Using Blockchain to Create a Decentralised Security Model for Distributed Systems

Adam David Bruce
a.bruce3@newcastle.ac.uk

April 2021

Abstract

//TODO

Contents

1 Introduction **4**
1.1 COVID-19 and Cyberattacks 4
1.2 Distributed Systems 5
1.3 Decentralised Systems 5
1.4 Blockchain 6

2 Project Aims and Objectives **7**
2.1 Aim 7
2.2 Objectives 7

3 Background **8**

Glossary **9**

Acronyms **10**

List of Figures

1.1 A Distributed System visualised as middleware [1] 5
1.2 An example of a blockchain [2] 6

List of Tables

Chapter 1

Introduction

1.1 COVID-19 and Cyberattacks

In the summer of 2020 during the midst of the COVID-19 pandemic, universities and research institutions worldwide were working hard to understand the structure of the virus and develop a vaccine in an attempt to return to normality. However, whereas some countries were making fast progress in understanding the virus, others were falling behind, and the virus began to put a strain on healthcare, and increasing critique on governments. In order to keep up with the nations at the forefront of vaccine development, nations turned to state-sponsored cyberattacks in order to both hinder nations, and also obtain research and information about other countries' vaccine efforts. One such example was the threat group 'Cozy Bear', formally known as Advanced Persistent Threat (APT) 29. APT29 used a number of tools to target various organisations involved in COVID-19 vaccine development in Canada, the United States and the United Kingdom. The National Cyber Security Center (NCSC) believe that the intention was highly likely stealing information and intellectual property relating to the vaccine [3].

In addition to the mortality of COVID-19, the virus also caused a number of economic issues across a number of nations. Global stock markets lost $6 trillion in value over size days from 23 to 28 February [4]. This gave private companies no other choice than to make large volumes of staff redundant, which increased job insecurity causing many people to become redundant, and in nations without suitable support or benefits, attackers turned to cybercrime for financial gain. These attacks represented the majority of cyberattacks aimed at both universities and the general public. A study of cyber-crime throughout the COVID-19 pandemic determined that 34% of attacks directly involved financial fraud with a number of attack surfaces used, the majority being phishing, smishing and malware [5].

University attacks became a frequent headline in the UK as universities suffered attacks from different threat actors. A number of threat actors launched attacks against multiple universities in the hope to find a vulnerability in at least one. One such attack was aimed at both Newcastle University and Northumbria University, two universities in extremely close proximity [6, 7]. The attack crippled both Newcastle and Northumbria Universities, however the attackers only managed to exfiltrate data from Newcastle University. Why was the attack successful on both occasions? Why wasn't knowledge of the attack shared?

One reason is that currently, there is no reliable or automated system in place to share this information. Such a system is what this paper will aim to create.

1.2 Distributed Systems

A distributed system is defined by Tanenbaum and van Steen as a "collection of independent computers that appears to its users as a single coherent system" [1]. Such systems are commonplace in peer-to-peer computing and sensor networks where each systems contributes some data via transactions to the system. A distributed system therefore should be autonomous and to the user, should appear as though they are interacting with a single system. Furthermore users and applications should be able to interact with the distributed system in a consistent and uniform way, regardless of where and when system interaction takes place. This requires a common interface provided by a stub which is used to bridge the gap between a programming language or protocol and the distributed system. This stub hides the differences in machine architecture and communication between the computer and the distributed system. The use of stubs creates a new software layer, known as middleware which runs on an Operating System (OS) and exposes distributed functions to higher-level applications and users.

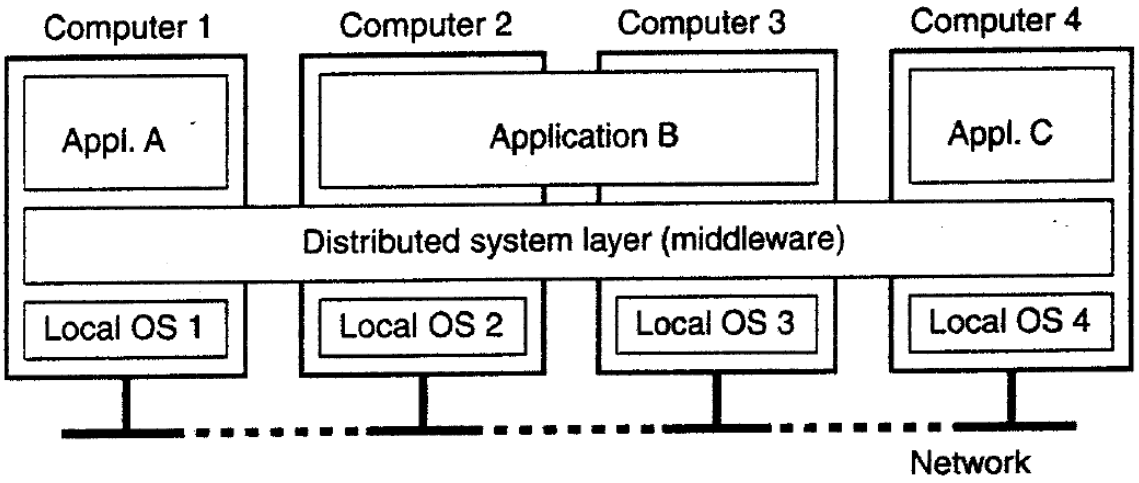

Figure 1.1: A Distributed System visualised as middleware [1]

1.3 Decentralised Systems

Reed defines a decentralised computer system as a computer system that "involves separation of the computers in the system by physical distance, by boundaries of administrative responsibility for individual computers and their applications, and by firewalls" [8]. Reed suggests that for a computer system to be decentralised, it must be separated by both physical distance and administrative responsibility, such that no single body administrates the system. One of the most well-known examples of decentralisation is cryptocurrency, a currency which takes no physical form, but instead exists entirely digitally. If cryptocurrency were to be governed by a central body, nefarious transactions could be used to launder money. Using a decentralised system ensures the transaction can only take place if all nodes within the system are in consensus that the transaction is genuine.

1.4 Blockchain

Nofer et al. define blockchains as "data sets which are composed of a chain of data packages (blocks) where a block comprises multiple transactions. The blockchain is extended by each additional block and hence represents a complete ledger of the transaction history." [2]. Nofer et al. describe the basic fundamentals of a blockchain, which is that numerous blocks of transactions contribute to a larger chain. This chain is never controlled by a single body, instead a copy of the chain is stored at each node within a system, making blockchain a popular candidate for controlling transactions over a decentralised computer system. Hence, blockchain is the foundation for the vast majority of cryptocurrencies including Bitcoin[9] and Ethereum[10]. One of the key aspects of blockchain is the use of cryptographic hashing algorithms, these algorithms represent a block as a fixed-length string. For a block to be added to the chain, it must contain the hash of the previous block.

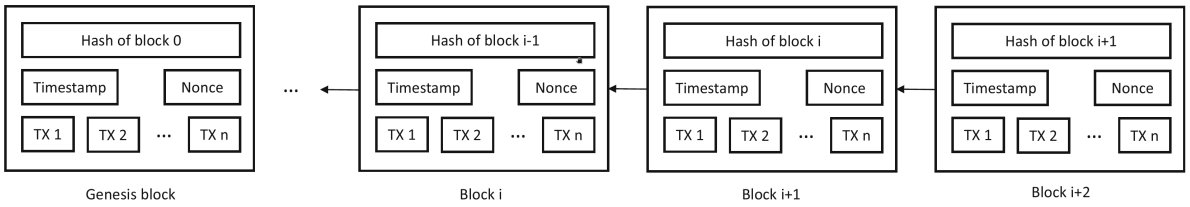

Figure 1.2: An example of a blockchain [2]

Chapter 2

Project Aims and Objectives

2.1 Aim

The original aim for this project was to design and create a decentralised firewall that could communicate knowledge of cyberattacks aimed at universities in real-time, allowing other universities to protect themselves from the same attacks. This system would be distributed, and hence must conform to the previous description of a distributed system in section 1.2. Following an extensive amount of background reading, there appeared to be no existing implementation or design of such a system which inspired me to alter my aim and instead focus entirely on designing a protocol and implementing a stub to demonstrate the protocol's effectiveness. This project will therefore not be implementing a firewall, but instead a system to coordinate firewalls. Further research determined that blockchain was the best choice for the underlying structure for such a protocol, and so this final change shaped the current aim for this project: **Using Blockchain to Create a Decentralised Security Model for Distributed Systems**.

2.2 Objectives

The following objectives provide an outline for what this project hopes to achieve:

1. Evaluate the effectiveness of existing distributed security mechanisms.
2. Investigate methods of establishing connections and synchronising computers within distributed systems.
3. Understand the structure of blockchains and adapt them for firewall transactions.
4. Implement and rest relevant resilience, fault tolerance and security mechanisms.
5. Compare the use of decentralised security mechanisms.

Chapter 3

Background

Glossary

blockchain A growing list of records, called blocks, that are linked using cryptography. 2, 6, 7

cryptocurrency A digital currency produces by a public network. 5

hashing The practise of taking data and representing that data as a fixed-length string. 6

ledger A record of all transactions executed on a particular cryptocurrency. 6

malware Malicious computer software that interferes with normal computer function or sends personal data about the user to unauthorised parties. 4

middleware Software that functions at an intermediate layer between applications and the operating system to provide distributed functions. 2, 5

phishing Sending an email that falsely claims to be from a legitimate organisation, usually combined with a threat or request for information. 4

smishing Sending a text message via SMS that falsely claims to be from a legitimate organisation, usually containing a link to a malicious website. 4

stub A piece of code that is used to marshal parameters for transmission across the network. 5, 7

Acronyms

APT Advanced Persistent Threat. 4

NCSC National Cyber Security Center. 4

OS Operating System. 5

Bibliography

[1] A. S. Tanenbaum and M. van Steen, *Distributed Systems: Principles and Paradigms*. Pearson Prentice Hall, 2007.

[2] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain," *Business & Information Systems Engineering*, vol. 59, pp. 183–187, 2017.

[3] NCSC and CSE, "Advisory: APT29 targets COVID-19 vaccine development." `https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development-V1-1.pdf`, 2020.

[4] P. Ozili and T. Arun, "Spillover of COVID-19: Impact on the global economy." `https://mpra.ub.uni-muenchen.de/99850/1/MPRA_paper_99850.pdf`, 2020.

[5] H. S. Lallie, L. A. Shepherd, J. R. C. Nurse, A. Erola, G. Epiphaniou, C. Maple, and X. Bellekens, "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic." `https://arxiv.org/pdf/2006.11929.pdf`, 2020.

[6] BBC, "Newcastle university cyber attack 'to take weeks to fix'." `https://www.bbc.co.uk/news/uk-england-tyne-54047179`, 2020. Accessed: 01/04/2020.

[7] BBC, "Northumbria university hit by cyber attack." `https://www.bbc.co.uk/news/uk-england-tyne-53989404`, 2020. Accessed: 01/04/2020.

[8] D. P. Reed, "Naming and synchronisation in a decentralized computer system." `https://dspace.mit.edu/bitstream/handle/1721.1/16279/05331643-MIT.pdf`, 1978.

[9] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system." `https://bitcoin.org/bitcoin.pdf`, 2008.

[10] V. Buterin, "A next generation smart contract & decentralized application platform." `https://whitepaper.io/coin/ethereum`, 2013.