Cloud encryption – Encrypt all the things!

Walter Tighzert

German Owasp Day 2014
About me

• Security researcher at SAP SE
  walter.tighzert@sap.com

• Focus on search over encrypted data
Cryptographic interlude

- Randomized encryption
- Deterministic encryption
- Order preserving encryption
- Homomorphic encryption

SQL operators: SELECT, COUNT

<table>
<thead>
<tr>
<th>Animal</th>
<th>Animal</th>
</tr>
</thead>
<tbody>
<tr>
<td>cat</td>
<td>09122014...</td>
</tr>
<tr>
<td>dog</td>
<td>080012...</td>
</tr>
<tr>
<td>cat</td>
<td>0171633...</td>
</tr>
</tbody>
</table>

AES - CBC
Cryptographic interlude

- Randomized encryption
- Deterministic encryption
- Order preserving encryption
- Homomorphic encryption

Animal

<table>
<thead>
<tr>
<th>Animal</th>
<th>09122014…</th>
</tr>
</thead>
<tbody>
<tr>
<td>cat</td>
<td>080012…</td>
</tr>
<tr>
<td>dog</td>
<td>09122014…</td>
</tr>
</tbody>
</table>

SQL operators: =, DISTINCT, GROUP BY, JOIN

AES - ECB
Cryptographic interlude

- Randomized encryption
- Deterministic encryption
- Order preserving encryption
- Homomorphic encryption

SQL operators: <, ORDER BY
Cryptographic interlude

- Randomized encryption
- Deterministic encryption
- Order preserving encryption
- Homomorphic encryption

\[
\text{ENC}(f(x, y)) = g(\text{ENC}(x), \text{ENC}(y))
\]
Cryptographic interlude

- SELECT animal, SUM(food) FROM animals WHERE quantity > 1 GROUP BY animal

- SELECT animal_RND, SUM(food_HOM) FROM animals WHERE quantity_OPE > 05ef GROUP BY animal_DET
Agenda

• Motivation
• State of the art
• Demo
• Challenges
Motivation - Cloud

• From personal finance (Mint) to company finance (Workday)

• What happens with my data?

• Encryption?
Cloud scenario

End User

SaaS Provider

DaaS Provider
Solution 1: between DaaS and SaaS
Solution 1: between DaaS and SaaS

- Attacker model: DaaS honest but curious
- CryptDB
## Solution 1: between DaaS and SaaS

<table>
<thead>
<tr>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complex queries supported</td>
<td>Encryption keys in the cloud</td>
</tr>
<tr>
<td>Transparent for the application</td>
<td>Plaintext on the SaaS</td>
</tr>
</tbody>
</table>
Solution 2: between End User and SaaS
Solution 2: between End User and SaaS

- Attacker model: SaaS honest but curious
- Commercial solutions from 3rd parties (CipherCloud, Vaultive...)
- HTTP Encryption Proxy for specific applications
- No application changes possible
Solu-on 2: between End User and SaaS

<table>
<thead>
<tr>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keys stay at the customer</td>
<td>Only a few applications are supported</td>
</tr>
<tr>
<td>Proxy at the customer</td>
<td>Simple queries (only textual values)</td>
</tr>
</tbody>
</table>
Solution 3: between Browser and End User
Solution 3: between Browser and End User

• New attacker model: SaaS malicious/compromised
• Research prototypes: ShadowCrypt, Mylar...
• Plaintext is encapsulated in a sandbox
### Solution 3: between Browser and End User

<table>
<thead>
<tr>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sandbox</td>
<td>Browser-specific</td>
</tr>
<tr>
<td>Lightweight client</td>
<td>Key management</td>
</tr>
<tr>
<td></td>
<td>Simple queries (only textual values)</td>
</tr>
</tbody>
</table>
Healthcare Application
Healthcare Application

- Only JOIN and simple WHERE conditions

ENCRIPT ALL THE THINGS

imgflip.com
Sales Dashboard

Sales by Region

Region
- AFR
- AMER
- APJ
- EMEA

Sales by Country

Country Codes

Sales in EUR

0 500k 1M 1.5M 2M
Sales Dashboard

• Complex queries with SUM and ORDER BY SUM (not supported on encrypted data)
Sales Dashboard

• Complex queries with SUM and ORDER BY SUM (not supported on encrypted data)
Challenges

• Not supported functions:
  – ORDER BY SUM
  – LIKE/FUZZY search queries

• Business logic on the server:
  TOTAL = SUM(PRICE);
  IF TOTAL > 200 THEN TOTAL *= 0.9;
  -> move it to the client?
Final Words – Trade-off

Security

Performance

Functionality
Thanks for your attention

Questions/remarks?

walter.tighzert@sap.com
Sources

- Mint: https://www.mint.com/images/rd/features/overview_hero.png
- CryptDB: http://css.csail.mit.edu/cryptdb/cryptdbdiag.jpg
- Cloud scenario: benny@fuhry.de