SOCIAL AUTHENTICATION FOR END TO END ENCRYPTION

Elham Vaziripour, Mark O’Neill, Justin Wu, Scott Heidbrink, Kent Seamons, Daniel Zappala

Brigham Young University
(IN)SECURITY AFFECTS LIVES

Hackers spied on 300,000 Iranians using fake Google certificate

Naked celebrity hack: security experts focus on iCloud backup theory

After intensive examination of file data leaked by one or more hackers, suspicion grows that iCloud backups were source of pictures - though precise method of attack still unclear

Jennifer Lawrence among...
CONTENT-BASED ENCRYPTION

Connection-Based

Content-Based
SOME PROGRESS

Signal

ChatSecure

SafeSlinger

Keybase

We should consider every day lost on which we have not danced at least once. And we should call every truth false which was not accompanied by at least one laugh.

All phones must match one of the 3-word phrases. Compare, and then pick the matching phrase.

- printer amusement ringbolt 153 264 174
- ahead decimal deadbolt 8 324 73
- deckhand disruptive merit 74 334 129

Recipient

laremdw

Message to encrypt

Sign the message (proof it’s from you, timbrey)
PROBLEM #1: KEY PORTABILITY
PROBLEM #2: KEY DISTRIBUTION AND TRUST

Key Signing Parties

Manual Inspection

Certificate Authorities
## PROBLEM #3: GENERALITY

<table>
<thead>
<tr>
<th>Type</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMS</td>
<td>![icon]</td>
</tr>
<tr>
<td>Voice</td>
<td>![icon] ![icon] ![icon]</td>
</tr>
<tr>
<td>IM</td>
<td>![icon]</td>
</tr>
<tr>
<td>Email</td>
<td>![icon] ![icon] ![icon]</td>
</tr>
<tr>
<td>Web</td>
<td>![icon] ![icon] ![icon]</td>
</tr>
<tr>
<td>Video</td>
<td>![icon]</td>
</tr>
<tr>
<td>Key Mgmt.</td>
<td>![icon] ![icon] ![icon] ![icon] ![icon] ![icon] ![icon] ![icon]</td>
</tr>
</tbody>
</table>
PROBLEM #4: USABILITY

Public Key?  Private Key?

Identity  Expired?
USERS NEED...

1. A portable, secure private key store
2. A way to automatically manage public keys
   • Discovery
   • Update
   • Validation
3. A general service for encryption/decryption and signing/verifying
   • For arbitrary types of communication
   • Interoperable with other apps
4. **Usability** for all this!
KEY PUBLICATION AND DISCOVERY

1. **Let's get started**
   - **Make ID**
   - **OR**
   - **Import ID**

[Diagram showing keys and a safe]
KEY PUBLICATION AND DISCOVERY

Alice's Profile

Alice's Profile

Alice's Tweet

Google+
KEY PUBLICATION AND DISCOVERY

Phone Contact Database

Alice’s Contacts’ Public Keys

Alice’s Friends

Alice’s Contacts’ Public Keys

Alice’s Followings and Followers

Alice’s Contacts’ Public Keys

Alice’s Circles
SOCIAL AUTHENTICATION API

- **Encrypt API**: message, recipient
  - encrypted message
  - Other App/Device

- **Key API**: recipient
  - recipient public key
  - Other App/Device

- **Signing API**: message digest
  - signed digest
  - Other App/Device

- **Verify API**: signed message, sender
  - result
  - Other App/Device

- **Decrypt API**: encrypted message
  - message
  - Other App/Device
POINTS OF DISCUSSION

• Usable Key Management
  • User key revocation
  • User key updating
  • Automatically receive updates about key changes via periodic checks of OSN data

• Inducting Novices
  • Leveraging OSN

• Authenticating a Stranger
  • Add them as a “friend” on one or more OSNs, immediately receive their public key

• Attack modeling
  • Evaluate resilience to attacks such as Sybil attack