Methods and Techniques of Security Testing:  
A Survey

Divya Nigam, Vinita Malik, Sarvagya Nigam  
Department of Information Technology, MSIT, Delhi, India

Abstract: Security Testing helps in protecting the software against unanticipated actions. The target of security testing is to provide assurance regarding that the software is safe and secure. Security testing is very helpful in identifying loop holes and security risk in the software. Our Objective is to provide comprehensive survey of security Testing methods and Techniques where security Testing Techniques can be classified as: Technical assessment Techniques and non-Technical Assessment Techniques. As a Result of classifying these approaches a direction for integration and future research topic is illustrated. This study presents sophisticated ideas in a simplified form that should be beneficial to both practitioners and researchers in solving software security testing issues.  
Keywords: Security Testing, Software Testing, Technical Assessment Techniques, Vulnerability.

1. Introduction
Software Testing is a very useful process of executing program with the intention of finding bugs. It is well known fact that 40% to 50% of the total development expenditure is allocated to software testing. Some of the most important techniques of software testing which are classified on the basis of purpose are correctness Testing, Performance Testing, Security Testing and Reliability Testing. Software testing can be called as a process of measuring quality of software being developed and also a process of uncovering bugs in a program. Not only this, it is also a process to determine the consistency of security features of software implementation with the design. Software security requirements mainly included are: confidentiality, authentication, availability, authorization, integrity and non-repudiation. Other requirements are privacy protection, access control, security management, audit etc. Software security is the defending ability of software against attack. The concern about security testing is growing now a days. Software Security Testing are further classified as Review Techniques, Target Identification and analysis and Target Vulnerability Analysis .Some Security Testing Tools have also been developed are source code analysis, code review , packet analyser, binary code analysis penetration testing, wireless sniffer, static analysis tool, application testing tools, source code security analyser, static code analysis, vulnerability scanning tools, , vulnerability assessment software and vulnerability assessment

A survey has major advantages over simple study because it not only simplifies evaluation but it also renders and simplifies all available research work which is relevant to the particular area of interest .The main motive behind survey is that the techniques and methods that are discussed in past reflect their suitability for the present need and are considered to be useful to fulfil the needs of the future perceptivity. We have gone through the research from 2004-2013 In 2004, G. mcgraw, [5] the complete background details of software security came into view. In 2005, G. mcgraw[1] about black box testing tools were introduced. In 2005,[14] the Information systems were secured using modelling language where security met as a measure for software engineering In 2006, C. Braz et al., [2]the usability and user acceptance of security systems had been become a major issue in research on the efficiency . In 2007, A C. Dias Neto et al. [3] a systematic review was performed on model based testing (MBT) approaches. In 2008,R J Barnett et al.[4], a review of security testing literature is performed, In 2010, E.T. Baadshaug et al.,[12] an overview of some approaches to graphical security modelling has been given and presented. In 2010, by G Tian -yang, [8] the definition in addition to classification of software security testing were discussed and methods and tools of software security testing has been investigated. In 2011, J. Bayuk et al., [7] Security metrics have evolved side by side with the advent of security tools and techniques. In 2013, D.Gupta et al.[6]According to him, the protection of data against unauthorized access and corruption of data due to malicious actions was the major issue.

The rest of the paper is organized as follows: in Section 2 the selection criteria of the specified topic is discussed, i.e., Security Testing Techniques and it is further subdivided into sub topic named as selection of search engines, searching of required material and storage criterion of searching material. In Section 3 few research issues related to our survey are discussed. In this section some research questions are described while conducting survey. Then after, the solutions of research questions has been given with
precise description and their complete description is
defined in other section. In Section 4 we discuss the
basic terms in our research background are discussed.
After that in Section 5 complete literature study is
mentioned and summarized table for the same is also
provided. Then after the analysis of current trends are
mentioned followed by section 6. At the End, the future
scope and few challenges are described

2. Selection criteria
The procedure of research has been explained in this
section. The main objective is to extract significant
fruitful research papers and filter out relevant data from
them based on Security Testing techniques and
methods. Figure 1 explains about creation of selection
criteria. It is an advanced selection process for
performing relevant research under the title. This
selection process based upon most famous journals,
conferences, search engines and articles. Hence we
have explored rich database of relevant research papers
for establishing good selection criteria. The selection
criteria can be divided further into following steps and
these steps are given as below [15]:

1. Firstly the selection of the relevant search engines,
   articles, conference proceedings and journals is done
2. Search a required material and their after
   contributing advancement in the search results
3. Storage criterion of the searched material.

2.1. How Research Proceeds
As shown in figure 2, firstly the research problem is
being defined. Then after the concepts and theories are reviewed and previous research is
analysed after that the research question being
formulated. Then, after the research is defined and the data is collected for execution. The
extracted data is analysed after it has been collected. Finally the interpretation and report
generation is performed.
But this survey of security testing classification is confined to years (2004-2013)

2.2 Selection on the basis of search engines, articles, conference proceedings and journals

The initial stage starts with searching the required content and it requires a minimum number of steps, hence efficient search engine is mandatory to choose. The following points need to be considered for selecting search engine [15](Kitchenham, 2004):

1. Search engines should be authenticated for providing expected search results.
2. Search Engine are renowned.
3. Search engines also feed us with advanced search facilities as it has the capability to refine the material to majority of extent and up to the different levels.

List of the selected search engines which can be used:
1. Google scholar.
2. Springer
3. IEEE explore
4. ACM Digital Library

Following are the selected journals/ conferences:

- IEEE Transactions on Software Engineering (TSE)
- IEEE (An International Conference on Software Testing Verification and Validation Workshop) (ICSTW)
- IEEE Security and privacy

For attaining a high level of search rate, a group of well-known journals and conferences should be set up for search process. Moreover, only the famous, fruitful, relevant search engines are to be put on highest priority for the purpose of searching relevant facts. We move on from specific to general keywords while searching keyword.

List of keywords preferably used for searching:
1 Security Testing
2 Security Testing Techniques
3 Security testing methods
4 Researches on Security Testing
5 History of Security Testing

2.3 Searching of required material

This section deals with searching of required material and extracting it according to requirement. Required material should be searched as follows:
1. In order to search any general or conference, searching should be performed using searching keyword from year to year. (2004-2013).
2. Materials which is being searched can be improved by finding the relevant material.

2.4 Storage criterion of searched material

The proper saving of the searched material is equally important as the search process itself. Many procedures have been adopted in order to store collected material according to requirement. A small database would be like Microsoft Word or Excel which is used for storage. The database categorise searched as well as selected material and provide brief description of the data with cross references. Hence duplicate entries of a searched or selected material do not get repeated.

2.5 Graphical analysis of searched or selected material

An analysis shows that the research study was not distributed evenly over the years of the defined period, i.e., 2004–2013. Figure 3 shows the number of collected research papers. Table 1 has defined the list of selected reference papers. The collected papers are divided into following categories:
1. Number of journals
2. Number of conferences and
3. Number of detailed study material,

<table>
<thead>
<tr>
<th>Selected Research journal/Conference</th>
<th>No. of papers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Journal</td>
<td>4</td>
</tr>
<tr>
<td>Conference</td>
<td>15</td>
</tr>
<tr>
<td>Others</td>
<td>3</td>
</tr>
<tr>
<td>Total</td>
<td>22</td>
</tr>
</tbody>
</table>

RQ 2: How Security Testing can be classified in different techniques

RQ 3: How security Testing can be classified in different Methods

RQ 4: How different Security Requirements can be classified.

4. Research background

4.1. How security Testing is related to software Testing

Software testing identifies the quality of software being developed and uncovers errors. The purpose of Software testing can be shown with the following Diagram in Table 5

<table>
<thead>
<tr>
<th>Purpose of Software Testing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quality assurance</td>
</tr>
<tr>
<td>Verification</td>
</tr>
<tr>
<td>Correctness</td>
</tr>
<tr>
<td>Validation</td>
</tr>
<tr>
<td>Reliability</td>
</tr>
<tr>
<td>Estimation</td>
</tr>
</tbody>
</table>

Table 2: Purpose and description of Software Testing

<table>
<thead>
<tr>
<th>Purpose Of software Testing</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quality assurance</td>
<td>Observing software engineering processes and methods which are used to ensure quality</td>
</tr>
<tr>
<td>Verification/validation</td>
<td>checking whether a software system meets specifications and fulfils its intended purpose</td>
</tr>
</tbody>
</table>

In Figure 3, these research papers were only related to Software and security Testing Techniques and methods and pertained to the selected journals or conference proceedings for the period of 2004–2013.

3. Research issues

The aim of this survey is to identify the solution of some research questions which depends upon existing evidence. We have summarized these evidence and gap in the current research has been identified and thus the basis of new research activity can be formed in software security. Some research questions that are mentioned below are being identified and these RQ are discussed in section analysis of current trend section 6 with their solution.
Correctness Testing deals whether software is meeting with the requirement or not which it is intended to do so. White box, black box or grey box testing are not limited to correctness testing only. Objectives of performance testing are to maintain a low latency of a website, high throughput and low. ‘Reliability Testing’ identifies all the failures of a system and removes them before the deployment of the system. ‘Security testing’ assures about authorized Access. Security Testing is all about finding the loopholes as well as weaknesses of a system.

4.2. Description for Security Testing

Software security can be expressed as the ability of software to provide required function when it is attacked. Software security testing can be defined as the process of identifying consistency of security features of software implementation with the design. Software security testing is divided into functional testing and vulnerability testing. Security testing basically validate the security functional as well as assurance requirements.

4.3. Classification of Security testing

Security testing can be classified as security Testing techniques and Security Testing methods. Figure 6 depicts its classification.

However, Software Testing means a process with the intent of finding bugs while program execution. The Software Testing can be subdivided into Correctness Testing, Reliability Testing, Security Testing and Performance Testing. Correctness Testing can be subdivided into White Box, Black Box, and Gray box. Where Black box is further divided into with user involvement and without user involvement and others methods. Performance Testing can be divided into stress Testing and Load Testing. Robustness Testing come under reliability Testing. Security Testing can be subdivided into Review Techniques, Target Identification and analysis and Target Vulnerability Validation. The diagram shown below represents some of the most important techniques of software testing which are classified on the basis of purpose. Figure 6 depicts the types of Software Testing.

<table>
<thead>
<tr>
<th>Correctness</th>
<th>It deals with whether the software so developed is meeting the user requirements or not</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reliability Estimation</td>
<td>It deals with estimation that how much our software is reliable i.e. its free from defects</td>
</tr>
</tbody>
</table>
4.3.1 Testing includes the following types of security testing methods

- **Formal security testing**
  Formal method of security testing deals with building a mathematical model of the software. It also provides a software form specification supported by some formal specification language. Formal security testing methods are basically theorem proving and model checking methods. There are some limitation of Method of formal security testing. As far as theorem proving is concerned, it is tough to achieve automatically, a good quality members are required to analyse it. Hence it verifies design instead the actual code. Where as in model checking method, practical implementation states are required, hence less efficient [8].

- **Model-based security testing**
  This kind of testing builds a software behaviour model and structure model analysing its behaviour and its dimensions exploring test cases from test model by G. Tian-yang et al. Various UML models like activity diagrams, sequence diagram, collaboration diagram and input output sequences are used to analyse the behaviour of software systems. [8]

- **Security Testing based on Fault injection**
  The main focus of this technique is on the interaction points of application and environment which includes user input, file system, environment variable and network interface. This technique helps the software to reach to such state which is not possible with other techniques [8].

- **Fuzzy testing**
  Fuzzy testing emphasizes on detecting vulnerabilities related to security purposes getting more awareness. Fuzzy testing intends to test the program by injecting some random data into it to check whether it can work normally with the unclear input. Fuzzy testing just creates jumbled data and find defects of tested software, which are very difficult to implement using other logical testing techniques [8].

- **Vulnerability scanning testing**
  Vulnerability scanning identifies software security risks and defects during scanning. [8]

- **Property-based testing**
It transforms security property of software into specification. Bishop. Property-based testing focuses on some specific security properties, which can meet requirement of classification and priority [8].

- **White box-based security testing**
  It is static testing technique and has objective to evaluate information directly from the source code without executing it. It can find security bug, such as buffer overflow. The main technologies of static analysis include data flow analysis, constraint analysis and deducting.. [8].

- **Risk-based security testing**
  B.A. Gary McGraw, etc made researches are made on risk-based security testing and the risk analysis, security testing with software development life cycle is combined, as early as possible to risky security vulnerabilities.[8]

### 4.3.2 Classification of Security Testing Techniques


There are many security testing techniques which exist and can be used to assess the security level of systems and software, are grouped into the following three categories:

1. **Review Techniques.** These techniques are used to evaluate systems and softwares in order to discover vulnerabilities. These techniques are generally performed manually.

2. **Target Identification and Analysis Techniques.** These testing techniques are used to identify services, and risky vulnerabilities.

3. **Target Vulnerability Validation Techniques.** These testing techniques identifies the presence of vulnerabilities depending on the specific technique being used.

#### 4.3.2.1 Review Techniques

- **Documentation Review**
  Document review is a way of collecting and analysing data by reviewing existing documents. General knowledge of security from policy perspective is needed to conduct documentation review. Documentation review helps in discovering gaps and weakness in the certain software. [20].

  - **Log Review**
    Log review is used to detect suspicious activities as soon as possible in order to minimize the impact of incidence. It can also perform prevention of incidence if possible. Various system such as server logs or any other logs are used to identify respective deviations from policy. Log review and analysis can also provide a dynamic picture of present system activities which can be compared with security policy [20].

  - **Ruleset Review**
    It helps in revealing holes in ruleset-based security controls. A ruleset is basically a collection of signatures. Review of these rulesets is done to identify gaps and weaknesses on security devices.[20].

  - **System Configuration Review**
    System configuration review is the process that evaluates the strength of system configuration. Knowledge of secure system configuration, including OS hardening and security policy configuration for a variety of operating systems and ability to use automated security configuration testing tools is needed for periodic system configuration review. Examples of security configuration files that may be reviewed are Windows security policy settings and Unix security configuration files [20].

- **Network Sniffing**
  Network sniffing refers to a utility that examine data packets on a network to gather data from a packet or to identify the content of packet. It is a passive activity of network packet of identification. It basically monitors network traffic on the local segment to capture information such as active systems, operating systems, communication protocols, services, and applications and verifies encryption of communications [20].

  - **File Integrity Checking**
    A file integrity checker basically computes and stores a checksum for every guarded file. It establishes a database of file checksums. Then after, It identifies unauthorised changes to important files and certain forms of unwanted files. Stored checksums should be recomputed regularly to test recent value against the stored value in order to identify any file modifications. [20].

#### 4.3.2.2 Target Identification and Analysis Techniques
The technical target identification and analysis techniques targets at identification of active devices and their associated ports and services, and analyzing them for potential vulnerabilities.

- **Network Discovery**

Open network port and communication paths are identified in network architecture. In other words we say it as a process of identifying edges and non-edges of unknown devices on a network. There are mainly two types of network discovery: [22]

- Active(testing) network discovery
- Passive(examination) network discovery

Passive techniques are used as a network sniffer to monitor network traffic and record the IP addresses of the active hosts whereas Active techniques send various types of network packets, such as Internet Control Message Protocol (ICMP) pings, to solicit responses from network hosts.

- **Vulnerability Scanning**

Vulnerability scanning is bit similar to the concept of a port scanning to some extent. A vulnerability scanner as similar to port scanner identifies hosts and open ports, besides it also provides information on the associated vulnerabilities and provides advice on identified vulnerabilities. Vulnerability scanning can also help identify outdated software versions, and misconfigurations [20].

- **Wireless Scanning**

Wireless Scanning identifies unauthorized wireless devices within range of the scanners and also discovers wireless signals outside of an organization’s perimeter. It also identifies and locates potential backdoors. [20]

  - **Wireless Passive Scanning**

Wireless tools for passive scanning send no data and don’t affect the functionality of the particular deployed devices. A passive scanning tool remains undetected by malicious users as it does not transmit the data.

  - **Wireless Active Scanning**

This kind of scanning is effective while using penetration testing for wireless devices. Tools which use scripted attacks try to bypass employed security measures and determine the security level of devices. Tools which are used to perform wireless penetration testing, try to find out the access point in order to connect itself with devices in the defined network with properly designed configuration. [20].

  - **Wireless Device Location Tracking**

It monitors wireless network traffic to identify the suspicious activity involving the protocols themselves. It also examines the security technologies in depth. Dedicated sensors can focus on detection and don’t need to carry wireless traffic.

They also have tendency to locate device at several distances [20].

- **Bluetooth Scanning**

It is a method to test the security of devices in a limited range. It can provide ample information about discoverable devices. Similar to active scanning, it can only be applicable when devices belong to particular organisation. The security mode in which Bluetooth device is working can be used to evaluate their security. The tools which are used to conduct security testing of Bluetooth devices, attempt to connect discovered devices and trigger attacks to gain access into devices [20].

**4.3.2.3 Target Vulnerability Validation Techniques**

These techniques are based on targets and used to explore the potential vulnerabilities.

- **Password Cracking**

Password cracking is the means to gain access into the systems by identifying weak passwords. As we know passwords in systems are not available in plain form, they are generally stored in the hash form and transmitted in the encrypted form, which protects the systems from breaching of security. The password entered by the user is compared to its stored hash and if there is match found only then genuine access allowed. The method for computing hashes are rainbow table, dictionary based attacks which uses all possible combinations of keys. There are also password cracking tools available to retrieve the password of standalone and networked devices such as ophcrack, l0pahcrack etc. [19]

- **Penetration Testing**

Penetration testing attempts to identify security weaknesses in the systems by attacking in order to trigger the vulnerabilities and gain access to system. Penetration testing tools like black box scanners which are unaware of internal working of the system and works only by analysing the responses. This kind of testing can be quickly applied to evaluate software security [1,19].

- **Social Engineering**

It is non-technical kind of attack. It just involves cheating people. It can be used with other kind of attacks like phishing which actually also relies on social engineering. [20]

**5. Literature study**

A survey provides supplementary benefits as compared to a simple study because it not only abridges assessment but it also renders all available research work appropriate to a particular occurrence of interest. The study derives from legitimate motive that
the techniques that are conferred in past to be a sign of their suitability for the current scenario and are considered to fulfil the needs of the future perceptivity. In 2004,[5] The progress in field of security testing has shown a remarkable impact as compared to network port scanning technique in order to check for behaviour of complex portion of the software system.

If security testing is performed in a correct manner than it can work much better than common black box testing (functional testing) in finding the loopholes. This can be more efficient by making use of security tools. In 2004, McGraw explained that in software engineering evolving best practices security of software should be taken into consideration. As we know requirements, design are relevant for security of software architecture and its analysis. The common criteria has been used to conduct security testing like authentication, access control, key management and cryptography. In 2005, [1] about black box testing tools were introduced. Black box testing tools are based on input and outputs. They are unaware of internal workings of the program. They work on analysing the responses and try to confirm the existence of particular vulnerability. Black box testing tools work similar to pen-test tools. In 2005,[14] the Information systems were secured using modelling language where security met as a measure for software engineering.

In 2006, C.Braz, [2] they provided their idea on enhancing the efficiency of security systems. As Knowledge based authentication work out to be efficient in minimizing the effect of unauthorized access. In 2007, A.C. D. Neto1 et al, [3] a study was performed on model based testing (MBT) approaches. This study resulted in deep analysis of where these MBT approaches have been used. The comparison criteria includes representation models, support tools, test coverage criteria, the level of automation, intermediate models, and the complexity. In 2008, [4] A scheme related to software security was proposed Which exploits the directory or database of all identified vulnerabilities that is useful to provide inputs to the next service for testing.

In 2010, [12] by E.T. Baadshaug et al., This study provided the idea on overview about the current approaches of security modelling using modelling tools and formalism. After that these tools and formalism can be selected for further analysis to explore more relevant ideas related to software security practices.

In 2010, by G.T.yang et al,[8] the definition and classification related to software security testing were discussed. The methods and tools for this have also been investigated. Along with merits and demerits of respected techniques this paper stresses on the future direction of security technology.

In 2011, J Bayuk et al., [7] described that security metrices have been emerging with the arrival of various security assessment tools and techniques. They represented best and currently used security metrices, which then further be used for verification and validation. In 2013, D.gupta et al.,[6] discussed about the how the data can be secured from unintended loss or from malicious hackers. It presents key concepts on security, also providing the basis for understanding existing challenges on developing and deploying secure software systems.

6. Analysis of current trends

RQ 1: How Security Testing Is Related to Software Testing. However, Software testing is a method to identify potential errors in the system so that it can be debugged soon. The Software Testing is divided into various subcategories like Correctness Testing, Performance testing, Reliability Testing and Security testing. Correctness testing is further divided into Black box, white box and gray box where Black box is further divided into with user involvement and without user involvement and others methods. Performance testing can further be divided into stress testing and Load testing. Robustness Testing come under reliability Testing. Security Testing can be subdivided into Review Techniques, Target Identification and analysis and Target Vulnerability Validation. Figure 7 depicts software Testing Techniques. Refer to Research section

RQ2: How Security Testing can be classified in different techniques. The Security Testing Techniques can be classified as Technical Security Testing and Non-Technical Security Testing. The Technical Security Testing is divided into review techniques, Target identification and analysis and Target vulnerability Validation. The non-technical Security Testing can be divided into Physical Security and Manual assets Identification. It can be shown in Figure 8
There are many security testing techniques (depicted in figure 9) that exists to evaluate the security measures of any system and networks. The different techniques of software security testing are:

1. Review Techniques
2. Target Identification and analysis techniques
3. Target vulnerability validation techniques.
RQ3: How security testing can be classified in different methods? Security Testing Methods can be classified as Property-based testing, Vulnerability scanning testing, Fuzzy testing, Model based security testing, Security testing, Formal security testing, Fault injection based security testing, White box based security testing and Risk based security testing and also a new security testing method is proposed that combines the advantages of both traditional “black box” (monolithic functional) testing and “white box” (functional synthesis-based) testing. For Explanation refer to Research Section.

RQ4: How different security requirements can be classified? The requirements for Security Testing can be categorised into security assurance and security functional. Security Functional Requirements can be classified in Figure 10:
7. Conclusion and future work

We have performed a comprehensive survey of security Testing Techniques and methods. From this we can conclude that target vulnerability analysis can help developer discover the vulnerabilities and fix more easily in an efficient way. Security Testing Techniques and methods. Moreover these techniques can be implemented in web vulnerability detection tools in order to confirm the respective vulnerability so that better scanner could be produced in future. We have made our efforts best to represent the subject in deep and in efficient way.

References:


Author’s Bibliography;

Divya Nigam (divyanigam90@gmail.com) is pursuing M.tech in Information Security from Ambedkar Institute of Advance Research and Communication, Guru Gobind Singh Indraprastha University, Delhi, India. She has completed her B.Tech in Information technology from Guru Prem Sukh Memorial college of Engineering, Guru Gobind Singh Indraprastha University, Delhi, India. Her research interests are software security testing.

Vinita Malik (Vinita.malik89@gmail.com) is an Assistant Professor in Maharaja Surajmal Institute Of Technology, Guru Gobind Singh Indraprastha University, Delhi, India. She received her Masters degree in Software Systems from BITS, Pilani, India. She received her B.Tech from D.C.R.U.S.T. She has published several papers in international journals and conferences.

Sarvagya Nigam (sarvagyanigam@gmail.com) is pursuing B.tech in Information Technology from Maharaja Surajmal Institute Of Technology, Guru Gobind Singh Indraprastha University, Delhi, India. His research Interests are many but one of them is security testing.