happiest minds
The Mindful IT Company
Born **Digital** . Born **Agile**

Thick client applications

Happiest People . Happiest Customers

Contents

Introduction

The very first step while implementing client/server architecture, is determining whether it is the ‘client’ or ‘server’ that will handle the bulk of workload. The term thick client is rather interesting; on one hand it can be denoted to describe hardware while on the other hand it can be used for applications or software. Here we will briefly glance at the the application part of it.

A thick client or Fat-client is a computer that does not necessitate a connection to a server system to run although they can benefit from being connected to a network and a server. In other words it is a networked computer with most of the resources installed locally. In fact, majority of thick clients have their own operating system and software applications and can be used offline i.e. when not connected to any network or server. PC’s (personal computers) for example, are thick clients because they have their own hard drive, DVD drives, software applications and so on.

Thick clients are almost unanimously preferred by network users. Thick clients offer more features, graphics and other choices making the applications customizable where the user has more control over what programs he installs in the specific system. Thick clients have several advantages – good architecture, decoupled design, can be used offline, improved performance for multimedia applications, increased flexibility and higher server capacity (allowing support of more users) that leads to better structure, modular caching, separating responsibilities and creating more static assets. Since most of the processing is done locally in case of thick client, the servers are accessed mainly for storage purposes. Thus, thick clients are not well suited for public environments and are often found in the business settings where servers are used to provide some data and application support.

Thick client and security

Vulnerabilities can be found at application layers and some of them may be severe enough and can lead to customer data disclosure or system compromise. To preserve a thick client, the IT department must maintain all systems for software deployment and upgrade them rather than just focusing on maintaining the application server.

Thick Client/Fat Client applications are frequently disregarded by the organizations during security valuation and internal auditing. Many organizations do not have enough internal security staff with the correct tools and experience to perform thick client assessments, which is a tough job. It requires painstaking calculations, certain specialized skills and the right tools to identify critical security vulnerabilities. The following are the list of security checks that can be performed on thick clients on top of the business logic checks.

Application profiling: This involves enumerating the application's functionality and behaviour, understanding the core security mechanisms employed by the application, identifying all of the different entry points for user input and establishing what technologies are being used on both the client and the server. This stage enables in determining the attack surface exposed by the application.

Test the authentication mechanism: This involves testing the authentication-related functionality implemented within the application including registration, login, password change and account recovery functionality.

Test the session management mechanism: This involves testing the mechanisms used for managing sessions and state including testing for insecure token generation and unsafe handling of tokens.

Test access controls: This involves understanding the various access control requirements for the application and testing the implementation of access controls for defects leading to horizontal and vertical privilege escalation.

Test the encryption control: This involves the testing for weak SSL/TLS ciphers suite usage, re-negotiation vulnerabilities, improper cryptography implementation, protection of private key and digital certificate related issues.

Test for input-based vulnerabilities: This involves probing for input-based vulnerabilities that may arise anywhere within a typical application's functionality, such as SQL injection, XSS, command injection and path traversal. It involves fuzzing every parameter to every request with a set of standard attack strings, and manually investigating all anomalous responses that may indicate the presence of vulnerability.

Test for business logic flaws: This involves testing all relevant items of interesting functionality for logic flaws, including multi-stage processes, security-critical functions, transitions across trust boundaries, checks and adjustments made to transaction prices or quantities.

Test for sensitive data storage on files and registries: During the installation and execution of thick client applications, the thick clients might write/modify sensitive details in the files and registries. The sensitive data amassed by these applications usually contain username, passwords, database credentials, license details, cryptographic keys and configuration details like IP address, port, etc.

Test for response modification: In the case of thick clients, most of the major processing/validations are carried at the client side. As a result both the request as well as response modifications play a key role in testing the thick client for vulnerabilities.

Reverse engineering method is used on the application to identify the presence of backdoors and hard coded credentials

using specific tools. The codes can be decompiled if necessary.
Test for DLL hijacking vulnerability involves attempt to hijack DLL files that was loaded by a software installer from the directory where the installer is executed.

Test for DLL hijacking vulnerability involves attempt to hijack DLL files that was loaded by a software installer from the directory where the installer is executed.

Testing Tools

Thick client applications are unique and testing thick clients requires patience and a methodical approach. A simple automated assessment scanning is not enough and one needs specialized tools and custom testing set up. Here are a few tools that can meet the requirements.

Echomirage is an open source tool that directly hooks with the client executable and starts intercepting traffic on the go. There is also an option to hook the client executable with its associated process.

Process monitor are tools that identify files accessed or registry modified when any user double clicks on client executables. In such cases it is important to look for interesting files and investigate further; file names can hint which file should be investigated. It can thus help in application of reverse engineering.

Regmon lists all registry entries which are accessed when someone double clicks client executables. The registry search feature should be used to find keywords, passwords and sensitive information.

BURP proxy invisible proxy mode or BURP proxy tool can be used in invisible proxy mode to intercept the request from non-proxy-aware thick client applications (HTTP/HTTPS traffic only).

Mallory (Transparent TCP and UDP proxy) is a proxy tool that can intercept TCP and UDP traffic and can be used to apprehend network traffic or thick client applications using both HTTP(S) and non-HTTP(S) traffic.

Ethereal/Wireshark is a network protocol analyzer tool that can be used to analyze the network traffic and can be used to study the non-encrypted traffic sent by the thick client applications.

I**nteractive TCP Relay** allows for intercepting the traffic for thick client applications. ITR serves as a TCP tunnel between the client and the server. By instructing the client to open its connection to the ITR instead of the server, the entire connection is shifted to work through the ITR, without the client or the server noticing a difference.

JAVA Snoop can be used to intercept the methods, alter data and also test the security of JAVA applications on a particular computer.

WinHex is a tool used for memory analysis.

There have been enough ongoing debates on the pros and cons of thick v/s thin clients and who will run the show in the future. With the ultimate goal of a more robust computing environment maybe a middle ground where there is a thinner type of thick client or what is gaining popularity as ‘smart client’ is the answer.   Newer technology released year on year is constantly bridging the gap, where thin clients are getting richer and more powerful and thick clients are adding more dynamism. The way forward will be to decide a technology application for a client depending on system requirement and not based solely on architects indulging in the political thick/ thin debate.

About the Author

Karthik Palanisamy,

Karthik Palanisamy, Technical Security Assessment Professional with 4 plus years of consulting experience in network & web application vulnerability assessment and penetration testing, thick client security, database security, mobile application security, SAP application penetration testing, source code audit, configuration review of devices and security architecture review (Applications and Infrastructures).Currently holding a position with Happiest Minds Technologies to deliver technical security assessment and penetration testing services covering application security, infrastructures security, mobile application security and source code review.

About Happiest Minds Technologies

Happiest Minds, the Mindful IT Company, applies agile methodologies to enable digital transformation for enterprises and technology providers by delivering seamless customer experience, business efficiency and actionable insights. We leverage a spectrum of disruptive technologies such as: Big Data Analytics, AI & Cognitive Computing, Internet of Things, Cloud, Security, SDN-NFV, RPA, Blockchain, etc. Positioned as “Born Digital . Born Agile”, our capabilities spans across product engineering, digital business solutions, infrastructure management and security services. We deliver these services across industry sectors such as retail, consumer packaged goods, edutech, e-commerce, banking, insurance, hi-tech, engineering R&D, manufacturing, automotive and travel/transportation/hospitality.

Headquartered in Bangalore, India; Happiest Minds has operations in USA, UK, The Netherlands, Australia and Middle East.

Email: business@happiestminds.com
Visit us: www.happiestminds.com

Follow us on