Stateless Encryption
GlobaLeaks

A platform that anonymizes whistleblowers as they transmit information to an organization.
Leaked Documents Confirm Ecuador's Internet Censorship Machine

Schedule 32. Chaos Communication Congress

lecture: Ecuador: how an authoritarian government is fooling the entire world

Guess what? The Government of Rafael Correa actually is totally against free-speech and we got proofs on that
The whistleblower

Saw something wrong
Left the office
Connected with a browser
Uploaded files
Filled out a form
Took a receipt
The organization follows up
Asks whistleblower for more information
Organization acts
- Writes a story
- Starts a trial
- Publishes a leak
The big picture
Go after the whistleblower
Go after the journalists
Go after the system
This works for the committed
Improvements can be made
Data stored by server for each submission
Requirements

Decrypt data at rest without client-side software

Admin reqs:
  Add new recipients to existing submissions
  Upgrade existing GlobaLeaks sites

Whistleblower Reqs:
  Store nothing in the browser
New scheme

Offline

- Receiver 1 key
  - prvR1

- Receiver 2 key
  - prvR2

- Receiver 3 key
  - prvR3

Whistleblower Creds
  - pass || R
  - password
  - 1234 5678 9876 5432

Server

- Tip meta data
  - Date, Last Access, Views, Actions

- Files
  - helloworld.txt

- Files
  - pub5

- Comments
  - pub5
  - pubM
  - msg
tut!

- Messages
  - pubR1
  - pubM
  - msg
tut!
Whistleblower’s initial connection

Client

Javascript loads

\( \text{Ca} \leftarrow \text{User input and PoW} \)

Server

\( \text{chooses C} \)

\( \text{checks } f(C) = \text{Ca: issues } T \)

\( T \to \text{foo} \)
Whistleblower creates submission

Whistleblower

\((\text{prvW}, \text{pubW}) \leftarrow \text{KeyGen()}\)
\((\text{prvS}, \text{pubS}) \leftarrow \text{KeyGen()}\)

\(\text{Pass} \leftarrow \text{MakePassword()}\)
\(R \leftarrow \text{ReceiptGen()}\)
\(Rk = \text{Scrypt}(R||\text{Pass}, s)\)
\(\text{pub_lst} = [\text{pubR1}, \text{pubR2}, \text{pubR3}]\)

\(\text{Enc(\text{pubS}, \text{file})\, stores\, \{\text{Enc(\text{pubS}, \text{file})} \ldots \}\, \text{Server}}\)

\(\text{T} : \text{T}\)

\(\text{PassEnc(Rk, \text{prvW})\, \text{Hash(Rk)\, Enc(\text{pub_lst, prvS})}}\)

\(\text{saves R\, \text{Server}}\)

\(\text{stores \{ PassEnc(Rk, prvW), \ldots \}\}}\)
After creation of submission

\[
\text{Hash(Scrypt}(R, s) \Rightarrow \{
\text{Enc}(\text{pub}_1\text{st}, \text{prvS}),
\text{Enc}(\text{pubS}, \text{file}),
\text{PassEnc}(Rk, \text{prvW}),
\ldots
\ldots
\}
\]
Whistleblower Access

1) Uses Credentials to authenticate
2) Decrypts prvW
3) Decrypts comments and messages
Whistleblower receipt authentication

Whistleblower

\[ R \leftarrow \text{paper} \]
\[ \text{pass} \leftarrow \text{brain} \]
\[ R_k = \text{Scrypt}(R||\text{pass}, s) \]

\[ \text{prvW} = \text{PassDec}(R_k, \text{PassEnc}(R_k, \text{prvW})) \]
\[ \text{msgs} = \text{Dec}($\text{prvS}$, $\text{enc_msgs}$) \]

Server

\[ \text{Hash}(R_k) \]

\[ \text{check Hash}(R_k) \text{ exists} \]
\[ \text{fetch Enc(prvW, msgs)} \]

\[ \text{Enc}($\text{pubS}$, new_file) \]
\[ \text{Enc}($\text{pubS}$, new_msg) \]

store
Bad Case time

Scrypt\((n=14, \, r=8)\)
- Uses 256 MB memory
- 17 H/s in python on laptop
- ~250 ms in JS

ASIC speed: 10 KH/s
Number of asics manufactured 50000.0
Attacker scrypt rate: 0.5 GH/s

0-9  4532  6980  2034  4294
Hex  3de5  12a9  b443  6ff1
Base 58  CNbt  MDqc  w6o5  GNn4
Keys on system
1) Authenticate and decrypt prvR1

2) Decrypt prvS

3) Decrypt files, comments, msgs
Side Notes

Adding new users

Recipient Environment

PassEnc()

Receipt size
Scrypt limits
Argon2
Questions, Quandaries?

OFTC #globaleaks

contact@logioshermes.org

www.globaleaks.org

www.github.com/globaleaks

synnick: A6BD 2D38 7F39 236C A9CB 0F86 DD77 3D6D 7326 078E
Sources

This presentation:  http://nskelsey.com/glbc-2016.pdf

GLBC spec:  https://docs.google.com/document/d/1Shdxubex1FPKedhO28i0RvnejHSiQU41ma5B0DSs2xsQ/pub


ASIC fab quotes:  http://asic-cost-calculator.sigenics.com/

Ecuador announcement:  https://events.ccc.de/congress/2015/Fahrplan/events/7134.html