FIXEdge Security Assurance

Preface

FIX Trading Community is constantly working on the analysis of the challenges in the field of cybersecurity and on the elicitation of the various security threat scenarios which represent possible strategies a hostile party may employ to disrupt, imitate or change legitimate message traffic between electronic trading counterparties. The FIX Security White Paper was developed as a result of community efforts to incorporate these scenarios.

FIX Antenna and FIXEdge follow the recommendations published by FIX Trading Community to address all the current issues and challenges on the front of the cybersecurity, to satisfy best practices and all the crucial requirements of the industry.

FIX Security White Paper Points

The section below describes main points extracted from the FIX Security White Paper and related features/measures implemented/envisaged in FIX Antenna and FIXEdge.

What considerations should be made in developing or testing FIX software?

Steps/Actions	Countermeasures in FIX Antenna C++/.NET	Countermeasures in FIXEdge
Buffer overflows, such as copying data into buffers without checking that the buffers are adequately sized, including a terminating NULL character if necessary	• FIX messages validation • Internal static code analysis against buffer overflows and other security breaches	• FIX messages validation • Internal static code analysis against buffer overflows and other security breaches
FIX formatting errors, such as improper handling of binary data fields in FIX (which may contain 0 or ASCII) and tags without values		
Data type errors, such as attempting to parse a text or binary string inappropriately placed in an integer or floating point field		
Data range errors, such as passing 0 or a negative number into a field that represents share quantities or passing invalid enumeration values		
Security errors, such as accepting messages sent prior to a valid Logon, or failing to detect if the counterparty's SenderCompID changes during the course of the FIX session		

Security Threat Scenarios

#1) Manipulation of trading activity

Steps/Actions	FIX Engine resposibility	Countermeasures in FIX Antenna C++/.NET	Countermeasures in FIXEdge
A Hacker "spoofs" a legitimate client IP address and establishes a FIX Session at a broker's connectivity platform. The hacker presents as a client by imitating the legitimate FIX message traffic. The hacker uses this "counterfeit" FIX channel to generate fake orders to trade as a client. The FIX orders generated by the hacker are sent down to the venue and acted upon creating potential error positions with the client, broker and/or market.	Partially	SSL/TLS support	SSL/TLS support
In this "man in the middle" scenario, a hacker penetrates a sell side broker network. The hacker intercepts the inbound order messages from a legitimate client and modifies the FIX payload with invalid parameters. The corrupt orders are then delivered to the execution venue. Examples of payload manipulation include changing the order quantity, side, traded security and or algorithmic trading parameters.	No	-	-

A hacker employs an agent to initiate an intentional or accidental replay of data. The intentional or accidental replay of data will make it extremely difficult for the sending/receiving firm to identify the genesis of the information.	No	-	-

#2) Illegal access to client order/trade information

Steps/Actions	FIX Engine resposibility	Countermeasures in FIX Antenna C++/.NET	Countermeasures in FIXEdge
A hacker is able to insert a passive listening agent between counterparties. One scenario of particular concern would be where a hacker introduces a passive listening device between a client and broker FIX sessions to listen for order and execution messages. The hacker would be in a position to parse network traffic to determine positions that a client has accrued with the intent of front running or trading ahead. The hacker can be listening on any number of FIX connections, including the order entry channel or an asynchronous drop copy line. Another variation of this scenario would be a hacker that was able to listen to messages related the clearing and settlement process.	Partially	SSL/TLS support	SSL/TLS support

#3) Denial of Service

Steps/Actions	FIX Engine resposibility	Countermeasures in FIX Antenna C++/.NET	Countermeasures in FIXEdge
A hacker is able to gain access to FIX Session ports at a sell side broker or an exchange. The hacker fires off a program to continuously attempt to open and close the session. This consumes system resources on the target host to the point where the system is compromised.	Yes	Protection from DDoS attacks and abnormal user behavior	Protection from DDoS attacks and abnormal user behavior
A hacker is able to open a FIX session imitating the characteristics of a legitimate client and sends in a continuous wave of small orders (that pass under the radar of pre-trade controls) and ultimately consume system resources on the target host to the point where the system is compromised.	No	-	-
A hacker introduces a passive listening agent on a sell side broker's connectivity network. The agent collects information on external client connectivity characteristics. The hacker then creates simulated client sessions binding to a given FIX port, preventing legitimate clients from establishing FIX connectivity.	No	-	-
Classic Buffer Overflow Attack. A hacker is able to open a FIX session imitating the characteristics of a legitimate client. Through previous observation of FIX traffic, the hacker is able to construct FIX messages that imitate legitimate order traffic. The hacker attempts to create instability by inserting individual FIX tag values that exceed the designed/expected string/buffer lengths causing unexpected 'overflow' into areas of system memory. Depending on how rigorous a level of FIX message validation is applied by the counterparty, it is possible that the corrupted messages could crash an electronic trading system.	Yes	Messages validation	Messages validation

#4) Hacker targets connectivity infrastructure as an avenue to introduce malware

Steps/Actions	FIX Engine resposibility	Countermeasures in FIX Antenna C++/.NET	Countermeasures in FIXEdge
A hacker identifies a weak link in the connectivity infrastructure that can be used as a channel to introduce a malware agent. Specific examples of vulnerabilities include flaws in the Firewall/ACL and the implications of direct cross connect wiring established at a co-location exchange data center.	No	-	-

Overall Security Features Supported in FIX Antenna C++/.NET and FIXEdge

Feature	FIX Antenna C++/.NET	FIXEdge
Internal static code analysis against buffer overflows and other security breaches	Yes	Yes
Protection from abnormal user behavior (including DDoS attacks)	Yes	Yes
SSL/TLS with keys management for both initiator and acceptor roles	Yes	Yes
Support for custom encryption algorithms	Yes	Yes
FIX messages validation	Yes	Yes
Filtering against IP range and ports to be used for connection	Yes	Partially, filtering against IP only
Settings for TCP protection	Yes	Yes

Related How-To Articles

FIXEdge related:

- How to configure SSL connection
- How to configure FIX messages validation
- How to configure TCP protection in FIXEdge
- Overload protection in FIXEdge
- How to specify multiple IP addresses per FIX Session
- FIXEdge installation with the principle of least privilege on Linux

FIX Antenna related:

- How to use SSL with FIX Antenna C++ and FIX Antenna .NET
- How to configure FIX messages validation
- How to specify multiple IP addresses per FIX Session