SCTP Security Threats

draft-stewart-tsvwg-sctpthreat-02.txt

Gonzalo Camarillo

Randall Stewart

Michael Tüxen

Origin of the document

- The initial version was based on a publication of T. Aura, P. Nikander, and G. Camarillo.
- Some additional findings have been added.

Address Camping/Stealing

- The attacker guesses the port number a victim will use and sets up an association with the server. The victim needs to be multihomed.
- Path verification (added in the IG) will shorten the lifetime of the association between the attacker and the victim.
- Random port number selection makes this attack harder...

Association Hijacking (1)

- The attacker takes over an IP-address of the victim and receives a packet of the association. Then the attacker sends an INIT and receives an INIT-ACK. Using the tie tags in the COOKIE it knows the verification tag of the victim and can send arbitrary packets.
- The IG now requires that the tie tags are not the original tags. So this procedure can not be used by an blind attacker to get the verification tags anymore.

Association Hijacking (2)

- The attacker takes over an IP-address of the victim and receives a packet of the association. Then the attacker performs a full handshake with the same address and port numbers. The other side will recognize a restart of the association.
- The application should pay attention to restart notification and take into account that the peer might have changed.

Bombing attack (1)

- The attacker sets up an association to a server providing a large amount of data and lists also addresses of the victim in the INIT. Now the attacker requests data and arranges the the data is sent to the victim.
- This attack works only if the victim does not support SCTP and the ICMP messages are not recognized. Also SACKs have to be spoofed. The IG now describes the ICMP handling, receiving SACKs for unsent data and also requires the path verification procedure which makes this attack impossible.

Bombing attack (2)

- The attacker sends an INIT and lists some addresses of the victim. On reception of the INIT-ACK it stores the COOKIE and sends the COOKIE-ECHO. Now the peer sends HEARTBEATs for the path verification procedure to the victim.
- The number of the path on which you do path verification should be limited.

Association redirection

- The server receives a packet containing the COOKIE-ECHO chunk, which contains port numbers, and also the port numbers in the common header. An attacker can try to use a non matching common header to attack the server.
- The IG requires that the port numbers in the COOKIE are checked against the port numbers in the common header.

Summary

- Some attacks are not possible anymore if you follow the IG.
- Some attacks have only a very limited life time depending on parameters.