Servers can't be trusted, and thanks to tamper-proof journals EteSync doesn't need to!

stosb.com/talks

tom@stosb.com
@TomHacohen
Simple Server Communication
What Are We Leaking?

**Data**
- Emails
- Calendars
- Personal notes
- Secret business information

**Metadata**
- IP address
- Social graph
- Time of access
- What data is used and how often
- When specific data is accessed
Metadata Is Data!

Exploiting Social Graphs
Metadata Is Data!

Exploiting Access Patterns
Real Example: CardDAV

Alice.vcf  Bob.vcf  Cher.vcf  Dan.vcf
Information Leaked

- Address Book Information
- IP address
- Social graph
- Time of access
- What data is used and how often
- When specific data is accessed
Potential Solutions

- Using Tor to hide origin
- Controlling access patterns
- Trusting the server:
  - Using a trusted provider
  - Hosting on our own server ("self host")
Should We Trust The Server?

- It could get hacked (remote or physical access)
- Could get stolen (literally someone picking it up and taking it)
- Hosted: a rogue employee could access your data
- Hosted: could be compelled to provide access
- Self-hosted: a lot of work and hard to maintain
Reducing Server Trust

- End-to-end encryption
- Mostly offline operation (if possible)
- Fake access patterns?
Hardened CardDAV

4355a.vcf 19d34.vcf 4183e.vcf 3c9e1.vcf
That's It, We Are Safe!

Questions?

Well, actually...
Our Data Can Be Manipulated!
Bit Flipping

Imagine the access level is stored encrypted

<table>
<thead>
<tr>
<th>Original</th>
<th>Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypted</td>
<td>0x4a</td>
</tr>
<tr>
<td>Decrypted</td>
<td>0x00</td>
</tr>
</tbody>
</table>
Data Omission

4355a.vcf 19d34.vcf 4.83e.vcf 3c9e1.vcf
Data Omission: Solution

Verify the state

4355a.vcf 19d34.vcf 4183e.vcf 3c9e1.vcf

State: b3fe06fad053beb8ebfd8977b010655bfdd3c3
Data Rollback

OLD VERSION

4355a.vcf 19d34.vcf 4183e.vcf 3c9e1.vcf

State: 1121cfccd5913f0a63fec40a6ffda444ea64f9dc1e
The Solution:
Tamer-proof journals!
What Is It?

Change Journal

Type: ADD
Content: Alice

Type: ADD
Content: Bobb

Type: CHANGE
Content: Bob

Type: DELETE
Content: Alice
What Is It?

Immutable And Tamper-Proof

UID is a HMAC of content + previous UID

UID: 1121cf  
Content: dWNoYW9ic23a

UID: 5913f0  
Content: YXNlbi5R1aGFib3Nu

UID: a63fec  
Content: NudWFvaGV1bm

UID: 40a6ff  
Content: FvdWhvdWhvCm50
Protections Against Tampering

- Immutable, so data can only be appended
- Signed, so data can't be manipulated or faked
- Prev UID is signed, no omission or reordering
- Verified on each client
Previously Unsolved Attacks

- Which data is accessed and modified
- Data Omission
- Data Rollback
Secure, end-to-end encrypted and journaled personal information cloud synchronization for Android, the desktop and the web.

A real-life example.
UID "7ecda2139a45a1674c1b991760f4ae56718b06c0d0b9ed459eea86f709c6d02b"
CONTENT {
    "action": "CHANGE",
    "content": "BEGIN:VCALENDAR\n    VERSION:2.0\n    PRODID:-//EteSync//com.etesync.syncadapter 0.16.0//ical4android\n    BEGIN:VEVENT\n    SUMMARY:Feed cats\n    ... snip ...\n    END:VEVENT\n    END:VCALENDAR"
}

UID "513da45c2d6562c511b898f6f191631c56dfa33d789a399000e99df9b6b8e480"
CONTENT {
    "action": "DELETE",
    "content": "BEGIN:VCALENDAR\n    VERSION:2.0\n    PRODID:-//E"
Having A Change History

- Auditing changes
- Recovering lost data
- Finding entries based on date
Signed Pages

- Devs PGP sign web pages
- Users add website config
- Extension verifies signatures
- Should be used in conjunction with subresource integrity
- Future: signature verifying service workers (collaboration with airborne.io)
Finishing Notes

- Privacy is a sacred right, don't give it up!
- You're the weakest link:
Useful Links

- My blog: https://stosb.com
- EteSync's website: https://www.etesync.com
- EteSync's sources: https://github.com/etesync
- Signed Pages: https://github.com/tasn/webext-signed-pages
Questions?
stosb.com/talks
 Attribution

- Icon by Freepik from flaticon.com is licensed under CC 3.0 BY
- Icon by Smashicons from flaticon.com is licensed under CC 3.0 BY
- Security by Randall Munroe (XKCD)