

Snake: a privacy-aware online social network

Usable end-to-end encryption and anonymity of data at rest

Alessandro Di Federico

30th Chaos Communication Congress

December 28th, 2013

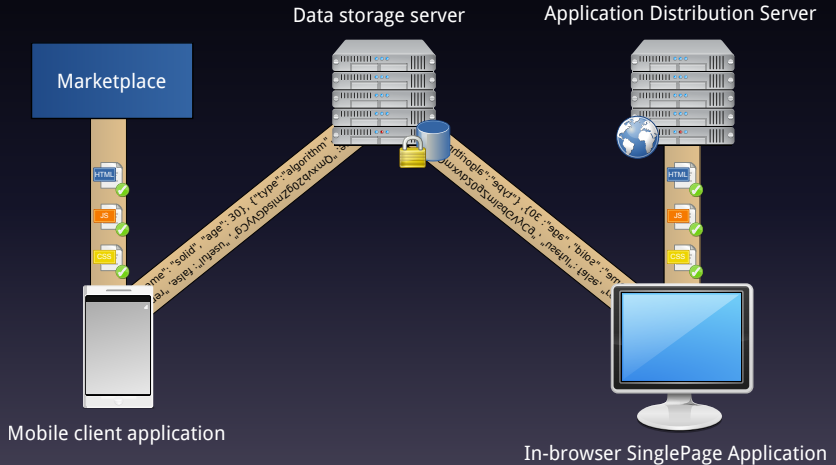
What is SNAKE?

SNAKE is a social network for
end-to-end encrypted
communications

Why do we need it?

Slide intentionally left blank

The architecture



The storage server

- Stores encrypted data
- Serves encrypted data
- It's considered an adversary (for now)

The client

- Encrypts and decrypts all the data transparently
- It's completely written in HTML5 and JavaScript
- Can be easily ported to a plethora of platforms
- It's Free Software!

Isn't cryptography in JS bad?

Not necessarily

Isn't cryptography in JS bad?

Not necessarily

We use WebCrypto API

Isn't cryptography in JS bad?

Not necessarily

We use WebCrypto API

OpenSSL

Mozilla's NSS

MS-CAPI

Our inspiration: OpenPGP



Our inspiration: OpenPGP



It works!

We identified 4 problems in PGP

#1

Usability

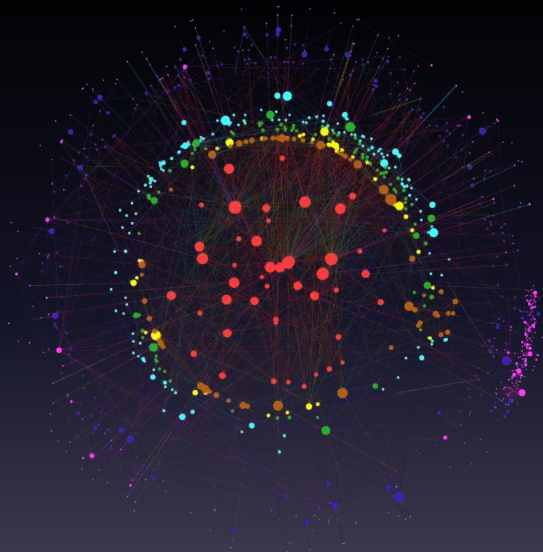
#2

Public key authentication

Key signing party




Manual verification
of public key



2 7 25 98 390

7 6 5 4 3 2 1



roger@firedrake.org
 ivo@iugrpa.com agl@imperialviolet.org
 tom@ritter.vg straluna@email.it me@thijsalkema.de
 freebsd-listen@fabiankeil.de elgaard@agol.dk
 dajhorn@vanadac.com
 lfranchi@gmail.com agl@imperialviolet.org arian@sanusi.de
 lee@colleton.net rlaager@wikifone.com seb@stian.lechte.net
 alessandro.lorenzi@gmail.com moses.mason@gmail.com
 gdt@lexort.com arma@mit.edu seb@stian.lechte.net
 dajhorn@vanadac.com lang@cs.uwaterloo.ca
 rms@gnu.org alexandre.allaire@mail.mcgill.ca
 vmom@riseup.net a@foo.sedehelp@debian.org zackw@panix.com
 adi@hexapodia.org bahn.seb@web.de
 nadim@nadimack.m.daly@gmail.com socio@gmail.com
 smurf@smurf.norfs.de michele@spagnuolo.me
 dmentre@linux-france.org sina@redteam.io me@justinbull.ca
 jz@laquadrature.net gdt@lexort.com
 tedks@riseup.net erinn@torproject.org art@baculo.org
 sean@alexan.org spiegel@gnu.org
 randy@psg.com scheuermann@informatik.hu-berlin.de
 yans86@gmail.com
 turbo@bayour.com aaron.toponce@gmail.com
 cri@linux.it
 astro@spaceboyz.net tss@iki.fi

2 7 25 98 390

7

6

5

4

3

2

1

Direct authentication in Snake

Socialist Millionaire Protocol (SMP)

Direct authentication in Snake

Socialist Millionaire Protocol (SMP)

- It exploits implicitly pre-shared secrets (Q&A)

Direct authentication in Snake

Socialist Millionaire Protocol (SMP)

- It exploits implicitly pre-shared secrets (Q&A)
- It doesn't reveal anything about the secret

Direct authentication in Snake

Socialist Millionaire Protocol (SMP)

- It exploits implicitly pre-shared secrets (Q&A)
- It doesn't reveal anything about the secret
- No bruteforce possible

Web of Trust in Snake

- It's formed by the list of friends of your friends

Web of Trust in Snake

- It's formed by the list of friends of your friends
- Not public!

Web of Trust in Snake

- It's formed by the list of friends of your friends
- Not public!
- Only single step paths

#3

Scalability in group
communication

Comparison of group communication

n : size of the group; m : amount of messages sent in the past

Action	Cost	
	PGP	Snake
Send message	n	1
New group member	m	0
Remove member	0	$\log(n)$

#4

Exposure of
communication metadata

Anonymity of data

SNAKE offers anonymity of data
through suppression of all the public metadata

In practice

For instance, looking at the database is not possible to:

In practice

For instance, looking at the database is not possible to:

- Understand who is the sender of a message

In practice

For instance, looking at the database is not possible to:

- Understand who is the sender of a message
- Understand who is the recipient of a message

In practice

For instance, looking at the database is not possible to:

- Understand who is the sender of a message
- Understand who is the recipient of a message
- Understand whether two users are friend or not

Change of scenario

To guarantee anonymity we have to trust the storage provider

Conclusions

We developed Snake, an online social network providing:

- End-to-end encrypted communications
- Ease of use
- No requirement of out-of-band communication
- Scalability
- Anonymity of data

Our benchmarks there's almost no delay for the end user

Future developments

- Real-time chat

Future developments

- Real-time chat
- Secure file sharing

Future developments

- Real-time chat
- Secure file sharing
- Collaborative online office suite

Coordinates

<http://snake.li/>

Or join me in Hall E

14:30-15:30: YBTI Usability

20:00-22:30: YBTI In Depth

License



This work is licensed under the Creative Commons Attribution-Share Alike 4.0 International License. To obtain a copy of this licence, visit <http://creativecommons.org/licenses/by-sa/4.0/> or send a letter to Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.