



TCP Vulnerability - Session attacks

Document Control	
Document	PLR04_WP-TCP_DM01_22-04.doc
Date Created	4/22/2004 11:54 AM
Version	1.00
Author	David Merry
Approved by	David Merry

Table of Contents

TCP Vulnerability - Session attacks	1
Document.....	1
Introduction	3
Theory of attack.....	3
Source identity	3
Attack Vectors.....	4
Communications network services	4
Immediate action	4
Pro-active measures.....	4
Caveats and Disclaimers	5
Technical	5
General.....	5

Advisory Information;

This document is released to individuals or organisations on a good-faith basis.

It may be passed to third parties, as long as the document is in it's entire form – including the caveats and copyright notices - Polar Computer Communications Ltd.

The document is provided for information and is provided as-is, without any warranty whatsoever, Polar Computer Communications and the Author do not accept liability for any errors or inaccuracies or any loss arising from the use of this information whatsoever.

© 2004 - This document is copyright Polar Computer Communications Ltd.

All Rights Reserved.

All trademarks are acknowledged.

This document may not be reproduced in part without the written permission of Polar Computer Communications Ltd.

Introduction

The internet uses the TCP/IP protocol suite to pass data from one place to another.

There are two key protocols used to carry data; TCP and UDP.

TCP ensures a reliable transmission of packets by managing the link between the two end points (computers).

To achieve this there is a sequence number assigned to each packet. As each packet is received the receiver can acknowledge that the stream has reached a particular point in the session successfully.

In some cases sequence numbers are predictable, in others they are more random. The more predictable the sequence number is, the easier it is for an attack to succeed.

UDP data transfers are not susceptible to this type of attack as there is no concept of a session with sequence numbers within UDP.

Theory of attack

An attack can take place by a third party sending a packet which instructs the end device* to close the session.

The end device will only close the session if sufficient information is given about the session state to determine that the source of the close message is authentic.

Because certain TCP protocols and the way they are used by the end device are more predictable than others, it is possible that an attacker will guess a sequence number close enough to the correct sequence number to be considered as authentic, thus closing the session (one host thinking that the close message has come from the other end).

Once a session has been closed, the attacker can potentially guess what the first sequence numbers will be when re-opening the session, so effectively could find it easier to kill a new session, once the initial session has been closed. This raises the possibility of a malicious attacker closing the session and then repeatedly stopping the session get re-established.

**Certain firewalls may also close the session as they monitor the sequence numbers and "proxy" the session.*

Source identity

The attacker must know the source and destination IP address of a session to perpetrate this attack, across the Internet, this may not be as easy as in an environment where two hosts regularly communicate using TCP.

Attack Vectors

Killing individual sessions can cause significant disruption – however significantly more damage could be caused by actually breaking the TCP sessions which control Internet routing (such as network routers).

Although immediate modifications should be made to any public facing systems that are susceptible, it is possible that a virus could be released with a payload which uses this vulnerability to attack internal network systems even if they are protected by a firewall.

Communications network services

In the context of breaking TCP sessions used by BGP (Border Gateway Protocol) it would be possible to cause the loss of connectivity to an entire network segment or site, by preventing routers communicating with peers.

Immediate action

- Determine if your (and your partners) networks communicate using TCP (as opposed to UDP)
- Determine which systems are key to your communications (routers, VPN, servers, databases etc)
- Determine if traffic is passing through segments that are shared with “user” traffic.
- Implement work-around and check with vendors for vulnerability / patches.
- Carefully review patches issued by manufacturers, modifying the TCP/IP software can easily cause loss of service if the patch isn't tested.
- Ensure client Anti-Virus updates are taking place (as they should be anyway) and that the latest protection is enabled.

Pro-active measures

- Use a firewall that can randomize sequence numbers (e.g. Cisco PIX) for limited protection.
- Ensure critical TCP/IP sessions are routed away from user traffic (wherever feasible).
- Use TCP mechanisms that incorporate authentication.

Caveats and Disclaimers

Technical

This information is provided in good faith, as-is for informational purposes only and is accurate to the best of our belief.

Polar Computer Communications accept no responsibility or liability whatever for any inaccuracies in this text.

Polar Computer Communications accept no responsibility or liability whatever for any consequential losses as a result of using (or not using) the information contained in this document.

It is the responsibility of the reader to satisfy themselves as to the accuracy of this information prior to acting upon it.

General

Please note: This information and all services and products are provided in accordance with our Standard Terms and Conditions of business which can be found at;
<http://www.polar-cc.co.uk/text/stc.html>