Action Needed! Helping Users Find and Complete the Authentication Ceremony in Signal

Elham Vaziripour, Justin Wu, Mark O’Neill, Daniel Metro, Josh Cockrell, Timothy Moffett, Jordan Whitehead, Nick Bonner, Kent Seamons, Daniel Zappala

Brigham Young University

Internet Research Lab
Importance of Secure Messaging

‘Send all.’

‘Read all.’

THE HILL

February 14, 2017 - 01:31 PM EST

Trump staffers using app that deletes their messages: report
End-to-End Encryption is a Solution
Verify the Identity Key
Verify the Identity Key
Last year at SOUPS...

- Users have a hard time finding and completing the authentication ceremony without instruction
  - 14% success rate with no instruction
  - 78% success rate with instruction
- It takes too long to complete the ceremony even with instruction
  - 7 minutes, average time to find
  - 11 minutes, average time to complete
How Can We Help People To Quickly Find and Use the Authentication Ceremony in Secure Messaging Applications, Without Instruction?
Our Approach

- Opinionated design: Make more decisions and leave fewer options \(^{(1)}\)
- Encourage the user to be security minded
  - Nudges \(^{(2)}\)
  - Monetary incentive

---

Our Approach

- Follow design principles from Schroder et al. - EuroUSEC 2016
  
  (1) Awareness of the security status of conversations
  
  (2) Comprehensible instructions for recommended actions
  
  (3) Clear risk communication
  
  (4) Easily accessible verification
Original Signal
Current path to find and use the authentication ceremony in Signal

Bob
Tap here for settings

New Message
Current path to find and use the authentication ceremony in Signal

1. Open the Signal app.
2. Tap on the 'Contact Info' button for the contact you want to access the authentication ceremony for.
3. Tap on the 'Show Safety Number' option.

This will allow you to find and use the authentication ceremony in Signal.
Current path to find and use the authentication ceremony in Signal

1. Tap here for settings
2. Tap on the contact info to view details
3. Tap on the Show Safety Number button
4. Tap on the Verify Safety Number button
5. Mark as Verified

You have not marked Bob as verified.

Verify Safety Number

[QR Code]

Tap to Scan

02171 10936 33801 16657
04872 86079 10987 98110
30887 90040 60307 83167

If you wish to verify the security of your end-to-end encryption with Bob, compare the numbers above with the numbers on their device.
Alternatively, you can scan the code on their phone, or ask them to scan your code.

Learn More
Current path to find and use the authentication ceremony in Signal
Modification 1

(1) Awareness of security status
(4) Easily accessible verification
Modification 1

(1) Awareness of security status
(3) Comprehensible instructions
(4) Easily accessible verification
Modification 1

Bob
Unanswered outgoing call
Action Needed

Bob
Tap here for settings

Verify Safety Number
You have not marked Bob as verified.
Tap to Scan

02171 10936 33801 16657
04872 86079 10987 98110
30887 90040 60307 83167

If you wish to verify the security of your end-to-end encryption with Bob, compare the numbers above with the numbers on their device. Alternatively, you can scan the code on their phone, or ask them to scan your code.

Learn More

Mark as Verified

You marked Bob as verified.

Conversation is secure. Safety number is verified.
Modification 2
Modification 2

(3) Comprehensible instruction
Modification 2 (Over a phone call)

Verification Needed
Signal needs additional information from your contact's device to secure your conversations. Would you rather do it in person or over a phone call?

Over a phone call
In person
Dismiss

Verify Safety Number
Your safety number is visible during the call. Verify that your contact's safety number and yours are identical.

Free Signal call
Dismiss

Verify Safety Number
This is your safety number with Bob. Ask Bob for the safety number and make sure your numbers match before mark this contact as verified!

02171 10936 33801 16657
04872 86079 10987 98110
30887 90040 60307 83167

Mark as Verified

Congratulations!
Your conversation is secure now.
Modification 2 (In person)

Verification Needed
Signal needs additional information from your contact’s device to secure your conversations. Would you rather do it in person or over a phone call?

- Over a phone call
- In person
- Dismiss

Congratulations!
Your conversation is secure now. Your safety numbers match.

You marked Bob as verified.
Lab User Studies to Evaluate the Modifications
Methodology

- Participants signed up in pairs (30 pairs total)
- Versions cycled through in round robin manner
- 10 pairs for each version
- During the study:
  - One participant was told to send a credit card to the other
  - Participants were given $7 with a $3 bonus to make sure the credit card number is transferred safely
  - Afterward, they filled out a survey and were asked questions about their comprehension
## Results: Find and Complete Ceremony

<table>
<thead>
<tr>
<th></th>
<th>Completion Rate (Self-Reported)</th>
<th>Found (Coordinator-Reported)</th>
<th>Completion Rate (Coordinator-Reported)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Original Signal</td>
<td>50%</td>
<td>25%</td>
<td>0%</td>
</tr>
<tr>
<td>Modification 1</td>
<td>90%</td>
<td>100%</td>
<td>30%</td>
</tr>
<tr>
<td>Modification 2</td>
<td>60%</td>
<td>95%</td>
<td>90%</td>
</tr>
</tbody>
</table>

- Half of the participants who used the original Signal, and the majority of participants who used the modified versions, *believed* that they completed the task safely
  - Original: none successfully performed the authentication ceremony
  - Modification 1: majority clicked the toggle before verification
“I was a little confused at first and I wondered if we needed to be in the same room to scan the QR code to make sure our conversation was secure. At the bottom it just asked if I could switch the conversation to verified and so I did.”

“I hit [the button] and then I was like, ‘well that did nothing’ and so I hit it again and nothing happened...I hit verify and then it says that I just unhit it immediately afterwards...I was just like, ‘verify what? What am I verifying?’ It didn’t really tell me...Honestly it meant nothing.”
No Need for Instructions

<table>
<thead>
<tr>
<th></th>
<th>Prior Study</th>
<th>WhatsApp Facebook Msgr (with instruction)</th>
<th>Viber (with instruction)</th>
</tr>
</thead>
<tbody>
<tr>
<td>This Study</td>
<td>Modification 1 (without instruction)</td>
<td></td>
<td>Modification 2 (without instruction)</td>
</tr>
<tr>
<td>Completion Rate</td>
<td>30%</td>
<td>70%</td>
<td>90%</td>
</tr>
</tbody>
</table>
Result: Timing

- Modification 1: time to locate ceremony drops to under a minute
- Modification 2: time to complete the task drops in half
- Between modification 2 and the previous study, time drops from 11 to 4.5 minutes

<table>
<thead>
<tr>
<th>Application</th>
<th>Time to Find the Authentication Ceremony</th>
<th>Completion Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Original</td>
<td>3.5</td>
<td>N/A</td>
</tr>
<tr>
<td>Modification 1</td>
<td>&lt; 1</td>
<td>7</td>
</tr>
<tr>
<td>Modification 2</td>
<td>&lt; 1</td>
<td>2</td>
</tr>
</tbody>
</table>
“I liked that it came up on the **middle of the phone call screen** rather than being sent through a text message that I would have to pull up during the conversation. There were **a lot of numbers**, which could be **hard to keep track of if you were reading them over the phone**, but the amount of numbers ensures greater safety.”
Result: Comprehension

- Participants were asked about the purpose of the authentication ceremony.
- Even though some expressed understanding of authentication and confidentiality, many of these participants were still unsure of their answers.

<table>
<thead>
<tr>
<th>Code</th>
<th>Original</th>
<th>M1</th>
<th>M2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>(A) Survey</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication</td>
<td>3</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Security</td>
<td>0</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>Trust</td>
<td>0</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Didn’t know</td>
<td>0</td>
<td>7</td>
<td>5</td>
</tr>
<tr>
<td><strong>(B) Interview</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication</td>
<td>7</td>
<td>7</td>
<td>6</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>3</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>Security</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Trust</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Didn’t know</td>
<td>5</td>
<td>7</td>
<td>5</td>
</tr>
</tbody>
</table>
Are you willing to use the authentication ceremony before you exchange messages with a friend the first time?

- Yes: 32
- No: 4
- For confidential information: 14
- Certain contacts: 6

“Am I willing? Yes. Will I? No. Because here is the thing, I don’t really care if my messages get intercepted because most of the time I am not sending my credit card number or social security numbers. Will I use it for things that are really important? For sure.”
Conclusion

• Finding and completing the authentication ceremony improves
  ○ Using opinionated design
  ○ Using nudges
  ○ Apply design principle
  ○ Encourage to be security minded

• Improvement made with no instructions

• Time to find and complete the ceremony is significantly shorter
Future Work

- Improve risk communication
- Determine the importance of comprehension
- Encourage people to be security-minded without monetary incentive
- Apply lessons learned to attack scenarios
- Find ways to automate the authentication ceremony