etherFAX Security Overview

August 2014

etherFAX is a virtual telephony cloud computing platform designed with high availability and dependability, allowing customers to completely rid themselves of traditional telephony infrastructure including: fax boards, telephone circuits, PBXs, long distance carriers, and so forth. From its inception, the etherFAX team regarded the confidentiality and integrity of customers' data/information to be of the utmost importance and critical to the success of the hosted service and the organization itself; especially when compared to traditional telephony systems. Since many of our customers are in the business segments of banking, financial services, trading, or medical (just to name a few), we knew full well that etherFAX would need to stand the test of its toughest critics and meet the strictest demands of our customers' security policies and requirements. When comparing the lack of security using e-mail based store-and-forward systems, T.38 (real-time fax over IP), and other similar solutions, etherFAX stands out as the clear leader.

etherFAX incorporates a multi-level encryption/security system known as a "defense-in-depth" approach. It is a layering tactic, conceived by the National Security Agency (NSA), as a comprehensive approach to information and electronic security. In addition, all fax transactions are processed in a secure and encrypted database utilizing the same standards. Lastly any images/content in the etherFAX system only persists for the life of the transmission and is then destroyed with all data being zeroed; ensuring etherFAX meets all regulatory compliance requirements.

We start with a secure communication channel over HTTPS that secures the "pipe" between the etherFAX client/customer and the back-end services hosted by etherFAX. Once a secure channel has been established, each customer is authenticated using his or her account, user name, and password. Lastly, the etherFAX web service model further encrypts and protects the communication on a "message level" even though the HTTPS channel is already arguably secure.

Many products and services in the market completely disregard security when it comes to communication with the back end services. Forwarding faxes as e-mail attachments, poorly designed communication systems, or even deploying T.38 right at the customer premise all contribute to poor (or NO) security at all. Think of it this way; HTTPS using certificates is only using "a" public/private key-pair system for communication where this base key is the basis for communication between all systems. With message level security, a new key is derived using a challenge/response mechanism that creates a key that is unique to each session with the etherFAX back-end system. Once the channel/pipe is secure using HTTPS, the etherFAX web service protocol then further protects (doubly encrypts) information on the message level within an already secure channel.

Some ask why we've implemented this level of security for fax. The simple answer is that we know security and implementing models like these with modern day tools (web services, SOAP, XML, .NET communications foundation, etc.) is actually not that complicated or foreign to us. Customers who use fax are used to a relatively secure medium, but are wary of Internet based solutions. We decided early on that we did not want to have security (or lack thereof) be a factor in NOT choosing an outsourced communication solution

PCI-DSS Certification (Level-1)

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards. There are 4 different levels within PCI, level 1 being the most strigent requiring the following:

- Annual Report on Compliance ("ROC") by Qualified Security Assessor ("QSA") or Internal Auditor if signed by officer of the company
- The internal auditor is highly recommended to obtain the PCI SSC Internal Security Assessor ("ISA") certification
- Quarterly network scan by Approved Scan Vendor ("ASV")
- Attestation of Compliance Form

etherFAX achived level 1 certification from Trustwave on 8/6/2014, taking nearly 12 months to complete. The AOC (Attestation of Compliance) is available upon request.

The PCI Data Security Standard specifies 12 requirements for compliance, organized into six logically related groups called "control objectives". Each version of PCI DSS has divided these 12 requirements into a number of sub-requirements differently, but the 12 high level requirements have not changed since the inception of the standard.

- Build and Maintain a Secure Network
  - Install and maintain a firewall configuration to protect cardholder data
  - Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect Cardholder Data
  - Protect stored cardholder data
  - Encrypt transmission of cardholder data across open, public networks
- Maintain a Vulnerability Management Program
  - Use and regularly update anti-virus software on all systems commonly affected by malware
  - Develop and maintain secure systems and applications
- Implement Strong Access Control Measures
  - Restrict access to cardholder data by business need-to-know
  - Assign a unique ID to each person with computer access
  - Restrict physical access to cardholder data
- Regularly Monitor and Test Networks
  - Track and monitor all access to network resources and cardholder data
  - Regularly test security systems and processes
  - Maintain a policy that addresses information security

Data Center Environment

etherFAX is hosted within Equinix IBX data center environments, the same world class data center facilities powering many of today's most demanding hosted service environments such as Amazon Web Services, the New York Stock Exchange, and many other prominent companies.

Power

Our centers provide a minimum N+1 redundancy for every power system, to maximize uptime availability. Our infrastructure includes Uninterruptible Power Supply (UPS) systems to prevent power spikes, surges, and brownouts, and redundant backup diesel generators provide additional runtime. Using proprietary automated telemetric systems, the data center Engineering Team can monitor all power system components on-site or remotely, to respond quickly to any situations.

Cooling

Each data center includes a robust HVAC system to provide stable airflow, temperature and humidity, with minimum N+1 redundancy for all major equipment.

Facilities are equipped with N+2 redundancy for chillers and Thermal Energy Storage, providing enhanced temperature stability.

Representative Specifications:

- 13,652 BTUH per cabinet
- Six (6) 750-ton centrifugal chillers
- Six (6) variable primary chilled water pumps
- Six (6) condenser pumps
- Six (6) cooling towers
- 24 air handling units in the colocation area

Flood Control

All data centers are built above sea level with no basements and have the following flood control features:

Fire Detection and Suppression

Key features of the fire detection and suppression system include:

- Multi-zoned, dry-pipe, double-interlock, pre-action fire suppression system3
- Very Early Smoke Detection and Alarm (VESDA)

Earthquake

Structural systems at our data centers centers meet or exceed local building codes for lateral seismic design forces. Equipment and nonstructural components, including cabinets, are anchored and braced.

Physical Security

Our data centers utilize an array of security equipment, techniques, and procedures to control, monitor, and record access to the facility, including customer cage areas.

All areas of the center are monitored and recorded using CCTV, and all access points are controlled. Every data center is staffed with 24-hour security officers. Visitors are screened upon entry to verify identity, and escorted to appropriate locations. Access history is recorded for audit.

Security Features:

- 24x7x365 security
- All doors, including cages, are secured with biometric hand geometry readers
- Kinetic and key locks on closed cabinets
- Colocation and critical areas have windowless exteriors
- CCTV digital camera coverage of the entire center, including cages, with detailed surveillance and audit logs
- Bullet Resistant Protection
- CCTV integrated with access control and alarm system
- Motion detection for lighting
- Equipment check upon arrival
- Shipping and receiving area walled off from colocation areas

Authorized Personnel and Screening

Only authorized and essential etherFAX personnel are permitted access to the data center facilities and systems used to support the etherFAX telephony network. Additionally, all access must be scheduled in advance both with the appropriate etherFAX management/officer responsible for data center support as well as the data center itself.

Background Checks

All etherFAX personnel are subjected to criminal background checks prior to employment and are performed at the unspecified intervals at the discretion of etherFAX management.

System Defenses

The etherFAX network provides significant protection against common security threats such as DoS (Denial of Service) and other brute-force attack mechanisms. Threats are continually monitored in real-time and will generate systems alerts to data center personnel, etherFAX engineering and support staff, and other parties as deemed required.

No fewer than two times per year, etherFAX conducts "unannounced" penetration tests using a third party organization. These tests are only known to the etherFAX security officers and essential management at the time(s) they are commenced.

pci Certified
Level 1 Service Provider

Carrier Grade Networking Systems

The etherFAX network makes every attempt to provide for system redundancy and never allows for any single points of failure.

Network Carriers

etherFAX is supported by multiple carriers, each with duplicate network interconnects in the event of failure. Also of significance, our data centers are home to many/all of the carriers used by etherFAX so interconnects are local to the data center facility.

Some of the carriers used by etherFAX are:

- Global Crossing
- Verizon
- Level 3
- Peerless Communications
- Paetec
- Others

Business Continuity Management

The etherFAX network and related systems have been designed to tolerate system or other hardware failures with no/minimal customer impact. Our high availability is achieved using a plural of web services, fax transport systems, telephony infrastructure, carrier interconnects, networking and load balancing hardware, as well as redundant data center sites in the event of a catastrophic failure.

Backups

All system configuration and data is backed up to an off-site facility in real-time at 15-minute intervals. Databases are replicated in real-time throughout the etherFAX infrastructure to ensure high availability, and fault tolerance.

Multi-Layer (Defense in Depth) Security Model

The etherFAX network and external interfaces to the system (web service APIs, etc.) were designed by security professionals experienced in providing information protection to military grade standards defined by the NSA and NIST organizations. etherFAX meets or regularly exceeds the guidelines defined by these organizations for the protection of sensitive information. To that extent, etherFAX employs multiple layers of security also known as a "Defense in Depth" that provides its customers an even greater protection against eavesdropping or other forms of cyber-attacks.

Authorization Systems

Authorization to the web service or administrative interfaces requires an account number, user ID, and password. Additionally, each customer may define one or more IP address rules authorizing access to the system (using CIDR notation). The etherFAX network separates credentials used for administrative and access to web services.

Web Service Security Model

The web service interfaces (APIs) are the primary vehicle used by remote client systems to access the virtual telephony network for the purpose of sending and receiving fax document transmissions. Access to these web services are subjected to the authorization systems requiring an account, API user ID, and password. In addition, the web service may optionally observe and enforce access from allowable endpoints only.

The initial connection to the etherFAX network is performed over an HTTPS (port 443) connection where the authorization credentials are presented to the etherFAX network. Once the session is established (and the authorization credentials have been accepted), the server and remote client will then generate a key-pair for further symmetric encryption within the already encrypted HTTPS transport. The key-pair and subsequent shared secret used for encryption is generated using Elliptic Curve Cryptography methods using 521 bits. Once an encryption key is established, each "message" between the etherFAX client and the hosted service is further encrypted using AES256.

All connections to the etherFAX network are inititiated by the client requiring no firewall ports to be opened. etherFAX also supports most Internet proxy configurations.

Data Security

etherFAX makes every attempt to NOT store any fax image data/content except for the life of the actual fax transmission. While etherFAX will maintain all call record details (fax number dialed, actual connect time, remote fax system ID, pages delivered, etc.), all fax image data is immediately destroyed upon termination of the call, whether a success or failure is detected.

During the in-transit period, all fax image data resides in a temporary data store and remains encrypted preventing even etherFAX personnel from observing the contents of the fax image/content.

Once the fax transmission has terminated, all fax/image content is FIPS-140 deleted and permanently removed from the etherFAX network altogether.

Monitoring and Alerting Systems

etherFAX uses standard network/system monitoring facilities as well as highly customized and integrated mechanisms allowing the network to automatically alert data center staff, etherFAX engineering and support staff, and even advise customers of local network outages.

The etherFAX network is designed around an escalation system making sure that the operational support staff is notified of potential threats or outages as they occur. Escalation from initial detection to an actual customer outage (for example) is achieved in as little as 15 minutes.

In many instances, customers use the etherFAX monitoring systems to detect outages in their own Internet connectivity.

Alerts are sent via SMTP email to one or more recipients as well as SMS to mobile handsets.