GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Hacker Tools, Techniques, and Incident Handling (Security 504)"
at http://www.giac.org/registration/gcih

GIAC (GCIH) Gold Certification

Exploiting Financial Information Exchange (FIX) Protocol?

Author: Darren DeMarco darrendemarco@aol.com
Advisor: Dr. Johannes B. Ullrich
Accepted: May 3rd 2012

Abstract

The Financial Information Exchange Protocol (FIX) has become the standard for pre-trade and trade communication messaging worldwide within the Financial Markets. According to the FIX protocol website, "FIX has experienced tremendous growth across Foreign exchange, Fixed income and Derivative markets."(FIX Protocol Ltd, 2012)Financial markets have become reliant on FIX messaging between brokerage firms to help grow business. FIX carries sensitive financial information worth billions of dollars for multiple financial instruments on a single connection line and has become essential when tracking an order from origination to completion. Exploiting FIX protocol and how businesses receive and acknowledge messages would have huge implications on the capital markets. There has been little to no focus on securing FIX protocol within the financial community. This paper will explore and hopefully shed some light on the strengths and vulnerabilities associated with the FIX protocol.

© 2012 The SANS Institute Author retains full rights.

1. Introduction

The FIX Protocol website defines The Financial Information eXchange ("FIX") Protocol as "a series of messaging specifications for the electronic communication of trade-related messages" (FIX Protocol Ltd, 2012). FIX has been a driving force for Financial Markets. FIX protocol website states that "FIX has been developed through the collaboration of banks, broker-dealers, exchanges, industry utilities and associations, institutional investors, and information technology providers from around the world" (FIX Protocol Ltd, 2012). As a former trader it is encouraging to learn a protocol has been developed by multiple financial sources. FIX website notes, "FIX is the industry-driven messaging standard that is changing the face of the global financial services sector, as firms use the protocol to transact in an electronic, transparent, cost efficient and timely manner" (FIX Protocol Ltd, 2012). FIX is free and open source which makes it very developer friendly. FIX is the financial markets leading trade-communication protocol and has become vital to many order management and trading systems.

1.1 History of FIX Protocol

FIX Protocol has played an enormous role in financial markets for many years. According to FIX website, "since the birth of FIX in nineteen ninety two as a bilateral communications framework for equity trading between Fidelity Investments and Salomon Brothers, FIX has become the messaging standard for pre-trade and trade communication globally within the Equity markets" (FIX History, 2012). As FIX turns thirty, it continues to add functionality. FIX website states that, " FIX Protocol is experiencing rapid expansion into the post-trade space, supporting Straight -Through- Processing (STP) from Indication-of-Interest (IOI) to Allocations and Confirmations" (FIX History, 2012). The protocol is gathering increased momentum, as it continues to expand across the Foreign Exchange, Fixed Income and Derivative markets. Before the introduction of FIX Protocol, traders used to deal by phone and information was relayed back to buyside clients (Hedge Funds and Pension Funds). Broker Dealers had to sit by the phone all day and wait for phone calls. Passing information back and forth by phone became very

© 2012 The SANS Institute Author retains full rights.

unreliable and very inefficient. FIX began to grow into an essential protocol for trading desks across Capital Markets. FIX added functionality so that it could be sent in binary form and added twenty-four seven support for customers worldwide with different symbology. The FIX protocol has become the most widely used protocol for electronic trading, with uses by Brokers, Portfolio Managers, and Exchanges worldwide

The significant acceptance of FIX within the financial services community was highlighted by the FIX Global Survey, which was conducted by TowerGroup at the end of last year. Tower Group states that "The results cited that 75% of buy-side and 80% of sell-side firms interviewed currently use FIX for electronic trading, and that both groups plan to focus substantial efforts on expanding their FIX usage to over 93%, as well as leveraging FIX across additional asset classes by 2012. The survey also revealed that FIX is developing a key role within the post trade space, as over 80% of buy-side firms, and over 95% of sell-side firms surveyed currently support, or plan to support FIX for allocations. Further to this, FIX is gaining increased attention within the exchanges community as over three quarters of all exchanges surveyed supported a FIX interface, with the majority handling over 25% of their total trading volume via FIX" (FIX Protocol Ltd, 2012). I believe by financial firms creating an "all your eggs in one basket" approach with one protocol makes financial electronic order flow vulnerable for attack.

1.2 Who uses FIX?

Multi-billion dollar buyside and sellside firms have become reliant on FIX messaging. FIX website states, "Almost ninety percent of order flow is done electronically" (FIX Protocol Ltd, 2011). For example, buyside firms like Soros Hedge Fund will send multiple orders worth a tremendous amount of money via FIX to sellside firms such as Goldman Sachs. Both Goldman Sachs and Soros have dedicated teams to analyze any issues that arise from bad messaging. Most of the time, if there is bad messaging the order or the execution report will be rejected and appear on an exception or error report that will be analyzed. Any mapping issues will be repaired by each firm's connectivity team. Fig 1 is a diagram of how FIX messaging looks between Buyside/Customer and Sellside/Supplier. The complexity of multiple connections can become overwhelming, especially when adding specialized plug –ins for particular customers. The

© 2012 The SANS Institute Author retains full rights.

managing and overseeing required by this complexity can become very error prone and lend itself to attack and/or disruptions.

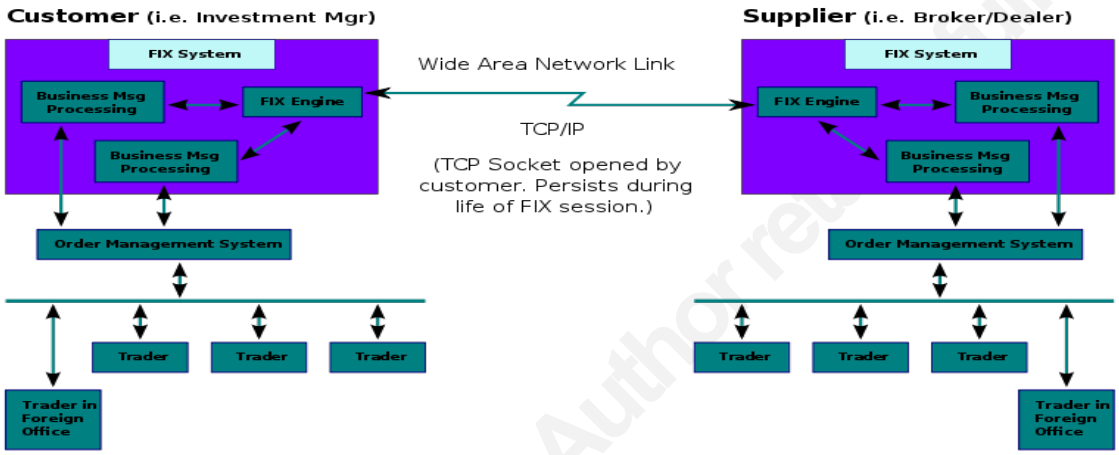

Fig 1: Diagrammatic representation of FIX system (FIX Protocol Ltd, 2012)

1.3 FIX Messaging

FIX messaging is a series of tag value pairs. "Tags" consists of hundreds of different fields that could be in the messaging. For example, a field in FIX messaging could be Symbol, Shares, Side, Order Quantity, Price, and Order ID. Each field is represented or mapped to a number value. For example, Symbol = 55, therefore if an order sent electronically in Apple Computer (AAPL) it would be represented as 55 = AAPL. A FIX message contains three parts, the Header, the Body, and the Trailer. There are two types of FIX messages, Application Layer, and Session Layer messages. The Header consists of administrative information about the message, such as who sent the message, who is the message going to, and what time it was sent. The body contains the actual financial information fields, like Symbol, Shares and Price. The Trailer is the

© 2012 The SANS Institute Author retains full rights.

checksum for the message, to insure message integrity. Fig 2 is an example of how FIX messaging looks like when parsed by a vendor or a proprietary application. Each number corresponds to an instruction.

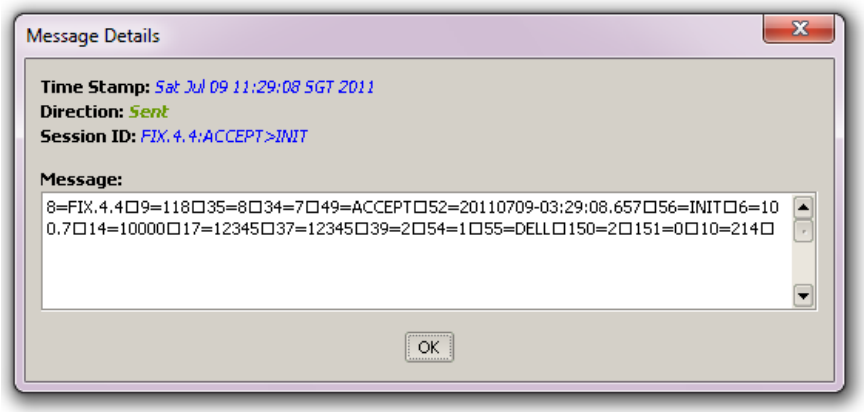

Fig 2: Fix Messaging (FIX Messaging, 2012)

1.4 FIX Connection Routing

When connecting, financial firms have three ways to decide what type of connection or network they would be hooking into. The three ways are Point-to-Point connections, IP tunneling or Virtual Private Network (VPN) and Hub-Spoke Network. Each firm has different reasoning of why and how they want to connect to one another. More often than not the cost of a connection beats out the security of a connection.

"Point to Point" connections involve connecting directly to each other, either through a leased line or either's party's private network. If a firm has multiple counter parties it will have to manage multiple connections and certify all of them.

© 2012 The SANS Institute Author retains full rights.

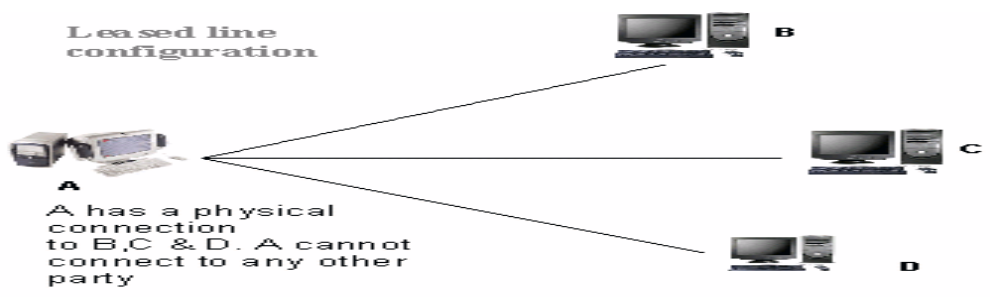

Fig 3: FIX Protocol Implementation Guide (FIX Protocol Ltd, 2012)

When using "IP Tunneling" or "Virtual Private Networks" (VPN), FIX engines do not connect directly to each other. Connectivity is done via a router that securely tunnels through the IP connection. There is no direct FIX monitoring when using this setup.

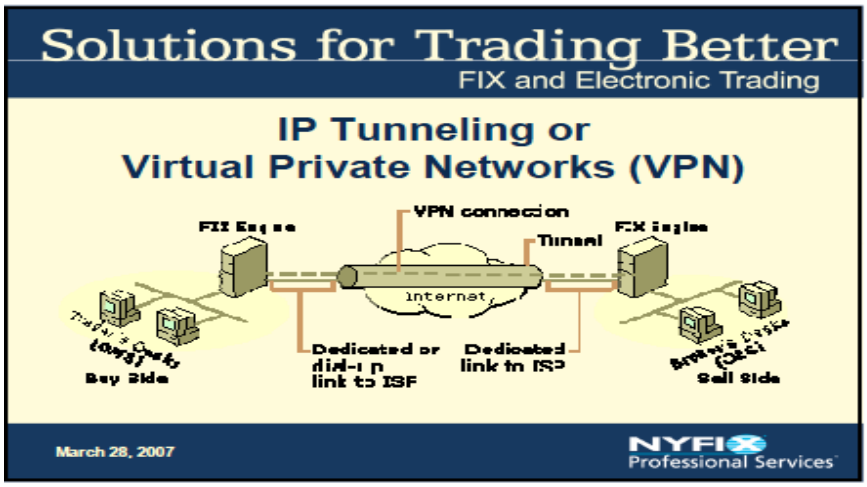

Fig 4: NYFIX Professional Services (NYSE Technologies, 2007)

According to the NYSE Technologies, "The "Hub and Spoke" model is most widely used model within the financial community" (NYSE Technologies, 2011). Firms are also known as "spoke sites" keep one connection to the hub site. This makes monitoring much easier and much simpler. Firms will dictate the rules to when and where a message should be routed to. They will only need to certify once to the hub site, and the hub site monitors the FIX activity to and from the spoke site.

© 2012 The SANS Institute Author retains full rights.

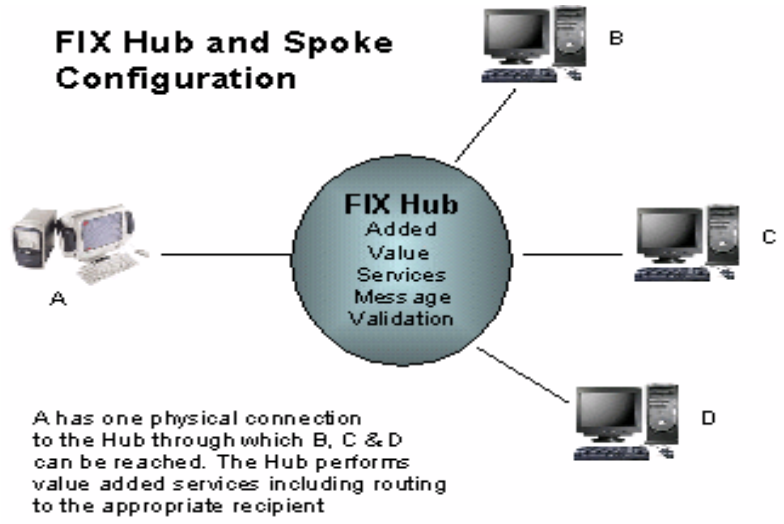

Fig 5: FIX Protocol Implementation Guide (FIX Protocol Ltd, 2012)

1.4.1 FIX Engines

Appia FIX engine was developed NYSE technologies (formerly known as NYFIX). APPIA is one of the most popular FIX engine within the financial community. According to NYSE Technologies, "Appia has the ability to execute a trade in less than a millisecond" (NYSE Technologies, 2011). With the adaptation of High Frequency Trading (HFT), it is essential for an engine to have tremendous processing power. NYSE Technologies states that "they have devoted years of research and development to creating one of the world's most widely deployed FIX engines" (NYSE Technologies, 2011). At my current firm, we have multiple Appia engines deployed to handle over 2500+ customers. According to NYSE, "Appia is a super-low-latency, extremely flexible way to manage and validate trading messages reliably across not only the NYSE Euronext global marketplace, but many third-party order-management systems, EMS systems and order-routing networks around the world. Institutional investors, exchanges, ECNs, and broker-dealers all benefit from the hundreds of features Appia offers to handle the many unexpected variables in high-speed, global trading" (NYSE Technologies, 2011). This plays an integral role with the explosion of High Frequency Trading (HFT). HFT firms will send thousands of orders a day within seconds of each other. Appia is well built solution that integrates easily with existing infrastructure, therefore speeding up installation and creates a more efficient workflow. NYSE Technologies states that, "Appia was built with pluggable

© 2012 The SANS Institute Author retains full rights.

architecture and fully customizable rules of engagement that can expand with market reach" (NYSE Technologies, 2011).

With Appia, Financial firms become part of the NYSE Technologies community of global traders. Firms will have a guarantee that orders won't be lost due to server failure. According to NYSE Technologies, "Not only do NYSE virtual servers provide backup on the fly, but geographical distribution equips buy-side firms, sell-side firms and exchange venues with the reassurance of a disaster continuity plan" (NYSE Technologies, 2011).

Cameron FIX Engine is another widely used FIX engine within the financial community. It is used mostly in overseas financial markets. According to their parent company ORC software, "CameronTec is the financial industry's leading provider of FIX infrastructure and connectivity solutions. Its latest market innovation Catalys takes FIX further and is the new industry reference for FIX ecosystems. Developed specifically to address the cross-functional needs of sell and buy side firms and exchanges. Catalys is a highly adaptive and integrated FIX infrastructure" (CameronTec, 2011). Today it is used by small to larger investment firms, brokerage houses, exchanges and regulators in multiple countries, on all five continents. ORC software states that , "Every day Cameron technology routinely processes over 600,000,000+ messages and is relied on to support the critical metrics for increasing customers, enhancing revenue streams, reducing market and operational risk as well as costs associated with pre and post trade services" (CameronTec, 2011). Each FIX engine has very similar functionality. The cost of hardware and setup is often the key factor in deciding to purchase one engine over the other.

© 2012 The SANS Institute Author retains full rights.

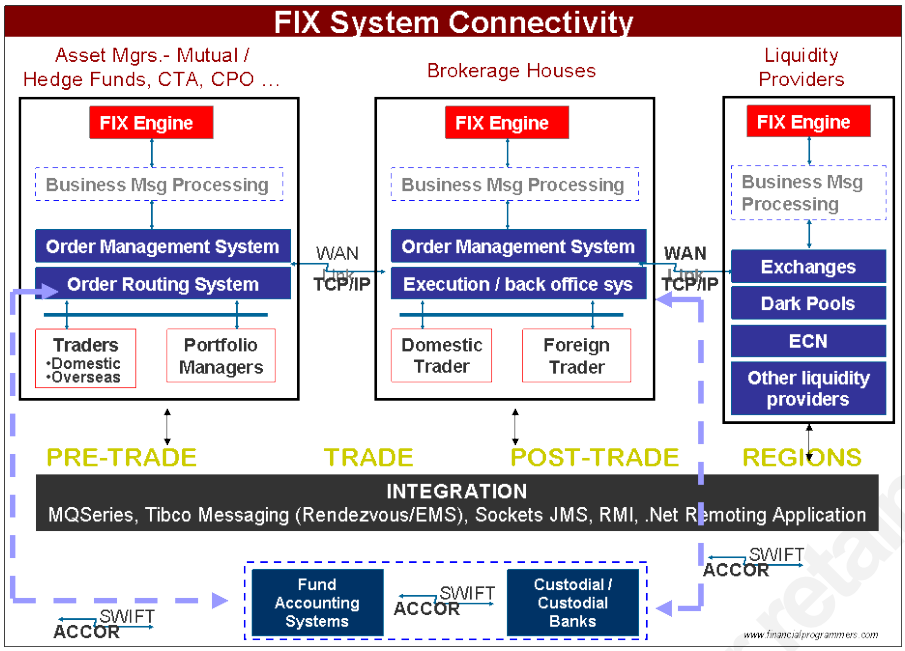

Fig 6: FIX System Connectivity (FIX System Connectivity, 2012)

As you can see the two most widely used FIX engines believe they are the best in the business of FIX messaging and processing. According to each company's website, there is very little mention to no mention of how secure their systems are. In my GSEC Gold Paper on Disaster Recovery for Trading Firms, I discuss "How complex trading floor architecture is to design. Information Technology teams must be very diligent in planning, monitoring connections, and securing multiple servers and desktops" (DeMarco, 2012). Monitoring, Hardening and Logging is definitely an arduous task that can be easily comprised if the proper controls are not put into place. Also network outages can be disastrous for financial firms trading millions of shares an hour. If you look at Fig 6 above you can see there is multiple ways or avenues an attacker can gain and disrupt access to sensitive data.

1.5 Tradescope – Fix Session Monitoring Application

TradeScope by NYSE Technologies is defined as "A trade messaging application monitoring tool that enables buy-side and sell-side firms to monitor all engines, sessions and application connections worldwide" (NYSE Technologies, 2011). Tradescope allows firms to customize that information to suit their specific needs. Complete FIX traffic and trade history is centralized in

© 2012 The SANS Institute Author retains full rights.

one easy to access location. Helpful tools let everyone from small trading firms to global brokers find, filter and sort information easily, by their own chosen parameters. The FIX tracking application allows customizable alerts to keep clients informed of possible trading issues, letting them address the issue before it escalates. NYSE states that, "TradeScope also provides on-boarding and connectivity management, as well as business and system-event management, and works seamlessly with any FIX engine" (NYSE Technologies, 2011). NYSE Technologies designed TradeScope to be easily adaptable to either buy-side or sell-side trading requirements.

A dedicated FIX team is responsible from monitoring lines when they connect and disconnect. Often, a FIX team has other responsibilities and can miss a disconnected FIX session. If this occurs, a large amount of business can potentially be lost. I believe that this is one avenue that can possibility be exposed because the application can have many false positives and false negatives. Therefore, allowing would be attackers to spoof critical infrastructure within a financial firm.

2. FIX Exploit Theory

This section will explore ways FIX protocol and financial firms might be penetrated or exposed. It will not be too explicit explaining " HOW TO", but will explain what possible vulnerabilities exist, how devastating it would be if an attacker decided to focus his interest on the Financial Information Exchange Protocol and the applications that surround it. There have been only a few research papers on this topic available on the Internet. Exploiting FIX protocol or processes that run side-by-side FIX is definitely not a widely discussed topic within the field of Information Security or Capital Markets. Throughout my research I have discovered multiple avenues of possibilities where an attacker can gain access to valuable information that is critical for financial firms and financial markets. The most recent security white paper on "FIX Security" was published in May 2008 with multiple authors. FIX Security Paper states "Any computer-to-computer communication comes with security risks and these risks are increased when communicating with external parties and networks" (FIX Protocol Ltd, 2008). However, external electronic communication is a fundamental requirement in the financial markets. Therefore, all parties involved must employ proper security measures and diligently manage

© 2012 The SANS Institute Author retains full rights.

security risk. The FIX Protocol leaves the choice of appropriate security measures open to the user community. It has been more than four years since the last "published" real in depth look at how FIX protocol can be secured or comprised. With the persistence of the hacking underworld and the state of economic affairs globally, Wall Street and Main Street establishments are being targeting at a rapid rate. Most recently, The National Security Agency was called in to help investigate recent hack attacks against the company that runs the Nasdaq stock market, according to a news report. The agency's precise role in the investigation hasn't been disclosed, but its involvement suggests the October 2010 attacks may have been more severe than Nasdaq OMX Group has admitted, or it could have involved a nation state. "By bringing in the NSA, that means they think they're either dealing with a state-sponsored attack, or it's an extraordinarily capable criminal organization," Joel Brenner, former head of U.S. counterintelligence in the Bush and Obama administrations, told the publication. He added that the agency rarely gets involved in investigations of company breaches" (Wired Magazine, 2011).

2.1 Vulnerabilities and Challenges

There are challenges to every protocol. The challenges that exist in FIX today are Reliability, Scalability, High Performance and Low Latency, and Application Intelligence. Reliability deals with the ability of the FIX provider to manually redirect traffic around a failed server, which will result in costly downtime. Scalability addresses the Information Technology administrator need to configure a one to one client to server path, causing the use of many IP addresses, which is very time consuming and very difficult to manage. High Performance and Low Latency deals with FIX servers having to connect to various outside systems, which require NAT (Network Address Translation) to public IP addresses. Currently routing equipment used for NAT is costly and will produce undesired traffic delays. Application intelligence challenge deals with routers and switches lacking the capability to provide application level features such as persistence and reading of FIX tag values such as Target CompID (tag 56), Symbol (tag 55). Each of the distinct FIX applications tags has an associated value passed along with it.

Even though FIX standards were intended for seamless automation of the exchange of time sensitive trading data, almost all FIX implementations use a manual process for FIX application

© 2012 The SANS Institute Author retains full rights.

connectivity. Financial services firms have pointed out that the following points have been a reason for lost business: Implementing FIX is a manual process and therefore error prone, new service creation is cumbersome because every customer is given a separate IP address and TCP Port, changes in networks/firewall infrastructure do not account for static pinholes and low latency is being achieved at the cost of security. Any change to the FIX service involves several maintenance windows because the change spans firewalls, routers and application servers. FIX is currently designed for point-to-point communication between two FIX systems with optional support to handle one system representing multiple firms via same FIX connection. Appia's FIX engine has a limitation that you can have same site redundancy via High Availability (HA) or diverse site redundancy but not both. High availability refers to a system or component that is continuously operational for a desirably long length of time. According to Tech Target, "Availability can be measured relative to "100% operational" or "never failing." A widely-held but difficult-to-achieve standard of availability for a system or product is known as "five 9s" (99.999 percent) availability" (Search CIO, 2012). Therefore, if there's an issue at the primary datacenter a financial firm would not be able to seamlessly failover to a secondary datacenter and keep in sync with clients.

2.1.1 Possible Avenues of Penetration/ DoS Attack

A useful tool in the attacker's repertoire is sending a series of connection requests to a target computer, resulting in a Denial of Service (DOS). A DOS attack involves an attacker preventing legitimate users from accessing a service. If an attacker is successful in bringing down critical Internet servers, or taking down your Internet connection, companies would stand to lose a lot of money in revenues and lose a lot of trust. Denial Of Service attempts are very hard to totally eliminate.

There are two types of Denial of Service categories: local Denial Of Service and network based Denial Of Service. There are two ways to execute a local DOS. The attacker can crash a service by stopping the process from running. Once the process is not running, it will not be able to handle any legit user requests. Another way to apply a local DOS, is to tie up the systems resources. An attacker could use up all the CPU cycles, hard drive space , memory space, or any other resource on the trading systems. For example, if an attacker's able to consume all CPU

© 2012 The SANS Institute Author retains full rights.

cycles, so HTTP could not run, an attacker would be able to prevent a trader from entering an electronic order across an internet connection. Most front-end trading applications require a Full T1 for a group of four traders, which can be easily flooded with an amplification attack using a 56k dial up line. The second category of DOS attacks is network based attacks. These attacks are launched across a network. Attackers sending DOS attacks targeting telco lines within financial datacenter infrastructure will cause the lines to get overloaded and crash. Most companies have auto failover but it needs to be finalized with human interaction, which can be costly if not monitored timely and effectively. Two types of network-based attacks are malformed packet and packet flood attacks. A malformed packet involves sending a single packet or small stream of packets to a system that is formed in a way not anticipated by the developers of the target financial system. The operating system, financial application, or networking software are not designed to handle abnormal packets. Malformed packets could cause the system to crash. Examples of malformed packets that are widely used are Ping of Death and the Teardrop attack. The second form of network-based attack is the packet flood. This type of attack has become easy to perform. The attack can be launched remotely, therefore putting space between the attacker and victim. The attacker can cause the FIX engine to receive more packets than it can handle. This can either cause the machine to be tied up by using all of the available processing power, or it can exhaust all bandwidth of the connection to the target.

2.1.2 Protocol Parsers in Trading Applications

Protocol parsers are a specific problem area for buffer overflow vulnerabilities. Even if each connection is encrypted it does not mean that the protocol parser of the financial trading product receiving this connection is safe from a simple DOS attack or a more dangerous buffer overflow and code execution. It will all depend on the FIX engine to perform field validation according to the settings on the machine. These parsers grab data from the network and parse it for a financial application. This type of attack would be a complete operational nightmare for clearing and trade settlement for any financial instrument. If the attacker is able to place himself in between an Appia FIX engine processing data for data to be sent to a 3rd party application, not only would he be able to spoof the data received by the application, but he would able to sniff data. Sniffing trading data would give an attacker the ability to act as an insider and profit from front running order flow. According to SEC Laws for Insider Trading, “Front running activities are highly

© 2012 The SANS Institute Author retains full rights.

illegally and punishable up twenty years in prison" (SEC Laws on Insider Trading, 2012).Not to mention jail time for illegally hacking into a financial network.

The act of separating these fields involves copying numerous different elements around in memory, an action that must be done with carefully checking the size of the data to be copied. Otherwise a buffer overflow vulnerability will occur. Flaws in these protocol parsers let the attacker obtain the privileges of the vulnerable financial program. Most of the programs running on a trading desk run with root or system privileges, because adjustments often are made on the fly without the interruption of calling desktop support for assistance.

2.1.3 FIX Session Sequence Numbers Attack

All FIX messages are identified by a unique sequence number, which relies on the Transmission Control Protocol (TCP). TCP provides reliable delivery of a stream of bytes from a program on one computer to another program on another computer. FIX Engines connect to each other over a TCP connection on agreed IP addresses and ports, if there is no logon message (35=A) something is wrong at the TCP (socket) level and TCP connection between client FIX Engine and broker Fix Engine has not been established. To verify this, check whether your host is connected to broker host or not by issuing following command. Many available rootkits can spoof the outcome of the netstat command, therefore keeping the FIX administrator in the dark.

netstat -a | grep port (port is the one which you are using to connect to broker)

FIX Sequence numbers are generated at the start of each FIX session starting at one and increment throughout the session. Monitoring sequence numbers will enable parties to identify and react to miss messages and to gracefully synchronize applications when reconnecting during a FIX session. Each session will establish an independent incoming and outgoing sequence series; participants will maintain a sequence series to assign to outgoing messages and a separate series to monitor for sequence gaps on incoming messages. If the incoming message has a sequence number less than expected and the "PossDupFlag" (Tag 43) is not set, it indicates a serious error. If the incoming sequence number is greater than expected, it signifies that

© 2012 The SANS Institute Author retains full rights.

messages were missed and retransmission of the messages is requested via the “Resend Request”. Resend Request (FIX tag 35=2 or MsgType=2) is used for asking of retransmission or replay of lost messages during transmission or due to incorrect sequence number. It’s normally sent by the FIX Engine, which is receiving message to initiate the retransmission of messages. FIX Engines use Resend Request (tag 35=2) if a sequence number gap is detected or if the FIX Engine of receiving application lost a message or as a part of initialization process to make sequence number in sync. It is generally recommended that the session be terminated and manual intervention be initiated. This will lend itself to a possible human error, as well as false positive alerts. After an attacker is able to penetrate the network he/she can masquerade possible down sessions causing mass confusion, therefore causing a full reset of the FIX Engine. This could lead to loss in production, failover capacity, load balancing, and loss in revenues.

2.1.4 Firewall Testing with Firewalking

In Fig 7 the diagram shows how a single firewall is in charge of what is allowed in or out financial network. For example, an attacker using a tool called Firewalk can test for vulnerabilities of a firewall and map the router hops of a network that sits behind a firewall. Firewalking is a method of disguising port scans. Firewalking is similar to tracerouting and works by sending into the firewall TCP or UDP packets that have a TTL set at one hop greater than the targeted firewall. If the packet makes it through the gateway, it is forwarded to the next hop where the TTL equals zero and displays a TTL "exceeded in transit" message, at which point the packet is discarded. By using this method, access information on the firewall can be determined if successive probe packets are sent.

© 2012 The SANS Institute Author retains full rights.

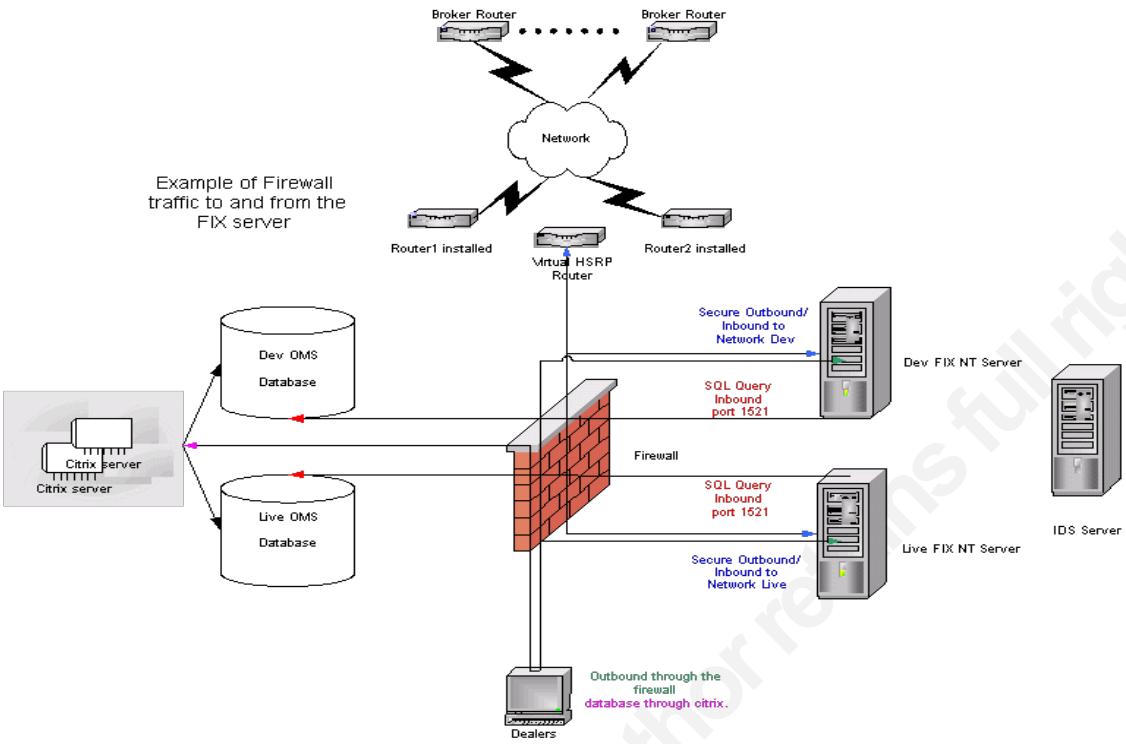

Fig 7: General FIX Infrastructure (FIX Protocol Ltd, 2011)

2.1.5 SQL Injection

Web-based attacks like SQL injection have a lower frequency and didn't even make the top ten on the annual report that will be published later this year. The rate of SQL injection attacks is usually much higher for "financial services organizations" said Wade Baker, Director of Risk intelligence at Verizon. This statement alone is cause for serious concern. Wade Baker of Verizon also states, "One problem that doesn't seem to improve from year to year has to do with breach discovery. It takes the majority of organizations months to discover a breach and some of them even take years. Furthermore, the discovery of these breaches is usually the result of external action, like law enforcement agencies or other organizations informing the affected companies. Finding a breach months or even years later is unacceptable and can be disastrous for financial firms. Wade Baker points out, "By Restricting outbound connections to ports that are necessary for the organization's communications is equally important as monitoring incoming traffic. This is known as egress filtering and can help prevent breaches. Whitelisting applications

© 2012 The SANS Institute Author retains full rights.

that are allowed to run on servers can prevent attackers from installing and executing malware on systems they've gained access to. It's much easier to allow only some applications and services to run and block everything else, then to build a list of malicious programs and continuously add to it" (Network World, 2012)

SQL Injections can be especially harmful when trying to access trade reporting via a financial firm's website. Vital statistics for compliance and trading employees that cannot be accessed due to a SQL injection can have a huge affect on post trade commissions and post trade allocations. Any disruptions in reporting trades to the tape will alert Financial Industry Regulatory Authority (FINRA) to investigate, which will cause unnecessary legal fees and valuable time spent.

3. Conclusion/Solutions

When dealing with FIX security defenses on an individual Engine basis it is necessary to be prepared. Knowing the company's disaster recovery plan is essential. Companies need to keep their systems patched, shut off any unneeded services, and implement anti-spoof filters at vital network gateways. Financial firms IT teams need to implement effectively the six stages of incident handling. (Preparation, Identification, Containment, Eradication, Recovery, Lesson Learned) (P.I.C.E.R.L)

Identification is a key and essential phase of the cycle. IT teams "MUST" identify the problem as quickly as possible by monitoring and diagnosing system issues. Without proper identification the following four steps cannot be completed correctly or effectively. By monitoring the existing FIX connections up/down status, the firm will be able to quickly identify a connection issue between Sender Comp (Tag 49) and Target Comp (Tag 56). If a hacker is able to penetrate the Tradescope application, which is used to monitor these types of connections, the hacker will essentially own the application and create havoc for a trading floor, by bringing down or spoofing connection status. Most firms rely on the firm hosting the connection to monitor each connection. One potential safeguard would be if other broker dealers could monitor the incoming and outgoing connections as well. The firm will need revert to fall back procedures until the problem has been successfully identified, contained, eradicated and recovered.

© 2012 The SANS Institute Author retains full rights.

Customers will have to telephone orders in to the trading desk while the back office and trade support deals with amends/cancels. Ensure your IT team can get their systems back in synch when everything is up and running again. Make sure you notify brokers or any other interested parties, such as settlements and clearing.

Current FIX implementations only allow static (manual) failover to a redundant data center by configuring the FIX clients with a backup FIX server IP address. Clients connect to the alternate site when connectivity to the primary site fails. Using client-enforced failover to a disaster site is neither reliable nor dependable. Any failure in connectivity between client and its corresponding servers will result in the client failing over to the alternate location, and not all clients will consistently failover. To make certain of consistent application performance and client service, the FIX application provider must implement rapid automatic and transparent disaster recovery that operates independent of the clients, and is strictly based on a network and application state.

A technology firm called Brocade amongst others in the space, has developed a product called ServerIron FIXSWITCH that helps create and manage virtual FIX application server farms, which separates client connectivity management from the internal network and the server farm management. According to Brocade, "FIX application providers simply need to expose a single virtual IP address to all external clients to connect to the FIX servers and the virtual IP address will logically bound to multiple real server addresses belonging to redundant pairs of FIX Servers" (Brocade, 2012). Client connections requests are first received by the switch, which identifies the client and bounces the request to the corresponding pair of redundant FIX engines assigned to the particular client. Client identity will be based on a choice of Layer 3 (IP), Layer 4 (TCP Port), and Layer 7(FIX header SenderCompID field) information. Brocade states that, "The ServerIron, will intelligently load balance, content switch, which will inspect deep into FIX application messages to indentify the FIX client and send connection requests to the corresponding redundant FIX servers" (Brocade, 2012). By switching client connections to the servers based on FIX message content as opposed to TCP/IP information gives financial trading firms added flexibility, scalability, and security for their FIX infrastructure

Other methods of protecting FIX messaging are useful as well. A lot of companies are implementing IPSec to protect FIX over the Internet. By installing a router with IPSec on the buy

© 2012 The SANS Institute Author retains full rights.

side and sell side just before your FIX elements will be very effective. This way both the end network elements can speak plain-text FIX, and the routers will encrypt and decrypt the FIX as it is transmitted over the Internet. Using 128/256-bit encryption and AES, will make it difficult to break and it will be safe from sniffers like Wireshark and Kismet. It is essential that your FIX engine listens on different ports, and binds each port to a client identity. The reason is that if a firm implements Stunnel. Stunnel is an open source multi-platform computer program, used to provide universal TLS/SSL tunneling service. Stunnel is a very useful tool, but cannot validate FIX fields. If you have two instances of Stunnel to the same port on your FIX engine, spoofing can occur.

In closing: I hope this paper adds value to the existing security infrastructure for financial firms by making trading staffs across Wall Street aware of the dangerous implications of malicious intent. Always keep in mind that it is a lot easier to hack "people" than it is to hack networks. Internal security is often at times is a lot more important than network security is. A company must be secure from top to bottom and always apply a multi-layer approach to Information Security.

Darren DeMarco

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

4. References

FIX Protocol Ltd. (2011). The FIX Protocol Organization. Retrieved December 1, 2011, from FIX Protocol Web Site: http://fixprotocol.org/what-is-fix.shtml

NYSE Technologies (2011). Appia FIX Engine. Retrieved December 11, 2011, from NYSE Technologies Web Site: http://nysetechnologies.nyx.com/enterprise-software/appia

CameronTec (2011). FIX Engine. Retrieved December 20, 2011, from ORC Software Web Site: http://www.camerontec.com/

Wired Magazine (2011). NSA investigates Nasdaq Hack. Retrieved December 21, 2011, from Wired magazine Web Site: http://www.wired.com/threatlevel/2011/03/nsa-investigates-nasdaq-hack/

Network World (2012). More Than Half of Organizations. Retrieved January 25, 2012, from Network World Web Site: http://www.networkworld.com/news/2012/030112-more-than-half-of-organizations-256830.html

FIX Protocol Ltd. (2008). Industry Driven Messaging Standard. Retrieved January 25, 2012, from FIX Protocol Web Site: http://www.fixprotocol.org/documents/5098/FIX%20Security%20White%20Paper-1.8-FINAL.pdf)

FIX Protocol Ltd. (2012). FIXimate. Retrieved January 28, 2012, from FIX Protocol Web Site: www.fixprotocol.org/**FIXimate**3.0/

FIX Protocol Ltd. (2012). Industry Driven Messaging Standard. Retrieved February 25, 2012, from FIX Protocol Web Site: http://fixprotocol.org/

FIX History (2012). Implementation Guide. Retrieved March 2, 2012, from FIX Protocol Web Site: http://fixprotocol.org/implementation-guide/introduction.shtml

Financial Information Exchange (2012). Diagrammatic representation of FIX system. Retrieved March 2, 2012 from Wikipedia Image Web Site: http://en.wikipedia.org/wiki/Financial_Information_eXchange

© 2012 The SANS Institute Author retains full rights.

NYSE Technologies (2007). Solutions for Trading Better. Retrieved March 2, 2012, from NYSE Technologies Web Site: https://nysetechnologies.nyx.com

FIX Messaging (2012). Quick FIX Messenger. Retrieved March 2, 2012, from Wikipedia Images Web Site: http://code.google.com/p/quickfix-messenger/wiki/Index

FIX System Connectivity (2012). Connectivity. Retrieved March 2, 2012 from Financial Programmers Web Site: http://financialprogrammers.com/blog1/the-fix-protocol/

Search CIO (2012). Tech Target. Retrieved March 2, 2012 from Tech Target Web Site: http://searchcio.techtarget.com/definition/99999

Brocade (2012). ServerIron FIX Switch. Retrieved March 4, 2012 from Brocade Web Site: http://www.brocade.com/solutions-technology

DeMarco, Darren (2012). "Disaster Recovery for Trading Floors". Retrieved March 5, 2012 from SANS Web Site: http://www.sans.org/reading_room/

SEC Laws on Insider Trading (2012). Insider Trading Laws. Retrieved March 7, 2012 from SEC Web Site: http://www.mystockoptions.com/faq/index.cfm/catID/1FD3C7CF-447A-495D-9F39DB594775DBE5/ObjectID/D943A6B7-30A9-11D4-B9080008C79F9E62

© 2012 The SANS Institute Author retains full rights.