

Forum:[Hack Forums](#)

Thread: [SCTP for Practical Network Exploration](#)

Oh_Well - September 17, 2025, 11:46 pm

SCTP for Practical Network Exploration

SCTP (Stream Control Transmission Protocol) is a transport layer protocol IETF-standardized alongside TCP and UDP.

While it's less common in consumer internet applications, it's extensively used in telecom core networks (especially SIGTRAN stacks like M3UA, SUA) for signaling transport, and sometimes in webRTC, SIP, and other applications requiring multi-homing or better resilience than TCP.

If you're probing telecom infrastructure, 5G cores, or certain critical services, understanding SCTP is essential.

Getting Started with SCTP tools

On Debian-based systems (Kali, Ubuntu), you can install the user-space utilities and kernel module:

```
Code sudo apt update && sudo apt install -y lksctp-tools wireshark-common tshark  
sudo modprobe sctp
```

The lksctp-tools package provides utilities like sctp_test, sctp_darn, and sctp_status for generating and inspecting SCTP traffic.

Basic Association Testing

A common way to check for an accessible SCTP endpoint is using sctp_darn in client mode:

```
Code sctp_darn -H <your_ip> -P <local_port> -h <target_ip> -p <target_port> -s
```

This command will attempt to set up an SCTP association. If successful, you can type messages to send over the association. The output will show the SCTP state changes, including COMM_UP when the association is established.

Inspecting Traffic

Using tshark or Wireshark to analyze SCTP traffic is highly recommended. A simple capture filter for terminal use:

```
Code sudo tshark -i any -Y "sctp" -V
```

You can observe the four-way handshake:INIT

INIT_ACK

COOKIE_ECHO

COOKIE_ACK

This is fundamental to understanding if a connection is successful.

Common SCTP Vulnerabilities & Attack Vectors

SCTP-Specific Security Issues:

1. Multi-homing Exploitation

SCTP's multi-homing can be abused for traffic redirection:

Code # Test for vulnerable multi-homed associations

```
sctp_test -H primary_ip -B secondary_ip -h target_ip -p target_port
```

Monitor for SCTP ASCONF chunks that change IP addresses

```
sudo tshark -i any -Y "sctp.chunk_type == 12" -V
```

2. Association Hijacking

Weak verification tag validation can lead to session takeover:

Code # Capture existing associations for analysis

```
sudo tshark -i any -Y "sctp" -T fields -e sctp.verification_tag -e ip.src -e ip.dst
```

Look for predictable verification tags (security weakness)

```
python3 sctp_tag_analyzer.py captured_sctp.pcap
```

3. Denial of Service Vectors

SCTP-specific DoS attacks targeting association state:

Code # INIT flood detection

```
sudo tshark -i any -Y "sctp.chunk_type == 1" -T fields -e frame.time -e ip.src | sort | uniq -c
```

Cookie-based attacks (malformed COOKIE_ECHO)

Use scapy or custom tools - exercise left to reader

4. Real-World Target Examples

Where you're likely to find vulnerable SCTP implementations:

- Telecom Equipment: Legacy Ericsson AXE switches, older Nokia BSC units
- VoIP Gateways: Cisco AS5400/AS5850 series with outdated firmware
- Industrial Systems: Siemens SIMATIC systems in power plants, water treatment
- Aviation: ACARS ground stations at smaller airports
- Maritime: AIS base stations in port authorities
- Cloud Services: Misconfigured Kubernetes clusters with SCTP load balancers

What someone could potentially do with that

Telecom infrastructure

Redirect voice traffic, intercept SMS/calls

Extract IMSI, location data, call detail records

Take down cell towers, cause regional service outages

Generate premium rate calls, manipulate charging records

Industrial control systems

Alter setpoints in power plants, water treatment facilities

Disable emergency shutdown procedures, alarm systems

Cause equipment failures, production line shutdowns

Aviation & Maritime

Inject false aircraft positions, ghost flights

Monitor pilot-to-ground communications

Disrupt GPS corrections, approach guidance systems

Manipulate vessel tracking, cargo management systems

VoIP & enterprise networks

Record executive communications, conference calls

Generate expensive international calls through PBX systems

Use VoIP infrastructure as entry point to corporate LANs

Take down corporate phone systems