UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

The Citizen Lab

Research Brief
Number 45 – July 2014

Iraq Information Controls Update: Analyzing Internet Filtering and Mobile Apps

Adam Senft, Helmi Noman, Jakub Dalek, Masashi Crete-Nishihata, Ron Deibert

Read media coverage of the report in the Mashable and Threatpost.

Read the Arabic Version / النسخة العربية translated by Cyber Arabs

KEY FINDINGS

- Since our last report, our test results have shown that prominent pan-Arab news sites and a local news portal critical of the central government have been added to the list of filtered content. In addition, test results show that filtering of prominent social network sites was also briefly removed, then restored, on three of the ISPs tested.

- Websites affiliated with or supportive of ISIS and other militant groups remain largely accessible.

- Mobile messaging app FireChat, which has grown in popularity in Iraq since the Internet shutdown and increase in filtering, is highly insecure for sensitive communications. The application transmits messages and stores sensitive user information on the device without encryption, anyone can easily display recent messages on the service, and it is relatively easy to impersonate another user without authorization.

- Our investigation shows that ISIS-affiliated Android application Dawn of Glad Tidings, which has been reported to use consenting user's Twitter feeds to spread ISIS-related information, is a relatively simple app built using a web tool which aggregates ISIS-related RSS/Atom feeds.

INTRODUCTION

In June 2014, we published a report documenting the results of our network measurement tests that found evidence of 20 URLs that were blocked in Iraq following the ongoing conflict with the jihadist group, the Islamic State in Iraq and Greater Syria (ISIS). Our results showed that a number of prominent websites, including Facebook, Twitter, Skype and YouTube, were blocked on three ISPs tested. These tests results

followed earlier reports of filtering in Iraq and of certain regions of the country which had been entirely disconnected from the Internet. The same research also found that websites affiliated with or supportive of ISIS and other militant groups in Iraq were accessible from Iraq.

Since the publication of that report, we have continued to conduct network measurement tests to identify instances of Internet filtering of websites representative of local, regional and international media, local oppositional portals, and websites containing Jihadi materials or supportive of ISIS and other militant groups in Iraq.

In addition to these tests, we have examined two mobile applications that have received significant attention in coverage of the Iraq insurgency. The first, FireChat, is a U.S.-developed mobile messaging platform that facilitates off-the-grid messaging; features which make it ideal in situations where Internet access is restricted, and that has resulted in growing user numbers in Iraq. However, it is crucial that as applications such as FireChat become more popular in dangerous environments like Iraq, that users are informed about the security features and limitations of using such tools. The second application, Dawn of Glad Tidings, is an Android app developed by ISIS that has been reported to broadcast messages using the Twitter accounts of users who install the application.

This post contains three parts.

- Part 1 describes the results of our network measurement tests, which have shown the addition of six URLs to the existing list of 20 blocked URLs, as well as significant fluctuations in the list of websites filtered since June.

- Part 2 is an examination of the FireChat application that shows it does not encrypt the communications or stored data on the device, and permits user accounts to be easily impersonated, a feature that can be exploited by security agencies and rival groups to trap and reveal information about their opponents.

- Part 3 is our analysis of the Dawn of Glad Tidings app that shows contrary to some reports, it is a relatively simple application that aggregates several pre-existing data streams (including YouTube videos, as well as Tumblr and WordPress posts) of ISIS-related information.

PART 1: INTERNET FILTERING

Methodology

We used two methods to determine if and how Internet filtering is being applied in Iraq:

- The first method performs remote lookups of DNS records to identify suspicious results that could be indicative of filtering.
- The second method undertakes remote testing of website accessibility through proxies. We wrote a script that performs a GET request of a list of websites through publicly accessible proxies located in Iraq. We then compare the results of these GET requests with attempts to access the same URLs from the University of Toronto network to identify instances of blocking.

Early reports from Iraq suggested that blocking was performed on some ISPs through DNS tampering. DNS converts domain names (such as “citizenlab.org”) to an IP address (74.208.36.253). If the information in DNS records is tampered with, domain names can resolve to an incorrect IP address, which can lead visitors to a

blockpage. In some cases, it is possible to perform lookups of the DNS records used by Iraq-based ISPs remotely, without being connected to that ISP directly. After performing these DNS lookups, we are able to compare the results for a given domain name with what we would expect to see to identify aberrations.

We performed a lookup of a list we compiled of 1,392 URLs to identify suspicious DNS results. We also did GET requests for these URLs on this list on the publicly accessible proxies we found in Iraq. This list contains content ranging from international news websites, social media platforms, and content specific to Iraq's domestic political, social and cultural context. A full list of URLs tested can be found in the Data section at the end of this post.

Results

Following the publication of our June 2014 report, we have continued to test for website accessibility using proxy servers and testing of DNS nameservers. This testing has documented three notable changes in blocking behaviour since June 2014.

First, on June 20 the websites of Saudi Arabia-based television news channel Al-Arabiya (alarabiya.net) and Qatar-based television channel Al-Jazeera (aljazeera.net and aljazeera.com), were blocked by all three ISPs tested. On July 18, Al Arabiya News Channel condemned the blocking of its website in Iraq saying that Iraqi prime minister Nouri al-Maliki is trying to restrict media freedom and the flow of information from Iraqi citizens amid "the government's successive failures to maintain stability in the country."

On July 2, filtering of all websites tested (with the exception of Al Arabiya and Al Jazeera) appeared to be removed. This change was noted elsewhere although there was no apparent explanation for the change.

Finally, on July 7, filtering of social networking services and other websites resumed, where it has remained until our last tests on July 21. Reports suggested this change was made due to the fact that "the war with ISIS is now [a] media war and the government wants to control those sites to prevent rumours being broadcasted." Local media quoted Iraqi telecom officials as saying that websites of 20 local, regional and international news organizations have been permanently blocked in Iraq as per orders from security officials because the institutions support terrorism. The officials said while the ban on social media is temporary, the blocking of the news websites is permanent. A telecom official later stated that the ban on social media would be lifted for the Eid holiday during the last week in July to allow citizens to communicate, although this official stated it was uncertain if the lifting of filtering would be permanent.

Our most recent round of testing identified a total of six new URLs which we had not identified as filtered in our June 2014 report, consisting of two news outlets — Al-Arabiya and Al-Jazeera — and four websites (herakiq.com, iraqislami.own0.com, muslm.org and hanein.info).

The website Herak Iraq, which means "Iraq [political] movement," reported on June 24, that its website was blocked in Iraq. The website is political and it reports on what it calls the Iraqi Shiite government oppression of Sunni citizens and the counter-Shiite mobilization in Sunni regions. The website "iraqislami.own0.com" is a forum that has been shut down by the hosting service provider, citing violation of its terms and conditions. The domain, which currently only contains a notification of the shutdown, is still blocked. An archived version of the site from June 25 shows that it was a discussion forum apparently run by ISIS. It included information about its operations, reports, and information products promoting its ideology and actions. The site "muslm.org" is an Arabic Islam-oriented news and views portal with no obvious militant content. Finally, "hanein.info" is a discussion forum with mostly militant topics that are critical of the central government in Iraq for being sectarian.

We summarize the changes to the list of blocked websites, per ISP, below:

ScopeSky

Tests of domain name resolution were conducted on the ISP ScopeSky using the nameservers ns1.itc.iq (185.23.153.242) and ns2.itc.iq (185.23.153.243). 19 unique URLs resolved to either 127.0.0.1 (or 'localhost', which refers to the IP address of the user's computer itself) or 185.23.154.26/185.23.153.235, IP addresses on ScopeSky's network which lead to the following blockpage:

Figure 1: Blockpage seen on the ISP ScopeSky

The instances where a tested URL resolved to one of these incorrect IP addresses are indicated in the following table (click image to enlarge):

ScopeSky Blocked URLs

Blocked URL	Date																	
	June 23	June 24	June 25	June 26	June 27	July 2	July 3	July 4	July 7	July 8	July 9	July 10	July 11	July 14	July 15	July 16	July 17	July 18	July 21
www.youtube.com	✖	✖	✖	✖	✖														
www.xroxy.com	✖	✖	✖	✖	✖														
www.whatsapp.com	✖	✖	✖	✖	✖				✖	✖	✖	✖	✖						
www.viber.com	✖	✖	✖	✖	✖				✖	✖	✖	✖	✖						
www.tango.me	✖	✖	✖	✖	✖				✖	✖	✖	✖	✖						
www.strongvpn.com	✖	✖	✖	✖	✖														
www.skype.com	✖	✖	✖	✖	✖				✖	✖	✖	✖	✖						
www.muslm.org														First test of URL → ✖	✖	✖	✖	✖	✖
www.hotspotshield.com	✖	✖	✖	✖	✖														
www.herakiq.com									✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖
www.hanein.info														First test of URL → ✖					
www.facebook.com	✖	✖	✖	✖	✖				✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖
www.dmoz.org	✖	✖	✖	✖	✖														
www.alarabiya.net			✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖
twitter.com									✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖
plus.google.com																✖	✖	✖	✖
iraqislami.own0.com								✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖
ec2-*amazonaws.com	✖	✖	✖	✖	✖														
aljazeera.com						✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖

Proxy testing conducted on this ISP on July 4, 2014 confirmed that this blockpage was displayed when attempting to access "aljazeera.net." However, this proxy testing also noted some inconsistencies in filtering on ScopeSky. While "aljazeera.net" was blocked, "www.aljazeera.net" was accessible.

EarthLink

Tests of domain name resolution were conducted on the ISP EarthLink using the nameserver "ns1.earthlinktele.com" (109.224.14.2) from June 23 to July 21, 2014. During these tests, 19 total URLs resolved to the IP address 192.168.222.66, a non-publicly routable IP address that on Earthlink led to the following blockpage:

Figure 2: Blockpage seen on EarthLink

The URLs that resolved to this address changed frequently. The instances where a tested URL resolved to this incorrect IP address are indicated in the following table (click image to enlarge):

EarthLink Blocked URLs

Blocked URL	Date																		
	June 23	June 24	June 25	June 26	June 27	July 2	July 3	July 4	July 7	July 8	July 9	July 10	July 11	July 14	July 15	July 16	July 17	July 18	July 21
aljazeera.com						✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖
ec2-*-amazonaws.com	✖		✖	✖	✖														
iraqislami.own0.com								✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖
plus.google.com																✖	✖	✖	✖
twitter.com									✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖
www.alarabiya.net			✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖
www.dmoz.org	✖	✖	✖	✖	✖														
www.facebook.com	✖	✖	✖	✖	✖				✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖
www.hanein.info															✖				
www.herakiq.com								First test of URL →	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖
www.hotspotshield.com	✖	✖	✖	✖	✖														
www.muslm.org															✖	✖	✖	✖	✖
www.skype.com	✖	✖	✖	✖	✖				✖	✖	✖	✖	✖						
www.strongvpn.com	✖	✖	✖	✖	✖														
www.tango.me	✖	✖	✖	✖	✖				✖	✖	✖	✖	✖						
www.viber.com	✖	✖	✖	✖	✖				✖	✖	✖	✖	✖						
www.whatsapp.com	✖	✖	✖	✖	✖				✖	✖	✖	✖	✖						
www.xroxy.com	✖	✖	✖	✖	✖														
www.youtube.com	✖	✖	✖	✖	✖														

We conducted proxy testing on four proxies on EarthLink on July 4, 16 and 17, 2014. This testing found some inconsistencies in blocked websites between proxies, and in some cases, it was not possible to confirm the status of a given URL. The following URLs were confirmed blocked, with the blockpage seen above, on these days:

[insert earthlink table]

Similar to results seen on ScopeSky, proxy testing also confirmed inconsistencies in how filtering is applied. In one example, attempts to access "hanein.info" delivered a blockpage, while attempts to access "www.hanein.info" lead to a redirect to "www.google.com."

IQNET

We conducted tests of domain name resolution on the ISP IQNet using the nameservers "nserver1.iqnet.com" (62.201.215.1), "nserver2.iqnet.com" (62.201.215.2), "nserver3.iqnet.com" (62.201.201.201) and "nserver4.iqnet.com" (62.201.201.202). During the testing period, "nserver1.iqnet.com" and "nserver2.iqnet.com" did not allow recursive queries and as a result did not display any abberant results. However, "nserver3.iqnet.com" and "nserver4.iqnet.com" did display abberant results, with a total of 13 unique domains resolving to the non-publicly routable IP address of 192.168.168.168 or displaying that nameserver as the Start of Authority (SOA) for a given domain. Both of these results are indicative of intentional filtering.

The following domains resolved to an incorrect IP address during the testing period (click image to enlarge):

IQNet Blocked URLs

Blocked URL	Date																			
	June 20	June 23	June 24	June 25	June 26	June 27	July 2	July 3	July 4	July 7	July 8	July 9	July 10	July 11	July 14	July 15	July 16	July 17	July 18	July 21
alarabiya.net		✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖
aljazeera.net		✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖
facebook.com		✖	✖	✖	✖	✖				✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖
google.com	✖	✖	✖	✖																
herakiq.com									First test of URL →	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖
iraqislami.own0.com									✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖
muslm.org															First test of URL →	✖	✖	✖	✖	✖
skype.com					✖	✖				✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖
tango.me					✖	✖				✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖
twitter.com		✖	✖	✖	✖	✖				✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖
viber.com	✖	✖	✖	✖	✖	✖				✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖
whatsapp.com	✖	✖	✖	✖	✖	✖				✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖
youtube.com	✖	✖	✖	✖	✖	✖				✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖

Tarinnet

We conducted proxy testing on the ISP Tarinnet on July 11, 2014. There was no evidence of any filtering on this Kurdistan-based ISP.

The lack of uniform Internet policy in Iraq and Iraq's Kurdistan reflects the political division between the central government and the autonomous Kurdistan region. Commenting on a previous dispute over federal Internet regulations, Karwan Sheikh Raza, head of Kurdistan's post and communications department, said a decision from the central government does not apply to Kurdistan. Renesys has noted recently that Kurdistan ISPs are increasingly providing transit for Iraq's international Internet connectivity outside the country. The division between the central government and the Kurdistan region on Internet regulation is likely fueled by Kurdistani efforts to seek independence from Iraq. The president of Kurdistan region asked the region's parliament in July 2014 to start preparing for a referendum on the region's right of self-determination.

PART 2: FIRECHAT

Since the increase in website filtering and complete shutdown of the Internet in some regions, the mobile messaging platform FireChat has garnered attention for its growth amongst Iraqi Internet users. Reports have suggested that the application has been downloaded 40,000 times in the country since June 14, making Iraq the second biggest user of the application after the United States. Additional reports have indicated that some 7,000 new chat rooms have been created in Iraq within a few days in June 2014, almost 10 percent of the total rooms created globally since the application launched in March 2014.

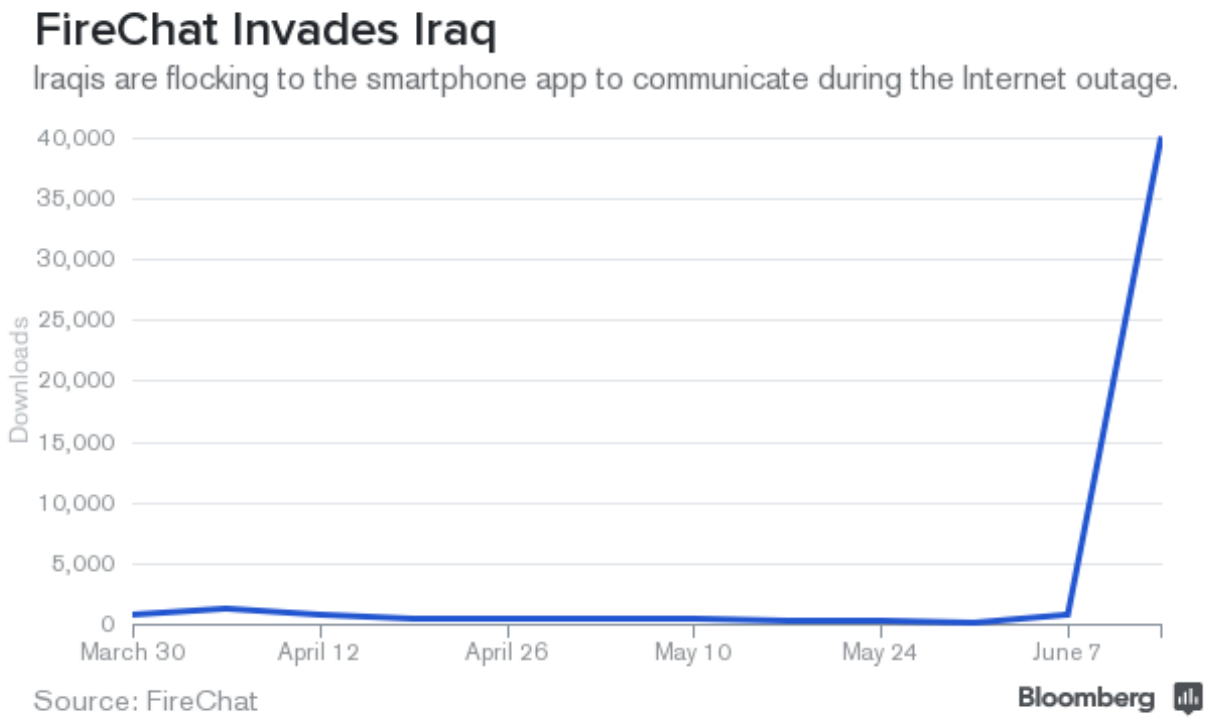


Figure 3: Increase in users of FireChat in Iraq. [Source: Bloomberg]

The FireChat app purports to be a tool for chatting "off-the-grid", allowing users to message anyone nearby, even without a mobile or wireless Internet connection. It does this through a device's Bluetooth functionality or Apple's Multipeer Connectivity framework (on iPhone devices) to permit users to continue to chat off-the-grid with users up to 200 feet away. The application's Google Play store listing describes "live and anonymous discussions" with "no Facebook or email login, no password to remember".

The initial reports about the growing popularity of FireChat described the benefits it could offer users in this restricted environment. Christophe Daligault, vice-president of sales and marketing at Open Garden, developer of FireChat said, "There are enough users of FireChat in Baghdad now to create many local 'intranets'. Even if no device in this local network has access to the internet, people can still exchange messages'. However by June 25, 2014, FireChat's developers acknowledged the potential security risks of using the application for sensitive communications:

"People need to understand that this is not a tool to communicate anything that would put them in a harmful situation if it were to be discovered by somebody who's hostile," he said. "It was not meant for secure or private communications."

Tools to facilitate communications during a conflict, particularly when a growing number of popular platforms remain filtered and in some regions the Internet is shut down entirely, are of crucial importance. In such an unstable environment, users may look to new tools and methods that allow them to communicate with each other, and to document and share the events occurring inside Iraq to the outside world. However, such tools can be a double-edged sword. Insecure tools can expose the sensitive communications of users and leave unencrypted data present on a user's device. As a result, it is crucial for users of such tools to understand any potential security features and limitations. We describe some of these features and limitations in more detail below.

Analysis

We tested version 2.5.1 of FireChat, which was last updated on June 20, 2014. We downloaded the application from the Google Play Store on July 10, 2014. The MD5 checksum of the APK file is: 5e928f558b8fda6d92f4b54218f1335c. We tested the application on an Android phone and used Wireshark to perform packet captures on the traffic sent and received by the application. In order to explain behaviours observed in packet captures, we also decompiled the apk with jd-gui, to explain how messages are generated.

The FireChat application consists of three messaging modes: "Everyone", "Nearby" and "FireChats". "Everyone" is a semi-global chatroom where up to 80 individuals are sorted broadly based on their geographic location. "Nearby" is the function of the application that pairs users who are in close geographic proximity to each other using Wi-Fi, Bluetooth, or Apple's Multipeer Connectivity functions. Finally, "FireChats" are Internet based chat rooms organized around a single theme word.

When starting the application, the user is only prompted to enter a username. After creating a username, the user can begin using the application.

Message transmission

When sending a message in the "everyone" mode, the application begins by doing a DNS lookup of firechat.opengarden.com, which during our testing was hosted at the IP address 209.237.236.194 and is used by a server in California. This is the only IP address that we were able to identify being used to send chat data.

When sending a message through FireChat containing the string "Tcp" with the username "zigzeer", the following traffic is sent to 209.237.236.194 unencrypted and in the clear:

```
..{"uuid ":"b4d96
ba8-7630 -4b97-b9
a5-00663 01dfdb2"
,"t":262 756.375,
"msg":"T cp","fir
echat":" Everyone
","name" :"zigzee
r"}.
```

Figure 4: Sample of unencrypted traffic sent when sending a message in "everyone" mode.

The chat model of FireChat focuses on anonymity at the expense of confidentiality. Throughout the application we see no encryption used, which makes the service inappropriate for sending sensitive communications. However, there is also very little information leaked that could de-anonymize users. For instance, the unique id (UUID) seen in Figure 4 above is unique to that specific message and is not tied to the sender. Instead, it is randomly generated at the time the message is sent, as seen in this decompiled source code:

```
82          try
83          {
84              ayl.e.put("name", s);
85              ayl.e.put("msg", s1);
86              ayl.e.put("firechat", aa.b(s2));
87              ayl.e.put("t", h());
88              ayl.e.put("uuid", UUID.randomUUID().toString());
89          }
90          catch(JSONException jsonexception)
```

Figure 5: Decompiled source code that serializes the chat message JSON object above.

Since no authentication takes place, anyone can read the messages, even from their browser by directly visiting the FireChat IP address on port 4175. As shown below, visiting this IP address in a browser displays the most recent messages sent on one of the "Everyone" public channels:

Figure 6: Chat messages displayed when visiting FireChat server at 209.237.236.194:4175

The most interesting feature of the app is not the Internet-based chat rooms but the "Nearby" mode – the ability to chat peer-to-peer even when no network is present. This communication is also not encrypted. A Bluetooth packet capture of a sample illustrates a discussion between two users "Andrei" and "zigzeer":

Figure 7: Packet capture of communication in "nearby" mode

Users may or may not have an expectation that their communications are encrypted, as there is no user authentication and the service uses pseudonyms. However, it should be assumed that any message sent through the application can be read by anyone in the target range. This can occur whether or not you see other users in the "Nearby" channel, as the Bluetooth packets themselves are unencrypted. In addition, network operators (such as an ISP or mobile provider) can see both the message content and IP address, which can be tied to a user's real name and subscriber information.

Something that is also not made clear in the app is the use of multicast UDP messages during "nearby" chat. Multicast is a network mechanism that allows for one to many communications on IP networks. If you are chatting with someone in the "Nearby" mode and your Wi-Fi is enabled the message you send via Bluetooth is also multicast, unencrypted, on the connected Wi-Fi.

```
0000  01 00 5e 40 00 00 20 64  32 53 2b c4 08 00 45 00   ..^@.. d 2S+...E.
0010  00 97 00 00 40 00 ff 11  af 84 8a 33 51 dd ef c0   ....@... ...3Q...
0020  00 00 1d 98 1d 98 00 83  90 b3 7b 22 75 75 69 64   ........ ..{"uuid
0030  22 3a 22 66 39 61 30 30  34 33 38 2d 33 64 32 63   ":"f9a00 438-3d2c
0040  2d 34 63 38 38 2d 38 66  31 65 2d 32 38 61 34 61   -4c88-8f 1e-28a4a
0050  33 36 38 64 36 64 35 22  2c 22 74 22 3a 32 38 37   368d6d5" ,"t":287
0060  32 30 31 2e 33 34 33 37  35 2c 22 6d 73 67 22 3a   201.3437 5,"msg":
0070  22 4c 69 6e 75 78 20 69  73 20 63 6f 6f 6c 22 2c   "Linux i s cool",
0080  22 66 69 72 65 63 68 61  74 22 3a 22 4e 65 61 72   "firecha t":"Near
0090  62 79 22 2c 22 6e 61 6d  65 22 3a 22 7a 69 67 7a   by","nam e":"zigz
00a0  65 65 72 22 7d                                     eer"}
```

Figure 8: An example of a multicast UDP packet payload in a "Nearby" chat session with Wi-Fi turned on.

It is important to note that only sent messages are mirrored on Wi-Fi, while received messages are not. This would mean that if a user was connected to a public Wi-Fi network while using nearby chat to send a message, even if the message was sent using Bluetooth mode, the message would also be sent unencrypted on the Wi-Fi. Therefore, users are advised to be aware of their Wi-Fi status if they wish to send local messages exclusively.

Data storage

All messages that are sent and received are stored unencrypted on the device in the folder:

/data/data/com.opengarden.FireChat/cache/<CHANNEL_NAME>

This includes conversations in the "Everyone," "FireChats" as well as the "Nearby" Bluetooth mode. This means that if someone's phone is physically examined then all prior chats, including those made offline, are trivial to retrieve.

```
{
    "direction": "SEND",
    "firechat": "Nearby",
    "msg": "Hello",
    "name": "zigzeer",
    "read": true,
    "t": 399429.21875,
    "uuid": "b472fc5b-5b4f-4d77-8499-d9db00fbd8ac"
}
```

Figure 9: A sample message from a "nearby" chat that is retained on the device.

Each user has a unique user id and registration id, which are not sent with individual messages but are stored, unencrypted, on the device at:

/data/data/com.opengarden.FireChat/shared_prefs/com.opengarden.FireChat_preferences.xml

Further, all channels that a user has joined are stored, unencrypted, on the device at:

/data/data/com.opengarden.FireChat/shared_prefs/com.opengarden.FireChat.Application.JOINED_FIRECHATS.xml

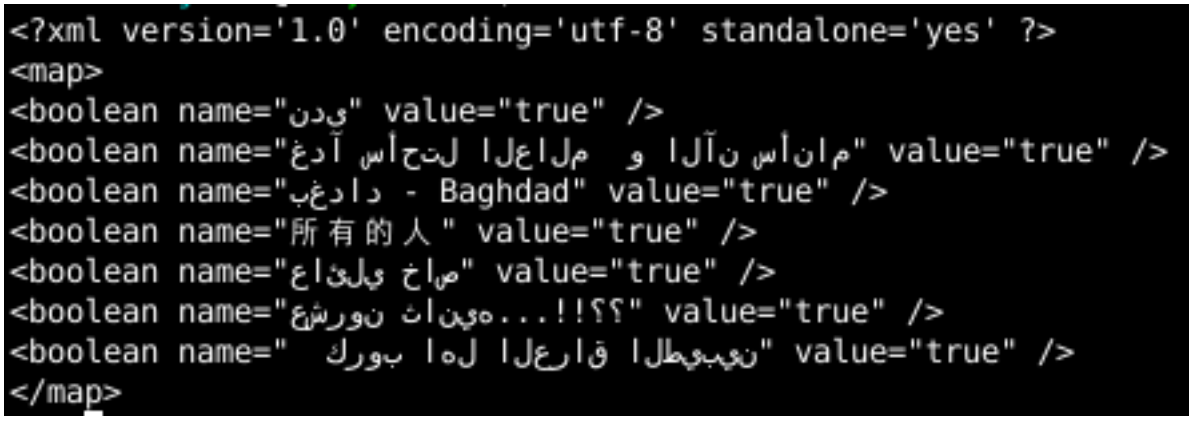


Figure 10: A sample of the joined_firechats file which stores channels a user has joined

Impersonating users

As the application does not authenticate users, there is no attempt to restrict who uses which username. Impersonating other users on the service is trivially done as well by simply forming chat strings in the FireChat JSON format and sending it directly to the FireChat server via the netcat tool. An example of such a string would be:

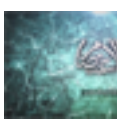
{“name”:”zigzeer”,”FireChat”:”Everyone”,”uuid”:”55555555-5555-5555-5555-555555555555″,”msg”:”Hello World!”,”t”:1623.122977}

Any individual can use this method to change their username and user id. This means that you cannot guarantee that a user you messaged one day is the same person the next. This risk is inherent in any non-authenticated chat system such as FireChat.

Iraqi Surveillance Practices and Context

The issue of the use of insecure telecommunication tools in Iraq is particularly interesting because of reports that local agencies and foreign entities are monitoring telecommunications in the country. In June 2014, local Iraqi media quoted (Arabic) senior security officials as saying that surveillance on telecommunications in Iraq is being conducted by a special security committee that was established in 2013.

The Iraqi Minister of Telecommunications has warned (Arabic) in March 2011 that the telecommunications used by over 90 percent of government staff and officials are monitored by international entities, urging Iraqis not to communicate sensitive issues over the phone. The minister did not name the entities. However, Iraqi parliament members have explicitly accused Iran of monitoring telecommunications in Iraq.

Name	RSS link	Web link	Associated image
عبوة لاصقة	http://gdata.youtube.com/feeds/api/users/UC0E80-y191XlvtBJMxDoebA/uploads?alt=rss&v=2&orderby=published&max-results=50	http://www.youtube.com/channel/UC0E80-y191XlvtBJMxDoebA/videos	
النصرة المقدسية	http://gdata.youtube.com/feeds/api/users/UCGI36g6ClvwH3bshAS37XHQ/uploads?alt=rss&v=2&orderby=published&max-results=50	http://www.youtube.com/channel/UCGI36g6ClvwH3bshAS37XHQ/videos	
الشيخ أبو عمر البغدادي	http://gdata.youtube.com/feeds/api/users/UC_7lZ9yBRTynm7bnTjm0DrQ/uploads?alt=rss&v=2&orderby=published&max-results=50	http://www.youtube.com/channel/UC_7lZ9yBRTynm7bnTjm0DrQ/videos	
أرشيف مؤسسة الإعتصام	http://gdata.youtube.com/feeds/api/users/UC1j6YHUqXl-kk7YPYA3fUWA/uploads?alt=rss&v=2&orderby=published&max-results=50	http://www.youtube.com/channel/UC1j6YHUqXl-kk7YPYA3fUWA/videos	
مؤسسة البتار الإعلامية	http://daawla.tumblr.com/rss	http://daawla.tumblr.com/	
وكالة الأنباء الإسلامية_حق	http://www.dawaalhaq.com/?feed=rss2	http://www.dawaalhaq.com	
شباب التوحيد	http://chababtawhidmedia.blogspot.com/feeds/posts/default?alt=rss	http://chababtawhidmedia.blogspot.com/	
بشائر اليوم	http://gdata.youtube.com/feeds/api/users/UCKJHjixQfQaMkQzmgU8I_bg/uploads?alt=rss&v=2&orderby=published&max-results=50	http://www.youtube.com/channel/UCKJHjixQfQaMkQzmgU8I_bg/videos	
مؤسسة الإعتصام 2	http://gdata.youtube.com/feeds/api/users/e3tsemo/uploads?alt=rss&v=2&orderby=published&max-results=50	http://www.youtube.com/user/e3tsemo/videos	

أخبار الدولة الإسلامية	http://theshamnews.wordpress.com/feed/	http://theshamnews.wordpress.com	
فجر الباشائر	http://el-pashaer.tumblr.com/rss	http://el-pashaer.tumblr.com/	
مؤسسة الاعتصام	http://gdata.youtube.com/feeds/api/users/UC92mC551Ro0iFAwwpHRVNIw/uploads?alt=rss&v=2&orderby=published&max-results=50	http://www.youtube.com/channel/UC92mC551Ro0iFAwwpHRVNIw/videos	
ترجمان الأسا ورتي	http://gdata.youtube.com/feeds/api/users/UChxtUZfNoXbEeGqUDkC87Yw/uploads?alt=rss&v=2&orderby=published&max-results=50	http://www.youtube.com/channel/UChxtUZfNoXbEeGqUDkC87Yw/videos	

In March 2012, an Iraqi parliament member has accused (Arabic) Iran of wiretapping the phones used by some members of the parliament in cooperation with one of the telecommunication companies working in Iraq. He did not name the company. He also demanded that all telecommunication companies operating in Iraq should pledge not to cooperate with any foreign state, adding that Iran can hack into the emails of parliament members and other individuals who oppose its influence in Iraq. Another Parliament Member said they have precise information that Iran has recruited 40 staffers to monitor the telephone lines and emails of 25 parliament members and politicians who oppose Iran's intervention in Iraq.

Moreover, a parliamentary committee revealed in 2012 that Chinese-made, inexpensive telecommunications equipment is widely available on the Iraqi market even though local laws criminalize possession of such equipment and punish those who bring them to the country with up to 10 years imprisonment. Lastly, Iraqi communications are subject to intense surveillance by the United States' National Security Agency, with some reports indicating that the aim of the NSA is to collect every Iraqi email, text message and phone-location signal in real time.

That a large and growing population of Iraqis is using an insecure chat application like FireChat in such a context of widespread and potentially aggressive surveillance practices is certainly noteworthy, and should be a cause for concern for anyone engaging in sensitive communications.

PART 3: ISIS ANDROID APP

We also examined the ISIS-affiliated Android application, Dawn of Glad Tidings, which has been reported to use the Twitter accounts of those who install the app to spread ISIS-related messages. The app was removed from the Google Play Store on June 17, with a Google spokesperson stating "We remove any applications that breach our community guidelines".

Our research has found that the app does not, as reported, automatically connect to a user's Twitter account to post tweets on your behalf. Instead, the app has been built using AppYet, a web-based tool that allows for the creation of simple Android apps that display feeds of information from websites or RSS/Atom feeds. After a

user specifies some basic details about which feeds to incorporate, an APK is emailed that can then be distributed and placed on the Google Play store. Users have the ability to share stories displayed from these feeds, but this sharing does not happen unless instigated by the user.

Once installed the app stores the RSS/Atom links in a SQLite database called data2.db located on the Android device in /data/data/com.pashaeer.myapp/databases/. The database contains six non-empty tables: android_metadata (stores locale), Module (stores name, groupname, icon), sqlite_sequence, Feed (lists the RSS links and web links for each module), FeedItem (individual feeds from source), and FileCache (cached images).

Investigating the application more closely permits examination of the specific feeds the application uses to display information to users. The following RSS/Atom links are displayed by the app, which are listed here alongside the associated name, web link and image:

We included the URLs found in this application to our filtering test list described in Part 1, and none were found to be blocked.

CONCLUSION

The events since our last post on this subject show that access to information in Iraq remains highly contested. As stable access to Internet content — and indeed the Internet itself — remains in flux, users are understandably seeking out alternative means of communication and access to information. However, in such a chaotic context, poor choices can be made on the basis of incomplete information and users can end up putting themselves unintentionally at greater risk by hastily seeking to evade information controls. The rising popularity of FireChat in Iraq is a case in point: the tool is functionally insecure, something even the developers have admitted, and yet users are flocking to it. The Citizen Lab will continue to monitor the situation and post updates to our findings.

DATA

A full list of data from these tests can be found in our GitHub repository.

ACKNOWLEDGEMENTS

Jakub Dalek, Adam Senft, Philip Winter, and Andrei Dranka undertook research and writing of this report, supported by the Social Sciences and Humanities Research Council (Canada) Grant 430-2014-00183, Prof. Ronald J. Deibert, Principal Investigator.