Crypto: a key ingredient in building respectful products

@LeaKissner
HI!
I’m lea kissner
Philosophy
1. Build products that respect users.
2. Understand what that means.
3. Make it easy.
Build products that respect users.
IDE integration

Using `getAddress` to get device identifiers is not recommended. For advertising use-cases, use `AdvertisingIdClient$Info#getId` and for analytics, use `InstanceId#getId`.
Understand what that means.
Make it easy.
Crypto time
Rolling one’s own crypto
1. They think they're smart.

2. They think it’s cool.

3. It’s not obvious.

4. It’s too expensive.
1. They think they’re smart.
2. They think it’s cool.
3. It’s not obvious.
4. It’s too expensive.
Moral of the story: Don’t give people excuses to roll their own crypto.
Privacy-preserving computation
Phone number

UserID for phone#
Moral of the story: Please make privacy-preserving computation faster.
Encryption at rest
Hardware breaks
Software breaks
Encryption!
Keys
Keys
System issues
System issues
Key rotation
<table>
<thead>
<tr>
<th>Restaurant ID</th>
<th>Review ID</th>
<th>Number of stars</th>
</tr>
</thead>
<tbody>
<tr>
<td>333</td>
<td>123456789</td>
<td>5</td>
</tr>
<tr>
<td>90224</td>
<td>987654321</td>
<td>3</td>
</tr>
</tbody>
</table>

**Object ID: 123456789**

<table>
<thead>
<tr>
<th>Group ID</th>
<th>Msg ID</th>
<th>Message text</th>
</tr>
</thead>
<tbody>
<tr>
<td>55632</td>
<td>10</td>
<td>“Never gonna give you up”</td>
</tr>
<tr>
<td>92132</td>
<td>22</td>
<td>“Never gonna let you down”</td>
</tr>
</tbody>
</table>

**Object ID: 55632 | 10**
Gmail | Photos | Docs | Storage | Key Management Server (KMS)
Moral of the story: Crypto is a tool for turning things into key management problems.
Morals of this story
Don’t give people excuses to roll their own crypto.
Please make privacy-preserving computation faster.
Crypto is a tool for turning things into key management problems.
Success must be evaluated in the full stack, including the humans
... and the squirrels
Thank you

lkissner@google.com
@LeaKissner
Questions you might want to ask:
1. What’s are those squirrels thinking?
2. Why wasn’t the crypto-based access control sufficient to remove the need for storage system ACLs?
3. What else makes key management hard?
4. Why aren’t there magical privacy experiences?

lkissner@google.com
@LeaKissner