Scientific Report: Short-Term Scientific Mission

COST Action CA15127 RECODIS

STSM Details

STSM Title

Overview of the Secure Virtual Private LAN Service Testbed

STSM Applicant

Nikita Korzhitskii, PhD Student in Computer Science

Linkoping University, Linkoping, Sweden

Host

Dr. Madhusanka Liyanage

University of Oulu, Oulu, Finland

STSM Period

Start date: *2017-11-26*

End date: *2017-11-30*

Working group

WG4 Malicious Human Activities

Purpose of the STSM

During the mission to the University of Oulu a Host Identity Protocol [1] network architecture that allows eavesdropping and man-in-the-middle (MITM) attacks has been deployed and studied.

The testbed consisted of two enterprise level *HIPSwitches* [2], a *Conductor* [3], a few routers, *MITM* host and two endpoint hosts. Such architecture allowed to study orchestration and tunnel establishment processes between HIP nodes and implement a simple attack on an overlay network which shows that only edge-to-edge connection authenticity is being provided.

Description of the work carried out during the STSM

A VPLS overlay network has been deployed on top of an underlying shared network using HIP enabled equipment by Tempered Networks [4]. The setup is presented on Figure 1.

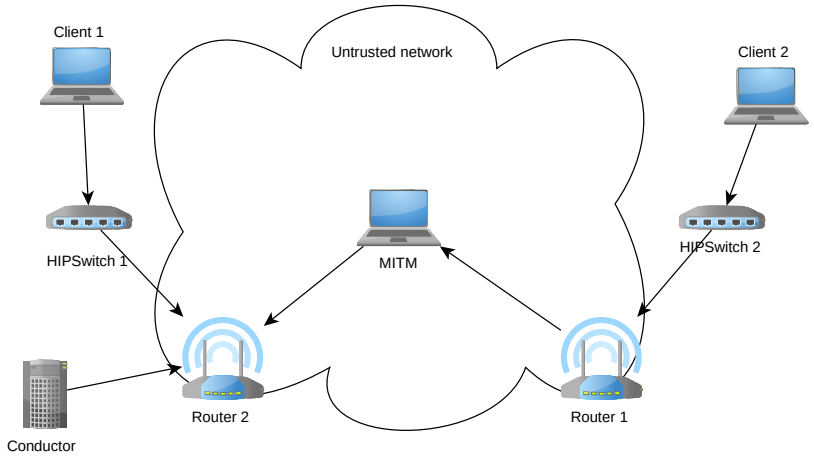

Figure 1. Implemented network architecture

The corresponding overlay network architecture can be displayed at the Conductor web interface and is presented on Figure 2. *Client 1* and *Client 2* on Figure 1 corresponds to Lenovo and Dell laptops on Figure 2.

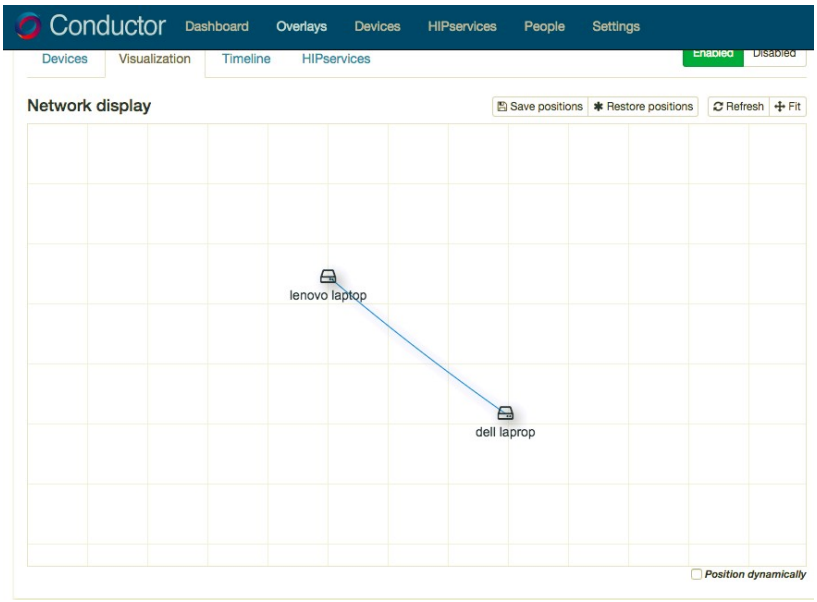

Figure 2. Overlay network architecture as presented in Conductor’s web-interface

Such setup had to be implemented from scratch using the equipment described in the following table.

Role	Device	Description
Client 1, Client 2	Generic laptop * 2	Generic Linux machine that allows use of various applications and network protocols.
Router 1, Router 2	D-Link DSR-250N * 2 [5]	Routers implementing underlying shared network. Two separate subnets are connected together by the bridge on the MITM host.

Role	Device	Description
MITM	Generic laptop	Generic Linux machine acting as a bridge between two routers with ability for dumping and modifying traffic. Wireshark [6] has been used as a monitoring tool.
Conductor	Tempered Networks Conductor [3]	A server used to orchestrate policies among HIP enabled switches and services. Allows configuration of overlay networks.
HIPSwitch	Tempered Networks HIPSwitch-300 [2] Firmware version: 1.12.1	Network-edge device for establishing encrypted tunnels with other HIPSwitches and services using Host Identity Protocol. Acts as a gateway for devices connected to equipment ports.

Table 1. Description of testbed devices

Devices have been wired and set up together as displayed on Figure 1. A simple overlay network has been deployed using the *Conductor* ensuing the initialization of *HIPSwitches* and policy distribution. A secure tunnel between two *HIPSwitches* has been established using the Host Identity Protocol 4-way handshake. Tunnel establishment and policy distribution traffic have been captured by *MITM* host and saved as Wireshark pcapng-dumps. Screenshot of such a dump for one the experiments is provided in the following figure.

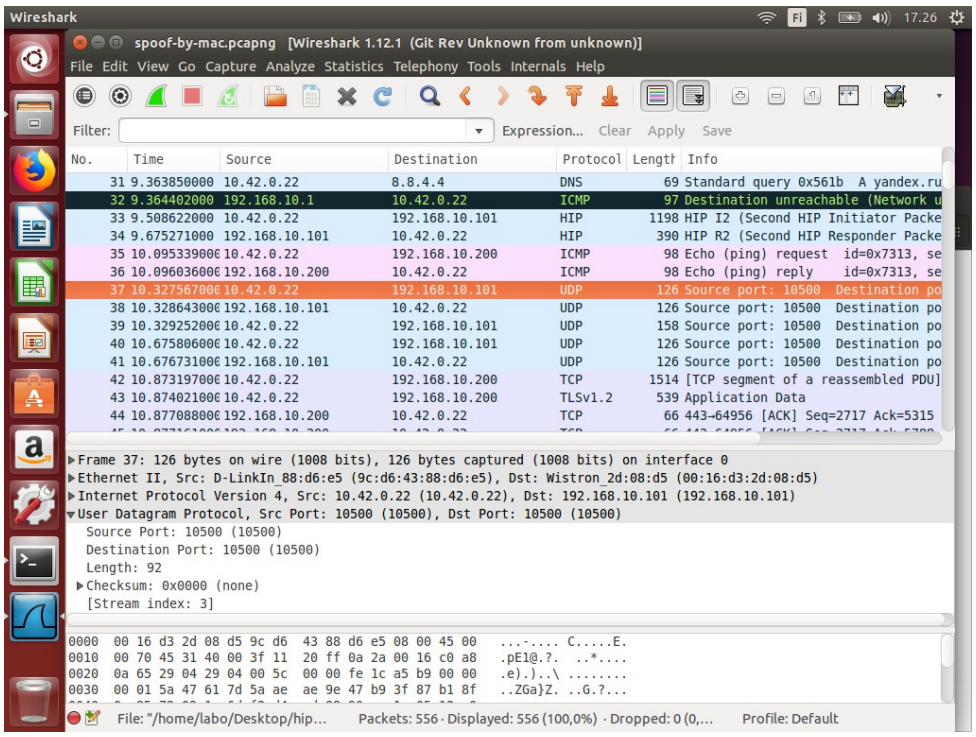

Figure 3. Screenshot of Wireshark interface after dumping traffic for one of the experiments.

Experiments

A few experiments have been conducted with the described setup. By default, *Conductor* discovers HIPServices and distributes policies using IF-MAP [7] server on port 8096. HIP-tunnels are established between HIPServices and HIP-enabled devices through UDP port 10500 on both ends.

Experiment 1. ICMP ping exchange between clients.

Unencrypted packets are captured on *Client 1* while encrypted data is captured on *MITM* bridge between *HIPSwitches*.

Outcome: ICMP packets are encrypted and sent using UDP with port 10500. One source packet could be sent as multiple UDP packets with some overhead on the amount of transferred data. Original ICMP ping request of 98 bytes resulted in 190 byte datagram after encryption. Secure tunnel between HIPSwitches is being established (if none exist) as soon as a packet is being sent from one *Client* to another.

Experiment 2. TCP connection establishment between clients.

Netcat [8] was used during this experiment. *Client 1* created a listening socket on the port 4444. After that *Client 2* established a TCP connection with a standard TCP handshake. A few messages containing text data have been sent back and forth. Unencrypted packets have been captured on *Client 1* while encrypted data was captured on *MITM* bridge between *HIPSwitches*.

Outcome: As in the previous experiment, a tunnel to *HIPSwitch 2* has been established by *HIPSwitch 1* upon the reception of a SYN packet from *Client 1*. TCP packets have been encrypted and encapsulated into UDP datagrams and then sent using ports 10500 on both ends with overall increase in packet size. Payload is not available to *MITM, assuming the security of payload encryption*.

Experiment 3. UDP datagram exchange between clients.

The above experiment is repeated using UDP protocol instead. No connection establishment sequence is required for UDP, so HIP 4-way handshake occurs upon the reception of the first datagram from one client to the other.

Outcome: datagrams were encapsulated the same way as in the previous experiment. A modified version of this experiment is used to demonstrate the lack of authentication between clients as well as between HIPSwitch and its connected equipment.

Experiment 4. HIPSwitch connected equipment spoofing.

This experiment repeats the previous one, but after tunnel establishment step and exchange of datagrams *Client 1* is then disconnected from *HIPSwitch 1* and substituted with another host (*Fake Client 1*) that disguises itself with MAC address of *Client 1*. The attack requires access to the physical medium, which is Ethernet cable in this case.

Attack is represented on Figure 4.

Unencrypted packets have been captured on *Client 2* while encrypted data was captured on MITM bridge between *HIPSwitches*.

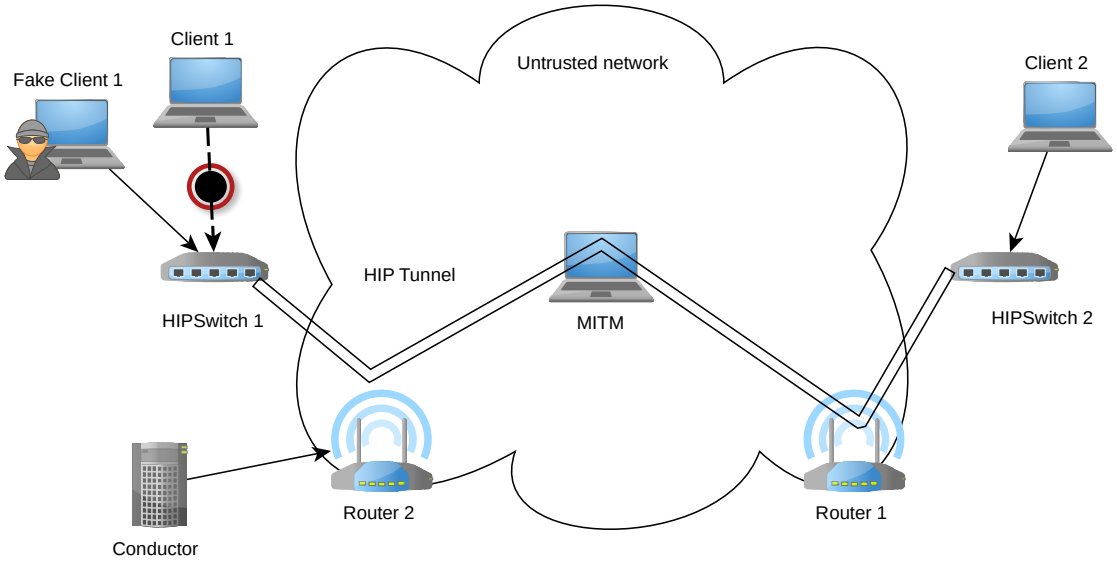

Figure 4. Substitution of *Client 1* with *Fake Client 1*.

Outcome: Client 2 continues its normal networking operation without noticing the fact that *Fake Client 1* took over the IP address and UDP port of *Client 1*. As a result the attacker is now able to send and receive packets to/from *Client 2*. *HIP tunnel* is intact.

Experiment 5. Throughput of the tunnel.

In order to measure throughput of the tunnel – *iperf* [9] utility have been used. The following figure shows the result of two generic throughput tests.

```
labo@labo-PC3:~/Desktop/hip$ iperf -s
------------------------------------------------------------
Server listening on TCP port 5001
TCP window size: 85.3 KByte (default)
------------------------------------------------------------
[  4] local 192.168.220.124 port 5001 connected with 192.168.200.132 port 40739
[ ID] Interval       Transfer     Bandwidth
[  4]  0.0-11.2 sec  15.2 MBytes  11.5 Mbits/sec
[  5] local 192.168.220.124 port 5001 connected with 192.168.200.132 port 40740
[  5]  0.0-11.3 sec  15.8 MBytes  11.7 Mbits/sec
```

Figure 6. Tunnel throughput measurement using *iperf*.

Tunnel throughput never reached more than 13 Mbits/sec for this setup although the throughput of the underlying route was around 50 Mbits/sec.

Main Results

During the STSM a HIP-based VPLS network has been deployed and studied. Multiple experiments have been conducted and as a result a successful attack has been implemented on the deployed architecture. A lot of useful traffic dumps have been captured during these experiments.

It turns out that no authentication is performed within *HIPSwitch* subnets and that leads to the possibility of authentication attacks. MAC addresses are easily spoofable, however this VPLS solution does not imply any mechanism to prevent such spoofing. To ensure equipment authenticity within HIPSwitch subnets and security of communication – a combination of the following measures is required: connection status monitoring, physical medium intrusion control, dynamic address allocation, tunnel termination, port-to-host association, stateful packet inspection, etc. Secure Device Identities Standard [802.1AR] implementation might complement such mechanism by ensuring identities within *HIPSwitch'* subnets.

The attack can be extended to any other protocol including TCP as soon as the attacker knows the internal state of the connection/session.

By obtaining physical access to the medium attacker may be capable of moving from one overlay network to the other by spoofing MAC addresses of equipment connected to HIPSwitch or even create a bridge between those virtual overlays.

Future work

A study on VPLS security reinforcement might be fruitful, while a study on other possible attacks on such architecture might lead to the discovery of new VPLS security threats.

Another topics worth of research are: attacks on the *Conductor,* behavior of the architecture in the event of *Conductor's* Denial of Service, determination of actions sufficient for network disruption, opportunistic mode and detection of VPLS services on the internet.

Foreseen publications

A contribution to the RECODIS book on the matter of VPLS and IDN is in progress, the following chapters are being written:

- Identity-Defined Networking
  - Introduction to IDN
  - Expected Benefits of IDN
  - Challenges in IDN

Future collaboration with the host institution

We are considering to deploy similar VPLS network between University of Oulu and Linkoping University.

I would like to thank Dr. Madhusanka Liyanage and other members of CWC for assistance.

References:

[1] RFC5201 Host Identity Protocol. Network Working Group at IETF. URL: https://tools.ietf.org/html/rfc5201

[2] Tempered Networks Hardware Products. URL: http://www.temperednetworks.com/products/hardware

[3] Tempered Networks Conductor Specification. URL: http://www.temperednetworks.com/sites/default/files/datasheets/ds_Conductor.pdf

[4] Tempered Networks Official Website. URL: http://www.temperednetworks.com

[5] DLink DSR-250N Specification. URL: http://www.dlink.com/uk/en/products/dsr-250n-wireless-n-unified-service-router

[6] Wireshark Official Web-page. URL: https://www.wireshark.org

[7] TNC IF-MAP Metadata for ICS Security. Trusted Computer Group. URL: https://trustedcomputinggroup.org/tnc-if-map-metadata-ics-security/

[8] nc(1) – Linux Man Page. URL: https://linux.die.net/man/1/nc

[802.1AR] – IEEE 802.1: 802.1AR - Secure Device Identity. URL: http://www.ieee802.org/1/pages/802.1ar.html

[9] iperf(1) – Linux Man Page. URL: https://linux.die.net/man/1/iperf