International Baccalaureate®
Baccalauréat International
Bachillerato Internacional

COMPUTER SCIENCE
CASE STUDY: NETWORK SECURITY

For use in May 2014 and November 2014

INSTRUCTIONS TO CANDIDATES

- Case study booklet required for higher level paper 3.

Introduction

Information technology has changed both the way individuals lead their lives and how companies manage their business. The use of networking has not only revolutionized businesses internally, but has given them global access to both resources and customers through the internet.

These benefits to businesses come at a price; the networks can equally be used by individuals and organizations to target company websites with a complex arsenal of malware designed to threaten their day-to-day operations.

The threat landscape has changed dramatically over the last few years. Previously malware was principally the province of the computer-savvy *script kiddies* attempting to wreak as much havoc as possible and in doing so create a name for themselves in the hacking world. Viruses disrupted IT systems, overloaded servers and deleted data, but the damage tended to be temporary and the costs incurred were mainly due to loss of operational time. However, the threats have increasingly become driven by financial gain and are now being run by criminal organizations with the consequence that companies are paying heavily both in direct losses and in costs incurred in trying to protect their networks and the data stored on them. The landscape has become further complicated by the involvement of state organizations in orchestrating attacks for political or ideological reasons.

Reliable figures showing the losses due to cybercrime are notoriously difficult to come by as companies are often reluctant to provide such data or even admit that they have been attacked. However Norton, in its 2012 cybercrime report, has estimated the global cost of consumer cybercrime to be US $110 billion annually[1].

In spite of the vast amount of resources spent in combating cybercrime, the majority of the threats continue to increase, as shown by statistics taken from the Symantec Internet Security Threat Report for 2011[2].

Threat	**2010**	**2011**
Bot Zombies	3 065 030	4 500 000
Unique variants of malware	286 million	403 million
Estimated global spam per day	62 billion	42 billion
Malicious web domains	42 926	55 294
New mobile vulnerabilities	163	315
Zero-day attacks	14 new vulnerabilities	8 new vulnerabilities

The increase in cybercrime has been paralleled with an increase in the services of network security personnel, either employed directly by the businesses themselves or hired from consulting agencies. This case study looks at the work of Susan Woo, who works for the fictitious security consultants *XXXSecurity*.

---

1 http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report _Master_FINAL_050912.pdf

2 http://www.symantec.com/threatreport/topic.jsp?id=threatreport&aid=2011_in_numbers

XXXSecurity

In a recent interview Susan outlined some of the trends being witnessed in both malware creation and detection and the work in which she is currently engaged.

Trends in malware creation

Susan talked of how malware often enters a system through browser-based attacks, but in contrast to the instant chaos of previous years would often now lie hidden whilst silently gathering the organization's data. She explained:

"Professional criminal organizations try to make use of *bots*, which is code that can replicate itself similar to the way that *worms* function. But the additional facility they have is that they can be controlled from some central location anywhere in the world, ready to accept commands and be activated at any time. There is a thriving underground industry in the production of custom-based malware using *toolkits* which can be bought and put together in order to achieve specific aims. The *Zeus Botnet*[3] is a particularly good example of this.

"The success of attacks such as *Stuxnet*, *Duqu* and *Flame* has led to the term *Advanced Persistent Threats* (APTs) which defines more a style of attack than one particular method. These attacks use an array of weapons, including social engineering, to specifically target certain organizations."

She also highlighted the dangers of *zero-day* attacks in which cyber-criminals use previously unknown vulnerabilities to breach security controls.

Methods of detection

The traditional antivirus packages which are *signature-based* and the use of *packet-filtering* firewalls still play a major role in protecting systems, but as the malware increases in sophistication, so do the tools. Susan continued by discussing the changes in detection techniques.

"Detection and prevention are moving from being solely signature-based to *anomaly-based* in which network traffic is compared to what is considered to be "normal". *Whitelisting* takes the opposite point of view from the way traditional anti-malware works by producing a local fingerprint of acceptable applications.

"A large proportion of internet traffic now uses protocols such as HTTP, HTTPS, IM and P2P, and while traditional firewalls are good at filtering, they are not particularly good at inspecting the contents of this type of traffic. *Next Generation Firewalls* (NGFW), however, have this facility, and can perform inspections on packets that go further than only looking at port and protocol values."

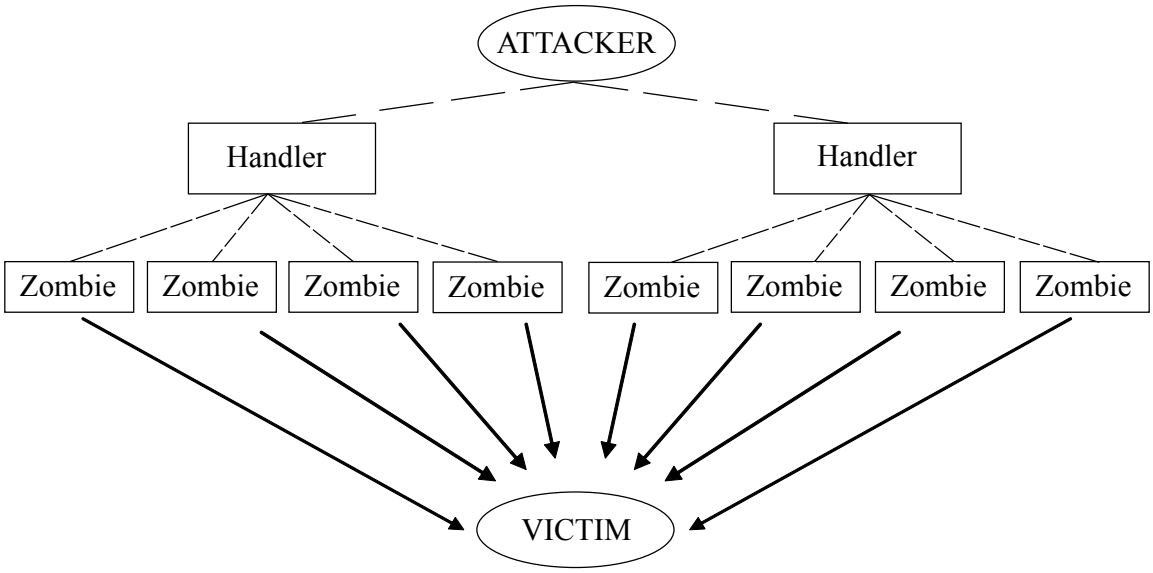
When asked about the safety brought about by encryption in the transferring of data, she urged caution, explaining that even the use of *SSL/TLS* protocols can be undermined by *man-in-the-middle* attacks.

[3] http://www.fortiguard.com/analysis/zeusanalysis.html

One of Susan's main areas of study is *Denial of Service* (DoS) attacks. These work in a variety of ways but their common goal is to overload a specific site to the point at which it can no longer function as normal. The perpetrators often form Botnets which are created from computers infected by malware which then become *zombies*. They then launch a concerted attack on a particular site, *eg* the attack on Amazon in 2008[4]. Although the use of Botnets usually has a criminal intent, there have however been occasions when popular opinion has led to organized attacks on particular websites, such as the mass attack perpetrated on the country of Estonia in 2007[5].

The basic configuration of a *Distributed Denial of Service* (DDoS) attack is shown by the diagram below.

Architecture of a DDoS Attack



XXXSecurity is currently producing a series of pages on its website dedicated to the various forms of malware. The information will not go down to the level of code, but will describe in detail how each piece of malware works together with methods of prevention.

Susan has been assigned DoS attacks as her subject and will be focusing on the following three forms of attacks, together with possible countermeasures, using actual examples as an illustration:

- *Stack-based Buffer Overflow*
- *SYN Flood*
- *Smurf Attacks*

---

4 Information Week Security: http://www.informationweek.com/security/management/amazoncom-ddos-attacker-busted-in-cyprus/240004073

5 International Affairs Review: http://www.iar-gwu.org/node/65

Susan is also currently advising two highly contrasting organizations: one is *Western Heights*, a large multinational pharmaceutical company, and the other is Guanjong HS, a city high school. The type and level of threats and the desired security measures are, not surprisingly, quite different:

"Although some security elements may be common to both, *eg* the use of proxy servers, installed security software *etc*, the location of the threats is quite different between the two organizations, and this dictates the level of security required. Whilst the main threats to the pharmaceutical company come from outside, the principal threat posed to the school comes from within – from the practices of its own students. Although the school will hold data it considers private, the surfing activities of the student body and their possible consequences will affect the choice of security measures.

"On the other hand, the actions of APTs will focus prominently in the minds of the security personnel at the pharmaceutical company. The installation and the maintenance of appropriate *IDS/IPS* systems for the inspection of traffic both entering and leaving the network, which feed into a *Security Information and Event Management* (*SIEM*) system, will be a priority for them."

When asked about the future and the sectors in which malware will increasingly pose problems, Susan focused on the increasing use of mobile devices and the phenomenal rise of social networking:

"Cyber-criminals will always go for the weakest links, and they see the proliferation of mobile devices with their inherent security weaknesses and the move by many companies towards a *Bring Your Own Device* (*BYOD*) policy as a golden opportunity. The continual threat of zero-day attacks, APTs and the inherent fallibility of personnel mean that organizations can no longer rely on just securing the perimeter.

"Social networking is also seen as a prime target thanks to its ability to move large amounts of data around and its extensive use in the workplace."

Challenges Faced

Susan's challenges for the immediate future are:

- to prepare the section on the company's website for Denial of Service (DoS) attacks;
- to discuss with the network administrator of Guanjong High School the appropriate network security set-up for their school;
- to advise Western Heights of measures they should take against the threat of APTs;
- to prepare a report for the board of *XXXSecurity* on the growing security threats posed by the move towards BYOD.

Additional Terminology to the Guide

APTs
Bots
Botnets
BYOD
DoS / DDoS attacks
Firewalls
IDS
IM
IPS
Malware
Man-in-the-middle
Packet-filtering
Proxy server
Script kiddies
SIEM
Smurf attacks
Spam
SSL
Stack-based buffer overflow
SYN flood
Threat landscape
Toolkits
TLS
Vulnerability
Whitelisting
Worm
Zero-day attack/vulnerability
Zombies/zombie computers

Companies, products, or individuals named in this case study are fictitious and any similarities with actual entities are purely coincidental.