



Search

Topic

[Home](#)

[Web Links](#)

[About This Site](#)

[Site of the Day](#)

[Y](#)

[Login/Create an Account](#)

Sponsored Links



Vulnerability in TCP/IP Exposed

Posted on Wednesday, April 21 @ 12:30:00 EDT by [mhamrick](#)

Network security practitioners are up in arms about a new twist on an old attack. Security researcher Paul Watson recently noticed that armed only with a C compiler and detailed knowledge of TCP/IP, an attacker could craft packets capable of terminating arbitrary TCP connections. What does this mean in English? It appears that version 4 of TCP/IP (that's the version that most everyone uses) is even less secure than suspected.



The UK's National Infrastructure Security Co-Ordination Centre issued a vulnerability announcement yesterday, alerting Internet software developers to the Denial of Service attack. (see [NISCC Vulnerability Advisory 236929 : Vulnerability Issues with TCP/IP](#) .) The advisory summarizes a potential attack on either end of a TCP/IP connection and describes circumstances under which craftily formed TCP headers could be used to fool either side into closing the connection.

How does this work? Buried deep inside every TCP/IP header is the reset bit. The legitimate use for the reset bit is for one party in a connection to signal it's peer that it believes it's trying to send a packet to an invalid connection. The standard response to receiving a reset is to close the connection and notify the application. If you've ever seen an error message that says something like "Connection Reset by Peer," this is likely what happened. Firewall and load balancing equipment, if misconfigured, can generate these error messages. Keeping a connection idle for long periods of time will sometimes result in such an error. One side of the connection hasn't heard from the other, so it simply gives up. If the other side of the connection didn't hear that it's peer was giving up the connection, the next packet it sends will be to a connection that it's peer believes doesn't exist. The reset mechanism is a way to effectively tell the peer, "sorry, didn't you hear? I hung up on you milliseconds ago!"

Security concerns about mis-using reset bits have been around for quite some time. Back in the old days when TCP/IP was "new," implementers developed a very simple heuristic for avoiding malicious reset requests: "only accept reset requests from your peer." In other words, if you send a packet, and you get a reset in return, double check the IP address the reset request comes from. If it comes from a machine you think you have a connection with, consider it valid. If not, consider it an attack and throw it away. (This is a bit of an oversimplification, as it's a good idea to also check the peer's port number as well, but the argument is conceptually similar...)

Several years later the massive influx of inexpensive workstations on college campuses started to worry network security practitioners. College students were notorious for playing practical jokes, especially jokes that required deep technical insight. Operational security staff at campuses deploying large networks were concerned about IP address spoofing. Skilled attackers can forge TCP/IP headers to fool their targets into believing attack headers come from a trusted machine.

But the network security community wasn't terribly worried about IP address spoofing and session hijacking. Why? Because another parameter buried inside TCP/IP connection headers, the initial sequence number, is needed (in "blind spoofing" scenarios) to launch a practical attack. The ISN (initial sequence number) is a randomly generated number shared

Related

- [NISCC Advisor: Vulnerability in TCP/IP](#)
- [Strange TCP/IP Analysis](#)
- [Strange TCP/IP Analysis](#)
- [More Network](#)
- [News](#)

Most Recent Attacks

[Hotm](#)

Article

Av

Please vote

- ★
- ★
- ★
- ★
- ★

Option

[Print](#)

Modules

- [Home](#)
- [Articles](#)
- [AvantGo](#)

- [Downloads](#)
- [Feedback](#)
- [Journal](#)
- [Members_List](#)
- [Stories_Archive](#)
- [Submit_News](#)
- [Surveys](#)
- [Topics](#)
- [Web_Links](#)
- [Your_Account](#)

between two machines in a network connection. It is a 32 bit number (though for compatibility reasons, implementers tend to only use 31 bits.) An attacker would have to guess that 31 bit value correctly in order to exploit the vulnerability. (Again, this is a bit of a simplification, the attacker actually has to guess the next number in the sequence, but it's supposed to be just as difficult to guess the next number as it is to guess the ISN used in a particular connection.) Such an attack is not impossible, but most network operators considered it an impractical attack. The attack space of 2^{32} was thought to be too large to attack.

 [Ser](#)

But researchers later noticed that ISNs were not completely random. A very good pair of papers by Michael Zalewski ([Strange Attractors and TCP/IP Sequence Number Analysis](#) and [Strange Attractors and TCP/IP Sequence Number Analysis - One Year Later](#)) describe why the less than random behavior of standard TCP/IP implementations can be a security problem. Zalewski's analysis is that modern operating systems could be successfully attacked with less than 200 trials. That's not a lot of traffic, and depending on how closely your security staff scrutinizes IDS logs, it could be somewhat difficult to detect.

The recent report from Paul Watson exacerbates an already difficult situation. The new results indicate attackers do not have to successfully guess an initial sequence number, merely a value within a particular window of acceptable ISNs.

Network users are advised to check with their OS vendors for patches or work-arounds.

User's Login

Nickname

 Password

Don't have an account yet? You can [create one](#). As a registered user you have some advantages like theme manager, comments configuration and post comments with your name.

"User's Login" | [Login/Create an Account](#) | 0 comments

Threshold Thread Oldest First

The comments are owned by the poster. We aren't responsible for their content.

No Comments Allowed for Anonymous, please [register](#).

Languages

Select Interface Language:

Badges



All logos and trademarks in this site are property of their respective owner. The comments are property of their posters, all the rest Cryptonomicon.Net. Syndicate our content using our [RSS interface](#).

Web site engine's code is Copyright © 2002 by [PHP-Nuke](#). All Rights Reserved. PHP-Nuke is Free Software released under the [GN](#)
 Page Generation: 0.207 Seconds