

TOP SECRET//SI//REL FVEY



# ***Exploiting Facebook traffic in the passive environment to obtain specific information***

NAME REDACTED

Capability Developer  
Global Telecommunications Exploitation (GTE)  
GCHQ

TOP SECRET//SI//REL FVEY

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK  
information legislation. Refer disclosure requests to GCHQ

CONTACT INFORMATION REDACTED

TOP SECRET//SI//REL FVEY



## Why OSNs?

- Targets increasing usage of Facebook, BEBO, MySpace etc.
- A very rich source of information on targets:
  - Personal details
  - 'Pattern of Life'
  - Connections to associates
  - Media

TOP SECRET//SI//REL FVEY

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on

CONTACT INFORMATION REDACTED

TOP SECRET//SI//REL FVEY



## Looking to the Passive Environment



- Many targets on Facebook lock down their profiles, so it is not possible to view all of their information...

**But passive offers the opportunity to collect this information by exploiting inherent weaknesses in Facebook's security model.**

TOP SECRET//SI//REL FVEY

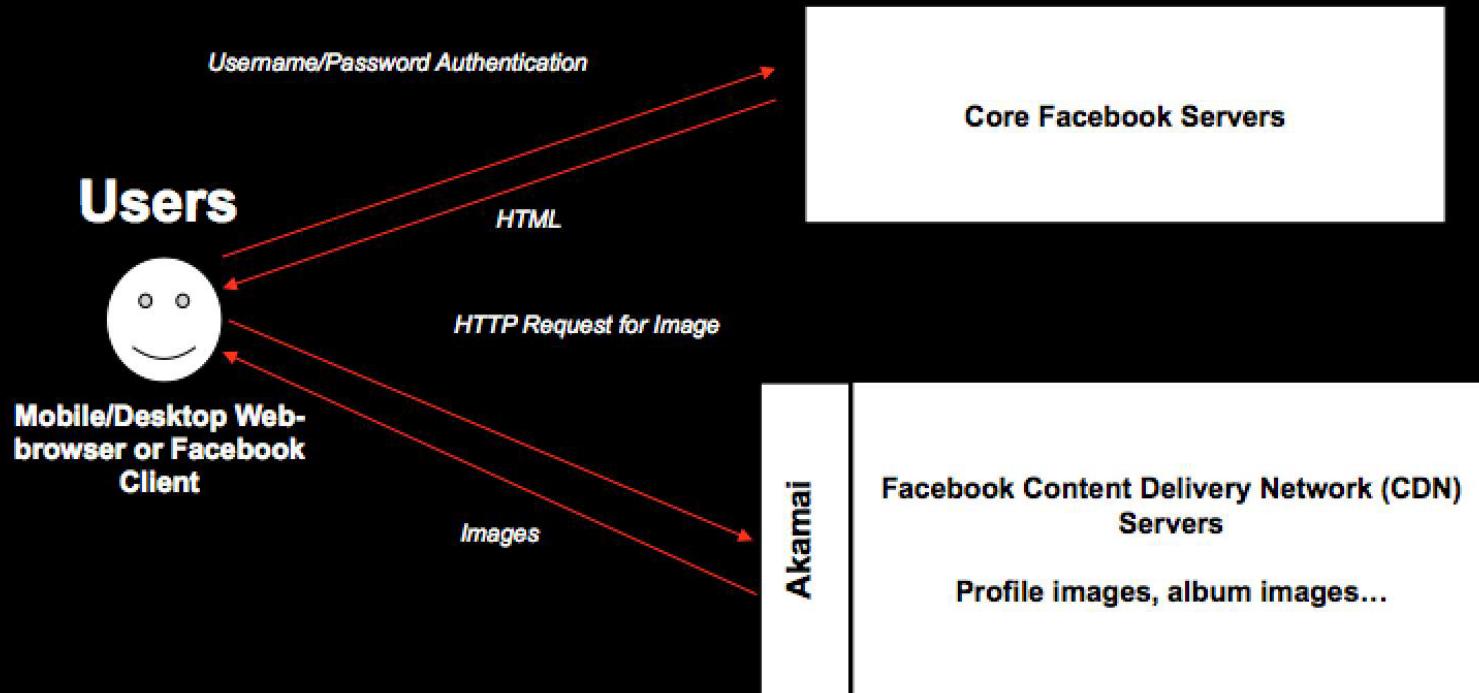
This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on

CONTACT INFORMATION REDACTED

TOP SECRET//SI//REL FVEY



## Facebook's use of the Akamai CDN



TOP SECRET//SI//REL FVEY

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on

CONTACT INFORMATION REDACTED

TOP SECRET//SI//REL FVEY



## Exploiting the FB CDN

- Weaknesses
  - Assumed Authentication
  - Security through obscurity

It is possible to dissect the CDN URL's generated by Facebook in order to extract the Facebook User ID of the user whose picture the file pertains to. For example, below is a typical profile image URL:

[http://profile.ak.fbcdn.net/hprofile-ak-sf2p/  
hs621.snc3/27353\\_ REDACTED 2215\\_q.jpg](http://profile.ak.fbcdn.net/hprofile-ak-sf2p/hs621.snc3/27353_2215_q.jpg)

The text highlighted in green specifically relates to the specific server within Facebook's CDN.  
And the text highlighted in yellow is the users Facebook User ID.

TOP SECRET//SI//REL FVEY

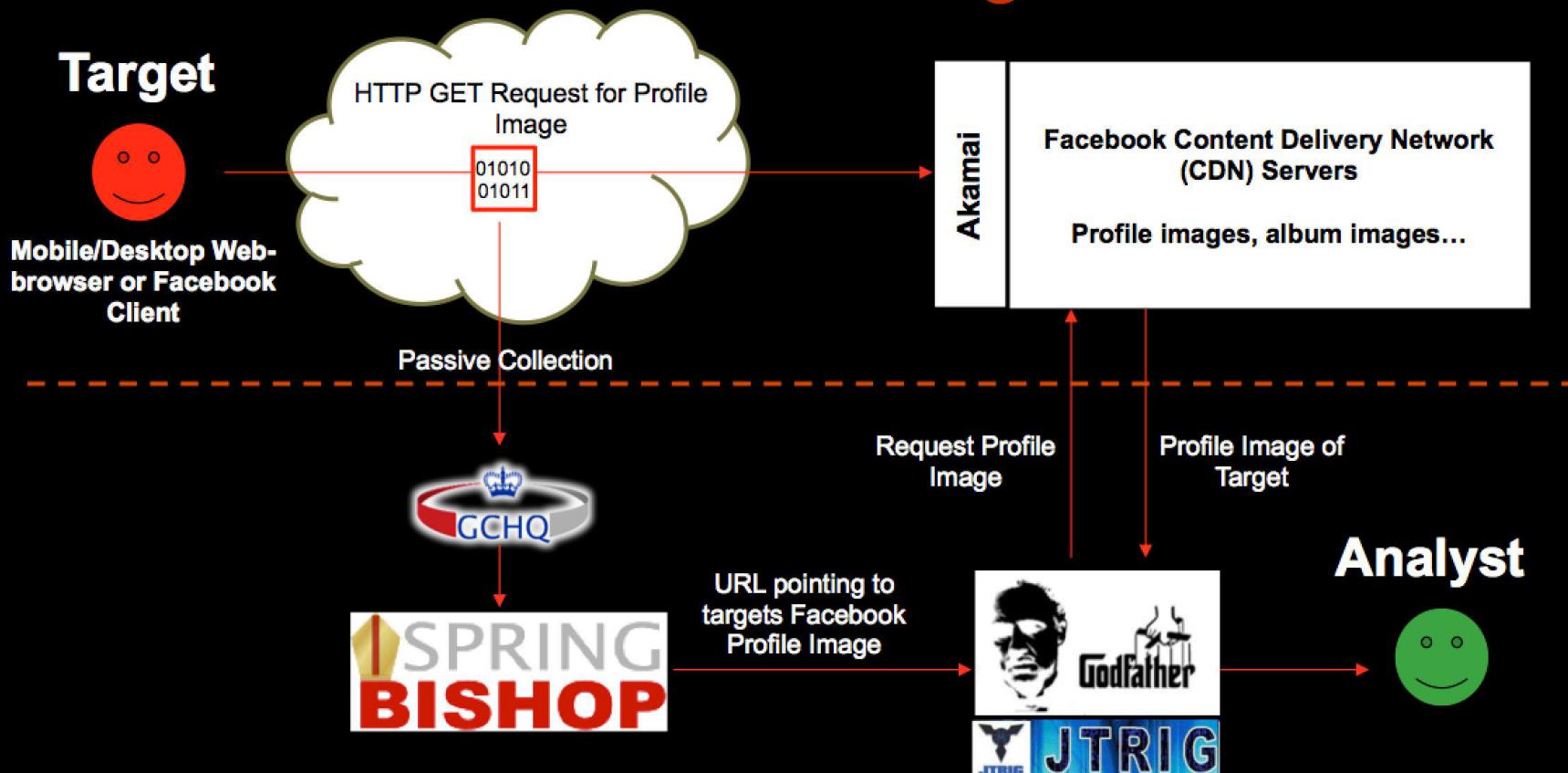
This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK  
information legislation. Refer disclosure requests to GCHQ on

CONTACT INFORMATION REDACTED

TOP SECRET//SI//REL FVEY



## Obtaining profile and album images



TOP SECRET//SI//REL FVEY

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on

CONTACT INFORMATION REDACTED