2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/ 2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)

Towards Achieving a Secure Authentication Mechanism for IoT Devices in 5G Networks

Bernardo Santos
Oslo Metropolitan University
Oslo, Norway
bersan@oslomet.no

Bruno Dzogovic
Oslo Metropolitan University
Oslo, Norway
bruno@oslomet.no

Boning Feng
Oslo Metropolitan University
Oslo, Norway
boningf@oslomet.no

Van Thuan Do
Wolffia AS
Oslo, Norway
vt.do@wolffia.net

Niels Jacot
Wolffia AS
Helsinki, Finland
n.jacot@wolffia.net

Thanh van Do
Telenor & Oslo Metropolitan University
Fornebu, Norway
thanh-van.do@telenor.com

***Abstract* – Upon the new paradigm of Cellular Internet of Things, through the usage of technologies such as Narrowband IoT (NB-IoT), a massive amount of IoT devices will be able to use the mobile network infrastructure to perform their communications. However, it would be beneficial for these devices to use the same security mechanisms that are present in the cellular network architecture, so that their connections to the application layer could see an increase on security. As a way to approach this, an identity management and provisioning mechanism, as well as an identity federation between an IoT platform and the cellular network is proposed as a way to make an IoT device deemed worthy of using the cellular network and perform its actions.**

Keywords - 5G networks, mobile identity management, identity provider, cellular IoT, cross-layer security, IoT security

I. Introduction

As we are experiencing the upcoming deployment of 5G networks, one of the goals that it would be interesting to achieve is the inclusion of Internet of Things (**IoT)** devices and their usage of the cellular network as a way to expand their application usage for new scenarios. Though they can facilitate some interactions that we have now for home electronics, health devices, among others, we have been noticing an exponential increase on exploits and attacks targeted to those types of devices due to their simple security mechanisms that usually are quite overlooked and are only addressed when something has happened (e.g. data breach).

More so, as we intend to bring the **IoT** paradigm to the cellular network as to inherit the security benefits from it, there's yet a way for such devices to be secure from the application point of view, as **IoT** applications have separate authentication systems that usually are quite exploitable. Considering all this, there should be a way in which **IoT** devices could share the security mechanisms from the cellular network, making them able to communicate their readings to their corresponding applications in a more secure and trustable way.

For this purpose, this paper proposes a new secure authentication mechanism based on identity provisioning and management of **IoT** devices, in which an identity federation is achieved between the cellular network and **IoT** platforms, enabling an unique and more manageable way to allow devices to perform their actions in a more trustable way. With this solution, our goal is to showcase the benefits of this mechanism as to provide a tool that allows to manage **IoT** devices and applications more easily while also keeping them secured while connected.

To do so, we briefly describe the technologies and procedures that are the basis of this work in II. In III, we describe our infrastructure testbed and also the components developed to achieve our goal, and in IV and V are dedicated to evaluate the procedures that we've developed and some considerations that are needed to be taked whilist implementing the solution. Finally, in VI and VII, we summarize the upcoming work that we will continue developing and also the results of our work thus far.

II. Related Work

A. Cellular IoT

Cellular Internet of Things (**CIoT**) is a fairly new term that describes the process of supporting common IoT connections and services through existing mobile network infrastructures [1][2] by using technologies such as Narrowband IoT (**NB-IoT)**, CAT-M, etc., having in mind the possibility of supporting a massive inclusion of devices while sharing the network's resources, as to support the new ways

978-1-7281-1661-7/19/$31.00 ©2019 IEEE
DOI 10.1109/CSCloud/EdgeCom.2019.000-7

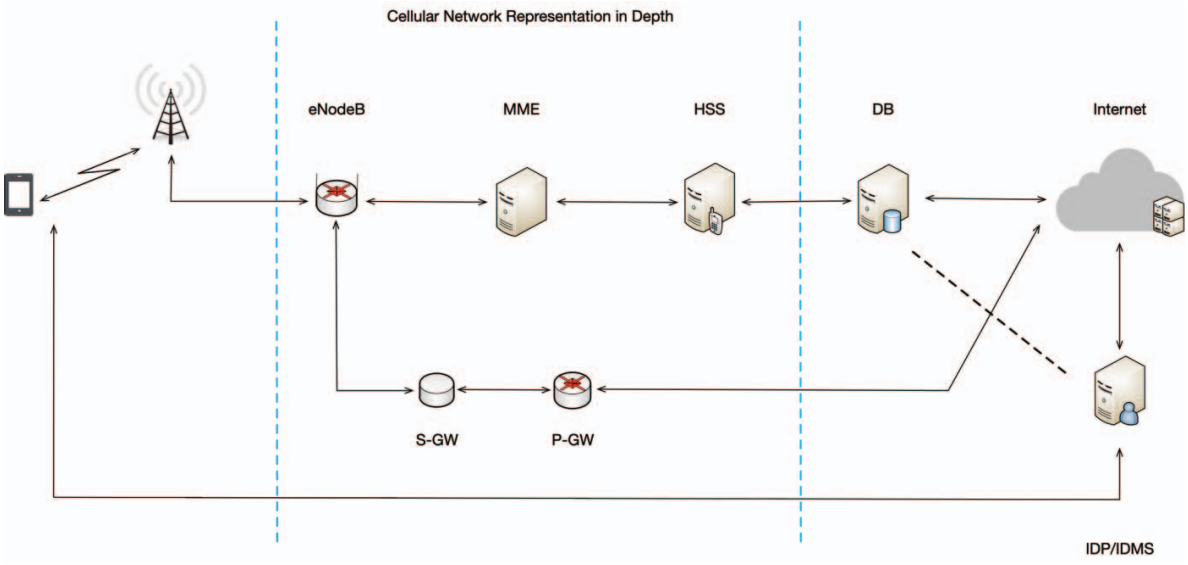

Fig. 1 Representation of proposed implementation

of user interactions that we are witnessing nowadays, from homes with smart meters and security devices (e.g. locks) to the e-health paradigm with the usage of activity trackers and bio-measurement devices, in a way that they are all integrated in one platform and can communicate through the same cellular service. These devices won't be connected to the network all the time, as energy consumption is also something quite relevant, but when their readings have to be communicated to its corresponding **IoT** platform, a connection must be ensured without disrupting others. Also, in [1], a summarized description of such devices and a behavior analysis is made as to better understand their needs.

B. Identity Provision and Management

As it is foreseen that the inclusion of **IoT** devices will achieve significant proportions once the deployment of 5G networks is concluded, there are concerns regarding the lack of proper security measures regarding both the connection and the usage of the network. Even today, security practices are overlooked by major corporations and have suffered data-exposing attacks, which compromises not only the affected corporations but also the individuals that are using their services. In the households, people are still not fully aware of these risks and the available mechanisms are quite cumbersome, which hinders the adoption.

This is also quite noticeable when dealing with **IoT** devices, as reported in [3], several wide spread attacks took place by targeting these devices due to their security mechanisms not being adequate, especially when considering its authentication methods, since most of them are still using basic authentication features with a credential set based on a username and a password. Also, manufacturers use fairly known credential sets that can be easily exploitable and users sometimes aren't aware nor have the technical knowledge to deploy another authentication factor.

As a way to solve this predicament, it would be beneficial to integrate an Identity and Access Management (**IAM**) system that, allied with the security mechanisms provided by the cellular network architecture and infrastructure, would allow **IoT** devices to share the same type of identification and authentication strength [4][5][6] when communicating with an **IoT** platform. Thus, an identity federation between the network layer and the application layer is needed. This federation aims to achieve a common ground on how to identify **IoT** (mobile) devices that are connected to a cellular network towards the application layer, by utilizing the unique identifiers coming from the Subscriber Identifier Module (**SIM**) card.

In order to provide an identity to an IoT device that is connected to the cellular network, so it can also be perceived and authenticated by the application layer, it is necessary to ensure that the device is registered in the network through its **SIM** card, meaning that is necessary to reach the network's Home Subscriber Server (**HSS**) (and its database) to see if there is any record - in this case, a database row that contains information regarding a registered SIM in the network and the device associated to it. Such information (e.g. IMSI, IMEI, among others) are identifiers that will help the identity management system identify a device connected to the network - that can match to the one that is trying to authenticate. However, this access to the component, or rather the access to the relevant data must be made in a way that no compromise nor data exposure can happen in any of the layers (Network and Application).

III. Proposed Solution

Our main objective, as it has been explained thus far, is to have an authentication mechanism that can be applied to **IoT** devices so that their communications can be secure and be protected from possible exploits. This means that such a device has **USIM** capabilities and can directly use the known cellular network mechanisms.

It is important to provide an identity to each **IoT** device connected to the network so that they can be authenticated when trying accessing the application layer (which in this case is where an **IoT** platform will reside). In order to do so, we are adding to our network architecture an identity management/identity provider server [7] that will take care and manage the identities of all **IoT** (mobile) devices that are or will be registered in the network. **Error! Reference source not found.**

A. Network Architecture – Cloud-Based Infrastructure

The infrastructure is based on OpenStack cloud instituted by Mirantis [8]. On the top of the OpenStack cloud, the Evolved Packet Core (**EPC**) service runs in a Docker [9] container, which connects directly to the Neutron service. From a remote location, we connect the base station – Evolved Node B (**eNB**) through an Edge rack, via public IP. The **eNB** is split into two segments: Remote Radio Unit (**RRU**), i.e. the radio frontend and Baseband Unit (**BBU**), the centralized processing of the radio sampling. The communication between the **RRU** and the **EPC** is redirected through the **BBU** Docker container, residing in the network edge.

The centralized unit utilizes the Calico BGP [10] networking, which can talk to the remote **EPC** deployed in the OpenStack cloud. The mechanism that allows inter-container direct link is the bypassing of layer-2 stacks created by the Open vSwitch [11] (**OvS**) in the OpenStack Neutron; namely, the plugin Kuryr integrates the Docker daemon with the **OvS** by authenticating the virtual machine with the Keystone service. It provides access to the Neutron networking with the specific user that is assigned to. As Kuryr is integrated with the Docker daemon in the VM, now it has relevant control for creating and editing Neutron networks in the specified user.

B. IDP/IDMS Server

This component will be responsible for issuing the identities for every **IoT** (mobile) device that will be registered in the network. In order to have this link between the Identity Provider (**IDP**) server and the cellular network, it is necessary to achieve an agreement and a consensus as to how to identify the **IoT** devices so that they can communicate with the **IoT** platform in a more secure and trustable form.

In order to identify and authenticate an **IoT** device, the **IDP** has to check if there's such a **SIM** registered in the cellular network (that is associated to an **IoT** device), by consulting the database managed by the **HSS**, which has all the records of registered devices. This access between the **IDP** and the **HSS** cannot have a direct repercussion on the normal behavior of the cellular network, so it cannot be a simple yet direct link between both components. To overcome this, an interface between the cellular network and the **IDP** is deployed - in the form of an Application Programming Interface (**API**) or by creating a secure replica of the **HSS**'s database exclusive to the **IDP**'s usage – so that it is possible to achieve a federation from the network side.

If there's a match, an identity will be issued for such device and will have access to the network and its resources. Fail to do so and if there isn't an alternative for a device to prove itself, an identity won't be issued. This identity is none other than a set of key-pair values that can be defined by an administrator, and by using the OpenID Connect [12] protocol, it gives the versatility needed upon identity creation and enough flexibility to be used in a mobile/**IoT** context.

1) Gluu Server

Gluu Server [13] offers identity management and provision services that allow to establish authentication mechanisms in network resources. More so, it has an integration plugin that allows to sync user information from an Active Directory (**AD**) [14] or Lightweight Directory Access Protocol (**LDAP**) [15] capable servers, which can have access to database information such a list of users or phone numbers. This is called **LDAP** Synchronization [16].

Another tool that Gluu provides to promote this interoperability is the System for Cross-Domain Identity Management (**SCIM**) specification that aims to reduce the complexity of user management operations by providing and common and easy-to-use user schema through a convenient **API**. With the usage of the User Managed Access (**UMA**) tool, which defines interfaces between authorization servers, a server that protects resources, such as the Gluu Server, it enables a more secure and scalable way to deal and manage with identity management [17][18].

C. IoT Platform

In order to deliver their readings, **IoT** devices have to communicate with an **IoT** platform. To avoid and mitigate the security issues that have been discussed thus far, the authentication method would have to change as to support and share the same mechanisms from the cellular network in a way that when a device is trying to authenticate towards the platform, instead of simply using a credential set, the platform will inquire an **IoT** device regarding its identity. Upon receiving an "identity proposal", the platform will communicate with the **IDP** as to ascertain the identity's authenticity – this is where the federation from the application layer side takes place as both the **IoT** platform and the **IDP** will communicate with each other to verify an **IoT** device's identity upon request – if there's a match, the platform will allow the **IoT** device to proceed with its actions and it is possible to consider it secure and trustable.

D. API Implementation

For the purpose of this specific work, and as described above, a way to achieve an identity federation between the cellular network and the **IoT** devices and, subsequently the corresponding platforms is to first achieve a federation between the network and the **IDP**. To that, a federation

integration **API** prototype (*5G4IoT Federation API*) was developed. Some pre-requisites are necessary to ensure the development of this **API**: **1)** the creation of a read-only access to the secure replica of the HSS' database as to limit possible exploits, **2)** the understanding of the procedures behind the **SCIM** client provided by Gluu [13] and **3)** some understanding of the Java [19] programming language.

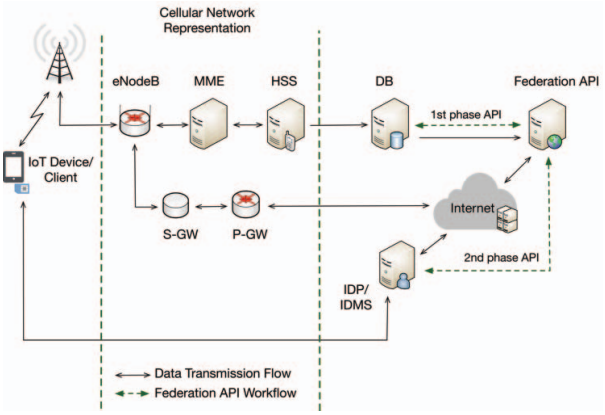

Fig. 2 API phase representation[1]

1) 1st Phase

To bridge the components, the first process is to query the existing registries in the secure replica and obtain only the necessary data that can be used as identifiers (e.g. **IMSI**/**IMEI**).

2) 2nd Phase

With the data obtained from the secure replica, the **IDP** will be queried about the possible existence of an identity. When positive, as of now, it is disregarded and the **API** moves onto another entry, but this is where we can update the identity if something relevant from the network side has arisen. When the **IDP** does not have a match for the queried identifier, it means that an identity must be issued, however it won't be immediately active and ready to use by a device before further proceedings (which will be described in a future work). This identity will be filled with the relevant data and, as a fallback access procedure, a randomly generated strong password will be associated to it.

Upon defining this identity in the API, a creation request is made to the **IDP**, which will confirm (or not) the success of the operation. When successfully created, this identity is recorded in the **IDP** and after further confirmation and activation, it can be used by an **IoT** platform for device verification and validation. Both the **IDP** and the **IDMS** will then deal with a device's identity as intended, even in a case of blacklisting.

To summarize the description of the functionalities of the developed API, a flow diagram is presented (*Fig. 3*).

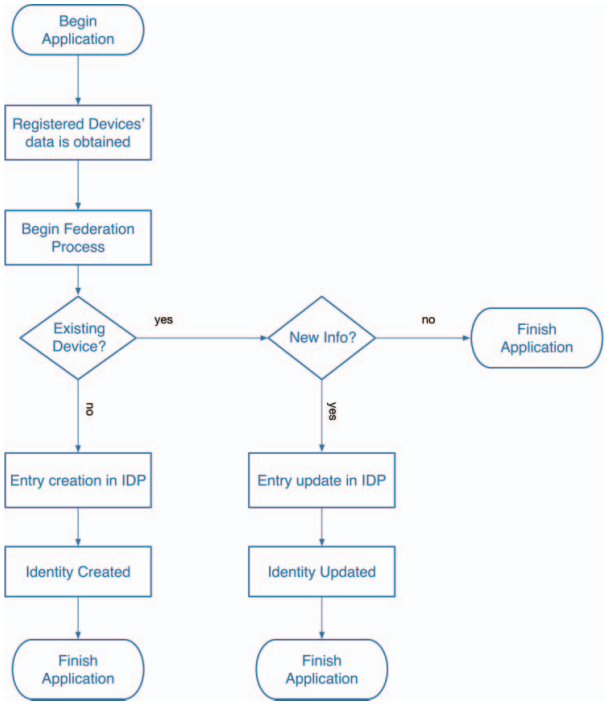

Fig. 3 API flow diagram

IV. Evaluation

In order to consider the proposed solution feasible, it is necessary that the developed **API** does not demand too much resources and performs significantly well. However, it is worth noticing that this is not something that will be running all the time, it should be used when the secure replica has new entries and thus new identities should be created or, in some cases, updated.

Having our testbed network in our 5G4IoT laboratory in the Oslo Metropolitan University, we have all the components mentioned in the proposed solution integrated where test mobile devices have been connected to study their performance while connected to the network. Will all these tests thus far, 48 entries have been accumulated in the network's **HSS** and subsequently in the secure replica. With our tests to our **API**, we were able to assert that for the federation process for all these entries, it performs around **3/4** seconds. The time performance was noticed when verifying identity updated (for the whole lot) and even for deletions.

```
[2019-04-05 16:19:39] [SCIMClient] [INFO] Beginning federation process!
[2019-04-05 16:19:40] [SCIMClient] [INFO] Creating 48 new identities....
[2019-04-05 16:19:44] [SCIMClient] [INFO] Finished creating identities!
[2019-04-05 16:19:44] [SCIMClient] [INFO] Finished federation process!
```

Fig. 4 Outcome example of the federation API - creation

[1] For the purpose of this illustration, the secure database replica and the federation API are represented seperatly, but in the implementation itself, they are deployed in the same machine.

```
[2019-04-05 16:32:31] [SCIMClient] [INFO] Beginning federation process!
[2019-04-05 16:32:32] [SCIMClient] [INFO] Deleting 48 identities....
[2019-04-05 16:32:35] [SCIMClient] [INFO] Finished deleting identities!
[2019-04-05 16:32:35] [SCIMClient] [INFO] Finished federation process!
```

Fig. 5 Outcome example of the federation API - deletion

It will be noticeable that, when trying to federate a significant number of devices between the secure replica and the **IDP**, the operation time will follow suit by taking a longer time. It is important to consider that this process isn't something that will affect the network's performance and availability, so it is considered a manageable cost. The bottle neck of this process is the representational state transfer (**REST**) calls from the **SCIM** client that are needed to be used in order for this **API** to function. It is impossible to avoid the iteration between entries as to verify if an identity has been issued to it, or if there's a need to create one, which requires a second **REST** call.

Despite the presented results and considering the possible impacts, the presented **API** provides good performance results, but having always some room for improvement in the future.

V. Discussion

With this federation, it is possible to achieve a secure way to authenticate **IoT** devices in an IoT platform, accessible through the Application layer, meaning that a common ground was obtained as to identify an **IoT** device that is connected to a cellular network.

There are two other issues regarding security and privacy addressed in [20], one of which is related to OpenID Connect identifiers and its reusability. This can be an exploit if such situation is allowed, but for the proposed solution, all identifiers will be unique, even if an **IoT** device shares some common details with another (e.g. device's owner), meaning that there are still different and enough elements that allow each identifier to be exclusively associated to each device.

Another concern regarding privacy was due to the fact that, in [20], the third-party identity providers that were used were from Google [21] (using OpenID Connect) and Facebook [22] (with a proprietary solution called Facebook Connect). The issue is that all data that goes through both providers may be stored by study/analysis purposes which means that it may occur that parts of a device's identity may be stored by either of these providers and their policies aren't quite clear on that department.

For the proposed solution, as we used Gluu Server, it is stated [23] that some of the device's data can be collected for security purposes, which can be classified as *de-identified data*. However, we have total access to the generated identities from the server and such information is exclusively used and owned by the device owner (its own identity) or the system administrator, which means that all identified data is not collected nor used by the platform.

VI. Future Work

By continuing the work that has been described thus far, we will proceed with the federation process between the **IDP** and the **IoT** platform, allowing us to complete the integration between all major components. By doing so, this will allow a unified device identification between the Network and Application layers.

With the previous step concluded, our testbed will undergo through several testing procedures, which allow us to make more reports on our findings. Lastly, to have a more in-depth insight on all types of devices that are able to use the network, we will also include more devices to our tests and analyze all the possible outcomes and present them afterwards.

VII. Conclusion

The **5G** network deployment will allow to shift the **IoT** paradigm to a purely cellular based context, so that the devices would be linked through a **SIM** and would benefit from the security mechanisms that a cellular network can provide towards authentication in the application layer. By achieving the proposed federation, it is possible to have an issued identity that it can be confirmed by the network' services and granting it access to the proper and necessary resources, so that the data that is obtained from the device to the **IoT** platform is considered trustworthy and secure. This will allow to have **IoT** devices connected in such a way that, while being completely manageable through their identities, they can be used in various contexts (also known as verticals) that will allow their massive yet secure integration in this upcoming network generation.

Acknowledgment

This paper is a result of the H2020 Concordia project (https://www.concordia-h2020.eu) which has received funding from the EU H2020 programme under grant agreement No 830927. The CONCORDIA consortium includes 23 partners from industry and other organizations such as Telenor, Telefonica, Telecom Italia, Ericsson, Siemens, BMW, Airbus, etc. and 23 partners from academia such as CODE, university of Twente, OsloMet, etc.

References

[1] J. S. Kim, S. Lee, and M. Y. Chung, "Time-division random-access scheme based on coverage level for cellular internet-of-things in 3GPP networks," *Pervasive Mob. Comput.*, vol. 44, pp. 45–57, 2018.

[2] Z. Ning, X. Wang, X. Kong, and W. Hou, "A social-aware group formation framework for information diffusion in narrowband internet of things," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1527–1538, 2018.

[3] S. Boddy and J. Shattuck, "The Hunt for IOT: The Growth and Evolution of Thingbots Ensures Chaos,", F5 Labs, Seattle, Washington, USA, 2018 - https://www.f5.com/labs/articles/threat-intelligence/the-hunt-for-iot-the-growth-and-evolution-of-thingbots-ensures-chaos.

[4] 3GPP: TS 11.11 Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) Interface, ver 8.14.0, 12-06-2007

[5] 3GPP: TS 31.102 Characteristics of the Universal Subscriber Identity Module (USIM) application ver 16-06-2017

[6] 3rd Generation Partnership Project: 3GPP TS 33.220 V8.2.0 (2007-12) Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA) Generic bootstrapping architecture (Release 8)

[7] B. Santos, V. T. Do, B. Feng, and T. van Do, "Towards a Standardized Identity Federation for Internet of Things in 5G Networks," in *2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, 2018, pp. 2082–2088.

[8] OpenStack Mirantis - https://www.mirantis.com/

[9] Docker – https://www.docker.com

[10] Calico BGP - https://www.projectcalico.org/why-bgp/

[11] Open vSwitch - https://www.openvswitch.org/

[12] OpenID Connect - https://openid.net/connect/

[13] Gluu Server – https://www.gluu.org

[14] Active Discovery - https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis

[15] LDAP - https://ldap.com/

[16] Gluu LDAP Synchronization – https://www.gluu.org/docs/ce/user-management/ldap-sync

[17] Gluu SCIM 2.0 User Management – https://www.gluu.org/docs/ce/user-management/scim2

[18] Gluu UMA 2.0 Authorization Server – https://www.gluu.org/docs/ce/admin-guide/uma

[19] Java Programming Language – https://www.java.com

[20] G. C. Batista, C. C. Miers, G. P. Koslovski, M. A. Pillon, N. M. Gonzalez, and M. A. Simplicio, "Using Externals IdPs on OpenStack: A Security Analysis of OpenID Connect, Facebook Connect, and OpenStack Authentication," *2018 IEEE 32nd Int. Conf. Adv. Inf. Netw. Appl.*, pp. 920–927, 2018.

[21] Google – https://www.google.com/

[22] Facebook – https://www.facebook.com/

[23] Gluu's Privacy Policy - https://www.gluu.org/privacy-policy/