

Proof of an IP level authentication algorithm

Eric Leblond
Project Manager
INL

Vincent Deffontaines
Research Engineer
INL

May 12, 2002

Abstract

The Efficas project[1] aims at researching ways of performing a real per-user authentication on security IP filters. We propose here an algorithm which securely authenticates connexions. The following article will present the algorithm and a proof of the obtained security

1 Introduction

Numerous algorithms can be used to provide authenticated filtering. Almost all of them relay on an assumption of the type $User == IP$:

By a mean, we know that user A is using computer B , thus any packets coming from computer B is coming from A .

Such algorithms perform an a-priori authentication. The persistence of link between User and Computer is necessary not null and this interval can be used by an attacker to steal identity from user A . This security scheme is by the way totally inefficient if computer B is hosting several users simultaneously.

1.1 An a posteriori algorithm

The Efficas project proposes a new algorithm that realises an a posteriori authentication of connections.

2 Algorithm

2.1 Component of the systems

Let A be a user, B a computer having a single IP address, F a firewall, S an authentication server and T the targeted service. A uses an authentication client C to interact with S .

2.2 An a posteriori algorithm for connection authentication

The figure 2 describes the authentication algorithm. The algorithm is described here

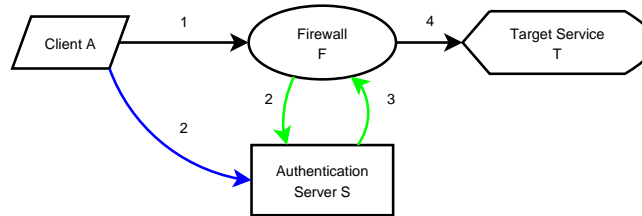


Figure 1: Authentication algorithm

under :

1. Application run by user A sends a datagram D to T .
2.
 - Firewall F intercepts datagram and asks S to decide
 - Authentication client C run by user A tells S that A sends a packet and asks authorisation.
3. S aggregates datas coming from A and F and sends an answer to F corresponding to the access policy of user A to T .
4. F forwards or drops packet depending on answer sent by S .

3 Proof

3.1 Hypothesis

3.1.1 Client

We assume that the user A runs a client C . Client and user system respect the following requirements :

1. Client authenticates only packets coming from user A .
2. No identity usurpation can occur from another user on same computer (a user X can not open a connection under A user name).
3. Other users of system can not hijack user A connections.

3.1.2 Network

We will distinguish two cases :

1. Network can be trusted : the topology of the systems is well known and active equipment are safe.
2. Network can not be trusted : the topology of the network is not under control or some active equipments can be unsafe.

3.2 Packet authentication

Let client A try to open a TCP/UDP connection to T . It sends a packet with specific IPV4 parameters Source IP:Source Port and Destination IP:Destination Port.

3.2.1 Enumeration of potential attack points

To obtain a fake authorization, an attacker can :

1. Use protocol level attack on the server S
2. Use machine substitution at IP level
3. Use packet interception and reemission

Internally used protocol is supposed to be strong enough in terms of encryption to avoid any protocol level attack. Thus remaining attack are :

1. Use machine substitution at IP level
2. Use packet interception and reemission

3.2.2 Trusted network

1. Use machine substitution at IP level : Attack of type arp spoofing can permit to an attacker to obtain the IP address of another machine.
2. Use packet interception and reemission : In a trusted network, attacks can only come from entity that don't know the content of packet or the nature of the traffic and can not intercept packet. Thus reemission type attacks are not feasible.

To be able to profit from another user's authentication packet (from client C) the attacker H has to have its packet arriving before the packet of the client C and this with same source IP and port and id. As he doesn't know these parameters, H has one chance out of 64511 to send the correct packet.

Furthermore it has to take control over IP of C to be able to use the source address. And it has to do that after emission of authentication packet, but as this packet is sent after this application packet, H has very few chances that his forged application packet arrives before the application packet of C .

3.2.3 Untrustable network

Machine substitution at IP level can occur with less restrictions than in trustable network as the attacker knows when it has to act.

Furthermore, the system is subject to reemission attacks.

Figure 2 describes the setting needed to a man in the middle attack. The attacker P has to be placed between client C and authentication server S and firewall F .

The following algorithm describes the attack :

1. Client C sends a application packet D to F
2. P intercept application packet D and send packet D' with same source port.

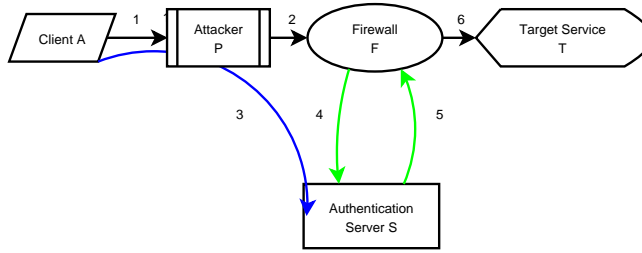


Figure 2: Man in the middle attack

3. C sends an authentication packet for packet D that P forward to S
4. F ask S about D'
5. S authenticate the packet D' as coming from C and send corresponding answer to F .
6. F forwards packet if S told him to do so.

Under this condition, the packet D' from attacker P is authenticated as coming from C .

Case of WiFi system The described attack does not apply to wireless network where WiFi access concentrator and active equipments are safe. P can not intercept packet, it has to physically be present on the path between C and routers.

3.3 Authentication of connections

The connection tracking system of modern firewalls allows the system to only authenticate the user at the initiation of the connection. All the packets of the connection are thus authenticated with the level of trust of the connection tracking of the system. More precisely, the risk of authentication hijacking is the same as the risk of session hijacking.

4 Conclusion

In the case of a corporate network, the condition necessary to the success of the described attack are the compromise of an active network equipment or a physical modification of the network topology. This type of condition is really severe and the condition of trustability is often implicit in corporate network.

Furthermore the described attack is somehow hard to setup and a classical session hijacking or session sniffing are easier than a direct attack to the described protocol.

Thus, the proposed algorithm is proven under weak hypothesis on client sanity for trustable network which is an hypothesis classically done in most corporate networks.

References

- [1] Eric Leblond, Vincent Deffontaines, and Xavier Desurmont. Eficaas project : Extending firewalling infrastructure capabilities and aggregating authentication systems. available at http://www.nufw.org/eficaas/eficaas_01.pdf.