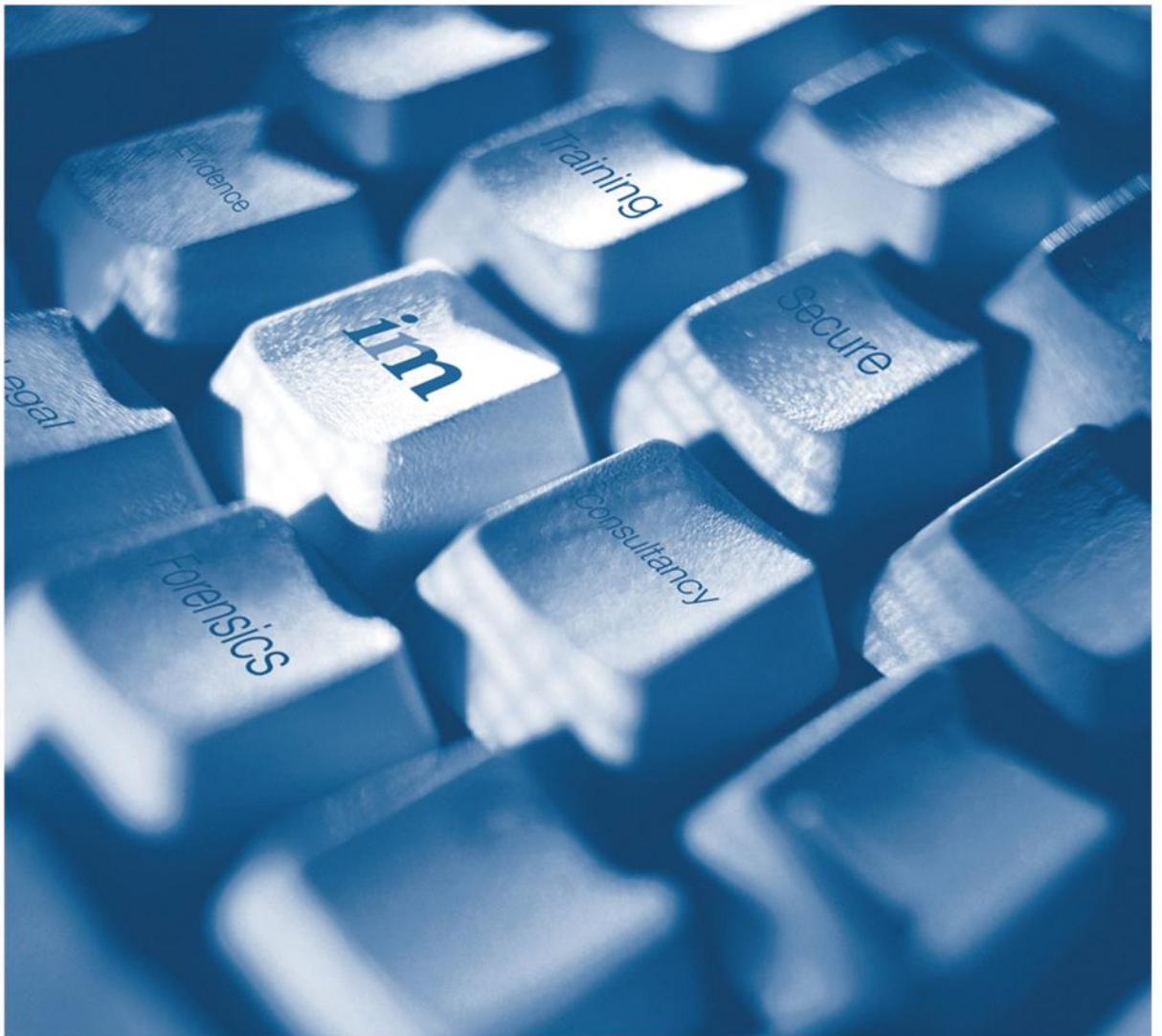




Risky Business – Hacking the Trading Floor

Gyan Chawdhary



Risky Business – Hacking the Trading Floor

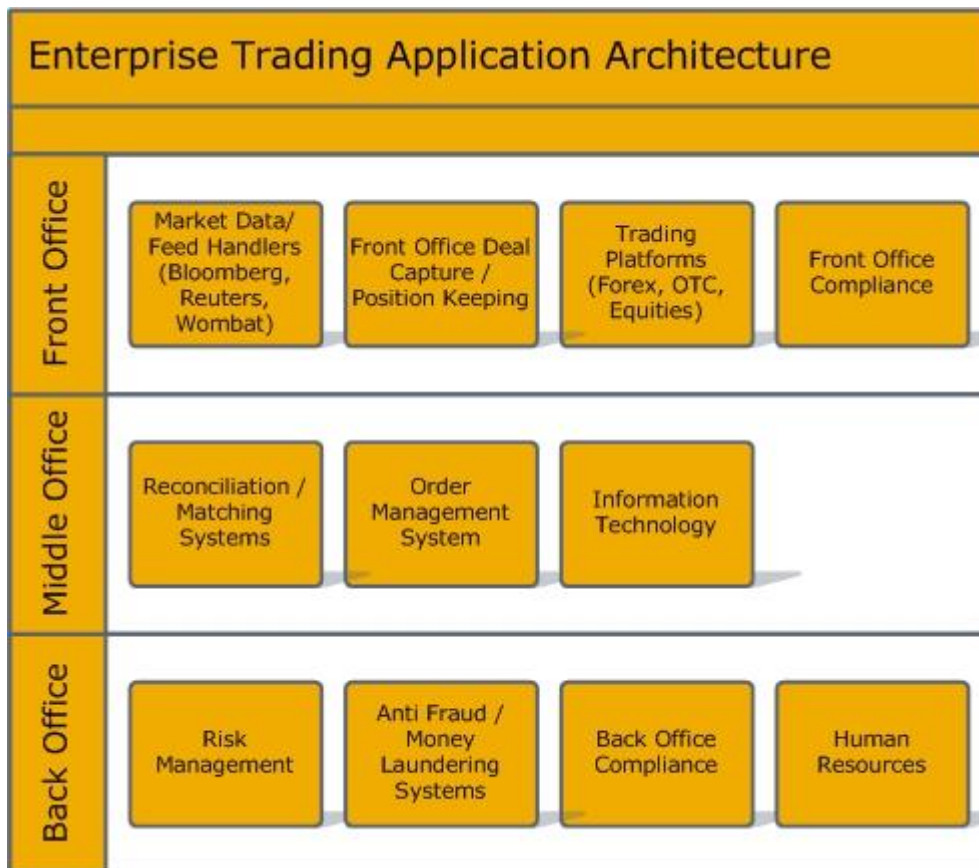
Introduction

When Nick Leeson, the infamous derivatives trader, brought down *Barings Bank* in 1995 by speculating on the Asian futures market, the financial world was shaken by the biggest cover-up fraud committed in the history of modern day banking. What further made this case interesting besides the spectacular losses and collapse of Barings itself was the use of technology to conceal his activity. Nearly a decade later, hardly much has changed with names such as Matt Piper, John Rusnak and more recently that of *Societe Generale's* trader Jerome Karviel who all successfully leveraged their knowledge of backend processing and risk control systems to perpetrate such frauds. Due to the very nature of these incidents, one might never fully understand the true attacks in this domain, and the nature of their manifestation across a banking organisation. However, with the rate of change and demand in today's fast-paced banking environments an even greater threat of application security issues lies within these trading platforms which has largely been left unaddressed.

Drawing on the author's experience of working on large Forex, over-the-counter and proprietary trading systems for Fortune 500 banks, this paper aims to highlight the current application security trends and issues within financial trading applications and the common business risks associated with these issues. This paper is aimed at security managers, strategic decision-makers or anyone who wishes to understand some of the business risks and potential impact of these threats and further gain a better understanding from the attack scenarios in order to implement appropriate countermeasures. The paper should also help security testers gain a high level understanding of these applications, and the true business implications of inherent vulnerabilities within these applications that if successfully exploited could be financially devastating to the victim organisation.

Application Risk Profile of a Trading Floor

Before we understand the various application level risks affecting a trading environment, we need to understand the risk exposure and vulnerability exploitation potential. We can gain a better understanding of how applications communicate within different environments and associated risks with their modus operandi through diagrammatically viewing the relationship between applications and their proximities. The following diagram presents a basic high-level architectural view of a trading floor application environment:



Front Office

The front office primarily supports the buying and selling operations of securities by traders and sales staff within a financial institution. The applications comprising support of the front office include trade execution, news data feeds, deal monitoring and position keeping applications. From a security viewpoint front office applications may be viewed as 'high risk' due to the placement and business critical functionality offered by these systems.

Middle Office

The middle office group primarily supports risk management operations and closely works with the front office, managing risk and conducting deal accounting operations. Further, the middle office provides post-trade support and portfolio modelling, and relaying relevant information to the back office support team. In some scenarios this function may be undertaken by the back office completely. Due to the cross-functional nature and interface

complexity, middle office applications are considered critical as accounting, reconciliation and book keeping is performed at this layer and processed at the back end.

Back Office

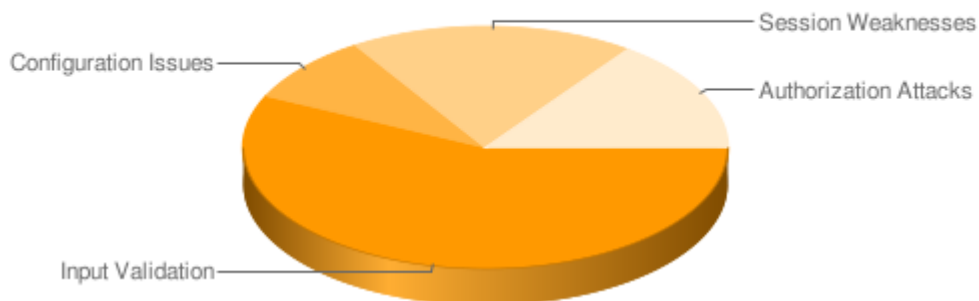
Often overlooked during security assessments, the back office primarily supports trading floor administrative tasks including clearance, deal settlements and acts as the main regulatory compliance and accounting body within a trading environment. Since all logging and compliance data is stored within the backend systems, the applications allowing access to this information are considered critical, especially for incident accountability.

Common Weaknesses & Design Flaws

Below is a list of the top 5 security issues identified by IRM which affect trading platforms. The analysis was derived using test data gathered from roughly 70 application tests conducted by IRM, specifically within the BFSI sector over the past year:

- Input validation threats were still the main cause of security compromises, and accounted for roughly 57% of all compromises within the trading application environments. The two main vulnerability classes included insufficient parameter validation and application logic related flaws based solely on client-side validation controls.

Industry Sector Meta-analysis : Types of Issues by Class



- A low number of SQL based issues were reported within web application environments. However these threats were more prevalent within thick client applications, namely Forex and back office application environments.
- Configuration related issues within web server hosting environments and web application server technologies comprised nearly 9% of application attacks. These included issues ranging from directory traversal and configuration file exposures to default vendor credentials, which provided avenues for completely shutting down the application hosting environment.
- Roughly 19% of attacks were related to session management and user segregation. These mainly included issues related to de-allocation of session management cookies and client-side authentication.

- Around 15% of issues whose security implications directly allowed unauthorised trading within trading applications resulted due to weak authentication and authorisation controls.

Example Threats

OTC (Over-The-Counter) Trading Platforms

Unlike exchange traded securities, OTC (Over-the-Counter) trading is carried out directly between two parties using OTC contracts. Organisations mainly dealing in OTC traded securities such as derivatives, debt instruments and discrete products may include large banks, institutional investors, market makers and hedge funds. Furthermore the applications supporting these products are generally designed in-house but may also be developed around third party COTS trading platforms. OTC trading platforms consist of a multitier cross-platform solution using a component-based architecture within the organisation's internal application environment for both scalability and application integration. Sales traders, marketers and certain middle office functionaries can access the application using both web-based and thick clients.

Unauthorised and Fraudulent Securities Trading

As most OTC platforms allow cross-functional access to the trading environment, privilege levels may be restricted and limited based on a users organisational profile. This access may be granted based on the user roles, such as sales traders, marketers and middle office functionaries. A common example may include sales traders vs. marketers or analysts. Sales traders can execute trade orders on behalf of their clients; the privilege level for such users is generally higher than those of analysts or marketers who may only require specific knowledge on a product being traded on these systems. Furthermore access requirements may change based on back office, product development teams and third party client access. Due to the complex user access and segregation requirements in the above scenario a key area of weakness may be the inadequate authorization and access controls enforced within these systems. IRM found numerous applications, both third party and in-house designed, susceptible to such attacks that directly allowed users to bypass, or override their account settings and execute unauthorised trades. A majority of the attacks were considered extremely trivial to exploit, simply requiring a browser to access restricted resources. Furthermore, the issues allowing such access were pertinent to applications written in both .NET and Java.

Securities Manipulation and Insider Trading

OTC systems generally contain application interfaces for accessing product specific data for clients. These may include both marketing collateral for a derivate product and risk models for the underlying assets. The key security controls to be investigated during a security assessment would involve segregation of information between multiple clients.

Once again it was observed that a high number of applications and systems adopting the above architecture were vulnerable to common input validation based vulnerabilities which allowed unauthorised clients to access documents pertaining to both pricing and risk modelling information for financial products supported by these applications. From a business risk perspective, these issues could allow competitors to influence the profit viability of derivative instruments whose underlying components can be manipulated such as currencies and equities based derivatives. Further, competitors may use this information to develop similar products by gaining access to this information.

Business Intelligence

As OTC instruments are directly traded between two parties, the applications supporting these products provide buy-side interfaces for clients to execute trades. These may either include dedicated application interfaces for a particular trading party, or a common application environment whereby investors can log onto a centralized trading environment to place orders. Other than the issues discussed above, a common issue found throughout OTC systems was lack of server-side controls which yielded the ability for a user to view client company logos of registered customers, thereby allowing enumeration of the trading system's entire client base. Although such issues cannot directly impact the security of the application itself, attackers may use this information to reverse engineer a client's portfolio, as this information is grouped based on asset class and industry sector.

Foreign Exchange (Forex) Trading Platforms

Foreign Exchange or Forex for short are financial instruments which involve the direct trading of currencies between two countries. These instruments can further be converted in specialized products such as currency swaps, FX options and traded directly as OTC contracts. Generally there are four main types of Forex brokers, however for the scope of this document we will only discuss Market Maker and Small Cap broker based client-side FX systems as these are mostly used in retail and interbank trading environments. Further the business risks and security issues discussed here are common across all Forex based platforms.

Unauthorised Manipulation of Client Spreads

Although some of the most business critical risks associated with Forex applications are similar to those encountered in any front office application environment, IRM identified certain application security issues which were unique to Forex trading environments.

In order to gain a better understanding of the business risk associated with client spread manipulation, we first need to understand where client spreads fit in the Forex trading environment. Like any brokerage business, profits are generally made on trading commissions. From a Forex broker's perspective, commission fees on Forex broking is based on each trade executed by the trader, and further leveraged using client spreads that are derived and internally set by brokerage firms. The client spread is calculated on the original client spread received from the market makers, which are indirectly based on market operator. Based on this fact, if a vulnerability existed within the application allowing client spread manipulation, malicious users could change the otherwise enforced client spread, thereby negatively impacting the initial BEP mark (Break Even Point) for a particular trade. A high number of in-house developed Forex systems were found vulnerable to such attacks which led to the manipulation of client spread, specifically due to authorisation and user segregation issues within these applications.

Unauthorised Currency Pair Manipulation

Forex instruments involve the buying and selling of currency against another currency. Currency pairs are generally set internally by the bank, based on volatility and other factors affecting its price movement. From an application security perspective, the ability to manipulate this information and trade invalid currency pairs which are otherwise not being traded by the firm can result in serious trading losses for an organization. IRM discovered that numerous FX applications were vulnerable to attacks allowing malicious traders to create unauthorised currency pairs with fraudulent base and quote prices, which are otherwise not traded on the Forex platform. This could directly result in creation of malicious currency pairs which can then be listed as valid for trading purposes.

Conclusions

The very nature of the investment banking industry involves buying and selling of risk. It is imperative that the systems employed to assist in handling of these risks are subjected to the same level of rigour with regards to risk assessment and management. Traditional application and product security assessments have always involved the auditor simply analysing and focussing on the application security issues without possessing a thorough understanding of the underlying business functionality. However unlike classic application testing scenarios, the arena of financial application security requires a thorough understanding of the underlying business functionality, primarily with regards to identifying the complex business risks associated with a threat. In conclusion, as these incidents are likely to increase both in size and frequency, the risk exposure from software implementation vulnerabilities should be addressed by organisations, especially due to the large financial risk at stake.

About the Author

Gyan Chawdhary is a Senior Consultant heading up the Financial and Embedded Systems Security Centre of Excellence at IRM's European Technical Centre in the UK. He is a key member of IRM's Code Auditing & AP team and performs a range of consultancy services which include code auditing, software security and vulnerability assessments. With over 9 years of experience in Information Security, Gyan's experience includes a broad range of market verticals with specialization in the financial services space. Prior to joining IRM, Gyan was a Managing Consultant at Mahindra British Telecom, where he was involved in establishing and managing MBT's Vulnerability Assessment Centre and conducting research and product assessments for various in-house and commercial applications.

About IRM

Information Risk Management Plc (IRM) is a vendor independent information risk consultancy, founded in 1998. IRM has become a leader in client side risk assessment, technical level auditing and in the research and development of security vulnerabilities and tools. IRM is headquartered in London with Technical Centres in Europe and Asia as well as Regional Offices in the Far East and North America. Please visit our website at www.irmplc.com for further information.