**Security Report**

[Document subtitle]

Luke Bruni

2018

Table of Contents

[1. Introduction 2](#_Toc507774109)

[1.1 Software Development 2](#_Toc507774110)

[1.1.1 Software Development Process 2](#_Toc507774111)

[1.2 Vulnerabilities 4](#_Toc507774112)

[1.2.1 Types of Vulnerabilities [4] 4](#_Toc507774113)

[2. Case Studies 6](#_Toc507774114)

[2.1 Yahoo 2013-2014 Data Breach 6](#_Toc507774115)

[2.2 NHS Cyber-Attack 6](#_Toc507774116)

[3. Mitigating Software Vulnerabilities 8](#_Toc507774117)

[4. Conclusion 9](#_Toc507774118)

# **1. Introduction**

## **Software Development**

Software development is the process of creating applications or software which is made using a specific programming language. This is an iterative process used to create these programs, to fulfil either a business or personal goal, process or objective. The process is usually made up of various steps within development to create the operational software in question.

The method of creating software is commonly referred to as a Software Development Life Cycle (SDLC) and the process is normally carried out through the software programmer, with initial research, data and process flow design, flow charts, technical documentation, testing and debugging. The process is commonly iterative, but there are other methodologies to adopt depending on the nature of the program [1].

### **Software Development Process**

All Software Development Life Cycle models have phases which are in the order that they are executed in. Each phase marks a point for the deliverables which are required by the next phase. Every Lifecycle model has these six development phases:

1. Requirement gathering and analysis
2. Design
3. Implementation or coding
4. Testing
5. Deployment
6. Maintenance [2]

#### Requirement Gathering and Analysis

This phase is where the requirements are collected and understood and is the main focus of the project managers and stake holders. Meetings are held in order to determine the requirements, with questions considered in relation to the software’s purpose, such as who is this system built for? Who will use the system? How will they use it? Etc. where then these requirements are analysed for the purpose of validation and use within development.

It is relatively important to gain these requirements because it sets the development of the project in stone. Each member of the team has a solid understanding of the product in their minds, so they can build of what they are given, supporting the next phases of development. To perfectly understand what the requirements are, it should be important to keep them clear and concise, that way a good understanding is used and the requirements can support the development [3].

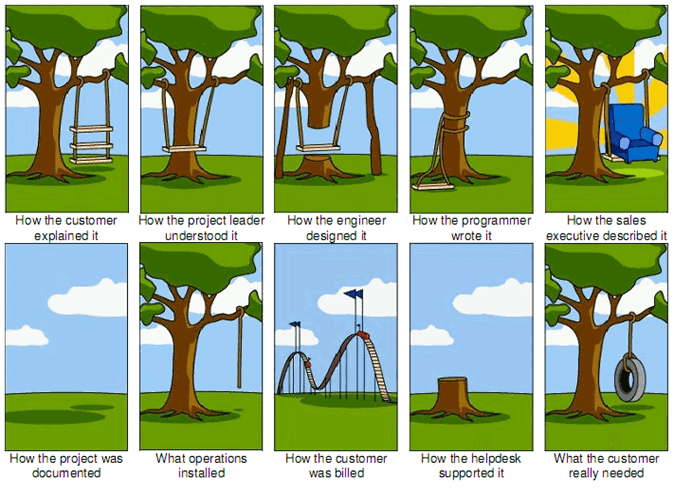


Figure 1: Tree Swing Project Management Comic [4]

The requirements to a project are heavily based on how they are perceived, as mentioned previously. Should the team not understand the requirements, then they won’t prove beneficial to the development and would more often result in the project being designed without the requirements in mind, confusion amidst each team member and ultimately leading to a product that the client didn’t ask for. The figure above showcases a simplified view of mishandled or misunderstood requirements.

#### Design

The system design is then prepared based on the requirements in the previous phase. The design helps in specifying the hardware and defining the overall system architecture, setting in place the next stage of development.

It is also worth noting that testers involved come up with a test strategy, detailing what to test and how to test it.

#### Implementation or Coding

When the design documents are completed, the work is then split up into units and modules and the actual coding starts. This phase is the main focus as it is where the features are implemented and the code is produced and it is also worth noting that this is the longest phase out of the entire development lifecycle.

#### Testing

After the code is developed, the initial product is tested against the requirements to make sure that the product meets the client’s needs and serves its purpose as stated within the first phase. All types of testing are carried out, such as unit testing, integration testing, system testing and acceptance testing as well as non-functional.

#### Deployment

This phase comes after successful testing, the product is then handed over to the product to see if said product fulfils the goals that were asked. As soon as it is deployed, the first beta testing will commence, where any changes requested are noted and bugs are discovered. The outcome of the beta testing will serve as a basis for the final release.

#### Maintenance

When the customer uses the system, problems will arise from time to time and would need to be solved. Care is taken for the developed system to ensure it still operates perfectly without any faults.

## **Vulnerabilities**

Regarding computing security, vulnerabilities are weaknesses within software, being a flaw within code or design that creates an opening for an attacker to breach security and either run code or access a system’s memory. Because these vulnerabilities are discovered, they are then exploited, allowing to be conducted through hacking scripts, applications or even free hand coding [5]. Once the attacker has breached access, they have the opportunity to gain access to information and can exploit the vulnerability to hide their actions [6].

### **Types of Vulnerabilities [7]**

This section describes each vulnerability that could occur in software.

#### Buffer Overflow

A buffer overflow is where an application attempts to write data past the end of a buffer. This can cause the program to crash, compromise data and provide an attack vector to compromise the system.

Applications that take input from the user, from a file or a network has to store that input. This storage is temporary, but there are two exceptions to where it can be stored, in either the stack or the heap. Buffer Overflow attacks occur by compromising either one storage or both.

#### 1.2.1.2 Unvalidated Input

This is unwanted input that can occur by having the attacker interfere and pass in abnormal data. Once the program crashes, then the attacker looks for exploits in the system and subsequently take control of the system, steal data, corrupt disk, etc.

Any form of input from an untrusted source is a more than likely target for an attack, such as:

* Text input fields
* Commands passed through a URL used to launch the program
* Files provided by users or other processes and read by the program
* Command line input
* Any data read from an untrusted server over a network
* Any untrusted data read from a trusted server over a network.

#### 1.2.1.3 Race Conditions

Race conditions are made when changes in events cause a behavioural change, to which the attacker can take advantage of the situation to either insert their code, change the name of a file or just interfere with the program’s operation. However, this may not always be the case, as if the correct order of execution is required for the operation of the program, then the change is a bug.

#### 1.2.1.4 Interprocess Communication

This is a mechanism that allows for data exchange between processes [8]. The methods involved include shared memory or a messaging protocol such as sockets. These messaging protocols are vulnerable as the end communication channel could be hostile, so programmers have to always assume that they are hostile.

#### 1.2.1.5 Insecure File Operations

An attacker can change the permissions of a file after creation, if not checked properly. This is the result creating insecure temporary files and can result in tampered files that the owner wouldn’t notice.

# **2. Case Studies**

## **2.1 Yahoo 2013-2014 Data Breach**

Recently, Yahoo had said that all 3 billion of its accounts were hacked in a data theft that had occurred in a disclosure during the company being sold to Verizon. It had been the biggest breach in history, tripling its earlier estimate [9].

An investigation was carried out in 2013 saying that 1 billion accounts were compromised, but went unnoticed. Yahoo did blame the breach on an “Unauthorized third party”, though most details weren’t provided until law enforcement had reported that the files were originally from yahoo but a third party had managed to obtain the files. The company had then verified that the stolen data was legitimate shortly after.

The data that was affected was mainly user data; names, emails, phone numbers, dates of birth and hashed passwords were obtained, mainly because they were protected with outdated encryption which was considered easy-to-crack and security questions along with backup email addresses, to which it was easy to break into the other accounts that were held by the users. However, the investigation had specified that the stolen information did not include payment card data or bank account information [10].

Another investigation was carried out, reporting another massive breach which affected 500 million in 2014 but botched its response. The security team at Yahoo had knew about what Yahoo report as a ‘state-sponsored hacker’ had stolen backup copies of backup files, containing personal details on users. The reason it was finally brought to light, two years after the breach, was because of a stolen database purportedly went up sale on the black market [9].

It wasn’t until much recently that additional information had been obtained by Yahoo, where it showed that all user accounts had been affected, the 3 billion figure including accounts that were opened but never or briefly used. In response, Yahoo emailed notifications to additional users that were affected.

The following breaches had affected a deal with Verizon where following the newer information about the first breach, lowering it by $350 million from Verizon’s original offer to buy the company and brought about 43 class action lawsuits against Yahoo. The original deal had closed in July 2017.

## **2.2 NHS Cyber-Attack**

NHS trusts were hit by a huge ransomware attack in May 2017, where more than a third of the trusts throughout England and Scotland were disrupted by the ransomware. As a result of this, at least 6,900 NHS appointments were cancelled but no data relating to patients was compromised. There was no evidence that any NHS organisation paid the ransom but the cost of the incident remained unknown [11].

The Ransomware in question was called ‘WannaCry’. A file encryption software, that encrypts the PCs files, that prevents user access to the PC and demands a payment to be made, in bitcoin, to decrypt them, usually demanding $300 in bitcoin. The Vulnerability that WannaCry exploits is in the Windows implementation of the Server Message Block (SMB) Protocol, which helps nodes on a network communicate [12].

The issue was that out of 236 trusts, 88 had failed the required cyber-security standards and a lack of action on critical alerts from NHS digital. Computers at the NHS were running the old Windows XP operating system, which were vulnerable due to the stopped support on 8 April 2014 [14]. A patch had been brought out but it was also discovered that also the Windows 7 OS was vulnerable, but that operating system was still supported. A plan was developed to help counteract such attacks, it wasn’t seen through properly, with poor management, lack of testing and the fact that it was not communicated properly.

# **Mitigating Software Vulnerabilities**

It is always beneficial to tackle Software Vulnerabilities, as often, the vulnerabilities mentioned earlier can have an adverse impact on the security of the app or system. An attacker can exploit the system in many ways, which in turn leads to different purposes, such as data stealing or to damage a mainframe.

Modelling out the vulnerabilities is a good first approach to gain an understanding of what vulnerabilities can come out of development. By using the model as reference, it helps towards more careful development and can give the developer an idea on how to counteract said vulnerabilities. However, it would be considered necessary to count on methods to prevent the risks related to vulnerabilities.

Software Inspection is a method of vulnerability mitigation, in which its process is to read or visually inspect the program code or documents in order to find any defects and correct them early in the development process. This can help with the development as if they are found later, it becomes costlier to fix. Good inspection depends on the ability and expertise of the inspect, along with the defects in what he’s looking for [16].

Well embedded and upheld user access controls will restrict the applications, privileges and data that users can access, making for tighter controls to prevent sudden unauthorised access. Secure configuration can remove unnecessary software and default user accounts, making sure that passwords are changed and automatic features that could activate any malware to be turned off.

Monitoring software activity and analysing it to identify malicious or unusual activity, is a good call to help recognise a breach [17].

# **Conclusion**

This conclusion ties with the case studies of both the Yahoo data breach and the NHS ransomware attack, it is revealed that the sole reason behind the attacks were down to the negligence of both organisations, where the difference lies in how the attack was brought on or handled. But in both cases on the matter to the cause of attacks, it is revealed that the attacks were caused because of outdated software, leaving an exploit open towards the attacker; where the case of Yahoo was because of outdated and easy-to-crack security tools that allowed the attacker to easily access Yahoo’ database, along with personal names, emails and hashed passwords, spanning over a devastating three billion users, and regarding the NHS case, an old unsupported operating system, Windows XP, was used as the main OS for all computers within the trust centre, lacking security controls currently implemented in more modern operating systems, having the attacker to exploit old tools and poorly embedded and maintained user controls to take control and access the files to encrypt.

Now, onto how each case was handled, both were handled poorly; the attack caused disruptions to the NHS centres and in turn had caused cancellation of appointments, leading to outrage amongst patients. Yahoo’s was more controversial, with them only issuing a disclosure of the breach three years later from the actual attack, the main issue being that the security team had the knowledge that the foundation was breached by a hacker, but failed to even try to enforce any prevention method. The NHS attack had sorted out in the end, despite the ongoing disruption to their workstations and systems, but the Yahoo breach had left all the accounts at risk and action taken was late. This dealing a massive blow to Yahoo.

Both were down to negligence and in my opinion on both matters, it seems that the issues were down to the lack of mitigation techniques. In the case of yahoo, the factors here where the outdated security tools, lack of analysis and lack of action, as it was clear that they knew the attack had been carried out, but only brought the breach to light at a later date. Had there been monitoring of user activity, finding any unusual activity would have meant that there was a breach and in turn would lead to quicker response. Updated tools would have also meant that the possibility of an exploit becoming apparent would be very unlikely.

In the case of the NHS, it would’ve been simple to impose the newest, modern operating system, containing tools that aren’t present in older operating systems. Forcing cyber security standards within every trust would also have proven beneficial as that can impose tighter security and better embedded access controls.

References

1. Software Development. [online]. Techopedia. Available from: <https://www.techopedia.com/definition/16431/software-development>. [Accessed 19 February 2018].
2. Elysium Academy Private Limited (2017). What are the Software Development Life Cycle (SDLC) phases? [online]. LinkedIn. Available from: <https://www.linkedin.com/pulse/what-software-development-life-cycle-sdlc-phases-private-limited>. [Accessed 2 March 2018].
3. Duncan Haughey (2014). REQUIREMENTS GATHERING 101. [online]. Project Smart. Available from: <https://www.projectsmart.co.uk/requirements-gathering.php>. [Accessed 02 March 2018].
4. Tree Swing Project Management [online]. (n.d). Available from: <https://www.tamingdata.com/2010/07/08/the-project-management-tree-swing-cartoon-past-and-present/>. [Accessed 02 March 2018].
5. Margaret Rouse, Matthew Haughn (2014). vulnerability. [online]. WhatIs.com. Available from: <http://whatis.techtarget.com/definition/vulnerability>. [Accessed 19 February 2018].
6. SecureList [online]. (n.d). Available from: <https://securelist.com/threats/software-vulnerabilities/>. [Accessed 19 February 2018].
7. Apple Developer [online]. (2016). Available from: <https://developer.apple.com/library/content/documentation/Security/Conceptual/SecureCodingGuide/Articles/TypesSecVuln.html>. [Accessed 19 February 2018].
8. Inter Process Communication (IPC). [online]. Techopedia. Available from: <https://www.techopedia.com/definition/3818/inter-process-communication-ipc>. [Accessed 19 February 2018].
9. OWASP (2016). Insecure Temporary File [online]. Available from: <https://www.owasp.org/index.php/Insecure\_Temporary\_File>. [Accessed 19 February 2018].
10. Jonathan Stempel, Jim Finkle (2017). Yahoo says all three billion accounts hacked in 2013 data theft. [online]. Reuters. Available from: <https://www.reuters.com/article/us-yahoo-cyber/yahoo-says-all-three-billion-accounts-hacked-in-2013-data-theft-idUSKCN1C82O1>. [Accessed 20 February 2018].
11. Vindu Goel, Nichole Perlroth (2016). Yahoo Says 1 Billion User Accounts Were Hacked. [online]. The New York Times. Available from: <https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html>. [Accessed 26 February 2018].
12. Michael Kan (2017). Yahoo execs botched its response to 2014 breach, investigation finds. [online]. CSO. Available from: <https://www.csoonline.com/article/3176181/security/yahoo-execs-botched-its-response-to-2014-breach-investigation-finds.html>. [Accessed 26 February 2018].
13. NHS 'could have prevented' WannaCry ransomware attack (2017). [online]. BBC News. Available from: <http://www.bbc.co.uk/news/technology-41753022>. [Accessed 1 March 2018].
14. Josh Fruhlinger (2017). What is WannaCry ransomware, how does it infect, and who was responsible? [online]. CSO. Available from: <https://www.csoonline.com/article/3227906/ransomware/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html>. [Accessed 1 March 2018].
15. Support for Windows XP ended [online]. (2014). Available from: <https://www.microsoft.com/en-gb/windowsforbusiness/end-of-xp-support>. [Accessed 1 March 2018].
16. Willy Jimenez , Amel Mammar and Ana Cavalli (2014). Software Vulnerabilities, Prevention and Detection Methods: A Review. Evry, France: ResearchGate. Available from: <https://www.researchgate.net/publication/253704494\_Software\_Vulnerabilities\_Prevention\_and\_Detection\_Methods\_A\_Review\_1>. [Accessed 03 March 2018].
17. Common cyber attacks: reducing the impact. (2016). National Cyber Security Centre. Available from: <https://www.ncsc.gov.uk/content/files/protected\_files/guidance\_files/common\_cyber\_attacks\_ncsc.pdf>. [Accessed 03 March 2018].