

BI-DIRECTIONAL COMMUNICATION IN A HEAVILY PROTECTED ENVIRONMENT

ROELOF TEMMINGH & HAROON MEER

SCHEDULE

Introduction

Why Trojans?

Brief History of Trojans & Covert Channels

The Hybrid model

Demonstration

Taking it further

Possible fixes



BlackHat

USA • EUROPE • ASIA

digital self defense



INTRODUCTION

SensePost
The speakers

Objective of presentation

Uses for bi-directional communication

WHY TROJANS?

Profile of Trojan users

Real criminals...

...don't write buffer overflows

The weirdness of the industry

Examples

BRIEF HISTORY OF TROJANS & COVERT TUNNELS

Trojans

From Quick Thinking Greeks ...
to Quick Thinking Geeks

Tunnels

Covert Channels

TROJANS..

Valid IP – No Filters

Valid IP – Stateless Filters

Private Addresses – Stateful Filters

Private
+ Stateful
+ IDS + Personal Firewalls
+ Content Checking
+ ...

TROJANS..

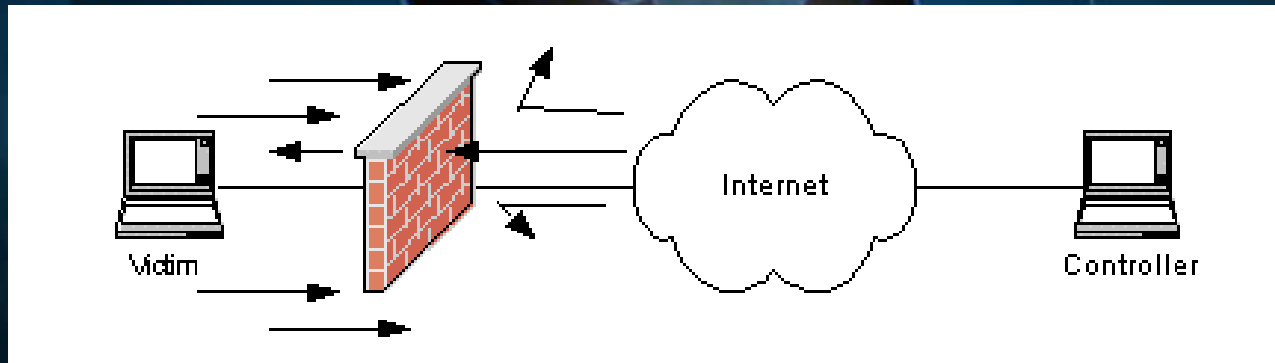
(VALID IP – NO FILTERS)



“get real..”

TROJANS..

(VALID IP – STATELESS FILTER)

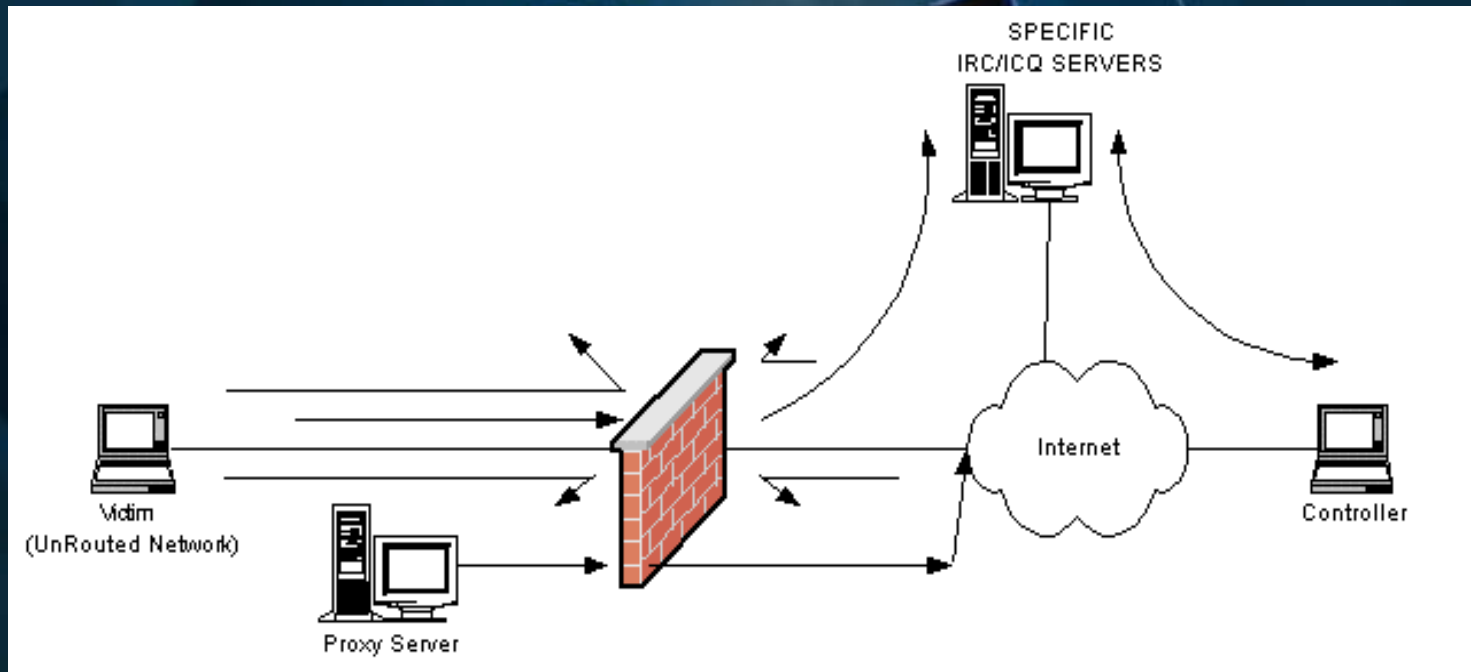


Dial Home Trojans

Random Ports / Open Ports / High Ports
[cDc]

ACK Tunneling
[Arne Vidstrom]

TROJANS.. (STATEFUL FILTERS)



Back Orifice - <http://bo2k.sourceforge.net>

Gbot
Rattler

BRIEF HISTORY OF TROJANS & COVERT TUNNELS

Trojans

From Quick Thinking Greeks ...
to Quick Thinking Geeks

Tunnels

Covert Channels

TUNNELS & COVERT CHANNELS

1985 – TSC Definition “Covert Channels”

1996 – Phrack Magazine – *LOKI*

1998 – RWWWSHELL – THC

1999 - HTTPTUNNEL – GNU

2000 - FireThru - Firethru

CONVENTIONAL TROJANS & HOW THEY FAIL

Stateful firewall & IDS

Direct model

Direct model with network tricks

ICMP tunneling

ACK tunneling

Properly configured stateful firewall

IRC agents +

Authentication proxy

HTTP tunnel ++

Personal firewall & Advanced Proxy

HTTP tunnel with Authentication +++

HYBRID MODEL: “*GATSLAG*”

Combination between covert
Tunnel and Trojan

Defenses mechanisms today:

Packet filters (stateful) / NAT

Authentication Proxies

Intrusion detection systems

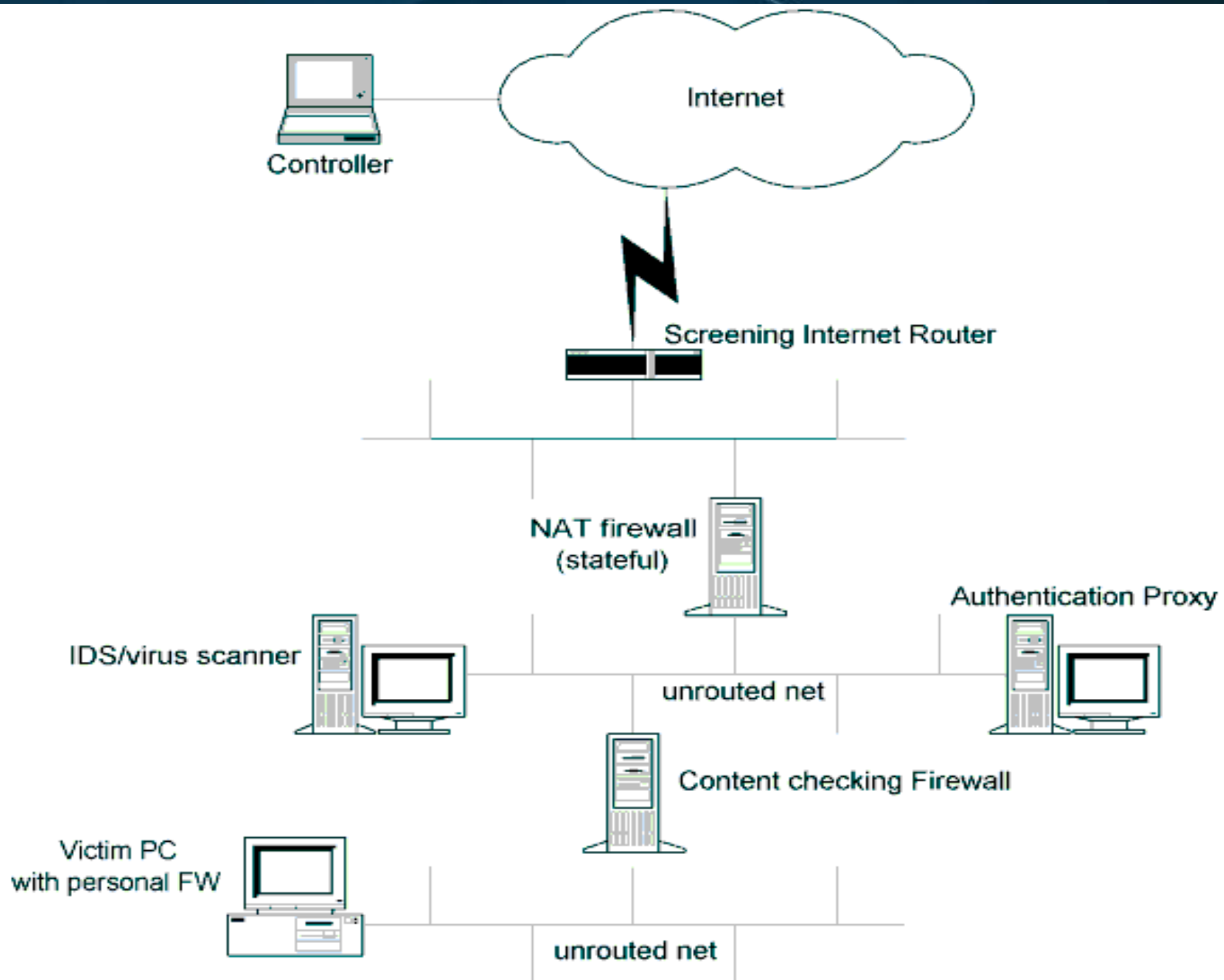
Personal firewalls

Content/protocol checking

Biometrics/Token Pads/One time passwords

Encryption

A TYPICAL NETWORK



HOW *GATSLAG* WORKS

Reverse connection
HTTP covert tunnel

Microsoft Internet Explorer as transport

Controls IE via OLE

Encapsulate in IE, not HTTP

Receive commands in title of web page

Receive encoded data as plain text in body of web page

Send data with POST request

Send alive signals with GET request

WHY *GATSLAG* WORKS

Integration of client with MS Proxy

NTLM authentication

SSL capable

Registry changes

Personal firewalls

Just another browser

Platform independent

IE on every desktop

Specify Controller

Via public web page – the MASTER site

HOW *GATSLAG* WORKS II

Creates invisible browser

Find controller at MASTER

Send request to Controller

If no Controller && retry>7, go to MASTER

Receive reply

Parse reply:

- + Upload file()
- +Download file
- +Execute command

Loop

WHY DEFENSES FAIL

Firewalls (stateful/NAT)

Configured to allow user or proxy out

Content level & IDS

Looks like valid HTTP requests & replies

Files downloaded as text in web pages

No data or ports to lock on to

SSL provides encryption

Personal firewalls

IE valid application

Configured to allow browsing

Authentication proxies

User surf the web

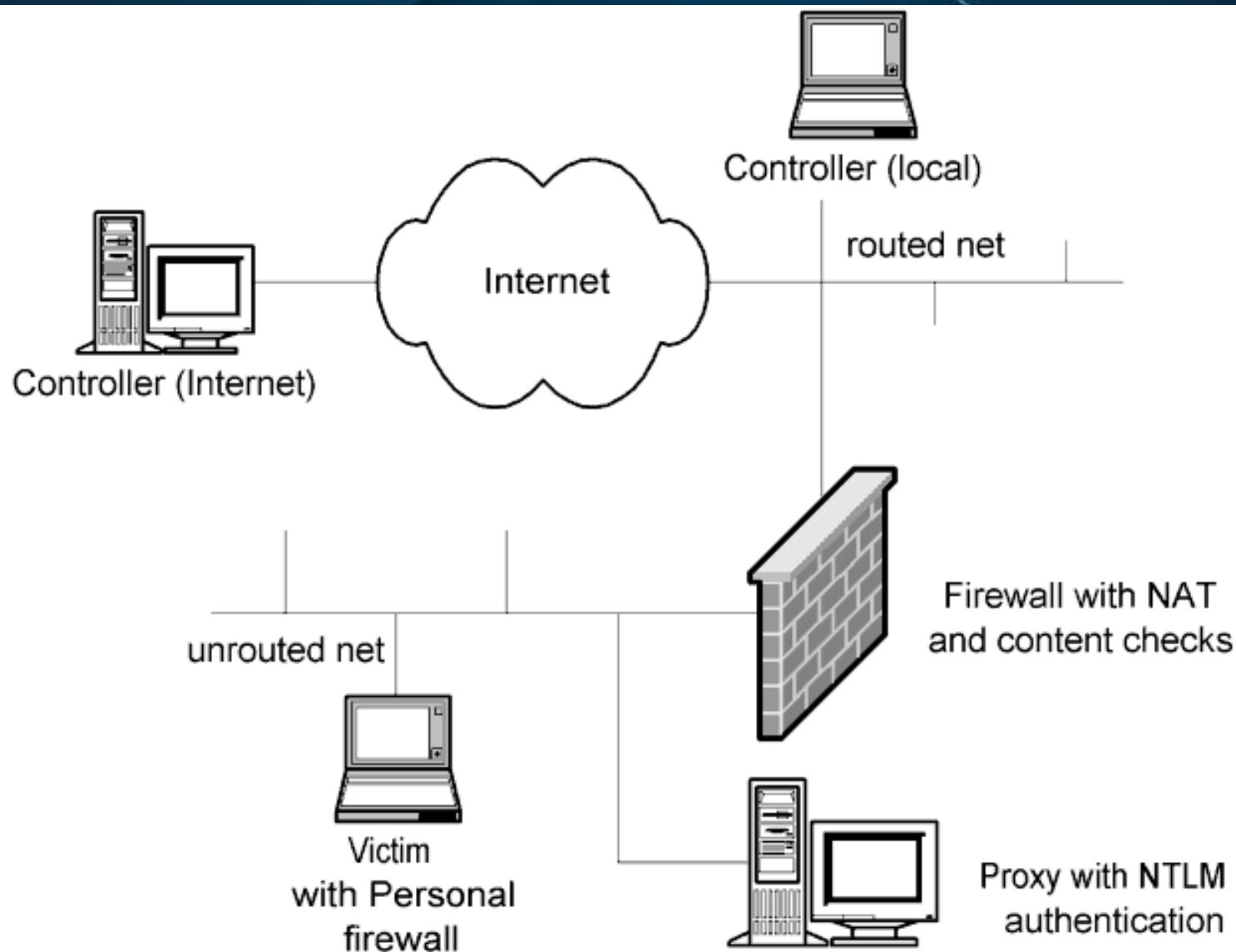
DEMONSTRATION

We will perform the following tasks **totally undetected**:

- File listing of C: drive
- Upload keyboard logger
- File rename
- Execute logger
- Download key-logger file
- List shares/environment
- Move the controller to Internet

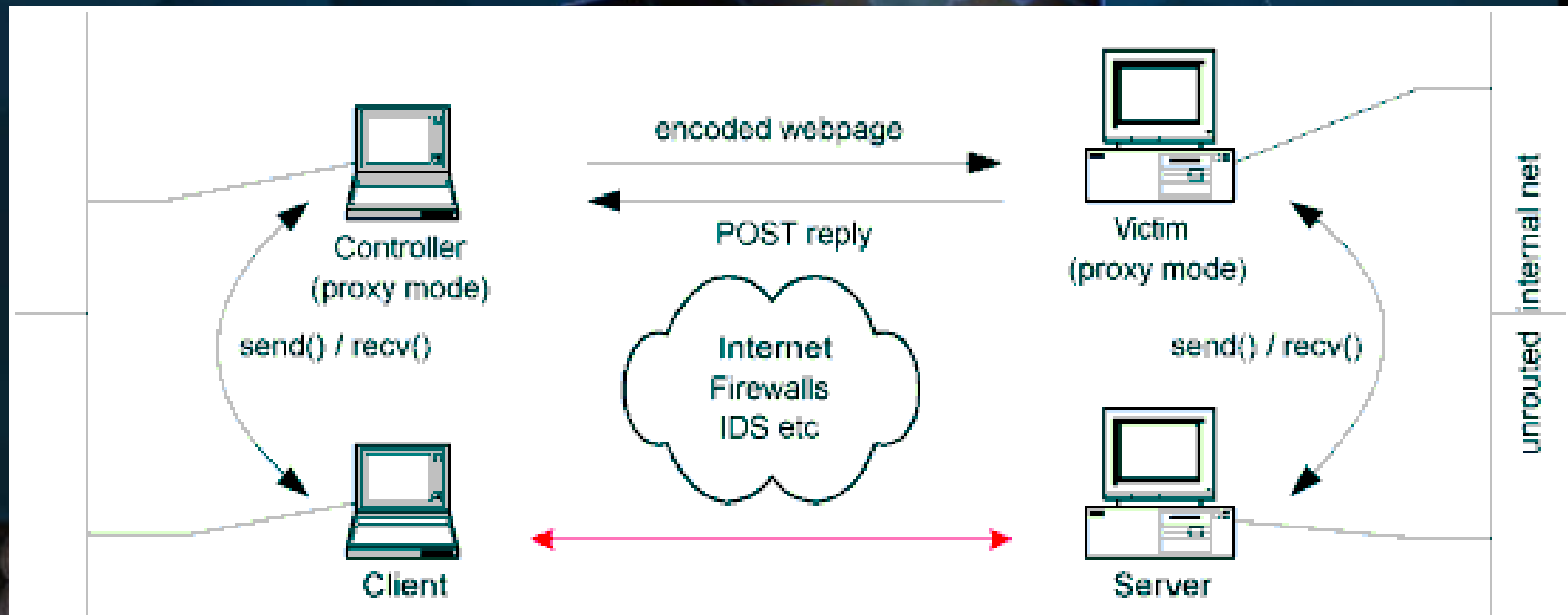
In the following network:

DEMONSTRATION

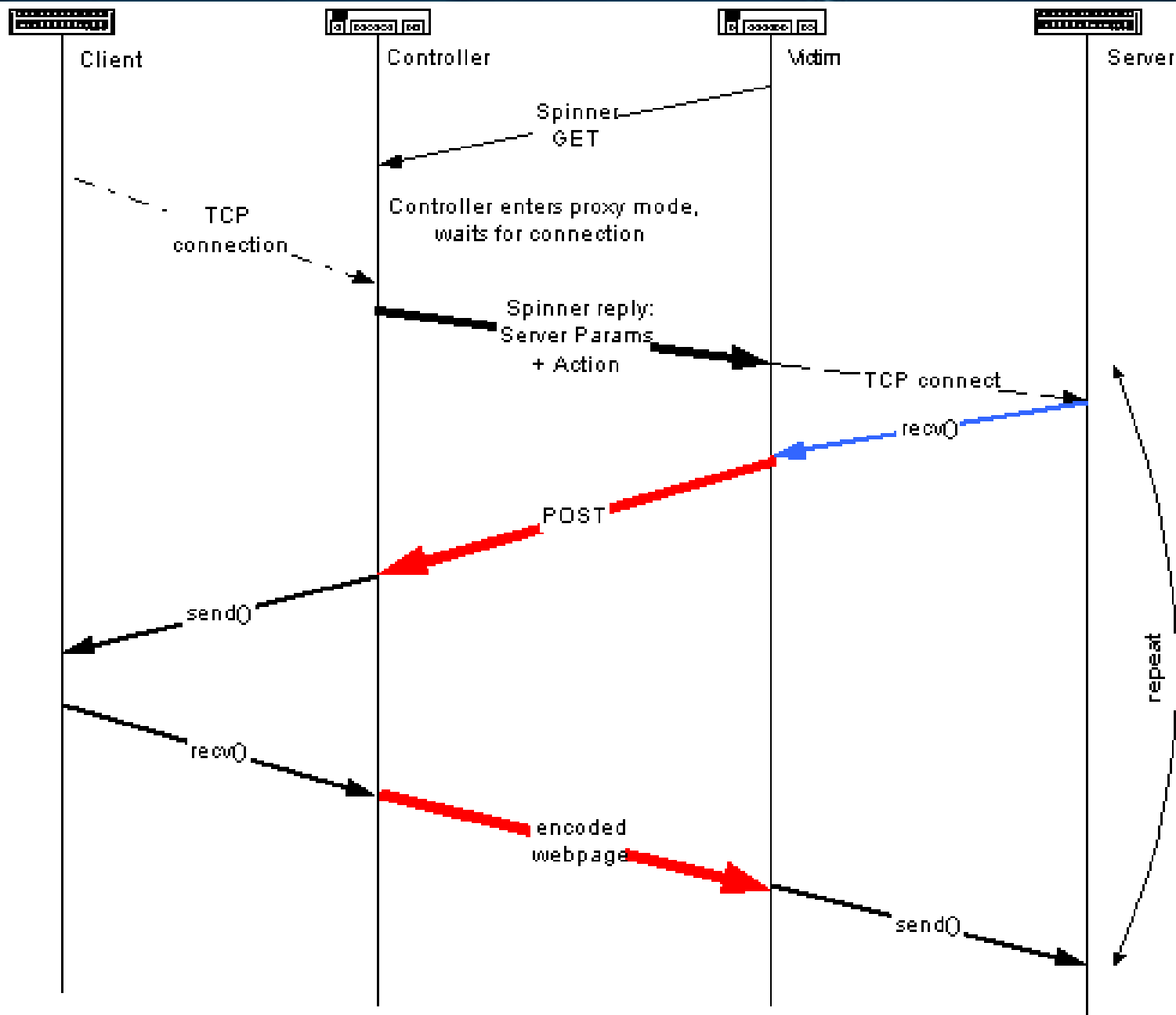


TAKING IT FURTHER

Session level tunneling



FLOW CONTROL



FLOW CONTROL CHALLENGES

How this is different from HTTP tunneling

A browser is not a socket

No select on browser

Train model

The Controller side

Cannot “send”

Buffering of data at Controller

The Trojan side

Multi-part POSTs

Multiple connections (HTTP)

True network level tunneling

SOLVING THE DILEMMA

Delivery

White listing

User education

Desktop profiles (SSL)

AV, personal firewalls

Should you allow everyone to surf the 'net?

CONCLUSION

Something could well be out there
Method not new – all elements exists

Us, the non-programmers

<http://www.sensepost.com>
info@sensepost.com
roelof@sensepost.com
haroon@sensepost.com