Can Unicorns Help Users Compare Crypto Key Fingerprints? (Supplementary Material)

**ACTIVITY TUTORIAL**

*(hex version)*

Scenario: Imagine that you work as an accountant at Print Idea Solutions and that your company is in the process of updating its employee database.

Your task is to retrieve the SSN for 30 different employees and enter them into the database.

Each employee will send you a message with his or her SSN. Before you can read the chat message, you’ll need to perform a security check. To ensure the chat session is secure, you will need to compare a pair of text strings, which are called “fingerprints.”

* [if compare-and-confirm] One fingerprint will be displayed on your computer. The other fingerprint is printed on the employee’s business card, located on your desk. If these two fingerprints are the same, your chat session is secure. If they are different, your session is not secure; someone else could be eavesdropping on your communications.

* [if compare-and-select] Three fingerprints will be displayed on your computer. Another fingerprint is printed on the employee’s business card, located on your desk. If one of the fingerprints on your computer matches the one on the business card, your chat session is secure. If none match, your session is not secure; someone could be eavesdropping on your communications.

Check for differences in the letters or numbers shown. The font size and type do not matter.

* [if compare-and-confirm] Since the two fingerprints shown here are the same, you should click the ‘Same’ button.

* [if compare-and-select] Since the first fingerprint shown here matches the one on the business card, you should select it and click Continue.

After performing the security check, you will need to enter the information shown in the chatbox into the highlighted database field.

You may enter the SSN with or without dashes or spaces (“123-45-678,” “12345678,” and “123 45 678” are all valid). You will need to manually type the SSN into the database, since copy/paste will not work.

For a $1 bonus, complete your task both quickly and correctly. The 15% fastest participants with the fewest mistakes will receive an additional $1 bonus.

This stopwatch will show you the current time to beat. Please note that beating this time does not guarantee the bonus; future participants may lower (or raise) the time to beat.

This is the end of the tutorial. If you need more practice, you can restart the tutorial. Otherwise, if you’ve got the hang of things, you may proceed to the actual activity.

**POST-ACTIVITY SURVEY**

Please fill out this short survey on the activity you just performed. At the end of the survey, you will receive a code that can be used for payment on Mechanical Turk.

**Rank the following in terms of what you thought was most important while performing this activity (1 = most important):**

- (dropdown containing 1-4)
  - Responding to employees in the chatbox
  - Completing the activity as fast as possible
  - Entering the correct SSN into the database
  - Correctly comparing [representation]s

**What was the hardest thing about this activity?**

[Textbox]

The following questions ask about the [representation] comparisons you just made. We’ve included an example below, as a reminder:

[Image of comparison dialog]

**It was easy to determine if [representation]s were the same or different.**

- Strongly agree
- Agree
- Somewhat agree
- Neither agree nor disagree
- Somewhat disagree
- Disagree
- Strongly disagree

**The amount of time it took to compare [representation]s is reasonable for a security check.**

- Strongly agree
- Agree
- Somewhat agree
- Neither agree nor disagree
- Somewhat disagree
- Disagree
- Strongly disagree
I feel confident that I could correctly compare [representations] as a security check.

- Strongly agree
- Agree
- Somewhat agree
- Neither agree nor disagree
- Disagree
- Strongly disagree

I was worried about incorrectly choosing “Same” when two [representations] were different.

- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly disagree

I was worried about incorrectly choosing “Different” when two [representations] were the same.

- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly disagree

[if missed attack]
You incorrectly answered the following security check.

Why do you think you failed to notice that the fingerprint shown on the business card did not match the one shown in the security check dialog?

[Textbox]

[if caught attack]
You correctly answered the following security check.

[Image of comparison dialog for attack instance]

What tipped you off that the fingerprint shown on the business card did not match the one shown in the security check dialog?

[Textbox]

Please describe your strategy for comparing fingerprints to determine if they are the same or different.

[Textbox]

What is the highest level of education you have completed?

- Elementary school only
- Some high school but did not finish
- Graduated from high school
- Some college but did not finish
- Two year college degree or A.A. or A.S.
- Four year college degree or B.A. or B.S.
- Some graduate school
- Graduate degree
- Prefer not to answer

What is your age (optional)?

What is your gender?

- Male
- Female
- Prefer not to answer

Which of the following best describes your primary occupation?

- Administrative Support (e.g. secretary, assistant)
- Art, Writing, or Journalism (e.g. author, reporter, sculptor)
- Business, Management, or Financial (e.g. manager, accountant, banker)
- Education or Science (e.g. teacher, professor, scientist)
- Legal (e.g. lawyer)
- Medical (e.g. doctor, nurse, dentist)
- Computer Engineering or IT Professional (e.g. programmer, IT consultant)
- Engineer in other field (e.g. Civil or bio engineer)
- Service (e.g. retail clerk, server)
- Skilled Labor (e.g. electrician, plumber, carpenter)
- Unemployed
- Retired
- College student
- Graduate student
- Prefer not to answer

Do you know any programming languages?

- Yes (list languages) [Textbox]
- No

People often ask me for computer-related advice.

- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly disagree

Did you encounter any technical issues while completing this HIT?

[Textbox]

Please provide any additional feedback you have about this HIT.

[Textbox]
ATTACKS
Here are the attacks used in our experiment. Attack #’s appearing in captions correspond to the attack IDs shown in Figure 4 of the paper.

Figure 1: hex, confirm, bothvis, $2^{60}$: Attack #1

Figure 2: hex, confirm, bothvis, $2^{60}$: Attack #2

Figure 3: hex, confirm, bothvis, $2^{60}$: Attack #3
Figure 4: **num**, confirm, bothvis, $2^{60}$: Attack #1

Figure 5: **num**, confirm, bothvis, $2^{60}$: Attack #2

Figure 6: **num**, confirm, bothvis, $2^{60}$: Attack #3
Figure 7: alt, confirm, bothvis, $2^{60}$: Attack #1

Figure 8: alt, confirm, bothvis, $2^{60}$: Attack #2

Figure 9: alt, confirm, bothvis, $2^{60}$: Attack #3
Figure 10: **word**, confirm, bothvis, $2^{60}$, Attack #1

Figure 11: **word**, confirm, bothvis, $2^{60}$: Attack #2

Figure 12: **word**, confirm, bothvis, $2^{60}$: Attack #3
Your moon sleeps by her example round our poison.
Your deep milk pushes inside the grip.
My fork prepares my profit darkly into my clean danger.

Figure 13: sent, confirm, bothvis, \textsuperscript{260}: Attack #1

His glass returns on my foolish woman.
My young window smiles.
Her payment loves my soup on his circle.
Her rare produce shows my pain.

Figure 14: sent, confirm, bothvis, \textsuperscript{260}: Attack #2

This school pulls thickly inside his fixed shake.
The sticky picture visits from that worm.
This sweet smash cries for our brain fitfully.
That clock sends.

Figure 15: sent, confirm, bothvis, \textsuperscript{260}: Attack #3
Figure 16: ssh, confirm, bothvis, $2^{60}$: Attack #1

Figure 17: ssh, confirm, bothvis, $2^{60}$: Attack #2

Figure 18: ssh, confirm, bothvis, $2^{60}$: Attack #3
Figure 19: uni, confirm, bothvis, 2$^{60}$: Attack #1

Figure 20: uni, confirm, bothvis, 2$^{60}$: Attack #2

Figure 21: uni, confirm, bothvis, 2$^{60}$: Attack #3
Figure 22: *vash*, confirm, bothvis, $2^{60}$: Attack #1

Figure 23: *vash*, confirm, bothvis, $2^{60}$: Attack #2

Figure 24: *vash*, confirm, bothvis, $2^{60}$: Attack #3
Figure 25: hex, select, bothvis, $2^{60}$: Attack #1

Figure 26: hex, select, bothvis, $2^{60}$: Attack #2

Figure 27: hex, select, bothvis, $2^{60}$: Attack #3
Figure 28: hex, confirm, toggle, 260: Attack #1

Figure 29: hex, confirm, toggle, 260: Attack #2

Figure 30: hex, confirm, toggle, 260: Attack #3
Figure 31: vash, confirm, toggle, $2^{60}$: Attack #1

Figure 32: vash, confirm, toggle, $2^{60}$: Attack #2

Figure 33: vash, confirm, toggle, $2^{60}$: Attack #3
Figure 34: hex, confirm, bothvis, $2^{40}$: Attack #1

Figure 35: hex, confirm, bothvis, $2^{40}$: Attack #2

Figure 36: hex, confirm, bothvis, $2^{40}$: Attack #3
Figure 37: uni, confirm, bothvis, $2^{40}$: Attack #1

Figure 38: uni, confirm, bothvis, $2^{40}$: Attack #2

Figure 39: uni, confirm, bothvis, $2^{40}$: Attack #3
Figure 40: hex, confirm, bothvis, $2^{80}$: Attack #1

Figure 41: hex, confirm, bothvis, $2^{80}$: Attack #2

Figure 42: hex, confirm, bothvis, $2^{80}$: Attack #3
Figure 43: ssh, confirm, bothvis, $2^{80}$: Attack #1

Figure 44: ssh, confirm, bothvis, $2^{80}$: Attack #2

Figure 45: ssh, confirm, bothvis, $2^{80}$: Attack #3
Figure 46: hex, confirm, bothvis, $2^{60}$, \textbf{2x time}: Attack #1

Figure 47: hex, confirm, bothvis, $2^{60}$, \textbf{2x time}: Attack #2

Figure 48: hex, confirm, bothvis, $2^{60}$, \textbf{2x time}: Attack #3
Figure 49: **hex (low)**, confirm, bothvis, $2^{60}$: Attack #1

Figure 50: **hex (low)**, confirm, bothvis, $2^{60}$: Attack #2

Figure 51: **hex (low)**, confirm, bothvis, $2^{60}$: Attack #3