VirnetX

Gabriel Secure Communications™
and
Gabriel Collaboration Suite™

Enabling Your Safe Neighborhood

March 2016

White Paper

GABRIEL
SECURE COMMUNICATIONS

"Take back your digital life."

Introduction

OUTLINE

- INTRODUCTION
- GABRIEL TECHNOLOGY
- GABRIEL SECURITY PLATFORM
- GABRIEL COLLABORATION SUITE
- SUMMARY

The Internet has become an integral part of people's lives today with wide spread use for commerce, business, news and information dissemination, as well as daily social networking. This wide spread use and dependence upon the Internet has brought major challenges to maintaining privacy and security for both individuals and companies. The use of mobile computing with centralized cloud storage has only exacerbated these challenges by providing hackers with information rich targets to extract sensitive data for large numbers of individuals and companies, which can be used for a wide range of nefarious purposes (e.g. identity theft, credit card fraud, corporate espionage, personal data mining, etc.). This white paper presents both a network security technology, designed for current and future demands and an application suite built upon this technology that enables both individuals and organizations to take back control of their personal and sensitive data, thereby protecting themselves from these attacks.

VirnetX Holding Corporation (VirnetX) has released a real-time secure communications product called Gabriel, which provides end-to-end encrypted communication between any two devices on the Internet and intranet. Gabriel is based upon patented technology, which enables instant private and secure connections for ANYONE, ANYTIME, and ANYWHERE across the Internet/intranet. This allows users the ability to privately chat, talk, and share information regardless of where the users are located or the devices being used. Included are smart phone, tablet, laptop, desktop, appliance, or server devices. End-to-end encrypted security is available to devices whether on private wired, Wi-Fi, public Wi-Fi or cellular networks. These end-to-end private connections are mutually authenticated and access-controlled by connection policies defined by the user. Gabriel is available and communicates seamlessly between all major operating systems and vender devices; which include:

- Apple iPhones, iPads, and Macintosh computers,
- Android smart phones and tablets,

- Windows 7, 8, & 10 tablets, laptops, desktops and servers,
- Linux laptops, desktops and servers

This white paper covers the features and benefits of the patented Gabriel technology and the application suite. The Gabriel technology brings robust real-time privacy and security to both individuals and organizations as they use the Internet or Intranet in their personal and professional lives.

Gabriel Connect Technology

The Internet was originally conceived and developed with a view toward openness and limited access controls. While this has contributed to its widespread use and betterment of people's lives, it has brought with it some major challenges to assuring privacy and security for those benefiting from its use. These challenges stem largely from the fact that the Internet by its very design is publicly accessible to everyone. Given that both good and bad actors have equal access to the Internet, any solution to protecting the good actors from the bad actors (i.e. hackers) must address challenges, which include:

- Assuring content privacy and controlling access,
- Authenticating participants (knowing with whom you are collaborating),
- Blocking unwanted participants (keeping out the bad actors),
- Overcoming on demand connection barriers (anyone, anytime, anywhere),
- Seamlessly connecting and communicating across dissimilar platforms, and
- Controlling and administering who can connect and access data (user defined security policy)

Gabriel has been designed, created and tested from its very inception to address these challenges by integrating VirnetX patented technology with industry standard cryptography, technology and practices.

Network address resolution is a process used in Internet communications, for example, this is the process by which a human readable domain name is resolved to a specific Internet Protocol (IP) address. The IP address is a sequence of numbers, which routers use to

determine where to send data destined for a specific device location. Traditional address resolution is performed by the Internet's Domain Name Service (DNS), which is a collection of devices capable of resolving domain names to IP addresses. For example, a user desiring to access the Amazon™ commerce site would enter the domain name www.amazon.com. This domain name is sent to a DNS server, which either knows the corresponding IP address or forwards the request to a server, which knows (e.g. 54.239.26.128) the address. When the address is found, it is returned to the requesting device. Unlike traditional DNS, Gabriel technology enhances the step of network address resolution by automatically determining the need for the initiation of a Virtual Private Network (VPN) to the destination computer and provisioning the VPN for communications that require it.

GABRIEL TECHNOLOGY

GABRIEL INSTANT SECURE CONNECT Intercepts the domain name look up before it is sent to legacy DNS to determine if it is a SECURE DOMAIN NAME.

GABRIEL SECURE DOMAIN NAME is designated by **.scom** and can only be accessed by Gabriel authenticated devices which have their own certificate.

As shown in Figure 1, Gabriel's *Instant Secure Connect™* technology intercepts the domain name lookup before it is sent to the legacy DNS and determines if the domain name is a *Secure Domain Name.* If the domain name is a Secure Domain Name, a Gabriel VPN is created between the requesting device and the destination (or target) device. The VPN uses a secure IP address, which is then returned to the user's requesting application. This secure IP address is then used by the application to connect to the target device through the VPN. If the requested domain name is not a Secure Domain Name then the domain name lookup request is forwarded to the legacy DNS. As an example, Amazon could have a www.amazon.com legacy domain name and a www.amazon.**scom** Secure Domain Name.

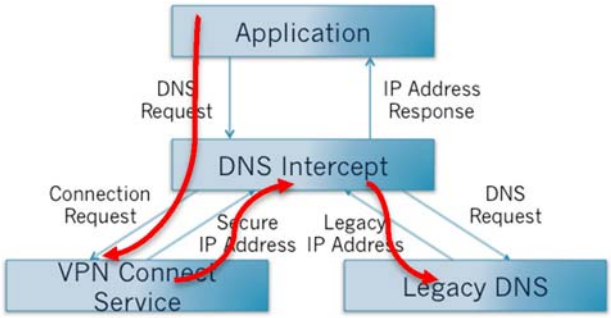

Figure 1 Gabriel's *Instant Secure Connect*

Comparing Figure 2 with Figure 3, we see how the user utilizes each name in the same way, but in the case of the Secure Domain Name a VPN is automatically established and a secure IP address is returned.

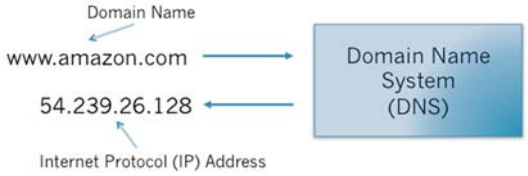

Figure 2 Legacy Address Resolution

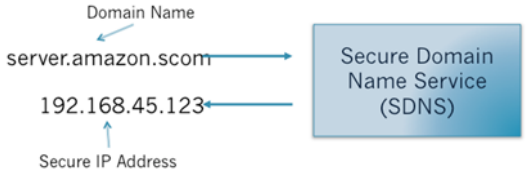

Figure 3 Secure Address Resolution

In this way, Gabriel is designed to allow applications to communicate in VPNs just as seamlessly as applications create non-secure communications. To achieve this, Gabriel handles secure key exchange and end-point authentication associated with VPNs. Moreover, Gabriel uses strong industry standard cryptography, including digital certificates signed and issued by the *VirnetX Certificate Authority*. Each Gabriel enabled device is issued a unique Secure Domain Name with a corresponding digital certificate signed by the VirnetX CA. The private key for that certificate is generated and secured on the owner's device. *Mutual Authentication* of the device/user to its peers and to the Gabriel servers that facilitate the VPN negotiation process, is performed by using this private key, together with the signed certificate.

The Gabriel's *Instant Secure Connect* technology includes cryptographic authentication of peering devices. A user is able to define which devices can connect and what information is shared, based upon a device/user identity. In this way, users can dynamically define and modify virtual private enclaves or *Safe Neighborhoods* within the Internet/intranet. This enclave, as illustrated in Figure 4, can include any collection of devices and users regardless of their location on the Internet/intranet. If a device is connected to the Internet/intranet, it can be in the enclave. Additionally, a device can be included in **ANY NUMBER** of enclaves at a given time, if the defined security policy permits. As described in the next section, Gabriel's Instant Secure Connect technology has

GABRIEL INSTANT SECURE CONNECT

MUTUAL AUTHENTICATION requires devices/users to authenticate with the peers before secure communications can be occur.

SAFE NEIGHBORHOODS are virtual private enclaves within the Internet/intranet of authenticated devices able to connect on demand no-click and enable real time secure communications.

been used to create a cross-platform security infrastructure referred to as the *Gabriel Security Platform*. This makes dynamic, on-demand secure enclaves possible.

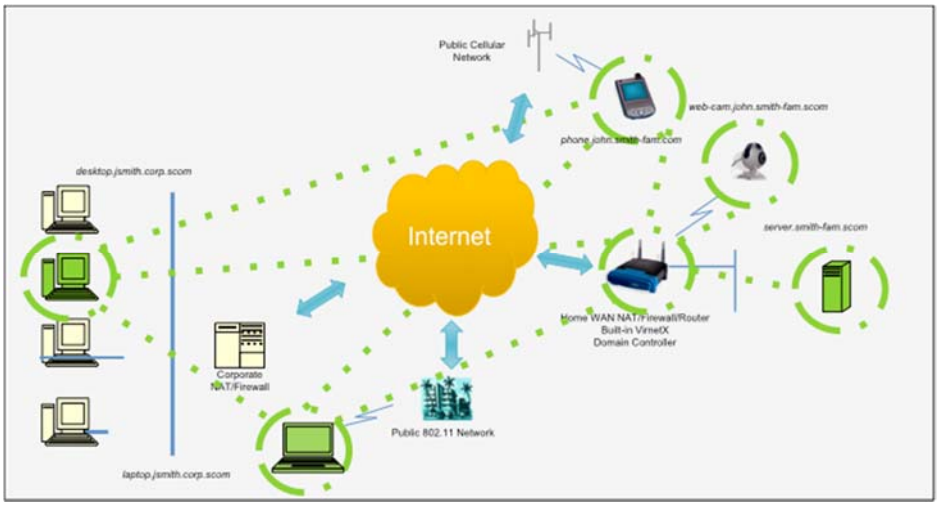

Figure 4 Gabriel Enables Dynamic Secure Enclaves / *Safe Neighborhoods*

Gabriel Security Platform

The Gabriel Security Platform provides the networking and cryptographic infrastructure that enables the following services:

- User defined security policy,
- Seamless VPN initiation,
- *Secure Domain Name Service (SDNS)* address request lookup feature:
    - Automatic VPN initiation,
    - Remote peer secure address resolution, and
    - Certified peer IP reverse address lookup
- Cryptographic peer authentication,
- Network Address Translation (NAT) firewall discovery and relay services when needed, and
- Secure peer presence discovery

GABRIEL SECURITY PLATFORM

Performs three basic functions: Issue, Revoke, Where-is on all major operating systems.

SECURE DOMAIN NAME SERVICE (SDNS) SYSTEM Address request lookup featuring:

- Seamless VPN initiation,
- Remote peer secure address resolution, and
- Certified peer IP reverse address lookup

The Gabriel Security Platform is available on all major operating systems and supports seamless interoperation across Windows, OS X, iOS, Android, and Linux devices. As shown in Figure 5, the Gabriel Security Platform implements both Registry Services and Registrar Services to register user devices, provide network presence services, and SDNS for Gabriel devices throughout the Internet/intranet.

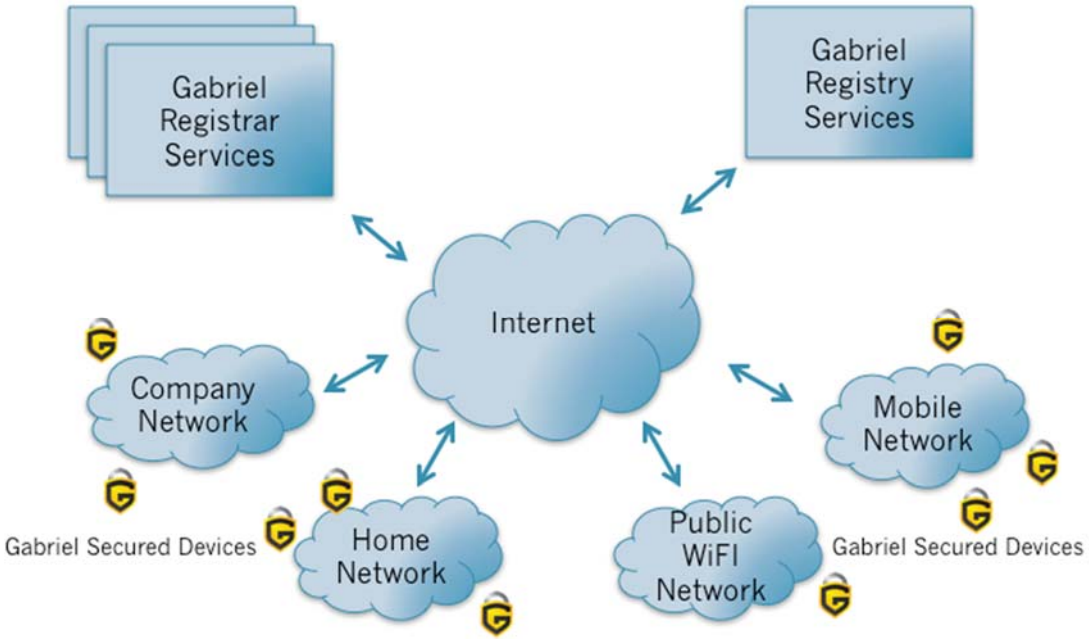

Figure 5 Gabriel Security Platform services

GABRIEL SECURITY PLATFORM

GABRIEL REGISTRY serves as system root CA to authenticate, register and issue signed certificates (and revoke) to Gabriel Secure Domain Registrars.

GABRIEL REGISTRARS register Secure Domain Names as well as locate authenticated peer devices, perform multiple security and connection services through **Gabriel Connect Servers** and **Relay Servers**.

The Gabriel Registry serves as the system root Certificate Authority. Among its primary functions is to authenticate, register and issue signed certificates to Gabriel secure domain name Registrars. The Gabriel Registry will revoke certificates being used by bad actors or deactivated devices and instantly enforces policies against any revoked certificates. The Gabriel Registry also provides the overall system integration function by responding to "*where-is*" requests from VirnetX and/or 3rd party Gabriel Registrars. This allows the registrars to locate Gabriel peer devices for cross-registrar connection services.

Gabriel Registrars provide multiple security and connection services to Gabriel devices. These services include one or more registration servers which are used for account signup and renewal, device activation and certificate signing as well as data base services which store and retrieve account configuration data used by the *Gabriel Connect Servers* and the Gabriel devices. Gabriel Connect Servers are interconnected to create a system of Secure Domain Name Services, both within and across Gabriel registrars. These registrars provide the mechanism by which Gabriel devices register their presence on the Internet/intranet, discover on-line status of their peers, perform Secure Domain Name address resolution and initiate secure peer-to-peer VPN connections. Gabriel Connect Servers support both peer revocation notification and push messaging to Android and Apple mobile devices. Gabriel Registrars utilize the *Gabriel Relay Server* to support:

GABRIEL SECURITY PLATFORM

GABRIEL CONNECT SERVER perform account signup and renewal, device activation and certificate signing, as well as data base services which store and retrieve account configuration data. Manages devices, register presence, on-line status of peers, perform Secure Domain Name address resolution and initiate secure peer-to-peer VPN connections.

GABRIEL RELAY SERVER perform the following functions:

- Peer-to-peer connection setup, where both peers are behind NAT firewalls,
- Session Traversal Utilities for NAT (STUN) firewall traversal discovery,
- VPN channel relay, when direct channels are not supported by local firewalls, and
- Out of band, periodic key exchange.

- Peer-to-peer connection setup, where both peers are behind NAT firewalls,
- Session Traversal Utilities for NAT (STUN) firewall traversal discovery,
- VPN channel relay, when direct channels are not supported by local firewalls, and
- Out of band, periodic key exchange to increase the security of an established, peer-based VPN as explained below in greater detail.

The third component of the Gabriel Security Platform is the *Gabriel Secured Device Services*. Figures 6 and 7 show these services running on the individual devices, which are secured by Gabriel Connect Technology. These figures show two architectures for providing security services. Figure 6 shows the basic architecture as implemented on OS X, Windows and Linux platforms. This architecture takes advantage of the operating system's internal packet router and IP stack, by intercepting DNS requests before they leave the device and using a virtual VPN network adapter for intercepting all packets associated with a VPN channel. This architecture allows

GABRIEL SECURITY PLATFORM

GABRIEL SECURED DEVICE SERVICES verifies authenticated devices, creates Gabriel on demand no-click, VPN connections through Gabriel Instant Secure Connect.

any application running on the device to use Gabriel VPN security without modifying the application. Specifically, if the application passes a Secure Domain Name to the network stack, Gabriel will automatically handle the request and initiate a VPN in which the application will communicate.

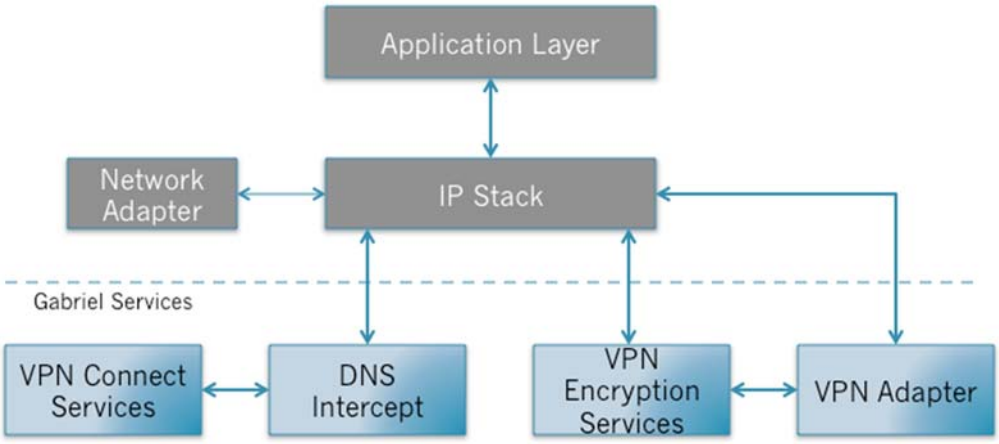

Figure 6 Gabriel Secured Device Services

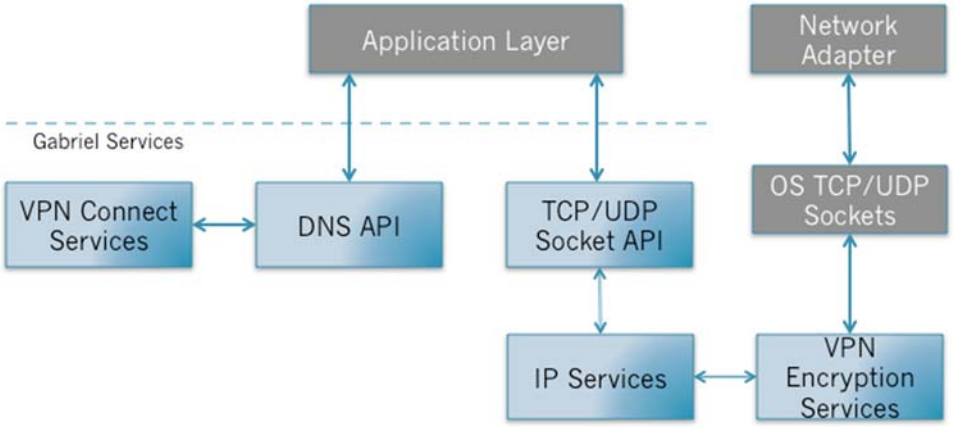

Figure 7 Gabriel Secured Mobile Services

GABRIEL SECURITY PLATFORM

GABRIEL API Developers can use API to utilize Gabriel's real time secure communications.

Figure 7 shows the architecture for mobile devices. Gabriel Secured Device Services is adapted to address the system level access limitations imposed by Android and iOS operating systems. These mobile operating systems limit the access that applications have to the platform's IP stack and DNS messaging. In order to accommodate these limitations and provide the same level of Gabriel security, VirnetX created an

Application Programming Interface (API), by which the application can access the DNS intercept functions and VPN transport for its TCP (transmission control protocol) and UDP (user data gram protocol) packets. The API allows a third party developer to build their applications and utilize Gabriel security when present on the device. The mobile version for Gabriel has a built-in IP stack and functions seamlessly with both Gabriel mobile devices and with Gabriel devices secured by the version shown in Figure 6. This allows Android, iOS, OS X, Windows, and Linux devices to interoperate and utilize the Gabriel VPN security. This version is also available for Windows devices, which use restrictive third-party anti-virus/firewall programs and allows Gabriel to operate seamlessly without conflicting with these programs.

A primary function offered by the Gabriel Secured Device Services is the Instant Secure Connect, whereby a name resolution request is intercepted. The service determines that the name is a Secure Domain Name, a secure connection is requested and established, and the corresponding secure IP address is returned. Subsequently, VPN encryption and packet routing is done while the VPN is connected and active. In order to assure a high level of security, the connection steps include:

1. Confirm allowed by local peer connect policy,
2. Send *InitiateConnection* message to the Gabriel Connect Server,
3. Gabriel Connect Server checks policy and forwards to remote peer,
4. Remote peer confirms remote peer connect policy, requests relay services (as needed), and sends *ConnectOK* message back to requesting peer,
5. Perform direct VPN negotiation between peers (includes key exchange), and
6. Return secure IP address to requesting application

Gabriel VPNs are negotiated using industry standard cryptographic software libraries and processes. Two encrypted channels are created, each of which encapsulate and encrypt the application's IP packets. The encrypted TCP connection with Secure Socket Layers (SSL-3) is used primarily for peer authentication, key exchange and as a backup to the second UDP channel. The second channel is an AES (advance encryption standard) encrypted UDP connection, which provides direct peer-to-peer routing when supported by the NAT

firewalls sitting between the peer devices and the public network. When NAT traversal is not an option, the UDP channel is routed through one of the Relay Servers. In either case, encryption/decryption is always peer-to-peer using 128-bit symmetric keys, which remain on the peer devices. Encryption keys are always generated and securely communicated between the peer devices. Peer authentication is performed by both the Gabriel Connect Server, as well as by each peer device using 2048-bit two-sided digital certificate authentication.

In summary, the Gabriel Security Platform enables peer-to-peer encrypted communications, which are:

- Adaptive; allowing secure connectivity adapting to wherever participants are located,
- Dynamic; able to quickly and easily add and remove peers,
- Cross-organizational; relying upon trusted third-party authentication of user identity, regardless of organization association, and
- Protected from third-party access; encryption and key exchange is always peer-to-peer, and independent of peer network location

GABRIEL SECURITY PLATFORM

- Enables peer-to-peer encrypted communications ANYONE, ANYTIME, ANYWHERE.
- Real-time secure communications.

VirnetX utilizes the features offered by the Gabriel Security Platform to build and secure a suite of real-time communication applications called the *Gabriel Collaboration Suite™.*

Gabriel Collaboration Suite

The Gabriel Collaboration Suite is an integrated set of real-time communication and collaboration applications built on top of the Gabriel Security Platform. The applications are accessible to the user through a single Graphical User Interface (GUI), offering a uniform user experience across all devices and operating systems. The collaboration applications can run effectively as a single application and perform multiple functions simultaneously. The real-time collaboration integrates multiple communications services, which include:

- *Secure Messaging* with file sending and screen sharing (platform permitting),
- *Secure Group Messaging*,

- *Secure Voice/Video Chat*, and
- *Secure Mail*

Additionally, Gabriel offers the following integrated set of secure network services:

- *Security Policy Management*,
- *Secure File Share*,
- *Secure File Backup* and *Sync*, and
- *Secure Gateway Services* for securing third-party network services (e.g. web, home monitoring and security, Windows Samba file share, remote desktop, etc.)

GABRIEL COLLABORATION SUITE

Provides real-time secure communication: Secure Messaging, Group messaging, Voice/Video chat and Mail along with Policy Management and File Share, Back up & Sync and Gateway services for 3rd party network services.

The Security Policy Management enables the user and/or domain administrator to customize peer access policies on a per-service and per-file directory basis. Both peers, as well as the peer domain can be specified to limit access to whom a user can securely chat, email, and share files. File sharing directories can be specified as read-only or read/write for specific peers and/or peer domains. Peers not given access will not see the presence of un-shared directories.

In addition to providing secure communication and network services, Gabriel can be installed and configured on network server and gateway devices. Using this capability, Gabriel supports Secure Gateway Services, thereby enabling secure, authenticated access to virtually any third-party server application and/or device on the private network. This is achieved by allowing the user to specify a communication port, which forwards data packets to third-party ports and IP addresses on the private network. These Secure Gateway Services allow home users and organizations private authenticated access to any number of private network services from anywhere on the Internet/intranet.

Gabriel provides a unified interface across all devices and platforms, by offering a common user experience among the user's mobile and non-mobile devices. Figures 8-12 show snapshots of the user interface screens associated with the various Gabriel functions. For more information or to register and install Gabriel, please visit our website at http://www.gabrielsecure.com.

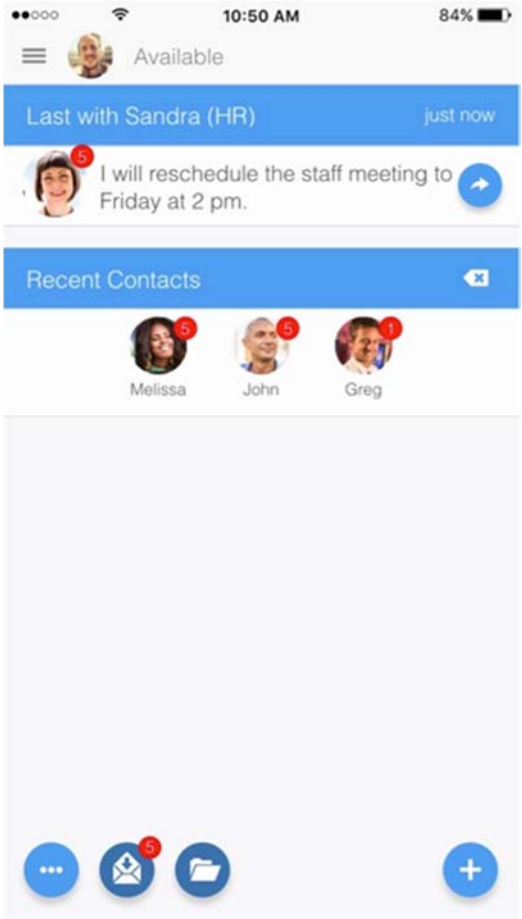

Figure 8 Peer Presence Screen

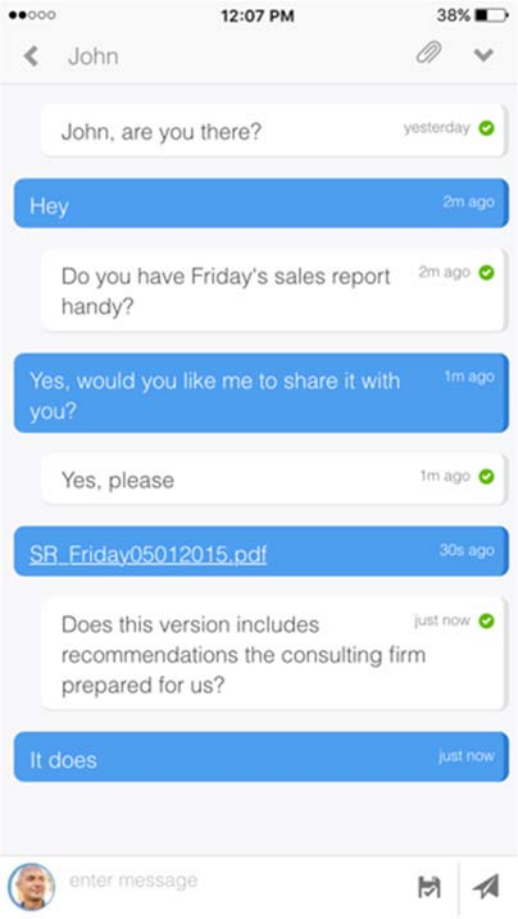

Figure 9 Secure Messaging Screen

Figure 10 Secure Voice/Video Screen

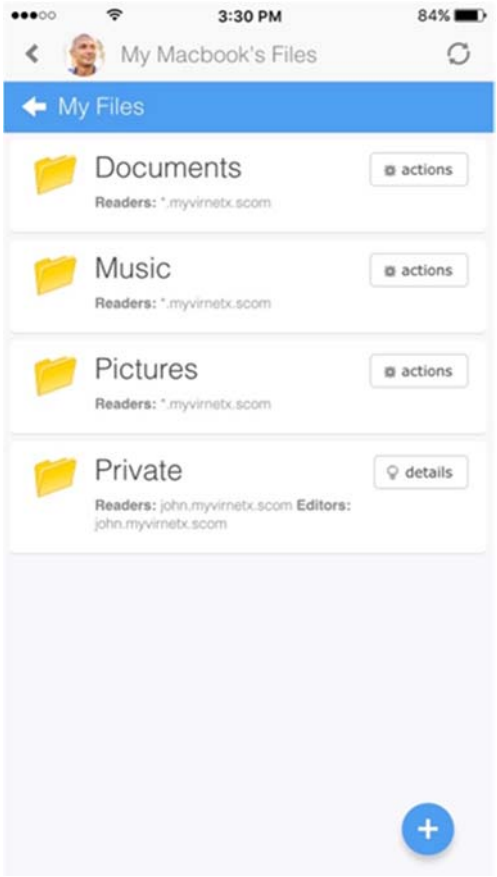

Figure 11 Secure File Share Screen

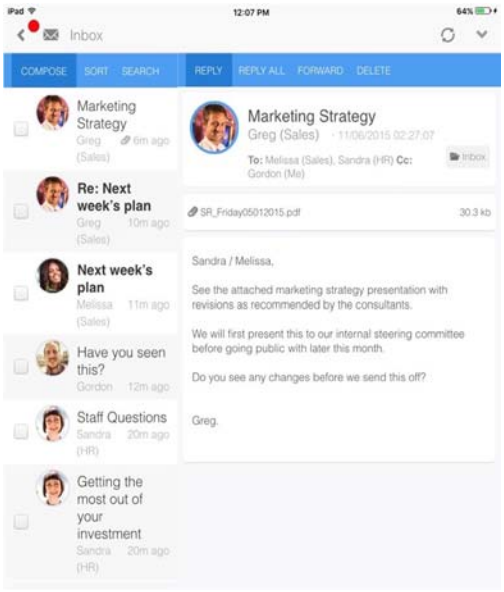

Figure 12 Secure Mail Screen

Summary

Gabriel empowers individuals, corporations and organizations of all sizes, as well as government agencies to establish and administer their own private network enclaves or *Safe Neighborhoods* across the public Internet or within their own intranet. Gabriel provides cryptographic privacy of all data, voice, and video within the private enclave and cryptographic authentication of its participants. Gabriel's flexibility allows the dynamic establishment, administration and teardown of these private enclaves, as needed, independent of device location.

Gabriel's ANYONE, ANYTIME, ANYWHERE secure communications allow users to take back control of their own data from third-party cloud services. These third-party cloud services may be mining and reselling user data, while at the same time providing information rich targets for nefarious computer hackers. By placing a Gabriel enabled server behind a home or company firewall, personal and corporate data will stay on user owned and controlled devices. The Gabriel configuration prevents potential hackers from locating and accessing user information. The private and secure Gabriel *Safe Neighborhood* allows for private access by the authorized users from anywhere on the Internet.

"Take Back Your Digital Life"