

COMP [1298] MSc Final Year Project Report

Security Implication in Java RMI

September 2014

Mahabubur Rashid

MSc Computer Forensics and System Security

000582762

Supervisor: Dr George Loukas

Dissertation submitted in partial fulfilment for the degree of University of Greenwich's
MSc Computer Forensics and System Security

Acknowledgements

I would like to express my sincere and genuine gratitude to the following individuals for their great support in this project.

My supervisor, Dr George Loukas, for the incredible support and guidance throughout the work.

Mr. Asif Malik, one of my favourite teachers at the University of Greenwich for being extremely helpful and supportive on numerous occasions.

Contents

1	Abstract:	1
2	Technical background:	2
2.1	What is RMI?	2
2.2	How does RMI compare to RPC?	2
2.3	Technical implementation of RMI:.....	4
2.4	Implementing security manager:	5
3	Security Analysis of RMI technology	6
3.1	Case study -1: security concerns in use of proxy:	6
3.1.1	Vulnerability analysis in light of CIA:	7
3.1.1.1	Client confidentiality:.....	7
3.1.1.2	Client integrity:	7
3.1.1.3	Service confidentiality:	8
3.1.1.4	Service integrity:	8
3.1.1.5	Service availability:	8
3.2	Case study -2: security concerns in serializing data in RMI application:	8
3.2.1	How does Serialization work?	8
3.2.2	How Serialization may affect in RMI applications:	9
3.3	Case study -3: security concerns posed by lack of type compatibility verification in RMI protocol implementation:.....	9
3.3.1	RMI protocol attack	11
3.4	Summary from case studies:.....	13
4	Test application - Breach of confidentiality:.....	14
4.1	Overview:	14
4.2	Application components:	14
4.2.1	Job Interface:	14
4.2.2	Remote Interface:	14
4.2.3	Server-side implementation:	15
4.2.4	Client-side implementation:	15
4.3	Things to take care of before running the service:	16
4.4	Application in action:	17
4.5	Attack through impersonating a client:	18
5	Test application –non-public data serialization:.....	19
5.1	Overview:	19

5.2	Application components:	19
5.2.1	Remote interface:	19
5.2.2	Server-side application:	19
5.2.2.1	Employee:	20
5.2.2.2	Manager:.....	20
5.2.2.3	Server-side application:	21
5.2.3	Client-side application:	21
5.3	Application in action:	22
6	Test application - absence of type compatibility verification in RMI protocol implementation:	25
6.1	Overview:	25
6.2	Application components:	25
6.2.1	Remote Interfaces:.....	25
6.2.2	Server-side implementation:	25
6.2.3	Client-side implementation:	25
6.3	Application in action:	26
7	Evaluation:	27
7.1	Methodologies and processes:	27
7.1.1	Conjugating technical jigsaws:	27
7.1.2	Literature review for security vulnerability:	27
7.1.3	Application development process:	27
7.1.4	Version controlling:.....	28
7.2	Strengths and weaknesses:.....	28
8	Reflection:	29
8.1	Challenges faced:	29
8.2	Further work:	29
9	References and Keywords:.....	30
9.1	References:	30
9.2	Keywords:.....	32
10	Appendices:	33
10.1	Appendix A – Technical Terms:	33
10.2	Appendix B – RMI Exceptions:	34
10.3	Appendix C – Project timelines and Gantt chart:.....	40

1 Abstract:

This project investigates the security measures in Java RMI, a technological mechanism allowing a server and a client to communicate by passing information relying on the Java Remote Method Protocol (JRMP^[Appendix A]). Java RMI allows an object running in one JVM^[Appendix A] to invoke methods on an object running in another JVM. Thus RMI facilitates the remote invocation of Java object methods and sharing of resources and services. RMI also allows a client and a server to load new object types dynamically as required.

RMI architecture is divided into Application layer, Stub and skeleton layer, Remote reference layer and Transport layer.

The advantages of Java RMI can be described as:

- ⇒ Portable to any JVM
- ⇒ Part of Java's write once run anywhere (WORA) approach
- ⇒ Safe and secure: uses built-in Java security mechanisms to facilitate system safety during user download implementations
- ⇒ Easy to write and maintain: facilitates writing of remote Java servers and Java clients that access those servers

(Techopedia n.d.)

RMI or Remote Method Invocation is a java API that is used to perform the Object Oriented equivalent of Remote Procedure Calls with support for serialized objects transfer and distributed garbage collection. Since the transfer of objects takes place between machines in different address spaces, there are various security measures which are controlled by java security manager.

This project will explore how and to what extent these security measures are controlled by the java security manager, whether there are any holes in the current scope of the java security manager, and how these security issues pose any threat to the host of a remote object when unaddressed.

This dissertation looks into the detailed technical implementation of RMI technology scrutinizing various security aspects. To achieve its purpose, the project is primarily divided into research and technical test bed development. The research is carried out to analyse both technical and security aspects of the RMI technology. Any *hypothetical concept* is then coupled with technical implementations to artificially create scenarios making attempts to demonstrate a *proof of concept*^[Appendix A].

2 Technical background:

2.1 What is RMI?

Java RMI is a mechanism to invoke a method on a remote object that exists in a different address space. The address that owns the object on which a method is invoked may be on the same machine or different one altogether. RMI can be seen as an object oriented way of RPC^[Appendix A].

(Baclawski, 1998)

2.2 How does RMI compare to RPC?

As Waldo (1998) explains in his comparative discussion, Java RMI or Remote Method Invocation is a java based Remote Procedure Call or RPC. This has many features which are similar to other RPC systems, such as allowing an object running in one Java virtual machine or JVM to make a method call on an object running in another JVM, which is often a different physical machine.

Although the RMI system seems like just another RPC mechanism on the surface, with a much closer look, RMI represents a very different evolutionary progression. This progression results in a system that not only differs in detail but also in the very set of assumptions made about the underlying distributed systems it operates in. This leads to differences in the programming model, capabilities, and the interaction mechanisms of the code with its implementation and the built distributed systems.

In RMI, like an RPC system, the proxy on the client (calling) side is known as a *stub*, while the proxy on the server (receiving) side is known as the *skeleton*. *Stubs* are compiled into calling code and render any call into some machine-neutral data representation, this process is called *marshalling*. The data then gets transmitted to the *skeleton* on the receiving machine which translates the transmitted information into appropriate data types for that machine; this process is known as *unmarshalling*. *Skeleton* identifies the code that needs to be called with the transmitted information, and will make the call. *Skeletons* also *marshal* any return values and transmit them back to the *Stub* that made the call, which in turn *unmarshals* the return values before returning to the calling code.

According to the Oracle's functional definitions of *stub* and *skeleton*, when a stub's method is invoked, it performs the following:

- ❑ initiates a connection with the remote JVM which contains the remote object,
- ❑ marshals, i.e. writes and transmits, the parameters to the remote JVM,
- ❑ waits for the result of the method invocation,
- ❑ unmarshals, i.e. reads, the return value or any exceptions returned, and
- ❑ returns the value to the caller.

On the other side, a *skeleton* is responsible to dispatch a call to the actual remote object implementation. When an incoming invocation is received by a *skeleton*, it does the following:

- ❑ unmarshals, i.e. reads, the parameters for the remote method,

- invokes the method on the actual remote object implementation, and
- marshals, i.e. writes and transmits, the result, i.e. a return value or exception, to the caller.

Waldo (1998) carries on in his paper, the generation of *stub* and *skeleton* in an RPC system happens automatically, based on language and machine-neutral interface-definition language descriptions (IDL) of the calls that can be made. This describes the procedures or methods that may be called over a network and the data that is passed to and from those procedures or methods. With the help of this description, the programmer can invoke an IDL compiler that produces *stub* and *skeleton* source code for *marshaling*, transmitting, and *unmarshaling* the data. This code is then compiled for the target machine and linked to the relevant application code. In RMI stubs and skeletons are generated by the *rmic* compiler.

While RPC, having a machine-neutral IDL, deal with heterogeneous language, RMI assumes that both the client and server are java classes running in Java Virtual Machine which makes the network a homogeneous collection of machines. The RMI system assumes that all objects forming a distributed system are written in Java. The concept has been made to be single-language assumption by RMI's designers to simplify the overall system. Another benefit of single-language assumption is that the RMI system does not need a language-neutral IDL but simply uses the Java interface construction to declare accessible interfaces remotely.

The Java-centric design of RMI lets the system take advantage of the Java environment's dynamic nature, allowing code to load any time during execution. While in RPC systems all code needed for communication between processes have to be available at some time prior to that communication, RMI makes extensive use of dynamic code loading, from stubs representing remote objects to real objects that can be passed from one part of a distributed system to another. The ability of downloading code between machines plays the most prominent role to pass full objects into and out of an RMI call. RMI's single-language assumption allows almost any Java object to pass as a parameter or return value in a remote call. Remote objects are passed by reference by passing a copy of the object's stub code whereas non-remote objects are passed by value by creating a copy of the object in the destination.

The objects that are passed through the network in an RMI system are real objects, not just data that makes up the object's state. This distinction becomes obvious when a subtype of a declared type passes from distributed computation member to another. Passing a subtype object could result in an unknown object being returned. As a subtype can change the behaviour of known methods in an object, simply treating the object as an instance of a known type might change the results of making a method call on that object. To avoid such changes, RMI uses a Java Object Serialization package to marshal and reconstruct objects. This package annotates any object with sufficient information to identify the object's exact type and its implementation code. So when an object of a previously unknown type is received on an RMI call, the system fetches the code for that object, verifies it, and dynamically loads it into the receiving process. In RMI system, therefore, distributed computations can use all the standard object-oriented design patterns that rely on polymorphism. On the contrary, RPC system does not allow

polymorphism; it means that the transmitted object's type or its reference type cannot be a subtype of the type expected by the skeleton.

In the RMI system, a remote object's stub is originated with the object and can be different for any two objects with the same apparent type. The system locates and loads these stubs at runtime as it determines what the exact stub type is. This association makes the stub an extension of the remote object in the client's address space, rather than some way of contacting the remote object built into the client. This approach allows programmers to build a variety of "smart" proxies.

2.3 Technical implementation of RMI:

According to Baclawski (1998), RMI employs three processes to support remote invocation. These are:

1. Client process: this is the process that invokes method on a remote object.
2. Server process: this process owns the remote object. The remote object is an ordinary object that resides in the address space of the server process.
3. Object Registry: this is a name server that relates objects to their names. Once a remote object is registered in the Object Registry, this can be accessed by a client process using the name of the object.

There are two types of classes used in java RMI, namely a Remote class and a *Serializable* class.

A Remote class is a class whose instances are used remotely. Such objects are sometime referred to as *remote object* and can be referenced in two ways:

- i. Like any ordinary object within the address space where the object is constructed.
- ii. Within a remote address spaces using *object handle*. There are some limitations on how an *object handle* can be used but mostly it can be used the same way as an ordinary object.

A *Serializable* class is a class whose instances can be copied from one address space to another. An instance of this class is often referred to as *serializable object*.

When a *serializable object* is passed as a parameter or return value of a remote method invocation, the value of the object is copied from one address space to the other. However, in such case for a *remote object*, the *object handle* is copied from one address space to the other. This begs the question, what happens when a class is both *Remote* and *Serializable*? A blog in StackOverflow (June 2011) addresses the answer to this as the object is serialized instead of being passed as a remote reference provided that the class of the object implements both the *Remote* and *Serializable*. Although this may be possible in theory, it is a poor design to mix the two notions and may make the design difficult to understand.

2.4 Implementing security manager:

Note that both the Client and Server programs must have access to the definition of any *Serializable* class that is being used. If the Client and Server programs are on different machines, then class definitions of *Serializable* classes may have to be downloaded from one machine to the other. Such a download could violate system security. This section discusses java security model as it relates to RMI.

As Baclawski (1998) continues in his article, a program written in java can specify a security manager to determine its security policy. A program usually needs a security manager to be specified. The Security policy is set by constructing a `SecurityManager` object and calling the `setSecurityManager` method of the `System` class. Some operations require a security manager. For example, RMI will only download a *Serializable* class from another machine if there is a defined security manager which allows the downloading of the respecting class from the machine. The `RMI SecurityManager` class defines an example of a security manager that normally allows such downloads.

The `SecurityManager` leverages a large number of methods with names beginning with `check`. If a `check` method returns, then the permission was granted. For example, a valid return from a call to `checkConnect` with a specified host and port means that the current security policy allows the program to establish a socket connection to the server socket at the specified host and port. If the security policy does not allow one to connect to this host and port, then the call throws an exception.

The original technique for specifying a security policy in Java was to define and install a security manager. Unfortunately, it is very difficult to design a class that does not leave any security holes and as a result of that a new technique was introduced in Java 1.2, which is said to be backward compatible with the old technique. In the default security manager, all `check` methods except `checkPermission` are implemented by calling the `checkPermission` method. A parameter is passed to the `checkPermission` method to specify the type of permission being checked. For example, the `checkConnect` method calls `checkPermission` with a `SocketPermission` object. The default implementation of `checkPermission` calls the `checkPermission` method of the `AccessController` class. This method verifies whether the specified permission is implied by a list of granted permissions. The `Permissions` class is used to maintain lists of granted permissions and for checking whether a particular permission has been granted.

While the security manager is a mechanism that checks permissions, it does not explain how one specifies or changes the security policy. This is done through another class named `Policy`. Like `SecurityManager`, each program has a current security policy that can be obtained by calling `Policy.getPolicy()`, and the current security policy can be set using `Policy.setPolicy`, providing one has permission to do so. The security policy is generally specified by a policy configuration file, otherwise known as "policy file", which is read by the program when it starts and any time a request is made to refresh the security policy.

3 Security Analysis of RMI technology

3.1 Case study -1: security concerns in use of proxy:

As described by Li, Mitchell and Tong (2004) in their paper titled ‘Securing Java RMI-based Distributed Applications’ on Computer Security Application Conference, in proxy-based architecture of Java RMI, a client interacts with a service through a proxy. This proxy is essentially some java code downloaded from a directory and installed on the client’s machine. In case of critical systems built using the proxy-based architecture, the security of these systems is a natural concern. The use of proxies introduces security vulnerabilities that need to be dealt with before any system using technologies such as Java RMI^[Appendix A] can be relied upon.

An attacker may control the communication channels and may compromise the confidentiality and integrity of the client and of the service.

The use of proxies poses several challenges in the provision of security mechanisms for proxy-based systems. The job of providing authentication between client and service applications is much complicated by the use of a proxy. A proxy is neither fully controlled nor trusted by the either of the client or service and yet the communication is made through this proxy. A proxy is generated by the service and thus the client cannot trust the proxy more than it trusts the service. On the other hand, this proxy is executed by the client under its control and thus the service cannot fully trust the proxy either. One approach to resolving this lack of trusts may be to treat the proxy as part of an insecure communication channel that connects the client and the server, and to implement standard authentication techniques to provide mutual authentication between the client and the server.

A graphical representation of the interactions among the service, client, and proxy is depicted in Figure 1. Three virtual machines (VMs) are involved in these process: the client VM^[Appendix A], the service VM, and the directory VM.

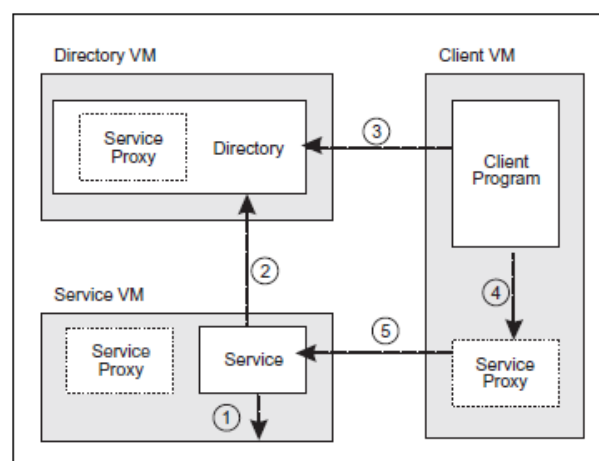


Figure 1. A normal client/service interaction

The whole process is done through the following steps:

In step 1 the service makes a call to the RMI runtime to export the service. This process creates a proxy for the service in the service VM.

In step 2 the service makes a remote call to a directory (e.g. rmiregistry) to register its proxy. With this process the directory VM gets the proxy object.

In step 3 the client looks up the service and downloads the proxy from the directory. This process enables the client VM to have the proxy.

Following the above steps, the client calls the proxy locally each time it needs to use the service as if it is the remote service. The proxy then communicates the client's request to the service to serve the desired outcome. Once the client has located and installed a proxy, it can reuse the proxy to make further requests as many times as needed as long as the proxy is considered valid by the service.

3.1.1 Vulnerability analysis in light of CIA:

In this vulnerability analysis for proxy-based systems, three parties are considered in the process, which are namely the user, the service provider, and the attacker. It is assumed that the user has full control over the client VM and the service provider has full control over the service VM. An attacker, however, may control the network and the directory VM, in other words, the directory is considered as *untrusted*.

The risks it poses to the client are:

3.1.1.1 Client confidentiality:

The client may transfer sensitive information to the proxy when using the service. One example of this is that if the service provides access to the user's investment accounts, the user would want to make sure that his information and instructions are only sent to the service provider, not to anyone else.

Another way that the attacker may breach client's confidentiality is by eavesdropping on the communications channel between the service and the proxy or between the client and the proxy.

3.1.1.2 Client integrity:

The user's VM and local environment may be inflicted by the proxy. Thus the client's integrity may be compromised by the attacker by getting the client to install and run a bogus proxy either by compromising the directory or by actively attacking the communication channel between the directory VM and the client VM or the channel between the directory VM and the service VM.

This type of attack can also pose risks to the service and like those on the client the service's confidentiality and integrity as well as the service's availability is affected by the attack.

3.1.1.3 Service confidentiality:

The service may send sensitive information to the client through the proxy. An attacker who gained control over the directory VM or the communication channel and thus have access to this proxy can extract this information and compromise the service's confidentiality.

3.1.1.4 Service integrity:

Sometimes a service may need to perform certain tasks on behalf of its client, and an attacker who successfully impersonates a client may result in damage or malicious use. The attacker can also compromise the service confidentiality and integrity by controlling the communication between the proxy and the service or by convincing the client to accept a bogus proxy.

An example of such attack where an attacker impersonates a client is demonstrated in section 4.

3.1.1.5 Service availability:

When an attacker gains control over the directory VM^[Appendix A], they can manipulate the service proxy such that the service is interrupted or denied. The client, being unaware of the attack, installs the proxy on his machine and calls the proxy with expectation of receiving the service when the service is denied. Thus the server suffers a denial-of-service attack by the attacker who controls the communication channels and/or the directory.

3.2 Case study -2: security concerns in serializing data in RMI application:

Java is generally considered to be a safe language with good security features. However, some characteristic and features of Java may pose security threat and compromise safety if they are misused or incorrectly implemented. One such Java feature is *Serialization*^[Appendix A].

W. Long (2005) of Carnegie Mellon University documented the issues with serialization in context of software security in his research showcase titled "Software Vulnerabilities in Java". This has been discussed in the following paragraphs.

3.2.1 How does Serialization work?

Serialization in a Java program enables the state of the program to be captured and preserved by writing it out to a byte stream. The preserved state can be later reinstated by another program as needed which is known as *deserialization*.

In order for a class to facilitate *Serialization*, the class needs to implement *Serializable* interface. Once the interface is implemented, all the fields of the class are captured. This includes non-public fields that would have been normally inaccessible, unless the fields are declared *transient* in which case they are not serialized.

For example, if we have an object called `someObject`, it can be serialized as follows:

```

ObjectOutputStream out = new ObjectOutputStream(newFileOutputStream
("SerialOutput"));
out.writeObject(someObject);
out.flush();

```

The serialized object can then be deserialized as follows:

```

ObjectInputStream in = new ObjectInputStream (newFileInputStream
("SerialOutput"));
someObject = (SomeClass) in.readObject();

```

3.2.2 How Serialization may affect in RMI applications:

In RMI application, a remote object (server-side) is exported to the Java RMI runtime so that it may receive Remote Method Invocation from the client-side. This is done by calling a *static* `export Object` method on `UnicastRemoteObject` class. The process generates a `Stub` which is then bound to the RMI registry with a name in `String` form and obtained by the client via a lookup. Here's an example:

```

RemoteInterface stub = (RemoteInterface) UnicastRemoteObject
                        .exportObject(remoteObject);
rmiRegistry.rebind("name", stub);

```

A generated `Stub` created using above method is a serialized object; this facilitates a Java method call to be transmitted over a network. However, this serialized object is written into byte stream and if the byte stream is readable then the values of the normally inaccessible fields can be read. Furthermore, it may also be possible to modify or forge the preserved values with the intention that when the object is deserialized, the values are corrupted.

Implementing a security manager in RMI application does not prevent the non-public fields from being serialized and deserialized (although permission must be granted to write to and read from a file or network if the byte stream is being stored or transmitted).

An example program demonstrating the issue of serializing non-public fields is given in section 5.

3.3 Case study -3: security concerns posed by lack of type compatibility verification in RMI protocol implementation:

A technical security report by Security Explorations (2012) titled "Security Vulnerabilities in Java SE" highlights, among various other Java security vulnerabilities, how RMI protocol implementation may be open to security exploitation. Following discussions are compiled in light of this report.

Java vulnerabilities are usually associated with their corresponding risks to users, especially of various web browsers. This is deemed as natural as the Java plug-in software has a widespread use among this community. In addition to this, there are also other exploitation scenarios which are worth mentioning. This section concerns the possibility to exploit Java security issues on remote servers.

Java runtime has a form of abstract Java Virtual Machine or JVM ^[Appendix A] whose goal is to provide secure execution environment for Java programs. A JVM has several components as depicted in figure-1 below:

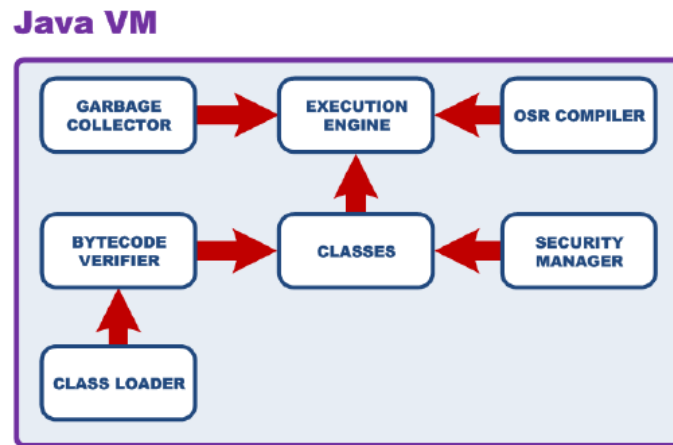


Figure 1. Java Virtual Machine security architecture.

, some of these components with critical nature to security include Java CLASS LOADER, BYTECODEVERIFIER and SECURITY MANAGER. In order to understand the security vulnerability in RMI protocol implementation, we have to first understand how the above mentioned Java components conduct their roles in relation to security.

Role of Java CLASS LOADER implicating security:

Class Loaders are special Java objects that inherit from `java.lang.ClassLoader` class or its subclass. They provide Java Virtual Machine with Class files, which may come from arbitrary locations such as remote hosts or local file system. Class Loader location denoting a base source of classes is called a *Codebase*.

The Java Class Loader objects implement several security critical methods. This includes method which is invoked whenever a definition of a target class name is not found in the Java VM and when an attempt is made to load it from some external location.

Class Loader objects are very powerful, they can:

- ⇒ provide class definitions to the VM,
- ⇒ specify permissions for loaded classes,
- ⇒ load native libraries into Java VM etc.

-these are just a few of the many reasons why a *ClassLoader* creation requires having a proper security privilege. The *ClassLoader* instance initialization method (`<init>`) implements checks for this privilege.

Role of Java BYTE CODE VERIFIER implicating security:

Bytecode Verifier is called during class loading process and is the primary gatekeeper of Java VM security. It ensures that a given sequence of bytes provided to the

`defineClass()` method of Class Loader conforms to the Class file format. It also verifies the integrity and safety of byte code instruction streams embedded in a Class definition.

Bytecode Verifier functions in multiple phases during which it verifies the VM constraints defined in JVM Specification. This Bytecode Verifier is responsible for the verification of type-safety of a target Java code. Any attempt of conducting an illegal type-cast (for example, from integer to object or vice-versa) should be detected by this VM component.

Bytecode Verifier performs a static analysis of a target byte code instruction stream. It does this work by emulating the effect of a target instruction to the content of Java VM state. The effect is analysed solely with respect to the type information held in registers and on the stack. In the past, Bytecode Verifier algorithm would infer all type information during the analysis of byte code instruction flow.

Role of Java SECURITY MANAGER implicating security:

Security Manager objects are instances of `java.lang.SecurityManager` class or its subclass. They verify and authorize all security sensitive operations in a VM environment. A special object in each JVM denotes the Security Manager and a reference to this object can be obtained by calling `getSecurityManager` method of `java.lang.System` class. A sample syntax can be described as:

```
SecurityManager secMangr = System.getSecurityManager();
if (secMangr != null) {
    secMangr.checkPermission(new RuntimePermission("setContextClassLoader"));
}
```

The absence of a Security Manager is indicated by its `null` value. In such case, no security checks are in place and Java programs can run without any restriction in a target JVM environment.

When a program is run in a JVM, a private `security` field of `java.lang.System` class holds a reference to the Security Manager which is in use by the environment. Therefore, the possibility of being able to create an instance of a Security Manager does not lead to a direct compromise of VM security.

Another special object in Java security context is permission; this is an instance of `java.security.Permission` class or its subclasses. Java Security Manager verifies whether a target class has specific permissions required for a given security sensitive operation. Java has dedicated permissions for specific operations, such as network access, specific API access, program execution etc. There is also one special permission object that denotes ROOT privileges in Java. This object is referred to as `AllPermission`; many single permissions may also be easily elevated to `AllPermission`.

3.3.1 RMI protocol attack

RMI^[Appendix A] protocol, known as JRMP^[Appendix A] or Java Remote Method Protocol, is the base protocol used for communication between clients and servers during Java Remote Method Invocation. It is a Java technology specific protocol designed for looking up and reference remote objects. JRMP is a wire level protocol running under the Java Remote Method

Invocation and over TCP/IP^[Appendix A]. It is a Java specific and stream-based protocol that requires both the server and client to use Java objects.

Implementation of RMI protocol supports the concept of 'Codebase' provided by the user. A Codebase is essentially a URL^[Appendix A] value that points to a resource, either remote or local, where the remote RMI server should look for unknown (non-system) classes. In RMI application, an RMI client can provide the Codebase URL as part of its RMI call. This will be taken into account by the RMI server provided that the `java.rmi.server.useCodebaseOnly` property is set to true. In such case, RMI server will create `RMI ClassLoader` instance with the client-provided Codebase URL. This will be further used as a base class loader during object deserialization by a `MarshalInputStream`.

RMI implementation does not verify the type compatibility of a deserialized object with the input argument of a target method call. The RMI server reads and instantiates object provided as an argument to the call using `RMIClassLoader`. Even if the concerning object (i.e. object to read) is of an unknown class, an attempt will still be made to fetch the class data from the Codebase URL provided by the client. This characteristic of the RMI implementation alone creates a possibility for remote loading and execution of user provided Java code.

An example program demonstrating 'absence of type verification in RMI protocol implementation' is given in section 6.

3.4 Summary from case studies:

A summary from the case studies discussed in above sections can be tabularized as below:

Threat	Why it is a threat	Impact	Difficulty Level
Use of proxy	This proxy is essentially some java code via which a client interacts with a service.	An attacker may control the communication channels and may compromise the confidentiality and integrity of the client and of the service.	Medium
Object Serialization	A generated Stub created on the server-side, by calling a <i>static</i> <code>exportObject</code> method on <code>UnicastRemoteObject</code> class, is a serialized object; this eventually facilitates a Java method call to be transmitted over a network.	The serialized object is written into byte stream and if the byte stream is readable then the values of the normally inaccessible fields can be read. Furthermore, it may also be possible to modify or forge the preserved values with the intention that when the object is <i>deserialized</i> , the values are corrupted.	Basic
Lack of type compatibility verification in RMI protocol implementation.	RMI implementation does not verify the type compatibility of a <i>deserialized</i> object with the input argument of a target method call. The RMI server reads and instantiates object provided as an argument to the call using RMI <i>ClassLoader</i> . Even if the concerning object (i.e. object to read) is of an unknown class, an attempt will still be made to fetch the class data from the Codebase URL provided by the client.	This characteristic of this RMI protocol implementation alone creates a possibility for remote loading and execution of user provided Java code.	Advanced

4 Test application - Breach of confidentiality:

4.1 Overview:

This RMI application consists of a server application, a client application and a remote interface. The server provides a service that receives various “jobs” from the client in order to run them on the server machine; this facilitates the client with the ability to perform a job that requires heavy resources that the client cannot provide. Once the job is performed on the server side the client can then invoke a remote method, through a proxy generated by the server, to retrieve the result of the job.

4.2 Application components:

The application has the following components:

4.2.1 Job Interface:

This is an interface that defines a job. A client-side class *implements* this interface to mark the class to be recognized as a job on the server-side. The result is returned to the client in the form of a *generic type* which is determined by the client-side class that defines the job. The interface looks like this:

```
public interface JobInterface<T> {  
    T commenceJob();  
}
```

Once a job is successfully instantiated on the client-side, it is then passed to the server to be performed through a proxy generated by the server application.

4.2.2 Remote Interface:

This interface is a subclass of `java.rmi.Remote` which makes it ‘the Remote interface’ for this RMI application. A server-side class *implements* this interface to provide the intended service. The interface is defined as below:

```
public interface RemoteJobInterface extends java.rmi.Remote {  
    <T> T retrieveJobReport(JobInterface<T>job) throws RemoteException;  
}
```

The interface is used for storing a remote object stub on the server-side application which is eventually bound to the `rmiregistry`. The client application, on the other hand, retrieves the remote object stub from the `rmiregistry` and uses the interface to *cast* the stub to a remote-interface object understandable by the client. The client then passes its job (i.e. a `JobInterface` object) to the server as parameter and retrieves the result by invoking the remote method (i.e. `retrieveJobReport` method) on this remote-interface object.

4.2.3 Server-side implementation:

The service provided by the server-side class, namely `RemoteJobExecutor`, receives a job from the client through remote method invocation, carries out the job on the server machine and then returns the result back to the client. The class provides its own implementation of the method signature defined in the remote-interface, `RemoteJobInterface`, to perform the task.

```
public class RemoteJobExecutor implements RemoteJobInterface {  
  
    @Override  
    public <T> T retrieveJobReport(JobInterface<T> job) {  
        ...  
        return job.commenceJob();  
    }  
}
```

The method `retrieveJobReport` receives a `JobInterface` object by the name `job` and calls a `commenceJob` method on this object, which is implemented on the client side.

A program called `ServerSideProgram` triggers the operation by first creating an object of the service instance (named `jobExecutor`) and exporting it to the Java RMI runtime so that it may receive incoming remote calls.

```
RemoteJobInterface stub = (RemoteJobInterface) UnicastRemoteObject  
    .exportObject(jobExecutor, 0);
```

The process of exporting the object returns a remote object stub which is stored in a `RemoteJobInterface` variable called `stub`. Following this, an instance of Java RMI registry, called `registry`, is created and exported on the local host, port 1099:

```
Registry registry = LocateRegistry.createRegistry(1099);
```

Finally, `stub` is bound to `registry` to bind the remote object's stub to the name "RemoteJobExecutor" in the registry:

```
registry.rebind("RemoteJobExecutor", stub);
```

4.2.4 Client-side implementation:

The client-side defines a class called that turns a plain textual message into an encrypted message using a *symmetric encryption* method and *encryption key*. The class implements the interface `JobInterface` which makes it a "job" recognized by the service on the server-side. The encryption method is an enumeration type which is one of SUBSTITUTION, TRANSPOSITION or BLOCKING. The encryption method is selected by the user at the time of creating an instance of the job before passing it onto the server-side. In order to be transported over a network, the class also implements `Serializable`.

```
public class SymmetricEncryption implements JobInterface<String>, Serializable  
{  
  
    public SymmetricEncryption(String message,  
        SymEncryptionMethod encryptionMethod, int key) {...}
```

```
@Override
    public String commenceJob() {...}
}
```

A program on the client-side, named `ClientSideProgram`, first gets hold of the registry and looks up for the remote object reference by its name, i.e. "RemoteJobExecutor", which is stored in `RemoteJobInterface` variable called `jobExecutor`.

```
Registry registry = LocateRegistry.getRegistry();
RemoteJobInterface jobExecutor = (RemoteJobInterface) registry
    .lookup("RemoteJobExecutor");
```

It then creates an object of `SymmetricEncryption` "job" and finally passes the "job" to the service by invoking a remote method on the remote object `jobExecutor`.

```
SymmetricEncryption symetricEncryp = new SymmetricEncryption("Hello RMI
application.",SymEncryptionMethod.SUBSTITUTION, 5);

String jobReport = jobExecutor.retrieveJobReport(symetricEncryp);
```

4.3 Things to take care of before running the service:

Before the service is started it needs to have prior knowledge of the classes it may receive from the client or clients. This could be achieved in the following ways:

- The service, when starting, has to have the clients' class files in its classpath when both the service and client are on the same machine, e.g. local host.
- The relevant class files can be placed in a designated directory and Java RMI Codebase feature may be used to point the service to this directory at service start time. Again, this works when the service and client are run on the same machine.
- In case of the service and client being on different remote machines, the clients' class files may be placed in a web server and the service would locate these files using http in the Java RMI Codebase feature.

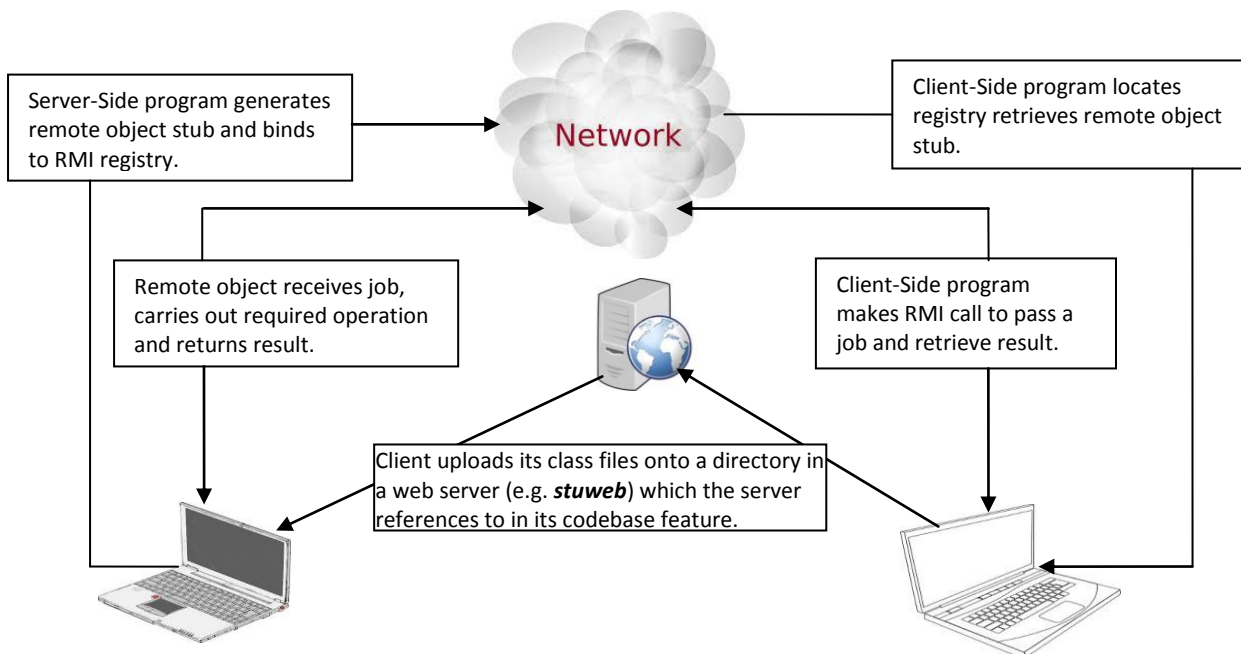
Without the step outlined above, the service will start up without any error; however, running the client application will throw an exception which will look like:

```
java.rmi.ServerException: RemoteException occurred in server thread; nested
exception is:
    java.rmi.UnmarshalException: error unmarshalling arguments; nested exception
is:
    java.lang.ClassNotFoundException:
uk.ac.rm950.breachOfConfidentialityClient.SymmetricEncryption
    at sun.rmi.server.UnicastServerRef.dispatch(UnicastServerRef.java:353)
    ...
    ...
java.rmi.server.RemoteObjectInvocationHandler.invokeRemoteMethod(RemoteObjectI
nvocationHandler.java:194)
Remote job client exception.
```

4.4 Application in action:

The `ServerSideProgram` initiates the service on machine A by creating an instance of the remote object, generating a stub and finally starting the RMI registry and binding the stub with this registry. Once the service is up and running, a `ClientSideProgram` on machine B then locates the registry and looks up the remote-object-reference in the registry. The remote method is then invoked on the remote-object-reference by the client program to pass the job to the service and to retrieve the result.

In this example, the `ClientSideProgram` creates a `SymmetricEncryption` job with message *“Hello RMI application”*, symmetric method `SUBSTITUTION`, and encryption key 5. Upon invoking the remote method `retrieveJobReport`, the client passes the job to the server-side and receives the result in the form of *String*.



As the client application is run, the server-side console outputs:

```
Sever side:
=====
RemoteJobExecutor bound
Server side received a remote job from client machine: 192.168.0.7
The job is being carried out on server machine: mahabuburs-mbp/192.168.0.5
```

On the client-side, the console displays the result and outputs:

```
Client side:
=====
Original message: Hello RMI application.
Encrypted message: Mjqqt%WRN%fuuqnhfynts3

The job was executed in machine: mahabuburs-mbp/192.168.0.5
```

4.5 Attack through impersonating a client:

We presume that an attacker gains access to the directory in the web server (*stuweb* in this example) where the RMI service looks into for reference to client classes. The attacker then creates an evil version of the `SymmetricEncryption` job; let us call this class `SymmetricEncryptionEvil`. The class contains malicious code which, outside of doing the normal symmetric encryption operation, will try to steal password information from the server machine by reading the *passwd* file.

Once the *evil* class is updated on the *stuweb* web server, the attacker impersonates a legitimate client to create a job with the class and makes an RMI call. This RMI call passes the job to the server-side, executes the operation with the malicious code and the stolen data is then returned to the client (i.e. the attacker in this case) with the job report.

The `SymmetricEncryptionEvil` class may look like this:

```
public class SymmetricEncryptionEvil implements JobInterface<String>,
    Serializable {

    public SymmetricEncryptionEvil(String message,
        SymEncryptionMethod encryptionMethod, int key) {...}

    @Override
    public String commenceJob() {
        ...
        ...
        return String.format("Original message: %s\nEncrypted message: %s"
            + "\n\nThe job was executed in machine: %s."
            + "\n\nFinally, this is the stolen data: %s",
            originalMessage, encryptedMessage, getIPAddress(),
            stealFileContent("less -N /etc/passwd"));
    }
}
```

As the client program is run the server-side console as usually outputs:

```
Sever side:
=====
RemoteJobExecutor bound
Server side received a remote job from client machine: 192.168.0.7
The job is being carried out on server machine: mahabuburs-mbp/192.168.0.5
```

And to the attacker's satisfaction, the client-side (i.e. attacker's) console displays:

```
Client side:
=====
Original message: Hello RMI application.
Encrypted message: Mjqqt%WRN%fuuqnhfynts3

The job was executed in machine: mahabuburs-mbp/192.168.0.5.
Finally, this is the stolen data:
nob
roo
dae
_uu
_ta
```

C E N S O R E D

```
ico
```

5 Test application –non-public data serialization:

5.1 Overview:

This RMI application has a server application, a client program and a remote interface. The server application packages the following:

- a class, named `Employee`, which has some attributes of different public and non-public access levels and getter methods to retrieve the values of these attributes.
- a `Manager` class, which is a subclass of `Employee`, with a private access levelled field.
- a server-side program, referred to as `ServerSideProgram`, that creates remote objects of *Type* `Employee` and `Manager` initializing various fields and values.

The server-side program generates stubs with locally instantiated remote objects and binds them to the RMI registry. The client program will eventually look up in the RMI registry to obtain the stubs. It will then read the remote objects to find out whether the non-public field values of the remote objects are exposed.

5.2 Application components:

The application has the following components:

5.2.1 Remote interface:

This is the remote-interface for this RMI application. The interface is called and has the following definition:

```
public interface RemoteEmployeeInterface extends java.rmi.Remote {  
  
    public String retrieveEmployeeName() throws RemoteException;  
    public String retrieveEmployeeRole() throws RemoteException;  
    public String retrievePersonalIdentificationNumber() throws RemoteException;  
    public String retrieveEmployee() throws RemoteException;  
}
```

The interface is used for storing a remote object stub on the server-side application which is eventually bound to the `miregistry`. The client application, on the other hand, retrieves the remote object stub from the `miregistry` and uses the interface to cast the stub to a remote-interface object understandable by the client. The only way a client may call a method on a remote object (which resides on the server-side) is by calling the method on the remote-interface object as the client doesn't have any knowledge of the server-side remote classes.

5.2.2 Server-side application:

Consisting of the following classes:

5.2.2.1 Employee:

This is an ordinary class that implements `RemoteEmployeeInterface` in order to be able to make remote object instances. The class has some usual fields that an ordinary `Employee` object would be expect of, such as `name`, `role` and `personalIdentificationNumber`. The access levels of these fields, however, are varied to cater for the purpose of this test. The class looks like this:

```
public class Employee implements RemoteEmployeeInterface {  
    public String name;  
    public String role = "Not assigned";  
    protected long personalIdentificationNumber = 0L;  
}
```

Finally, the class implements the methods defined in the `RemoteEmployeeInterface` interface which will eventually be called by the client program.

```
@Override  
public String retrieveEmployeeName() throws RemoteException {...}  
  
@Override  
public String retrieveEmployeeRole() throws RemoteException {...}  
  
@Override  
public String retrievePersonalIdentificationNumber() throws RemoteException  
{...}  
  
@Override  
public String retrieveEmployee() throws RemoteException {...}
```

A call to the *implemented* `retrieveEmployee` method returns the attributes belonging to an `Employee` object in *String* form.

5.2.2.2 Manager:

This class inherits the `Employee` class above and has a private access levelled field called `secretInfo`. To serve the purpose of a private field, the value of this field will only be exposed to other appropriate classes through its getter methods. The class looks like this:

```
public class Manager extends Employee {  
    private String secretInfo = null;  
  
    void setSecretInfo(String secretInfo) {...}  
    public String getSecretInfo() {...}
```

The class generates its own `personalIdentificationNumber` via method `generatePersonalIdentificationNumber`, which accepts a `dob` parameter in *String* form and generates a `personalIdentificationNumber` based on some calculation.

```
public void generatePersonalIdentificationNumber(String dob) {...}
```

This class also provides its own implementation of the `retrieveEmployeeRole` method, which returns values of `role` and `secretInfo` specific for a `Manager` object back to the caller.

```
@Override  
public String retrieveEmployeeRole() throws RemoteException {...}
```


5.2.2.3 Server-side application:

This class, name `ServerSideProgram`, initiates the process of the server application. The class first implements a Java security manager and starts the RMI registry, called `registry`.

```
System.setProperty("java.security.policy", "security/client.policy");
if (System.getSecurityManager() == null) {
    System.setSecurityManager(new SecurityManager());
}
try {
    Registry registry = LocateRegistry.getRegistry();
```

It then creates instances of `Employee` and `Manager`, exports them to the java RMI runtime to create stubs and finally binds those stubs to the `registry`. The core code looks like this:

```
Employee transportingEmployee = new Employee("Michael");

RemoteEmployeeInterface employeeStub =
(RemoteEmployeeInterface)UnicastRemoteObject.exportObject(transporting
Employee, 0);
registry.rebind("employee1", employeeStub);

Manager aManager = new Manager("George Loukas");
aManager.setSecretInfo("George's secret info.");
Employee employeeWrapper = aManager; // wrapped Manager object
//into a Employee wrapper

RemoteEmployeeInterface managerStub = (RemoteEmployeeInterface)
UnicastRemoteObject.exportObject(employeeWrapper, 0);
registry.rebind("employee2", managerStub);
```

5.2.3 Client-side application:

The client-side program makes use of a class, called `ClientSideProgram`, to carry out remote method invocation on stubs, obtained from the RMI registry, produced by the server-side program. The class starts with implementing Java security manager and locating the RMI registry on the network.

```
System.setProperty("java.security.policy", "security/client.policy");
if (System.getSecurityManager() == null) {
    System.setSecurityManager(new SecurityManager());
}

try {
    Registry registry = LocateRegistry.getRegistry();
```

It then looks up the stubs(remote object reference) by the names they were bound by the server program and stores the stubs into remote-interface variables.

```
RemoteEmployeeInterface transportedEmployee1 = (RemoteEmployeeInterface)
registry.lookup("employee1");

RemoteEmployeeInterface transportedEmployee2 = (RemoteEmployeeInterface)
registry.lookup("employee2");
```

Finally, the program calls the remote methods on the obtained stubs to get the results.

```

System.out.println(transportedEmployee1.retrieveEmployee());
System.out.println(transportedEmployee2.retrieveEmployee());
System.out.println(transportedEmployee2.retrieveEmployeeRole());

```

5.3 Application in action:

The `ServerSideProgram` starts the service on machine A by creating instances of the remote objects `Employee` and `Manager`, generating stubs and binding the stubs with RMI registry. Once the service is up and running, a `ClientSideProgram` from machine B locates the registry and looks up the remote-object-reference in the registry. The remote methods are then invoked on the remote-object-references by the client program to fetch the details of the remote objects.

In this example, the `ServerSideProgram` creates an `Employee` object as follows:

```

Employee transportingEmployee = new Employee("Michael");

```

This creates an `Employee` object with fields {name="Michael"; role="Not assigned", personalIdentificationNumber=0L}. The field `personalIdentificationNumber` is a protected attribute; the value of this attribute can only be directly read or set (i.e. without any accessing method or property) by a child class of `Employee` or other classes in the same package. In other words, `personalIdentificationNumber` field is a restricted and non-public attribute and its value can only be disclosed under certain criteria.

The `ServerSideProgram` class also creates a `Manager` object as:

```

Manager aManager = new Manager("George Loukas");

```

Being a child object of `Employee` (i.e. `Employee` is a super class of `Manager`), the `aManager` object has direct access to attribute `personalIdentificationNumber` of `Employee` class (*protected* field) and sets the value of this attribute in a designated method named `generatePersonalIdentificationNumber` based on some calculations. Furthermore, the `aManager` object also sets a private attribute named `secretInfo` which is strictly visible to this object alone. In other words, these fields are non-public and designed not to be disclosed to the outside world.

```

aManager.generatePersonalIdentificationNumber("02/02/1975");
aManager.setSecretInfo("George's secret info.");

```

The object `aManager` is then stored in an `Employee` wrapper to facilitate stub generation to be transferred over the network.

```

Employee employeeWrapper = aManager;

```

Once created, these objects, namely `transportingEmployee` and `employeeWrapper` are exported to the RMI runtime. The resulting stubs, referred to as `employeeStub` and `managerStub`, are then bound to the RMI registry.

```

RemoteEmployeeInterface employeeStub = (RemoteEmployeeInterface)
    UnicastRemoteObject.exportObject(transportingEmployee, 0);
RemoteEmployeeInterface managerStub = (RemoteEmployeeInterface)

```

```

        UnicastRemoteObject.exportObject(employeeWrapper, 0);
registry.rebind("employee1", employeeStub);
registry.rebind("employee2", managerStub);

```

When the ServerSideProgram is run on machine A, the following output is printed on the console:

```

Sever side (Mahabuburs-MacBook-Pro.local/192.168.0.5):
=====
I am a server application serving some locally instantiated objects with noble
intention to make necessary information available to enquiring clients to satisfy the
objective of AVAILABILITY in CIA principle.
Hopefully I'm not breaching CONFIDENTIALITY by giving away non-public information.

Exported an employee object in RemoteEmployee wrapper...
Exported a manager object in RemoteEmployee wrapper...

```

The client program, named ClientSideProgram, on machine B eventually consumes the stubs. The details of the client program's operation have already been described in section 5.2.3.

When the ClientSideProgram is run, following information is printed on the client's console:

```

Client side (Toshiba/192.168.56.1):
=====
I am a client application enquiring some publicly disclosable data about employee.

```

The client program stores the first stub, named as "employee1" on the server-side (i.e. remote reference to the Employee object), into a RemoteEmployeeInterface variable transportedEmployee1:

```

RemoteEmployeeInterface transportedEmployee1 = (RemoteEmployeeInterface)
registry.lookup("employee1");

```

, and when the remote method retrieveEmployee is called on transportedEmployee1object

```

System.out.println(transportedEmployee1.retrieveEmployee());

```

, it prints the following:

```

Received first employee information pack, unpacking wrapper...
{
Name: Michael;
Role: Not assigned;
PID: 0
}
I got more that the information I need! At least the personalIdentificationNumber
isn't anything meaningful.

```

As the output shows, although a protected attribute, the personalIdentificationNumber of the Employee object is serialized on the server-side and transported over the network to the client side and deserialized. Thus a protected data of a class can be easily exposed inadvertently to unintended users if it is used improperly or implemented incorrectly.

The next stub, named as “employee2” on the server-side (i.e. remote reference to the Manager object) is stored in variable `transportedEmployee2`:

```
RemoteEmployeeInterface transportedEmployee2 = (RemoteEmployeeInterface)
registry.lookup("employee2");
```

, and when the remote method `retrieveEmployee` is called on `transportedEmployee2` object

```
System.out.println(transportedEmployee2.retrieveEmployee());
```

, it prints the following:

```
Received second employee information pack, unpacking wrapper...
```

```
{
```

```
Name: George Loukas;
```

```
Role: Management;
```

```
PID: 57912020
```

```
}
```

```
Why do I see personalIdentificationNumber? Isn't this supposed to be a protected
info?
```

The output shows that the value of the `personalIdentificationNumber` attribute is also serialized for a Manager object the same way as the parent `Employee` object. This demonstrates that although the Manager class itself doesn't implement the Java RMI remote interface, it also equally exhibits RMI data serialization characteristics (along with the consequence of any incorrect implementation) through inheritance from its parent class.

Finally, when the remote method `retrieveEmployeeRole` is called on `transportedEmployee2` object

```
System.out.println(transportedEmployee2.retrieveEmployeeRole());
```

, it prints the following:

```
{
```

```
Role: Management
```

```
Secret info: George's secret info.
```

```
}
```

```
Whoa!!! that's a lot of private data you've disclosed there!
```

This output demonstrates that because of improper use or incorrect implementation, not only the *protected* but also the *private* data can be equally vulnerable in an RMI application due to the nature of serialization technique. Even if the class itself doesn't implement the Java RMI remote interface, the behaviour is still inherited from its parent class.

6 Test application - absence of type compatibility verification in RMI protocol implementation:

6.1 Overview:

This RMI application consists of a server application, a client application and two remote interfaces. The server-side program generates a *stub* with locally instantiated remote object and binds it to the RMI registry. The client program looks up in the RMI registry to obtain the *stub*. However, as the client-program attempts to *cast* the *stub* using a different remote-interface, a `ClassCastException` would occur. This would demonstrate that although a type verification is carried out when the stub is attempted to be *cast* into an incompatible type, the remote *stub* was allowed to be looked up successfully due to the absence of type verification in RMI protocol level.

6.2 Application components:

6.2.1 Remote Interfaces:

For this application, we would use the two previously use remote-interfaces, namely `RemoteJobInterface` and `RemoteEmployeeInterface`. Details of these interfaces have been given in sections 4.2.2 and 5.2.1.

6.2.2 Server-side implementation:

A server-side program instantiates a remote `Employee` object, then generates a *stub* (of type `RemoteEmployeeInterface`) and binds it to the RMI registry as described in section 5.2.2.3. The implementation looks like this:

```
Employee transportingEmployee = new Employee("Michael");
RemoteEmployeeInterface employeeStub = (RemoteEmployeeInterface)
    UnicastRemoteObject.exportObject(transportingEmployee, 0);
registry.rebind("employee", employeeStub);
```

6.2.3 Client-side implementation:

As described in section 5.2.3, a client-side program looks up in the RMI registry in search of the remote object reference (of type `RemoteEmployeeInterface`) by its name, represented in *String* (i.e. "employee"). Once the program obtains the *stub*, it then deliberately attempts to *cast* the *stub* into an incompatible remote-interface type, more precisely `RemoteJobInterface` type. This should result in an *Exception* being thrown, which is a `Throwable` object.

```
Registry registry = LocateRegistry.getRegistry();
Throwable thrownException = (Throwable) ((RemoteJobInterface)
    registry.lookup("employee"));
```

If this `Throwable` object proves to be a `ClassCastException`, then the purpose of this demonstration is achieved.

```
if (thrownException instanceof ClassCastException) {  
    System.out.println("RMI call successful.");  
} else {  
    System.out.println("RMI call unsuccessful.");  
}
```

6.3 Application in action:

For this application, both Server and Client applications are run on the same machine. As the server program is run, it outputs the following on the console indicating that the service has started successfully:

```
Sever side (mahabuburs-mbp/192.168.0.6):  
=====
```

Exported an employee object in RemoteEmployeeInterface wrapper...

Once the service is up and running, the client program is run and the following message is printed on the console:

```
Client side (mahabuburs-mbp/192.168.0.6):  
=====
```

RMI call successful.

This demonstrates that the casting is only in effect once the *stub* is obtained and attempted to be *cast* to an incompatible type. Therefore, this has been proved that there is no type verification in place in the RMI protocol implementation.

7 Evaluation:

7.1 Methodologies and processes:

At a high level, the work done in this project was mostly carried out using *incremental approach* ^[Appendix A], more precisely the WATERFALL ^[Appendix A] methodology, which is a commonly used strategy in Project Management. Once essential research in the aspects of RMI ^[Appendix A], technical and security context were completed and sensible extracts were summarised, only then the development of prototype ^[Appendix A] applications could begin to support any exertion of statements.

However, the incremental process of the WATERFALL methodology was used with a twist of *iterative approach* ^[Appendix A] as the project was broken into various activities with SMART ^[Appendix A] objectives, such as planning, defining objectives, literature review and technical implementation. Each of these activities was further broken into activity specific tasks repeatedly revisited following consultation and feedback with the supervisor of this project until an agreed standard of quality was achieved. Therefore, each activity adopted its own methodology to accomplish the tasks.

7.1.1 Conjugating technical jigsaws:

Having used the RMI technology for the first time in this project, the author of this report knew little about the technology before undertaking this project. Consequently, a substantial amount of time and artefacts were spent in understanding, troubleshooting and experimenting as well as documenting the technical aspects. At the face of many obstacles, progress was being made through trials and errors using CABTAB ^[Appendix A] methodology; more discussion on these technical challenges has been given in section 8.1. It was an interesting learning phase which later played a very important role developing the prototype applications.

7.1.2 Literature review for security vulnerability:

Extensive research on potential RMI security weaknesses had to be carried out in order to develop the *proof of concept* ^[Appendix A] prototype applications. The security and safety features of Java technology is acclaimed by many experts, such by Gong and Ellison (2003) in their publication, by Security Explorations (2012) in their security research, by W. Long (2005) in his research showcase and many others. So, RMI already being a part of a secure technology, it was hard to find enough evidences of real vulnerability in the existing technology. This also explains why this technology is used by businesses and corporations around the world.

However, perseverance was eventually rewarded through conceptual findings on some of the literature reviews. Based on these findings, once it was possible to shed light on some vulnerability, development the *proof of concept* prototypes were undertaken.

7.1.3 Application development process:

The applications were developed with simplicity in mind and with focus on exploiting a concerning security issue within. The applications are, therefore, purposefully kept free from

any unnecessary functionality or fancy graphical user interfaces. However, the usual software development best practices and OOAD ^[Appendix A] approach, such as *principle of high cohesion and low coupling*, *DRY* ^[Appendix A] etc. were adopted as part of the development process. Considerations were given to ensure writing elegant and reusable code that may be of use to various other scopes inside and outside of the classes. Various attributes and functions inside the classes are properly documented to give explanation of their roles. Finally, the test results are communicated through clear message on console outputs.

7.1.4 Version controlling:

Version controlling was maintained throughout the research and application development process using *distributed version control system* ^[Appendix A] namely **Git** ^[Appendix A] and **GitHub**. Thus the progress of work could be continuously tracked, updated and rolled back (in the event of any inadvertent or detrimental changes) on a remote repository^[Appendix A] from multiple machines. The remote repository link for the project is: <https://github.com/mahabrashid/MSc-Project>.

7.2 Strengths and weaknesses:

In order to measure the strengths and weaknesses of a piece of work, whether technical or non-technical, it is essential to be able to compare the work with other similar works in the area. From the research and observation undertaken for this project, no work of this type had been found to be producing comprehensive critical discussion followed by demonstrative prototypes. There are various research and elaborative reports on the security evaluation of Java as a whole, but nothing that targets one specific feature in an exclusive manner.

8 Reflection:

Working on this project has been a great experience of stepping into the unknown. The feeling was really diverse by sometimes being frustrated with blockers while at other times being fascinated with discoveries. Although the outcome from the project was initially very uncertain, every bend of the course felt like an ecstatic learning curve. This section is merely an effort to share some of these experiences.

8.1 Challenges faced:

The greatest challenge faced during the project was the challenge of piecing together the technical jigsaws. The technical work naturally started with tutorial on the website of Oracle, the owner of the technology. While the tutorials and the overall website are found useful to develop understanding of the technology, the technical implementation eventually led to a long period of troubleshooting as something wasn't working as expected. After weeks of head scratching and running around being mad, it was later realised that the tutorial wasn't updated following recent enhancements made to the core JDK by the company, details can be found in [section 10.2: **Appendix B**- RMI Exceptions](#) with references provided in [section 9.1 - *Exception resolutions and troubleshooting*](#).

In addition to the out-of-date tutorial, there were also other technical hitches and glitches resulting in prolonged yet adventurous trial and error phases during development, these are discussed in detail in [section 10.2: **Appendix B**- RMI Exceptions](#) with references in [section 9.1 - *Exception resolutions and troubleshooting*](#).

The literature review in search of security vulnerability also proved somewhat challenging due to the lack of enough material in this area, which is [discussed in section 7.1.2](#). Other challenges included personal and work commitments allowing restricted availability for the project.

8.2 Further work:

While doing the research work for this project, it was noticed that necessary support and documentation for this technology is declining gradually. Part of this reason may be the near obsolete state of the technology itself amongst the expert users within the industry. Therefore, further work in this area does not feel to be necessary at this time.

Finally, it is undeniable that this work may not be the best of its kind and could be deserving of more time and resources than what could be afforded. It wasn't always easy finding adequate time outside of working in a full time job and part time studying, but nevertheless it was truly engaging whenever worked upon. This work has been a phenomenal experience of working and experimenting things that was never worked with before.

9 References and Keywords:

9.1 References:

- Baclawski, Kenneth (1998). *Java RMI Tutorial*. [online]. URL: http://www.eg.bucknell.edu/~cs379/DistributedSystems/rmi_tut.html.
- Chris Greenhalgh (March 2008). *Java RMI programming by example*. [online]. University of Nottingham, School of Computer Science and IT. URL: <http://www.cs.nott.ac.uk/~cmg/G53ACC/java-rmi/rmi-tutorial.html>.
- Dabhi, Vipul K.; Prajapati, Harshad B. (Sep 2010). “Dissection of the internal workings of the RMI, possible enhancements and implementing authentication in standard Java RMI”. URL: <http://dl.acm.org/citation.cfm?id=1866135>.
- Oracle.com (n.d.). *An Overview of RMI Applications (The Java™ Tutorials > RMI)*. [online]. URL: <http://docs.oracle.com/javase/tutorial/rmi/overview.html>.
- Oracle.com (n.d.). *Getting started using Java RMI*. [online]. URL: <http://docs.oracle.com/javase/1.5.0/docs/guide/rmi/hello/hello-world.html>.
- Oracle.com (n.d.). *Dynamic code downloading using Java RMI*. [online]. URL: <http://docs.oracle.com/javase/7/docs/technotes/guides/rmi/codebase.html>.
- Oracle.com (n.d.). *RMI's Multiplexing Protocol*. [online]. URL: <http://docs.oracle.com/javase/jp/8/platform/rmi/spec/rmi-protocol7.html>.
- Oracle.com (n.d.). *Stubs and Skeletons*. [online]. URL: <http://docs.oracle.com/javase/8/docs/platform/rmi/spec/rmi-arch2.html>.
- Oracle.com (n.d.). *Java Remote Method Invocation: 10 - RMI Wire Protocol*. [online]. URL: <http://docs.oracle.com/javase/7/docs/platform/rmi/spec/rmi-protocol7.html>.
- Oracle.com (n.d.). *Frequently Asked Questions - Java™ RMI and Object Serialization*. [online]. URL: <http://docs.oracle.com/javase/7/docs/technotes/guides/rmi/faq.html>.
- Li, Ninghui; Mitchell, J.C.; Tong, D. (2004). “Securing Java RMI-based distributed applications”, Computer Security Applications Conference, 2004. 20th Annual, vol. no. pp.262,271, 6-10. Dec. 2004, doi: 10.1109/CSAC.2004.34. [online]. URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1377233&isnumber=30059>.
- Gong, Li; Ellison Gary (2003). “Inside Java(TM) 2 Platform Security: Architecture, API Design, and Implementation”. URL: <http://dl.acm.org/citation.cfm?id=599797>.
- Gong, Li (1998). “Secure Java class loading”, published in *Internet Computing, IEEE* publication, sponsored by IEEE. [online]. URL: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=735987&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxppls%2Fabs_all.jsp%3Farnumber%3D735987.
- Security Explorations (2012). “Security Vulnerabilities in Java SE”, Technical Report, Ver. 1.0.2, SE-2012-01 Project. URL: <http://www.security-explorations.com/materials/se-2012-01-report.pdf>

StackOverflow (June 2011). *Java RMI, making an object serializable AND remote*. [online]. URL: <http://stackoverflow.com/questions/6268435/java-rmi-making-an-object-serializable-and-remote>.

W. Long, Frederick (2005). *Software Vulnerabilities in Java [Research Showcase]*. [online]. Carnegie Mellon University, October 2005. URL: <http://repository.cmu.edu/sei/422/>.

Waldo, J. (1998), "*Remote procedure calls and Java Remote Method Invocation*", Concurrency, IEEE , vol.6, no.3, pp.5,7, Jul-Sep 1998. [online]. URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=708248&isnumber=15346>.

Java remote method invocation. (n.d.). In Wikipedia. Retrieved June 5, 2014, from: http://en.wikipedia.org/wiki/Java_remote_method_invocation.

Java Remote Method Protocol. (July 2014). In Wikipedia. Retrieved August 2, 2014, from: http://en.wikipedia.org/wiki/Java_Remote_Method_Protocol.

Techopedia (n.d.). *Java Remote Method Invocation (Java RMI)*. URL: <http://www.techopedia.com/definition/23999/java-remote-method-invocation-java-rmi>.

Exception resolutions and troubleshooting:

Oracle.com (n.d.). *Enhancements in JDK 7*. [online]. URL: <http://docs.oracle.com/javase/7/docs/technotes/guides/rmi/enhancements-7.html>.

Oracle.com (n.d.). *RMI: access denied*. [online]. URL: <https://community.oracle.com/thread/1177999?start=0&tstart=0>.

Oracle.com (n.d.). *RMI Tutorial Error*. [online]. URL: <https://community.oracle.com/thread/2580182>.

Coderanch.com (Dec 2007). *Object already exported exception with RMI*. [online]. URL: <http://www.coderanch.com/t/210349/java/java/object-exported-exception-RMI>.

StackOverflow (Dec 2011). *How to close rmiregistry running on particular port?* [online]. URL: <http://stackoverflow.com/questions/8386001/how-to-close-rmiregistry-running-on-particular-port>.

StackOverflow (Feb 2012). *How to set the classpath that rmiregistry uses?* [online]. URL: <http://stackoverflow.com/questions/9440619/how-do-i-set-the-classpath-that-rmiregistry-uses/13829325#13829325>.

StackOverflow (Sep 2013). *Terminate Java RMI server application*. [online]. URL: <http://stackoverflow.com/questions/18782937/terminate-java-rmi-server-application>.

StackOverflow (June 2011). *What port is used by Java RMI connection?* [online]. URL: <http://stackoverflow.com/questions/3071376/what-port-is-used-by-java-rmi-connection>.

StackOverflow (Nov 2010). *Why RMI localhost client uses a no localhost ip to connect the RMI localhost server*. [online]. URL: <http://stackoverflow.com/questions/4258016/why-rmi-localhost-client-uses-a-no-localhost-ip-to-connect-the-rmi-localhost-ser>.

StackOverflow (June 2014).*RMI Exception: proxy cannot be cast to remote object*. [online]. URL: <http://stackoverflow.com/questions/25126037/rmi-exception-proxy-cannot-be-cast-to-remote-object/25128187>.

StackOverflow (Jul 2014).*RMI client throws “error unmarshalling return” exception when looking up*. [online]. URL: <http://stackoverflow.com/questions/24809576/rmi-client-throws-error-unmarshalling-return-exception-when-looking-up>.

StackOverflow (May 2012).*Java RMI simple Hello World program throwing RemoteException*. [online]. URL: <http://stackoverflow.com/questions/10752288/java-rmi-simple-hello-world-program-throwing-remoteexception>.

StackOverflow (June 2012).*Java RMI and ClassNotFoundException*. [online]. URL: <http://stackoverflow.com/questions/11273353/java-rmi-and-classnotfoundexception>.

StackOverflow (Nov 2011).*RMI Connection error Client Side*. [online]. URL: <http://stackoverflow.com/questions/4214916/rmi-connection-error-client-side>.

StackOverflow (Mar 2012).*Java.rmi.ServerException: RemoteException occurred in server thread*. [online]. URL: <http://stackoverflow.com/questions/9531158/java-rmi-serverexception-remoteexception-occurred-in-server-thread>.

pdplab.it (n.d.). “*An Improved RMI Tutorial*”. URL: <http://pdplab.it.uom.gr/teaching/sunjava/eclipse-rmi.html>.

9.2 Keywords:

- a) RMI – Remote Method Invocation; RPC – Remote Procedure Call; Remote class; Serializable class; object-oriented languages; object-oriented programming; programming environments; remote procedure calls; Distributed Common Object Model; Java Remote Method Invocation; Java virtual machine; RMI system; RPC mechanism; RPC systems; distributed applications; distributed systems method call; remote procedure call systems; Java; Operating systems; Skeleton; client-server system; message authentication;

10 Appendices:

10.1 Appendix A – Technical Terms:

- CABTAB: stands for “Code A Bit Test A Bit”, informally known as *Hacking*. It is a software development methodology more suited to projects handled by a single individual.
- Distributed version control system: a *distributed version control*, also known as *decentralized version control*, allows many software developers to work on a give project at the same time without sharing a common network. At the end of the software development, each developer stores their revision of the software in a *distributed version control system*.
- DRY: stands for “Don’t Repeat Yourself”. It is a principle of software development aimed at reducing repetition of information of all kinds in a codebase.
- Git: a *distributed version control system* designed to handle small to very large project with speed and efficiency.
- GitHub: a Git repository web-based hosting service offering all of the *distribute version revision control* and *source code management* functionality of Git as well as adding many of its own features.
- JRMP: stands for Java Remote Method Protocol. It is a java technology specific protocol for looking up and referencing remote objects.
- JVM: stands for “Java Virtual Machine”. It is a code execution component of Java platform that can execute Java bytecode.
- OOAD: stands for “Object Oriented Analysis and Design”. It is a popular technical approach to analyzing, designing an application, system, or business by applying the object-oriented paradigm.
- Prototype: a prototype is an early sample or model built to test a concept or process or to act as a thing to be replicated or learned from.
- RMI: stands for “Remote Method Invocation”. It is a Java API that allows an object running in a JVM to call a method on another object running on a different JVM.
- RPC: stands for “Remote Procedure Call”. It is an inter-process communication that allows a computer programme to cause a procedure to run in a different address space without needing the programmer to write the details for this remote communication.
- Serialization: a process of preserving the state of a Java object by writing it to a byte-stream.
- Incremental approach: a software development methodology where a software is designed, developed, tested and implemented in little steps, i.e. a little more added each time, until the product is finished.

- Iterative approach: this software development approach focuses on creating a prototype quickly by visiting all of the *Software Development Lifecycle Phases* in a repetitive manner.
- Proof of concept: it is a realization of a method or idea to demonstrate its feasibility and its purpose is to verify that some concept or theory has the potential of being used. A proof of concept is usually small and may or may not be complete.
- SMART: stands for “Specific Measurable Achievable Relevant Timed”. It defines the criteria of activities in project management that guides the manager of a project to using necessary action and resources appropriately.
- TCP/IP: short for ‘Transmission Control Protocol/Internet Protocol’. It is a suite of communication protocol used to connect a host to the internet.
- WATERFALL: a software development methodology based on *incremental approach*. As the name suggests, using this methodology the development of software is done using small steps one at a time. Activities in each step are completed fully before the result from this step is taken forward to the next step.
- URL: stands for Uniform Resource Locator. It is a specific character string that constitutes a reference to a web resource.
- VM: stands for Virtual Machine that emulates a particular computer system.

10.2 Appendix B – RMI Exceptions:

Several exceptions were faced while following the RMI tutorial on the official website of Oracle, the owner of this technology itself. The tutorial website is:

<http://docs.oracle.com/javase/tutorial/rmi/overview.html>

After setting up all necessary skeletons, RMI interfaces, server and client side implementation it was time to see it working. At that point, several things got in the way, the first of which turned out to be the security policy written by Oracle as part of their online tutorial. The security policy saved in a file, called ‘*server.policy*’, look like:

```
grant codeBase
"file/Users/tanvir/Documents/Developments/Workspace/RMISecurityInvestigation2S
erverSide/security/" {
permission java.security.AllPermission;
};
```

This didn’t work due to access permission issue as following:

```
ComputeEngine exception:
java.security.AccessControlException: access denied (java.net.SocketPermission
127.0.0.1:1099 connect,resolve)
at
java.security.AccessControlContext.checkPermission(AccessControlContext.java:3
76)
at java.security.AccessController.checkPermission(AccessController.java:549)
at java.lang.SecurityManager.checkPermission(SecurityManager.java:532)
```

```

at java.lang.SecurityManager.checkConnect(SecurityManager.java:1034)
at java.net.Socket.connect(Socket.java:522)
at java.net.Socket.connect(Socket.java:476)
at java.net.Socket.<init>(Socket.java:373)
at java.net.Socket.<init>(Socket.java:187)
at
sun.rmi.transport.proxy.RMIDirectSocketFactory.createSocket(RMIDirectSocketFac
tory.java:22)
at
sun.rmi.transport.proxy.RMIMasterSocketFactory.createSocket(RMIMasterSocketFac
tory.java:128)
at sun.rmi.transport.tcp.TCPEndpoint.newSocket(TCPEndpoint.java:595)
at sun.rmi.transport.tcp.TCPChannel.createConnection(TCPChannel.java:198)
at sun.rmi.transport.tcp.TCPChannel.newConnection(TCPChannel.java:184)
at sun.rmi.server.UnicastRef.newCall(UnicastRef.java:322)
at sun.rmi.registry.RegistryImpl_Stub.rebind(Unknown Source)
at engine.ComputeEngine.main(ComputeEngine.java:30)

```

After hours of effort when nothing was found wrong while support information is very limited, one of the blogs in orcle-community came handy, the full address of the blog is: <https://community.oracle.com/thread/1177999?start=0&tstart=0>, and this turned out to be a flaw in the security policy itself.

Once the security policy was rectified, the application was attempted to run again with appropriate JVM arguments. This time there was a *ClassNotFoundException* exception which didn't make much sense. As the exception suggests, the compiled class doesn't exist in the classpath which it superficially wrong, because the class clearly exists. After much effort to identify the real problem and days of investigation, this turned out to be a problem with a configuration not being set, namely Codebase configuration, which is only been introduced in java 7! The exception occurred on the server-side and looked something like this:

ComputeEngine exception:

java.rmi.ServerException: RemoteException occurred in server thread; nested exception is:

```

java.rmi.UnmarshalException: error unmarshalling arguments; nested exception is:
java.lang.ClassNotFoundException: compute.Compute
at sun.rmi.server.UnicastServerRef.oldDispatch(UnicastServerRef.java:419)
at sun.rmi.server.UnicastServerRef.dispatch(UnicastServerRef.java:267)
at sun.rmi.transport.Transport$1.run(Transport.java:177)
at sun.rmi.transport.Transport$1.run(Transport.java:174)
at java.security.AccessController.doPrivileged(Native Method)
at sun.rmi.transport.Transport.serviceCall(Transport.java:173)
at sun.rmi.transport.tcp.TCPTransport.handleMessages(TCPTransport.java:556)
at sun.rmi.transport.tcp.TCPTransport$ConnectionHandler.run0(TCPTransport.java:811)
at sun.rmi.transport.tcp.TCPTransport$ConnectionHandler.run(TCPTransport.java:670)
at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1145)
at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:615)
at java.lang.Thread.run(Thread.java:744)
at
sun.rmi.transport.StreamRemoteCall.exceptionReceivedFromServer(StreamRemoteCall.java:27
5)
at sun.rmi.transport.StreamRemoteCall.executeCall(StreamRemoteCall.java:252)

```

```

at sun.rmi.server.UnicastRef.invoke(UnicastRef.java:378)
at sun.rmi.registry.RegistryImpl_Skel.rebind(Unknown Source)
at engine.ComputeEngineStarter.main(ComputeEngineStarter.java:40)
Caused by: java.rmi.UnmarshalException: error unmarshalling arguments; nested exception
is:
java.lang.ClassNotFoundException: compute.Compute
at sun.rmi.registry.RegistryImpl_Skel.dispatch(Unknown Source)
at sun.rmi.server.UnicastServerRef.oldDispatch(UnicastServerRef.java:409)
at sun.rmi.server.UnicastServerRef.dispatch(UnicastServerRef.java:267)
at sun.rmi.transport.Transport$1.run(Transport.java:177)
at sun.rmi.transport.Transport$1.run(Transport.java:174)
at java.security.AccessController.doPrivileged(Native Method)
at sun.rmi.transport.Transport.serviceCall(Transport.java:173)
at sun.rmi.transport.tcp.TCPTransport.handleMessages(TCPTransport.java:556)
at sun.rmi.transport.tcp.TCPTransport$ConnectionHandler.run0(TCPTransport.java:811)
at sun.rmi.transport.tcp.TCPTransport$ConnectionHandler.run(TCPTransport.java:670)
at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1145)
at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:615)
at java.lang.Thread.run(Thread.java:744)
Caused by: java.lang.ClassNotFoundException: compute.Compute
at java.net.URLClassLoader$1.run(URLClassLoader.java:366)
at java.net.URLClassLoader$1.run(URLClassLoader.java:355)
at java.security.AccessController.doPrivileged(Native Method)
at java.net.URLClassLoader.findClass(URLClassLoader.java:354)
at java.lang.ClassLoader.loadClass(ClassLoader.java:425)
at sun.rmi.server.LoaderHandler$Loader.loadClass(LoaderHandler.java:1206)
at java.lang.ClassLoader.loadClass(ClassLoader.java:358)
at java.lang.Class.forName0(Native Method)
at java.lang.Class.forName(Class.java:270)
at sun.rmi.server.LoaderHandler.loadClassForName(LoaderHandler.java:1219)
at sun.rmi.server.LoaderHandler.loadProxyInterfaces(LoaderHandler.java:729)
at sun.rmi.server.LoaderHandler.loadProxyClass(LoaderHandler.java:673)
at sun.rmi.server.LoaderHandler.loadProxyClass(LoaderHandler.java:610)
at java.rmi.server.RMIClassLoader$2.loadProxyClass(RMIClassLoader.java:646)
at java.rmi.server.RMIClassLoader.loadProxyClass(RMIClassLoader.java:311)
at sun.rmi.server.MarshalInputStream.resolveProxyClass(MarshalInputStream.java:255)
at java.io.ObjectInputStream.readProxyDesc(ObjectInputStream.java:1558)
at java.io.ObjectInputStream.readClassDesc(ObjectInputStream.java:1514)
at java.io.ObjectInputStream.readOrdinaryObject(ObjectInputStream.java:1771)
at java.io.ObjectInputStream.readObject0(ObjectInputStream.java:1350)
at java.io.ObjectInputStream.readObject(ObjectInputStream.java:370)
... 13 more

```

; again, there was no explicit mention of this new feature in the tutorial (which makes the tutorial out-of-date!). Hint to a solution to the problem was found in Oracle's community website: <https://community.oracle.com/thread/2580182>

, and a brief mention on one of the Oracle's documentation website: <http://docs.oracle.com/javase/7/docs/technotes/guides/rmi/enhancements-7.html>.

The same exception may also occur with *unmarshalling* a return value (previously occurred for *unmarshalling* method arguments) on the server side:

```

ComputeEngine exception:
java.rmi.UnmarshalException: Error unmarshaling return; nested exception is:

```



```

    java.net.MalformedURLException: no protocol:
(file:/Users/tanvir/Documents/Developments/Workspace/RMITutorialFromOracle/RMISecurity
Investigation2ServerSide/thirdParty/compute.jar
    at sun.rmi.transport.StreamRemoteCall.executeCall(StreamRemoteCall.java:246)
    at sun.rmi.server.UnicastRef.invoke(UnicastRef.java:378)
    at sun.rmi.registry.RegistryImpl_Stub.rebind(Unknown Source)
    at engine.ComputeEngineStarter.main(ComputeEngineStarter.java:40)
Caused by: java.net.MalformedURLException: no protocol:
(file:/Users/tanvir/Documents/Developments/Workspace/RMITutorialFromOracle/RMISecurity
Investigation2ServerSide/thirdParty/compute.jar
    at java.net.URL.<init>(URL.java:585)
    at java.net.URL.<init>(URL.java:482)
    at java.net.URL.<init>(URL.java:431)
    at sun.rmi.server.LoaderHandler.pathToURLs(LoaderHandler.java:769)
    at sun.rmi.server.LoaderHandler.getDefaultCodebaseURLs(LoaderHandler.java:140)
    at sun.rmi.server.LoaderHandler.loadClass(LoaderHandler.java:169)
    at java.rmi.server.RMIClassLoader$2.loadClass(RMIClassLoader.java:637)
    at java.rmi.server.RMIClassLoader.loadClass(RMIClassLoader.java:264)
    at sun.rmi.server.MarshalInputStream.resolveClass(MarshalInputStream.java:214)
    at java.io.ObjectInputStream.readNonProxyDesc(ObjectInputStream.java:1612)
    at java.io.ObjectInputStream.readClassDesc(ObjectInputStream.java:1517)
    at java.io.ObjectInputStream.readOrdinaryObject(ObjectInputStream.java:1771)
    at java.io.ObjectInputStream.readObject0(ObjectInputStream.java:1350)
    at java.io.ObjectInputStream.readObject(ObjectInputStream.java:370)
    at sun.rmi.transport.StreamRemoteCall.executeCall(StreamRemoteCall.java:244)
    ... 3 more

```

The exception also occurred on the client:

```

ComputePi exception:
java.rmi.UnmarshalException: error unmarshalling return; nested exception is:
    java.net.MalformedURLException: no protocol:
(file:/Users/tanvir/Documents/Developments/Workspace/RMITutorialFromOracle/RMISecurityI
nvestigation2ServerSide/thirdParty/compute.jar
    at sun.rmi.registry.RegistryImpl_Stub.lookup(Unknown Source)
    at client.ComputePi.main(ComputePi.java:34)
Caused by: java.net.MalformedURLException: no protocol:
(file:/Users/tanvir/Documents/Developments/Workspace/RMITutorialFromOracle/RMISecurityI
nvestigation2ServerSide/thirdParty/compute.jar
    at java.net.URL.<init>(URL.java:585)
    at java.net.URL.<init>(URL.java:482)
    at java.net.URL.<init>(URL.java:431)
    at sun.rmi.server.LoaderHandler.pathToURLs(LoaderHandler.java:769)
    at sun.rmi.server.LoaderHandler.loadProxyClass(LoaderHandler.java:527)
    at java.rmi.server.RMIClassLoader$2.loadProxyClass(RMIClassLoader.java:646)
    at java.rmi.server.RMIClassLoader.loadProxyClass(RMIClassLoader.java:311)
    at sun.rmi.server.MarshalInputStream.resolveProxyClass(MarshalInputStream.java:255
)
    at java.io.ObjectInputStream.readProxyDesc(ObjectInputStream.java:1558)
    at java.io.ObjectInputStream.readClassDesc(ObjectInputStream.java:1514)
    at java.io.ObjectInputStream.readOrdinaryObject(ObjectInputStream.java:1771)
    at java.io.ObjectInputStream.readObject0(ObjectInputStream.java:1350)
    at java.io.ObjectInputStream.readObject(ObjectInputStream.java:370)
    ... 2 more

```

This reason behind the above exception is the *Codebase* feature not being properly set; there are discussions on this in many blogs on the Oracle community as well other

programming sites, such as StackOverflow. A good explanation of why this exception happen and how to prevent this is described in [section 4.3](#).

In addition to the above mentioned *Exceptions*, there are other subtle ones likely to occur as results of incorrect implementation.

One of them is:

```
java.rmi.ConnectException: Connection refused to host: 192.168.0.6; nested exception
is:
    java.net.ConnectException: Connection refused
        at sun.rmi.transport.tcp.TCPEndpoint.newSocket(TCPEndpoint.java:619)
        at sun.rmi.transport.tcp.TCPChannel.createConnection(TCPChannel.java:216)
        at sun.rmi.transport.tcp.TCPChannel.newConnection(TCPChannel.java:202)
        at sun.rmi.server.UnicastRef.newCall(UnicastRef.java:341)
        at sun.rmi.registry.RegistryImpl_Stub.lookup(Unknown Source)
        at
uk.ac.rm950.breachOfConfidentialityClient.ClientSideProgram.main(ClientSideProgram.java
:24)
Caused by: java.net.ConnectException: Connection refused
    at java.net.PlainSocketImpl.socketConnect(Native Method)
    at java.net.AbstractPlainSocketImpl.doConnect(AbstractPlainSocketImpl.java:339)
    at
java.net.AbstractPlainSocketImpl.connectToAddress(AbstractPlainSocketImpl.java:200)
    at java.net.AbstractPlainSocketImpl.connect(AbstractPlainSocketImpl.java:182)
    at java.net.SocksSocketImpl.connect(SocksSocketImpl.java:392)
    at java.net.Socket.connect(Socket.java:579)
    at java.net.Socket.connect(Socket.java:528)
    at java.net.Socket.<init>(Socket.java:425)
    at java.net.Socket.<init>(Socket.java:208)
    at
sun.rmi.transport.proxy.RMIDirectSocketFactory.createSocket(RMIDirectSocketFactory.java
:40)
    at
sun.rmi.transport.proxy.RMIMasterSocketFactory.createSocket(RMIMasterSocketFactory.java
:147)
    at sun.rmi.transport.tcp.TCPEndpoint.newSocket(TCPEndpoint.java:613)
    ... 5 more
```

-this usually occurs on the client-side and indicates that the service is not running.

There's also:

```
java.rmi.server.ExportException: remote object implements illegal remote interface;
nested exception is:
    java.lang.IllegalArgumentException: illegal remote method encountered: public
abstract java.lang.Object
uk.ac.rm950.remoteInterface.RemoteJobInterface.retrieveJobReport(uk.ac.rm950.remoteInte
rface.JobInterface)
    at sun.rmi.server.UnicastServerRef.exportObject(UnicastServerRef.java:198)
    at java.rmi.server.UnicastRemoteObject.exportObject(UnicastRemoteObject.java:310)
    at java.rmi.server.UnicastRemoteObject.exportObject(UnicastRemoteObject.java:252)
    at
uk.ac.rm950.breachOfConfidentialityServer.ServerSideProgram.main(ServerSideProgram.java
:27)
```

```

Caused by: java.lang.IllegalArgumentException: illegal remote method encountered:
public abstract java.lang.Object
uk.ac.rm950.remoteInterface.RemoteJobInterface.retrieveJobReport(uk.ac.rm950.remoteInte
rface.JobInterface)
    at sun.rmi.server.Util.checkMethod(Util.java:262)
    at sun.rmi.server.Util.getRemoteInterfaces(Util.java:241)
    at sun.rmi.server.Util.getRemoteInterfaces(Util.java:211)
    at sun.rmi.server.Util.createProxy(Util.java:144)
    at sun.rmi.server.UnicastServerRef.exportObject(UnicastServerRef.java:196)
    ... 3 more

```

-this happens when one or more method signatures in the remote interface does not throw RemoteException.

Another likely exception is:

```

java.rmi.ConnectException: Connection refused to host: 192.168.0.7; nested exception
is:
    java.net.ConnectException: Operation timed out
        at sun.rmi.transport.tcp.TCPEndpoint.newSocket(TCPEndpoint.java:619)
        at sun.rmi.transport.tcp.TCPChannel.createConnection(TCPChannel.java:216)
        at sun.rmi.transport.tcp.TCPChannel.newConnection(TCPChannel.java:202)
        at sun.rmi.server.UnicastRef.newCall(UnicastRef.java:341)
        at sun.rmi.registry.RegistryImpl_Stub.lookup(Unknown Source)
        at
uk.ac.rm950.breachOfConfidentialityClient.ClientSideProgram.main(ClientSideProgram.java
:24)
Caused by: java.net.ConnectException: Operation timed out
    at java.net.PlainSocketImpl.socketConnect(Native Method)
    at java.net.AbstractPlainSocketImpl.doConnect(AbstractPlainSocketImpl.java:339)
    at
java.net.AbstractPlainSocketImpl.connectToAddress(AbstractPlainSocketImpl.java:200)
    at java.net.AbstractPlainSocketImpl.connect(AbstractPlainSocketImpl.java:182)
    at java.net.SocksSocketImpl.connect(SocksSocketImpl.java:392)
    at java.net.Socket.connect(Socket.java:579)
    at java.net.Socket.connect(Socket.java:528)
    at java.net.Socket.<init>(Socket.java:425)
    at java.net.Socket.<init>(Socket.java:208)
    at
sun.rmi.transport.proxy.RMIDirectSocketFactory.createSocket(RMIDirectSocketFactory.java
:40)
    at
sun.rmi.transport.proxy.RMIMasterSocketFactory.createSocket(RMIMasterSocketFactory.java
:147)
    at sun.rmi.transport.tcp.TCPEndpoint.newSocket(TCPEndpoint.java:613)
    ... 5 more

```

-this indicates that the client cannot access the service, which may be due to a firewall-block or any other reason.

10.3 Appendix C – Project timelines and Gantt chart:

Task ID	Task Name	Start Date	End Date	Dependencies	Duration	% Complete	Comments
1	Initial works						
1.1	Researching ideas and Project selection			Not Applicable		100%	These tasks are now completed.
1.2	Getting supervisor's approval on project idea						
1.3	Hands on RMI technology, fixing & resolving technical issues, research, working on various tutorials, getting a basic working application						

2	Proposal, Literature Review and Initial Report	14	01/07/14	08/07/14		9	100%	Project Investigation of security implications of Java RMI.	Title:
2.1	Proposal and planning	14	01/07/14	02/07/14		2	100%		
2.2	Submission of proposal	14	03/07/14	03/07/14	2.1	1	100%		
2.3	RMI Technology based literature review and documentation + upload on Project Portal	14	04/07/14	07/07/14	2.2	4	100%		

2.4	Feedback from Supervisor (Afternoon session would be helpful)	07/07/14	07/07/14		1		<p>A literature focused feedback at this stage will be regarded very beneficial and would help me:</p> <ol style="list-style-type: none"> 1. Identify and close any gaps in RMI technology based research and documentation 2. Gauge the depth of research and documentation needed for security analysis 3. Discuss the appropriateness of the planned testbed prototype application
-----	---	----------	----------	--	---	--	--

2.5	Reflection & Evaluation of the feedback and implementing any suggestion	14	08/07/09/07/14		1		
3	Analysis of RMI security aspects	14	10/07/28/07/14		18		
3.1	RMI security focused literature review and documentation	14	10/07/20/07/14		11		

3.2	Feedback from Supervisor	21/07/ 14	21/0 7/14		1		<p>Need to discuss what exploitation and experiments can be carried out:</p> <ol style="list-style-type: none"> 1. What to be achieved? 2. How to demonstrate this achievement? 3. Revisit the planned testbed prototype application
-----	-----------------------------	--------------	--------------	--	---	--	---

3.3	Reflection & Evaluation of the feedback and implementing any suggestion	14	22/07/28/07/14		6		
4	Test bed prototype development	14	01/08/19/08/14		20		
4.1	Prototype Application and GUI layer	14	01/08/07/08/14		7		Currently the plan is to write a simple program that carries out various exhaustive calculations with different number of threads and gauges the performance for lapsed time. This application will measure whether increasing number of threads will increase performance for a given task.

4.2	Feedback from Supervisor (Afternoon session due to other appointments in the morning)	08/08/14	08/08/14		1		Feedback here may be focused on: 1. How the application serves the purpose 2. What can be done to cause a security vulnerability and exploit it
4.3	Adding security vulnerability code to the Client Side	09/08/14	10/08/14		2		Client application will try to access user areas on the Server side
4.4	Exploitation of security vulnerability	11/08/14	12/08/14		2		

4.5	Feedback from Supervisor	13/08/14	13/08/14		1		Discuss the findings, what and what not went well, how to present this effectively.
4.6	Documentation	14/08/14	19/08/14		6		
5	Report Writing	20/08/14	02/09/14		14		
5.1	Consolidation of documentations	20/08/14	22/08/14		3		

5.2	Reviewing and Critical evaluation: what worked well and what didn't	23/08/14	26/08/14		4		
5.3	Evaluation of strengths and weakness	27/08/14	28/08/14		2		
5.4	Future works	29/08/14	29/08/14		1		
5.5	Tidying up, referencing and finalising report	30/08/14	02/09/14		3		

