Yeshwantrao Chavan College Of Engineering

NETWORK SECURITY

Arnab Chakraborty
Engineering | 2025

OVERVIEW

- Introduction
- Problem
- Literary Review
- Objectives
- Methodology
- Implementation
- Result
- Conclusion
- Thank You

INTRODUCTION

As the Internet of Things (IoT) continues to grow, ARM-based devices have become integral components of the connected ecosystem, serving diverse applications ranging from smart homes to industrial automation. However, this proliferation of ARM devices has also exposed a widening attack surface, making network security a paramount concern.

PROBLEM

YCCE

Problem 1

Hackers have the power to launch assaults and enter thousands or millions of unprotected connected devices, destroying infrastructure, taking down networks, or accessing confidential data

Problem 2

Cybercriminals can compromise a large number of IoT devices and create botnets. These botnets can be used to launch distributed denial of service (DDoS) attacks, overwhelm online services, and disrupt the internet.

PROBLEM

Problem 3

Smart Home devices like assistants, cameras, appliances, etc. often collect sensitive data, such as audio and video feeds, and user preferences. Unauthorized access to this data can lead to privacy breaches.

Problem 4

Some IoT devices, like connected cars or medical devices, have physical safety implications. If these devices are compromised, they can endanger lives and property.

LITERARY REVIEW

01 Literary Review

Evaluating the Vulnerability of Network Traffic Using Joint Security and Routing Analysis - Patrick Tague, David Slater, Jason Rogers, Radha Poovendra

02 Literary Review

DNS Amplification and DNS Tunneling Attacks Simulation, Detection and Mitigation Approaches - Sanjay, Balaji Rajendra, Pushparaj Shetty D

Year: 2020 | Conference Paper | Publisher: IEEE

03 Literary Review

Autonomous NAT Traversal - A. Muller, N. Evans, C. Grothoff, S. Kamkar

Year: 2010 | Conference Paper | Publisher: IEEE

04 Literary Review

IEE Colloquium on 'RISC Architectures and Applications' (Digest No.163)

Year: 1991 | Conference Paper | Publisher: IET

LITERARY REVIEW

05 Literary Review

Internet of Things Security – Multilayered Method For End to End Data Communications – Craig Lee, Andrea Fumagalli

Year: 2019 | Conference Paper | Publisher: IEEE

06 Literary Review

Experimental performance comparison between TCP vs UDP tunnel using OpenVPN – Irfaan Coonjah, Pierre Clarel Catherine, K.M.S Soyjaudah

Year: 2015 | Conference Paper | Publisher: IEEE

OBJECTIVES

Objective 01

To understand the scope, scale, implications and consequences of network based attacks especially on IoT devices based on the ARM architecture family of computers .

Objective 02

To research and develop solutions to help overcome these security vulnerabilities using pre-existing tools and solutions in a user friendly manner.

METHODOLOGY

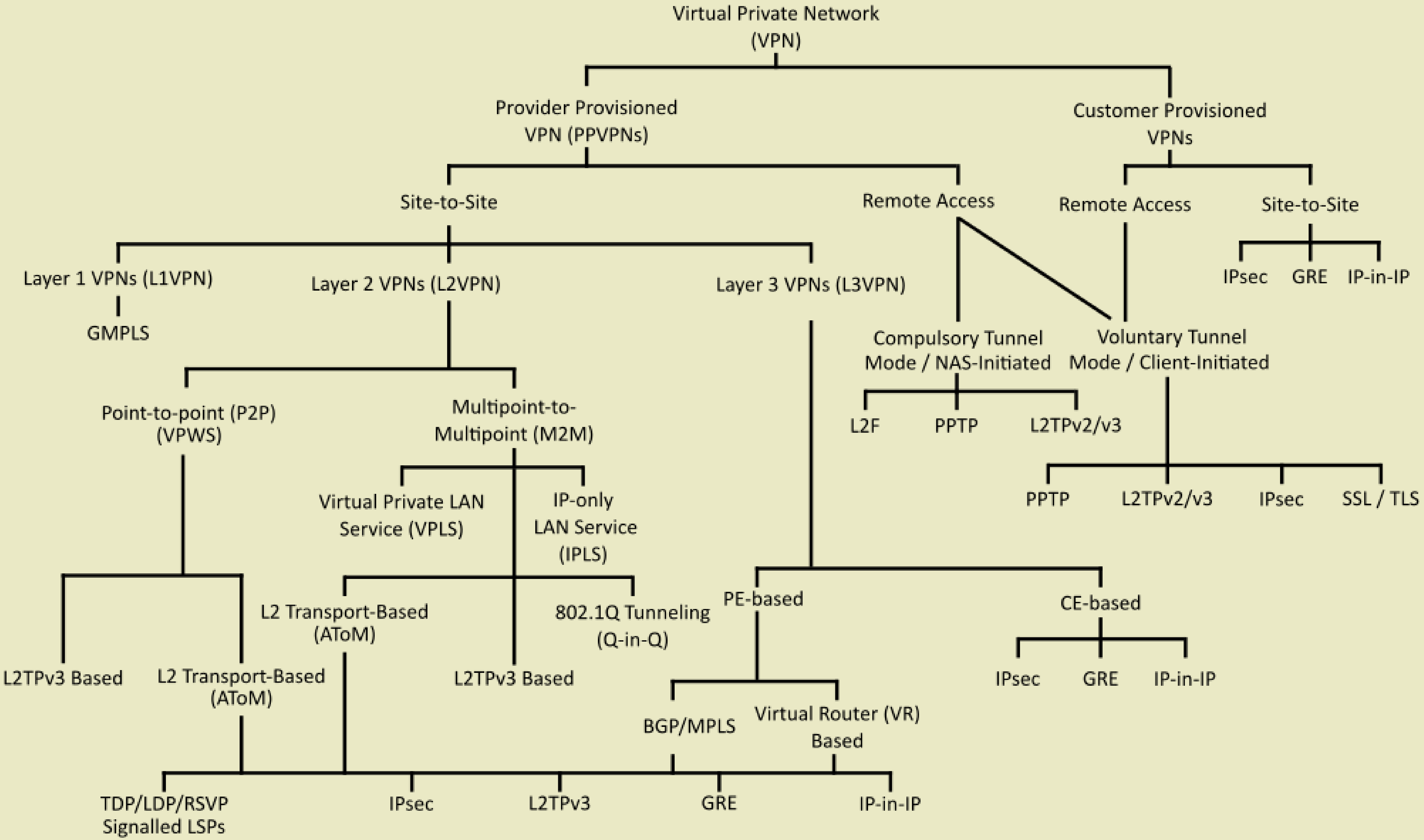
Methodology 01

DNS sinkhole or black hole DNS is used to spoof DNS servers to prevent resolving hostnames of specified URLs. This can be achieved by configuring the DNS forwarder to return a false IP address to a specific URL. DNS sinkholing can be used to prevent access to malicious URLs at an enterprise level. The malicious URLs can be blocked by adding a false entry in the DNS and thus there will be a second level of protection. Normally firewalls and proxies are used to block malicious traffic across the organization.

METHODOLOGY

Methodology 02

A virtual private network (VPN) is a mechanism for creating a secure connection between a computing device and a computer network, or between two networks, using an insecure communication medium such as the public internet. A VPN can extend access to a private network to users who do not have direct access to it. A VPN is established by creating a virtual point to point connection through the use of tunneling protocols over existing networks.



Virtual Private Network (VPN)

Provider Provisioned VPN (PPVPNs)

Customer Provisioned VPNs

Site-to-Site

Remote Access

Remote Access

Site-to-Site

Layer 1 VPNs (L1VPN)

Layer 2 VPNs (L2VPN)

Layer 3 VPNs (L3VPN)

IPsec

GRE

IP-in-IP

GMPLS

Compulsory Tunnel Mode / NAS-Initiated

Voluntary Tunnel Mode / Client-Initiated

Point-to-point (P2P) (VPWS)

Multipoint-to-Multipoint (M2M)

L2F

PPTP

L2TPv2/v3

PPTP

L2TPv2/v3

IPsec

SSL / TLS

Virtual Private LAN Service (VPLS)

IP-only LAN Service (IPLS)

L2 Transport-Based (AToM)

802.1Q Tunneling (Q-in-Q)

PE-based

CE-based

L2TPv3 Based

L2 Transport-Based (AToM)

L2TPv3 Based

IPsec

GRE

IP-in-IP

BGP/MPLS

Virtual Router (VR) Based

TDP/LDP/RSVP Signalled LSPs

IPsec

L2TPv3

GRE

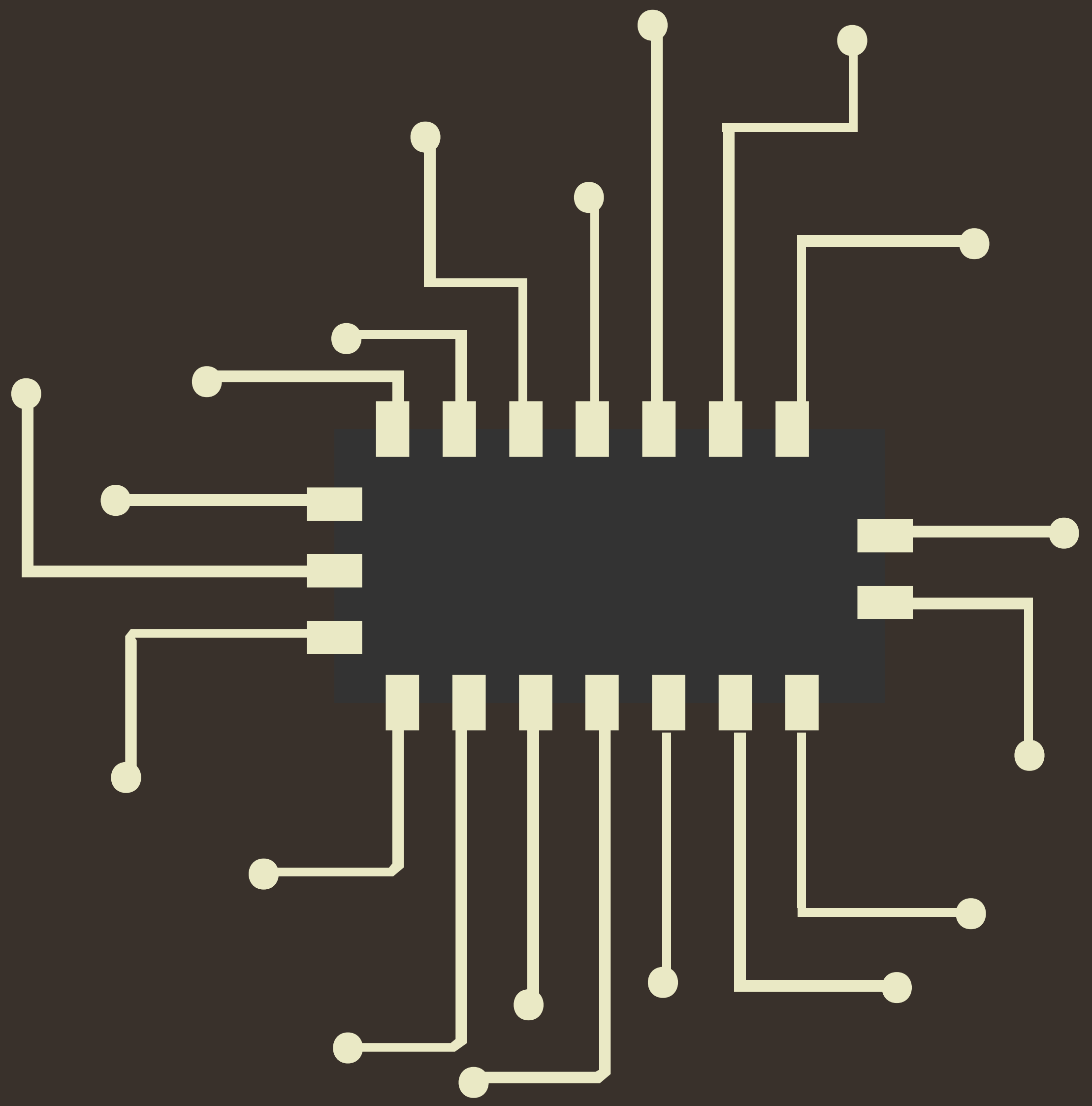
IP-in-IP

IMPLEMENTATION

User friendly sinkholes like Pi-Hole that can run off of a cheap Raspberry Pi 0 running the ARMhf architecture can be used to block access to malicious websites and IPs. Tools used to evaluate this hyopthesis were a laptop computer running a barebones Linux Distro based on Arch Linux and CLi tools such as nmap, iftop, dnsmasq and tcpdump among many others as well as a single board computer Raspberry Pi 0-2 running a Debian based Raspberry Pi OS. Connections from the computer to the internet were routed through the SBC which was configured to block malicious IP addresses and websites. The SBC also acted as a VPN that would mask the orignal IP address of the computer. Other implementations were also put into place like force usage of TCP(Transfer Control Protocol) instead of UDP(User Datagram Protocol) and force disabling of javascript while using some suspicious websites. Testing was done of private and public networks

RESULT

Intesive testing and trial and error of network security implementations with different software working individually or in tandem shows positive results which means that the defense put into place was successful at resisting network attacks up to a certain extent.



CONCLUSION

In conclusion, partial success during the testing phase shows that with a substantial increase in resources and budget, a layer of security could potentially be developed, implemented and integrated into modern IoT and ARM devices that may prevent breach of privacy, leaks of confidential information and even the loss of life.

LITERARY REVIEW

01 References

a)Mirai Malware:
https://en.wikipedia.org/wiki/Mirai_(malware)
Source Code:
https://github.com/jgamblin/Mirai-Source-Code

b)DNS Sinkhole:
https://en.wikipedia.org/wiki/DNS_sinkhole

02 References

c) Virtual Private Network:
https://en.wikipedia.org/wiki/Virtual_private_network

d)Pi-Hole:
https://docs.pi-hole.net/

e)Poisontap:
https://github.com/samyk/poisontap

LITERARY REVIEW

03 References

f)RISC Machines: https://en.wikipedia.org/wiki/ARM_architecture_family

YCCE

THANK YOU

Arnab Chakraborty
Engineering | 2025