Cling - Design #79

privacy related ideas

13.04.2017 07:23 - bernhardz

Status:	New	**Start date:**	13.04.2017
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			

Description

Attack-Vectors:

1.) Some Client which implements the CLING-Protocol collects the interest-profiles from as many persons as possible. If they interests are hashed strings they could be deanonymized easily by a precomputed rainbow table.

2.) A personal movement profile could be collected based on the uniqueness of a cling-installation which will get detected over long time on many spots in the world

ad 1.) Method: "Byte4Byte-Reveal"

Assumptions:

- interests are stored as a list(map) of hashed strings
- communication protocol has cheap roundtrips (or switch from a phone2phone to a TCP-Connection)

Goal:

Alice and Bob will check if the have the same hashes in their maps without transferring the complete hashes to the other.

Alice Hashes:

c5e1e375404e82cfd0434d0542cbbe50d28ee4bc88b84f26123c33650779287d (cars)
17c42f4f137875367fd2df5b95f60dd0f12382549026e71caf0ced27d3c77897 (vw-bully)
9910eefa7940ddab19d4df8018b8ea07cb53d56a233417f81f7a39a07e5cdd42 (acdc)

Bob's Hashes:

a9ce7b1074290c1cdf0546f34d8d8a94138c37bf53652d242ad8f80f1fff2c6c (oldtimer)
a090a4aa88ad01bc62a3b506a7fb1fe4e5f443253061fd80b061b6623ff613aa (jaguar)
17c42f4f137875367fd2df5b95f60dd0f12382549026e71caf0ced27d3c77897 (vw-bully)
9910eefa7940ddab19d4df8018b8ea07cb53d56a233417f81f7a39a07e5cdd42 (acdc)

Protocol:

Alice -> Bob: Do you have a Hash which start with "c5e"
Bob -> Alice: No, Do you have one which starts with "a9c"
Alice -> Bob: No, Do you have one which starts with "17c"
Bob -> Alice: Yes, does it continue with "42f4f1"
Alice -> Bob: Yes, does it continue with "37875367fd2df5b95f60dd0f12382549026e71caf0ced27d3c77897"
Bob -> Alice: Cool! We have something to talk!
Bob -> Alice: Do you have one which starts with "991"
Alice -> Bob: No, want to stop the compare, because also the number of hashes is a fingerprint which can identify me

ad 2.) "Location-based-ID's"

Goal:

- Users needs to detect if they have already matched their profiles
- Users don't want to broadcast their personal-id over longer time

Behaviour:

- CLING-Client generates a new broadcast-id when he detects a location chance by i.e. new mobile cell, or wlan
- If the client has finished the "Byte4Byte-Reveal"-Method they send the other person an contact-id based on a personal-id and a hash of the list of matches.
  So after the "Byte4Byte-Reveal"-Method they can detect that they are already known to each other.