficult to manage and offer less protection.
- PDC or DLP/CMP for endpoint data protection (on top of encryption).
The Plan

• Segregate known transaction networks and enforce strict monitoring and egress controls.

• Use DLP and database discovery to find other data sources. Trust me, they are out there.

• Start activity monitoring (DAM).
  • Focus VA and penetration tests on these systems, especially if accessed via web applications. This is the single biggest channel for major financial breaches.

• Encrypt all laptops.

• Egress filter transaction networks.

• Slowly minimize use of protected data. Do you really need to let that many people access it? Can you consolidate/tokenize it?
The Future?
Cloud Info-Centric Security Building Blocks

Labels
Cloud Info-Centric Security Building Blocks

Encryption
Cloud Info-Centric Security Building Blocks

EDRM

Thursday, June 3, 2010
Cloud Info-Centric Security Building Blocks

DLP
Cloud Info-Centric Security Building Blocks

IAM

Inigo Montoya
(You killed my father prepare to die)
Labels are applied via context and content analysis
Create

Apply Contextual Labels

Analyze Content

Apply Mandatory and Discretionary Rights
New Granularity in “Unstructured” Content

What Mac Users Need to Know About Security
By Rich Mogull

Few topics in the Mac community are as contentious as security. On one side are vendors and the press; hyping every new potential threat like it’s the end of the world with the hope of selling more products or getting more readers. On the other side are the religious zealots who consider Macs immune to security problems, and react to any discussion of potential weaknesses like a personal assault. Caught in the middle of these competing agendas is the vast sea of average Mac users, who desire little more than to know what they need to do.
New Granularity in “Unstructured” Content

In database content we can apply labels/rights at the row/field level.

In document-based content we can now apply at the paragraph or object level.
### Cross-Domain Information Protection

<table>
<thead>
<tr>
<th>ID</th>
<th>Last</th>
<th>First</th>
<th>SSN</th>
</tr>
</thead>
<tbody>
<tr>
<td>1111</td>
<td>Mogull</td>
<td>Richard</td>
<td>555-12-5555</td>
</tr>
<tr>
<td>1112</td>
<td>Smith</td>
<td>John</td>
<td>324-86-3456</td>
</tr>
</tbody>
</table>
Cross-Domain Information Protection

<table>
<thead>
<tr>
<th>ID</th>
<th>Last</th>
<th>First</th>
<th>SSN</th>
</tr>
</thead>
<tbody>
<tr>
<td>1111</td>
<td>Mogull</td>
<td>Richard</td>
<td>555-12-5555</td>
</tr>
<tr>
<td>1112</td>
<td>Smith</td>
<td>John</td>
<td>324-86-3456</td>
</tr>
</tbody>
</table>

Customer Report
Customer retention grew 13% YoY. Customer 138-56-8375 held return value while...
Cross-Domain Information Protection

<table>
<thead>
<tr>
<th>ID</th>
<th>Last</th>
<th>First</th>
<th>SSN</th>
</tr>
</thead>
<tbody>
<tr>
<td>1111</td>
<td>Mogull</td>
<td>Richard</td>
<td>555-12-5555</td>
</tr>
<tr>
<td>1112</td>
<td>Smith</td>
<td>John</td>
<td>324-86-3456</td>
</tr>
</tbody>
</table>

Customer Report
Customer retention grew 13% YoY. Customer 138-56-8375 held return value while...
Data Dispersion
Data-In-Motion/Rest

Shared Storage
Where This Take Us

- Content analysis fully integrated into both productivity and transaction applications.
- Rights (and thus encryption) applied at the point of creation, at the data-element level.
- Choke points between on-premise, off-premise, and between cloud services enforce policies at the data level, enforced by encryption/DRM.
- Rights transfer and are maintained between state changes.
Rich Mogull
Securosis, L.L.C.

rmogull@securosis.com
http://securosis.com
AIM: securosis
Skype: rmogull
Twitter: rmogull