4

Security Flows Analysis of the ATM Emulated LAN Architecture

*Maryline LAURENT**
Télécom Bretagne
rue de la châtaigneraie - BP 78
35512 CESSON Cedex - France
Email : mlaurent@rennes.enst-bretagne.fr

Abstract

As currently adopted by the ATM Forum LANE SWG, LAN Emulation specifications include many security weaknesses making communications on Emulated LANs (ELANs) vulnerable to heavy threats (in the sense of X800) such as masquerade, information disclosure and denial of service.

This paper aims at highlighting ELAN's security problems. To this end, a number of attacks scenarios are studied over the ELAN architecture and details relating to the way an attacker may perform each attack - how, from where, with which collusion (if any), which facilities, which level of difficulty - are given.

Keywords

Security, ATM, Emulated LAN, ATM LAN

1 INTRODUCTION

There are no doubts that ATM technology will be used as the means to support end-to-end data communications in the near future. However, since today's data communication infrastructures are built around "legacy LANs" (e.g., Ethernets, Token Rings), a radical change from the legacy LAN's technology to the ATM one seems impossible in practice.

In the LAN environment, ATM offers considerable advantages (Jeffries, 1994) (Vetter, 1995) (Biagioni, 1993) over the existing legacy LANs (referred to as "LANs"): it brings performance increase, but above all, it considerably simplifies LANs management since the virtual LAN concept developed in ATM enables simple virtual LANs reconfiguration from a management platform instead of having to change the wiring as normally done in legacy LANs.

Legacy LANs or LANs provide users with a vast base of reliable communications applica-

*. This work is funded by DRET

P. Horster (ed.), *Communications and Multimedia Security II*

tions, which takes several years of trial and error to develop. That's why, now, since standards are mature and interoperability between constructors is solved, LAN users are quite reluctant to change from this reliable technology to another.

The main concern with the LAN to ATM transition is that these two technologies - frame broadcasting for LAN and cells switching for ATM - differ in many aspects (Truong, 1995). (1) The Protocol Data Unit size is variable for the frame-based LAN and fixed for the cell-based ATM technology. (2) The access mode is connectionless for LANs and connection-oriented for ATM networks. (3) The broadcast/multicast services are naturally supported by the LANs due to their shared-medium LAN features but are not natural in ATM networks point-to-point principle. As a consequence of all those differences, the vast base of communications applications developed for LANs appears unreusable in the ATM environment.

From all these observations, the ATM Forum* deduced the Emulated LAN (ELAN) concepts (Truong, 1995) (Newman, 1994) (Ellington, 1995), whose attractive idea is to both take advantage of the ATM technology and allow the reuse of the vast base of LANs' communications applications. ELAN is designed based on a client-server architecture which emulates LANs' applications over an ATM network, and as such enables any LANs' devices (e.g. workstations, servers, bridges, routers) to connect themselves to an ATM network and behave as if they were connected to a LAN. Thus ELANs allow several LANs to be interconnected through an ATM network and also, thanks to the ATM virtual connection concept, they allow many totally independent virtual LANs to be configured on the same physical ATM network.

Despite these ELAN advantages, many problems remain unsolved, one of them is the security problem which the ATM Forum completely ignored when writing the ELAN specifications. Now, as currently specified, ELAN specifications include many weaknesses making communications on ELANs vulnerable to heavy threats (in the sense of X800) such as masquerade, information disclosure and denial of service (UIT-T X.800, 1991). The aim of this paper is to highlight ELAN's security problems by studying a number of attacks scenarios on the ELAN architecture and by specifying the feasibility level of each attack.

The remainder of this paper is organized as follows. Section 2 gives some basic features of the ATM technology. Section 3 describes the ELAN's client-server architecture (Ellington, 1995). Section 4 analyzes several attacks and provides details on the way an attacker may proceed. Table 1 summarizes all the results. Finally, section 5 presents conclusions and directions for future work.

2 ATM FEATURES

To make the explanations below easier to understand, it is necessary to introduce first a number of ATM features concerning the ATM technology, the ATM classes of service and the connection establishment method (Vetter, 1995), (De Prycker, 1991) (Stiller, 1995).

ATM provides users with a connection-oriented transfer service. Each ATM connection is identified by a pair of identifiers, VPI and VCI, which respectively stands for Virtual Path Identifier and Virtual Channel Identifier. Each data flow's information unit, also called ATM cell, bears its respective connection's identifiers so that ATM makes it possible to multiplex multiple data flows of different connections over the same support. Also, it should be known that VPI/

*. The ATM Forum is an international consortium whose goal is to accelerate the use of ATM products and services through the development of interoperability specifications and the promotion of industry cooperation.

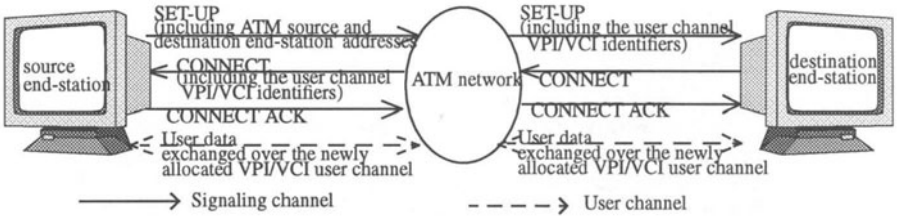

Figure 1 ATM signaling messages exchanged at call set-up.

VCI identifiers have only local significance across a particular link and have to be remapped, as appropriate, at each switch thanks to VPI/VCI mapping tables.

From the user's point of view, the ATM network is expected to provide some Quality of Service (QoS) suitable for each of his connection. Four ATM classes of service have been pre-defined. The CBR (Constant Bit Rate) and VBR (Variable Bit Rate) classes guarantee users a QoS defined in terms of delays and cell loss ratio. Both classes require ressource reservation from the ATM network for all the connection duration. In contrast the ABR (Available Bit Rate) class only guarantees cell loss ratio and the UBR (Unspecified Bit Rate) class provides no QoS guarantees. Since the ABR and UBR classes do not need any ressource reservation*, they appear suitable for supporting bursty traffic, contrary to the CBR or VBR classes which, if used, will cause bandwidth under-use.

User data communications in ATM network takes place after the set up of an ATM connection, which is based on signaling messages exchange. The typical point-to-point scenario is shown in Figure 1. First, the source end-station issues a call request to the ATM network by transmitting a SET-UP message containing the ATM addresses of the source and destination end-stations. Then the ATM network selects the appropriate end-to-end path ; it allocates a VPI/VCI virtual channel (user channel) designed to carry the end-users' data to each end-station ; finally it forwards the SET-UP message with the additional user channel's VPI/VCI information to the destination end-station. In case of call acceptation, the latter sends back a CONNECT message that the ATM network retransmits to the source end-station along with the user channel's VPI/VCI information. Once a final CONNECT ACK message is transmitted across the network, both end-stations are allowed to transmit their data on the newly-allocated user channel.

3 LAN EMULATION DESCRIPTION

The Emulated LAN (ELAN) function is to emulate a LAN on top of an ATM network, that is, to emulate the LAN datagram service, including multicast and broadcast, over ATM. In the ATM Forum specifications, the LAN Emulation service is realized by inserting an additional layer (the "ELAN entity" layer) between the ATM Adaptation Layer AAL5 (middle part of Figure 2) and the IEEE 802.2 Logical Link Control layer LLC (left part of Figure 2). Within that ELAN model (right part of Figure 2), since the IEEE upper layers behave as if the network was a LAN and as such require that the lower layers provide all the classical LAN communications applications, the ELAN entity layer has to adapt the LAN frames coming from the upper layers to the ATM cells, and vice versa. To do that, the ATM Forum has defined four specific servers

*. Actually a Minimum Cell Rate (MCR) can be specified for ABR.

(see section 3.1) enabling the ELAN entity layer to process the broadcast frames and to map the MAC addresses used by the IEEE upper layers to ATM addresses.

To make the ATM network used by the ELAN as efficient as possible, it is essential to define appropriate ATM parameters, and the class of service in particular. Since the LAN traffic is bursty and unpredictable by nature (see section 2), the ABR and UBR classes of service appear suitable for ELAN.

In this section, ELAN concepts are briefly described. See section 3.1 for the client-server architecture description and section 3.2 for ELAN functions.

3.1 Client-server architecture

The Emulated LAN follows the client-server architecture model as depicted on Figure 3. In particular, Figure 3 shows that multiple ELANs may coexist simultaneously on the same ATM network and that each Emulated LAN includes a number of clients and three servers - a LAN Emulation Server, a Broadcast and Unknown Server and a LAN Emulation Configuration Server - whose respective functions are hereafter described.

- The LAN Emulation Client (LEC).

Any facility (workstation, bridge, router, server, etc) directly connected to an ELAN has a basic LEC component which is built upon the ELAN model of Figure 2. The LEC component allows these facilities (later referred to as "LECs") to communicate through the ATM network. However, prior to any transmission, the LECs have to successfully join an ELAN, i.e. they have to successively connect themselves to the three following servers.

- The LAN Emulation Configuration Server (LECS).

When a LEC needs to join an ELAN, it first connects itself to the LECS which accepts or refuses to assign it one or multiple ELANs according to many criteria such as the LECS's own rules, the existing ELAN configuration and the originating LEC's identity and requirements. In case of ELAN assignment, the LECS directs the LEC to the LES server responsible for that ELAN by sending back to the LEC the LES's ATM address.

- The LAN Emulation Server (LES).

The LES performs control coordination functions within a single ELAN. Firstly, the LES maintains cache tables with the MAC to ATM address mappings of all the LECs attached to that particular LES. The memory where the cache tables are stored is called the "ARP cache" memory. Secondly, it supports the LAN Emulation Address Resolution Protocol (LE-ARP) which allows

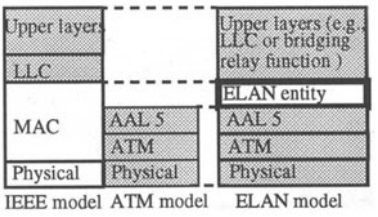

Figure 2 Layered architecture of LAN Emulation.

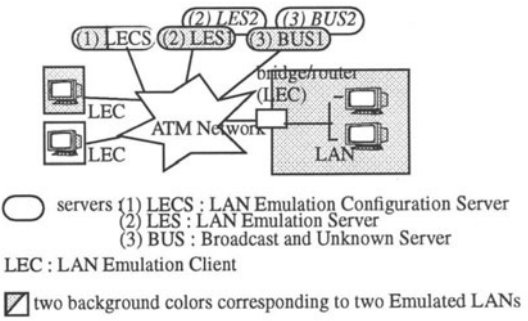

Figure 3 The client-server architecture of two ELANs sharing the same physical support.

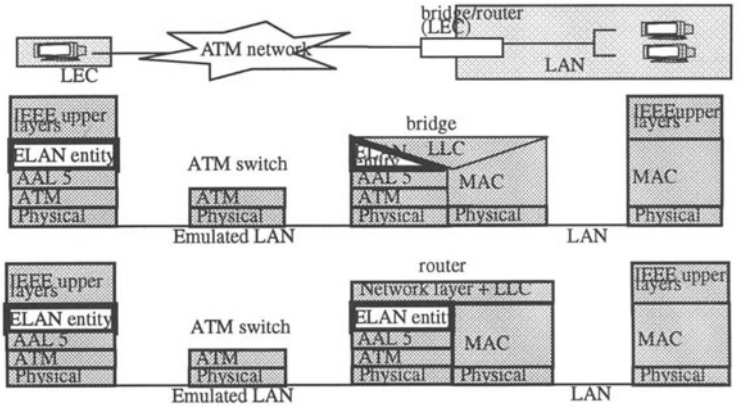

Figure 4 Interconnection of a LAN and an ATM network through a router or a bridge.

any LEC to determine the ATM address of the LEC which is responsible for a certain destination MAC address. Thus, like in the LAN environment, thanks to the LES cooperation, any network device can communicate with any other device it only knows the MAC address.

- The Broadcast and Unknown Server (BUS).

Within its ELAN, the BUS handles the legacy LAN broadcast and multicast traffics, and the unknown traffic (where the destination ATM address is "unknown") by broadcasting the traffic to all or part of its attached LECs.

3.2 ELAN functions

Prior to any data transmission through the ATM network, LECs (workstation, bridge, router) have to successively connect themselves to the ELAN servers - LECS, LES and BUS - in order to successfully join an ELAN. In particuler, LECs have to register all the MAC addresses they represent with the LES, i.e. all the MAC addresses of the workstations that are reachable through them. If the LEC is an ATM station, only one address pair (ATM address ; MAC address) needs to be registered, but if the LEC is a router or a bridge, there are as many MAC addresses to register as LAN stations connected to its LAN.

After the initialization phase completion, LECs are allowed to communicate through the ATM network. Either (1) they send data to a specific destination end-station or (2) they broadcast data to multiple end-stations. The alternatives are described below.

(1) Assume that a source LEC, say LECso, with the MAC address, say MACso address, needs to transmit data to a destination, say LECd. All the operations implied by this data transfer are performed by the LECso's ELAN entity layer. If that layer knows the LECd's ATM address, it sets up a direct connection to LECd or it re-uses a previously-opened connection. Otherwise, it sends a LE-ARP request to the LES which informs it of the LECd's ATM address and then it sets up a direct connection to LECd. The alternative is to forward all the data to the BUS which then will redirect them either to LECd if it knows the LECd's ATM address, or to all or part of its attached LECs. In either way, data will be retrieved by LECd.

As depicted on Figure 4, the procedure for transfering data across an ELAN through a router/bridge depends on whether the data transfer originates from an ATM station or a LAN station. Since the ATM network considers routers and bridges as LECs through which many LAN

stations can be reached, and since LANs consider them as normal LAN network elements, routers and bridges have to fulfill, besides their classical functions, adaptation functions - ATM/MAC address resolution and cells/frames adaptation - which are actually processed by their ELAN entity layer. It is worth noting that data transfer through a bridge requires only one address resolution (ATM/MAC addresses) whereas data transfer through a router requires two address resolutions, the classical one (MAC address/network address - typically IP) normally performed by the router and the ATM/MAC address resolution required by the ELAN method.

(2) If a LEC needs to broadcast data, its ELAN entity layer transmits its data to the BUS which, in turn, will forward them to all its attached LECs.

4 ELAN SECURITY WEAKNESSES

As currently adopted by the ATM Forum, LAN Emulation specifications provide few security features to ELANs connections. One of them is due to the ATM networks topology enabling to limit passive tapings since on ELANs unicast frames are not broadcasted as it is done on LANs but are usually sent to the destination end-station only. Another one is the physical authentication of the call originating end-station which is performed from the ingress switch and consists in checking the consistency between the ATM address claimed by the originating end-station and the switch ingress port on which the call request arrives. Considering that such protective measures remain limited and rarely implemented, communications on ELANs are vulnerable to various threats such as masquerade, information disclosure and denial of service.

In the following sections, security threats are studied and indexed into three classical categories - confidentiality, integrity and availability - which serve as the base of many documents dealing with security, such as the ATM Forum contribution (Pierson, 1995) and the ITSEC, JCSEC Security Evaluation Criteria (ITSEM, 1993) (ITSEC, 1991) (JCSEC, 1992).

Table 1 summarizes ELAN threats and for each threat provides the information - attack's origin, equipment, skillness, collusion and feasability - whose meaning is explained below:

- The *attack's origin* is the point in the network from where an attacker mounts his attack. The positions envisaged are the transmission medium (regenerator), ATM switches, ELAN servers (LECS, LES or BUS), LAN stations, ATM stations, routers or bridges.
- The *equipment* encompasses all the ressources an attacker needs to attack the ELAN. The equipment can be a workstation, an electronic device, any hardware or software tool. When "none" equipment is mentioned in table 1, it means that the attacker needs no specific equipment other than those used for network operations.
- The *skillness* is the knowledge an attacker should have to mount the attack. Three skillness levels are used: none, good and high.
- The *collusion* lists all the persons whose support is required to mount the attack. In particular, the administrator's collusion is assumed to be required each time the attacker needs to use some network operation equipments - routers, bridges, ATM switches or ELAN servers (LECS, LES or BUS) - which are assumed to be logically and physically protected to remain under the administrator's control.
- The *feasability* information indicates if the attack is possible to succeed (yes) or not (no).

4.1 Confidentiality

An attack on confidentiality occurs when an attacker acquaints himself with information in transit, which is not destined for him.

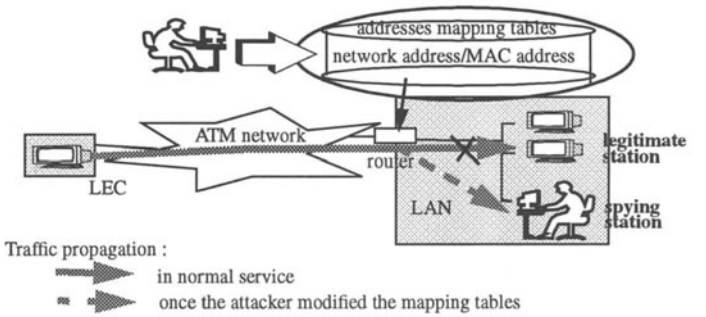

Figure 5 Connection diversion: Modifying the router mapping tables as appropriate causes all the traffic to be diverted from a LAN station onto a spying station located on the same LAN.

Three possible threats are hereafter studied:
- connection diversion
- connection eavesdropping
- improper connection.

4.1.1. Connection diversion

This attack consists in diverting the traffic onto a spying station so that an attacker can retrieve the data of interest to him and deduce their content. This section discusses two ways to perform such an attack depending on whether the attack takes place (1) after a connection set up or (2) prior to a connection set up.

4.1.1.1. Connection diversion after a connection set up

To mount this attack a radical method is to replace the legitimate station with a spying station in order to make the latter retrieve all the traffic initially sent to the legitimate station. To this end, the attacker may either cut the legitimate station's cable or disconnect it and plug a spying station instead. This attack expects no administrator's collusion but a good skillness level is required.

The attacker may also realize such a connection diversion by modifying, in the ATM switches or routers, the information used to route the traffic through the network. For ATM switches, this consists in modifying the mapping tables (see section 2) so that all the cells of the connection to spy (carrying the same VPI/VCI) are forwarded to a spying station by means of a connection intentionally set up before by the attacker. For routers (see section 3.2), this attack consists in modifying the addresses mapping tables (MAC address/network address) so that all the traffic initially sent to a network address is redirected to a spying station (see Figure 5). Note furthermore that a connection diversion realized from a router is only possible if the spying station is located on the same side of the router as the legitimate destination station.

Another alternative requiring the administrator's support is to modify the BUS server's processing in such a way that part or all the traffic going through the BUS is redirected to any spying station belonging or not to the same ELAN (cf Figure 6).

4.1.1.2. Connection diversion prior to a connection set up

Two methods (1) and (2) are studied.
- (1) The first method is to modify a LEC's processing (i.e. its microprogram) or to download a falsified LEC's microprogram so that, each time the LEC needs to set up a connection to a

destination station, say station D, its microprogram replaces in the SET UP message the ATM address of station D with the ATM address associated with a spying station. Thus, as a result of this attack, when the LEC needs communicating with station D, a connection is set up between the LEC and a spying station and since the LEC believes being connected to station D, all the traffic it sends to station D is diverted onto the spying station. Note however that mounting such an attack assumes that no protection measures are used to guarantee the software integrity of the LEC.

- (2) The second method is depicted on Figure 7 . The attacker at a spying LEC tricks his LES into thinking that his LEC represents a subnetwork with any ATM addresses he wants (cf section 3.2). He then registers with his LES, besides his own addresses pairs (the ATM address of the spying LEC ; the MAC address of the spying LEC), some additional ATM addresses pairs, specifically the addresses pair (the ATM address of the spying LEC ; the MAC address of an existing station, say LECd), if necessary, erasing the legitimate addresses pair (the ATM address of LECd ; the MAC address of LECd) from the LES. As a consequence, when the originating LEC, say LECso, needs to communicate with LECd, it first issues an ARP request to the LES which sends back the ATM address of the newly registered addresses pair instead of the legitimate LECd's ATM address. LECso thus sets up a direct connection to the spying LEC instead of LECd and since LECso believes being connected to LECd, it sends all its data initially addressed for LECd to the spying LEC which can then retrieve and analyze them.

Note that the second attack (2) can only succeed if the spying station and the station to spy (LECd) share the same ELAN, i.e. if they are attached to the same LES. As such, the spying station can be any LECs of the ELAN, i.e. ATM stations, routers or bridges, the most suitable of which are ATM stations since attack (2) does not use any specific routers/bridges' properties, and since mounting it from routers/bridges requires the administrator's support.

Also, instead of remotely modifying the LES's ARP cache memory from any LEC as described on Figure 7, the alternative is to perform such modifications directly on the LES concerned, so that the attacker may redirect the traffic of interest to him to a spying station belonging or not to the same ELAN.

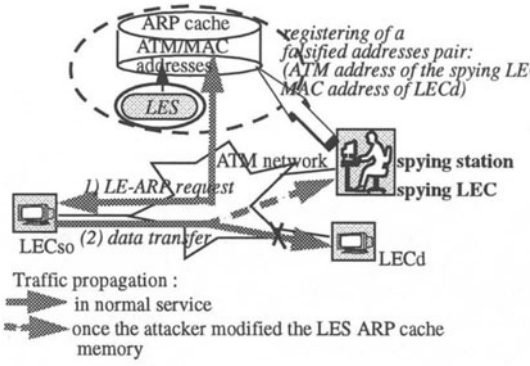

Figure 6 Connection diversion: If the attacker registers a falsified MAC/ATM addresses pair with the LES, he causes the traffic to be diverted from LECd onto his own station ((1)+(2)).

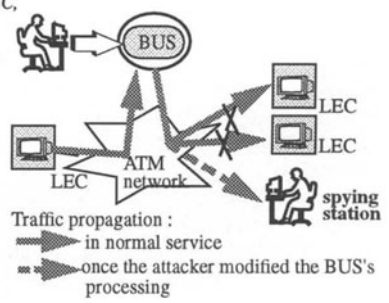

Figure 7 Connection diversion: Modifying the BUS's processing as appropriate causes all the traffic going through the BUS to be redirected to a spying station.

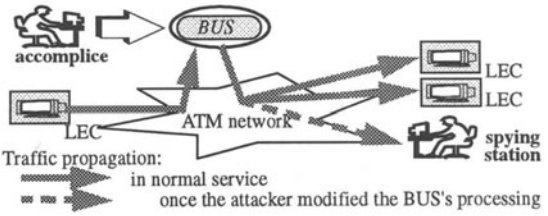

Figure 8 Connection eavesdropping: Modifying the BUS's processing as appropriate causes the traffic passing through the BUS to be duplicated to a spying station.

4.1.2. Connection eavesdropping

This attack assumes that an attacker positions himself at a point in the network from which he can observe the traffic, i.e. ATM cells (cf section 2) and retrieve all the ATM cells of the connection of interest to him (same VPI/VCI) so that the content of the messages can be inferred. This assumes that the attacker knows which VPI/VCI user channel has been assigned by the network to that connection. For instance, he may have learnt it as a result of a previous eavesdropping effected when the connection was being set up.

The attacker can position himself at any intermediate systems - ATM switches, routers, bridges and BUSs - through which a large part of the traffic passes and then he can eavesdrop the desired connection by filtering the traffic on the VPI/VCI identifiers. Also, he can mount his attack from the transmission medium but, as explained in (Voydock, 1983), practical realization significantly varies with the medium type (coax cable, optic fiber, etc).

Another attack directly results from the fact that ELANs emulate the LANs communication applications and that those applications are not secure. In particular, broadcasting which is naturally performed in LANs thanks to the shared-medium is emulated on ELANs through the BUS server, so that in both LANs and ELANs contexts, an attacker can eavesdrop all or part of the broadcast traffic by properly modifying the filter of his LAN station or his ELAN LEC (ATM station, router or bridge). However, whereas in LANs context, eavesdropping applies to all the traffic passing through the LANs, in ELANs context, it is limited to the broadcast/multicast/unicast traffic transmitted by the BUS.

Another ELAN-specific solution is to modify the BUS's processing in order to make it set up, if required, some additional connections to a spying station and then duplicate all or part of the traffic passing through it to the spying station (cf Figure 8).

4.1.3. Improper connection

An improper connection occurs when an attacker at a station (LAN station or LEC) succeeds in joining an ELAN he is not normally authorized to join by impersonating an authorized station to each ELAN server contacted (LECS, LES and BUS). Illegitimately joining an ELAN is very attractive for the attacker since he can then receive the ELAN broadcast traffic he can analyze based on the method of section 4.1.2 and also he can connect himself to any LEC of the ELAN by retrieving first the LEC's ATM address from the LES.

This attack consists in directly emitting some bogus messages on the network, and not in affecting the integrity of the data in transit like in section 4.2.1. Hereafter two forms of improper connection are studied, one originating from an ELAN, the other from a LAN station.

If located on an ATM LEC (LEC stations, ELAN servers, routers, bridges or ATM switches), an attacker performs this attack at connection set up by emitting bogus SET UP messages

(see section 2) with a falsified source ATM address. Such bogus SET UP messages are obtained either by synthesis or after having modified the LEC's characteristics (its ATM address). However, such masquerade attempt may fail if the ATM ingress switch checks the consistency between the port number from where the SET UP request comes and the ATM address claimed inside the SET UP message (see Figure 9). To make this attack undetectable by the ingress switch, a solution is to disconnect the station to impersonate and to plug a spying station instead.

In a LAN environment, this attack consists in emitting bogus frames either synthesized or obtained after having changed the LAN station's characteristics (its MAC address). Contrary to what happens in ELANs, this attack affects not only the first message (here the first frame) sent to the destination to trick but also all the following frames since they all carry the MAC source and destination addresses. As for ELANs, it is possible to detect such an attack from routers/bridges by comparing the network/link layer source address claimed in the packets/frames against the router/bridge's configuration (Kaufman, 1995), but this detection is not generally done and, if implemented, is limited to specific cases. For instance, if the attacker impersonates a station of the same LAN, no detection based on the source address can occur ; all the frames will be forwarded by the routers or bridges, as ordinary done. On the other hand, if the attacker impersonates a station of another LAN or a LEC, detection is possible.

4.2 Integrity

An attack on integrity occurs when an attacker succeeds in injecting, modifying or erasing information in transit. It should be noted that, even if most of the attacks on integrity such as those described in sections 4.2.1 and 4.2.2 result in information disclosures, attacks on integrity should not be confused with attacks on confidentiality since the latter are passive attacks which do not affect the integrity of the data in transit, i.e. they entail no data modifications.

Three possible threats are hereafter studied:

- masquerade at a connection set-up
- masquerade once the connection is set-up
- data injection.

4.2.1. Masquerade at a connection set-up

This attack assumes that two parties wish to communicate. Then the attack consists in modifying the signaling messages in transit as appropriate, so as to force the connection to be set up between a malicious station and one of the two parties. This attack is known as a masquerade since the party which remains connected to the malicious station believes it is connected to the other party.

Considering the connection set up procedure illustrated on Figure 1, there are two ways of mounting such an attack, either by replacing in the SET UP message the ATM destination ad-

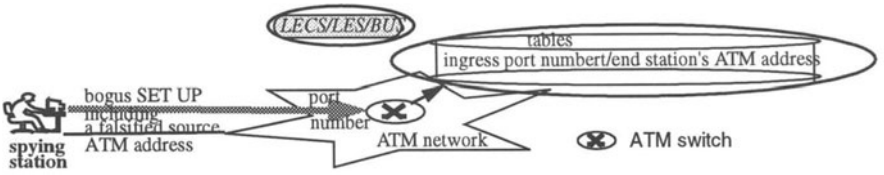

Figure 9 Improper connection: The ATM ingress switch may detect the masquerade attempted by the spying station if it checks the consistency between the incoming port number and the ATM source address included inside the SET UP message.

dress with the ATM address of the attacker's station, or by replacing the VPI/VCI identifiers of the SET UP or CONNECT message with the VPI/VCI of another connection previously set up by the attacker.

Such an attack can theoretically be mounted from any intermediate system - ATM switch, regenerator, transmission medium - by inserting a cells filtering/modification device, but actually this attack seems infeasible today because the current hardware is not efficient enough compared to the ATM performance.

4.2.2. Masquerade once the connection is set-up

This attack assumes that a connection is already set up between two parties. An attacker then masquerades as one of the two parties. To this end, as depicted on Figure 10, an accomplice to the attacker is at a point on the network, either on a LAN or the ATM network and modifies the information in transit so that all or part of the data in transit are redirected to a spying station.

If located on the ATM network (ATM switches, transmission medium), the accomplice may redirect all the data cells exchanged over the same connection (same VPI/VCI) to a connection previously set up by the attacker by employing one of the two following methods. (1) By injecting a cells filtering/modification device, the accomplice may filter the traffic on VPI/VCI identifiers and adequately modify the VPI/VCI fields. (2) Providing that no protection measures guarantee the integrity of the ATM switches' microprograms, the accomplice may then modify an ATM switch's microprogram or download a falsified one instead so as to make it modify the VPI/VCI identifiers as appropriate. It appears that attack (1) is infeasible because such a cells filtering/modification device requires such a performance level that it can not be designed with current techniques and attack (2) is technically feasible since it affects the ATM switch's processing itself so that, unlike attack (1) it makes it possible to modify cells simultaneously with their usual switching treatment.

If located on a LAN (i.e. a router/bridge), the accomplice may redirect all the data of the same connection identified by the addresses pair (source address ; destination address) to a spying station by replacing the network/MAC destination address of the legitimate destination with the network/MAC address of the spying station. Like in section 4.1.1, it is necessary for the spying station to be located on the same side of the router/bridge as the legitimate destination station.

4.2.3. Data injection

This attack consists in injecting some user data (ATM cells or frames depending on which network - ATM network or LAN - the attacker resides) over a connection in process. This aims

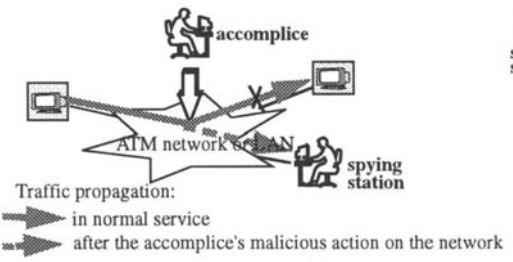

Figure 10 Masquerading once the connection is set up: Appropriate modifications of the information exchanged over the network causes the traffic to be redirected to a spying station.

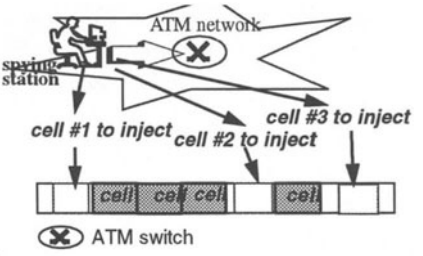

Figure 11 Data injection: Located on an ATM switch, an attacker injects cells #1, #2 and #3 into a flow of cells while being careful that no legitimate cells are erased.

at disrupting the connection, rather than misleading the destination end station since most of the injected cells are detected by the destination end station's upper layers and the detection processing is time-consuming.

From the ATM network (i.e. an attacker is positionned at an ATM switch or the transmission medium), the attack consists in injecting some ATM cells with the same VPI/VCI identifiers as these of the connection to disrupt (see Figure 11) without erasing any legitimate cells. Given the ATM performance, this attack seems infeasible today since current hardwares are not fast enough to be able to inject cells at the right positions in the ATM cells flow.

From a LAN (i.e. LAN station or a bridge/router), the attack consists in injecting some packets/frames with the same network/link layer source and destination addresses than these of the connection to disrupt. Either the attacker is at a LAN station, then he generates packets/frames according to the method of section 4.1.3 and injects them on the LAN, or the attacker is at a router/bridge, then he generates packets/frames with a specific software and injects them into the router/bridge which regards and processes them as legitimate packets/frames.

4.3 Availability

An attack on availability, usually called a denial of service, consists in making the ressources of the network unavailable for the authorized users.

Two possible attacks are hereafter studied:

- repetitive and unauthorized access to ressources
- falsified information presentation to ATM switches, routers or bridges.

4.3.1. Repetitive and unauthorized access to ressources

This attack occurs when an attacker repetitively attempts to access ressources on the network by connecting himself to ELAN servers, LEC or LAN stations many times. In this manner, the attacker may cause a terminal to overload so that the terminal's ressources are no longer available to other users. Also he may seriously disrupt the ATM network since all the ELAN traffic is either UBR or ABR (see section 3). Indeed, ELAN connections all share the network ressources (i.e. bandwidth) and so the more traffic a connection sends, the less bandwidth there is available for the other connections and the less performant the other connections are. However, note that only attacks through the BUS can totally overload the ATM network and that a solution to thwart this is to include a protection mechanism into the BUS so that the attack's impact remains limited to the broadcast traffic.

The attacker can mount his attack from many positions on the network, but LEC stations appear as the most suitable ones since ELAN servers, routers and bridges require obtaining first the administrator's support and LAN stations provide no direct access to ELAN servers so that the number of attacks possible to mount are limited. On the other hand, ATM switches or transmission medium are unsuitable because mounting this attack would require data injection in the ATM traffic, which is not feasible today as indicated in section 4.2.3.

4.3.2. Falsified information presentation to ATM switches, routers or bridges

This attack consists in overloading an ATM switch or router/bridge by sending them falsified information (e.g. destination addresses) which will disrupt their activity or preclude them from processing the legitimate incoming traffic.

An ATM switch can be disrupted by incoming bogus SET UP messages (e.g. with a falsified ATM destination address) which will cause the ATM switch to waste a lot of time consulting its routing tables vainly. This attack can be managed from a LEC station, any ELAN server, a

bridge, a router, an ATM switch or the transmission medium, the most suitable of which is the LEC station for the same reasons as those discussed in section 4.3.1.

Disrupting a router/bridge assumes that an attacker is at a LAN station and sends some bogus messages (e.g. with a falsified packet/frame destination address) to the ATM network so that the router/bridge wastes time trying to find the corresponding destination location and may generate dense traffic on the ATM network if it contacts the LES (ARP request) or the BUS (for brodcasting cells over the network).

Table 1 Threats analysis results

threat's type	attack's origin	equipment	skill nes	collusions	feasi bility
Connection diversion - attack (4.1.1.1)	transmission medium	workstation	good	none	yes
	ATM switch/routers	none	none	administrator	yes
	BUS	none	good	administrator	yes
Connection diversion - attack (4.1.1.2 - 1)	LEC station	none	good	none	yes
Connection diversion - attack (4.1.1.2 - 2)	LEC station	none	good	none	yes
	router/bridge	filtering device+packets/cells injecting device	good	administrator	yes
	LES	none	good	administrator	yes
Connection avesdropping	ATM switch/router/ bridge/BUS	workstation+filtering device	good	administrator	yes
	transmission medium	diverse equipment	diverse	none	yes
	LEC station/LAN station	workstation	good	none	yes
	BUS	workstation	good	administrator	yes
Improper connection	LEC station/LAN station	workstation	good	none	yes
	router/bridge	packets/cells injecting device	good	administrator	yes
	LEC station/LES/BUS	none (software)	good	administrator	yes
	transmission medium	workstation	good	none	yes
Masquerade at a connection set-up	transmission medium/ ATM switch	cells filtering/modification device	good	none/administrator	no
Masquerade once the connection is set-up	transmission medium	(1)cells filtering/ modification device	good	none	no
	ATM switch	(1) cells filtering/ modification device/ (2) microprogram modification or downloading	good	administrator	(1) no/ (2) yes
	router/bridge	packets/cells filtering/modification device	good	administrator	yes

Table 1 Threats analysis results

threat's type	attack's origin	equipment	skill nes	collusions	feasi bility
Data injection	transmission medium/ ATM switch	cells injecting device	high	none/admi-nistrator	no
	LAN station	workstation	good	none	yes
	router/bridge	packets/cells injec-ting device	good	administrator	yes
Repetitive and unauthorized access to ressour-ces	LEC station/LAN sta-tion	workstation	none	none	yes
	router/bridge	packets/cells injec-ting device	good	administrator	yes
	LECS/LES/BUS	none (software)	good	administrator	yes
	transmission medium/ ATM switch	cells injecting device	high	none/admi-nistrator	no
Falsified informa-tion presentation to ATM switches	LEC station/LAN sta-tion	workstation	none	none	yes
	transmission medium/ ATM switch	cells injecting device	high	none/admi-nistrator	no
	router/bridge	packets/cells injec-ting device	good	administrator	yes
	LECS/LES/BUS	none (software)	good	administrator	yes

5 CONCLUSION

This paper lists a number of security attacks that could be mounted on ELANs connections in an ELAN architecture composed of the mixed ATM and traditional LAN technologies. The security analysis end results are resumed on table 1 which gives information on the attack feasibility level, the equipment type to use, the skillness and collusions required depending on which attack's type is performed and from which location. Note that all the assessments relative to the threats realization - the feasibility and the skillness level - are based on the efficiency expected from the current technology and my own point of view, so they may only be considered as a rough guide.

In particular, it should be noted that most of ELANs security weaknesses are inherited from legacy LANs and ATM networks security weaknesses due to non-secure connections. Actually very few of them are ELAN's architecture specific.

Among the attacks studied, some are not currently feasible because of today's hardware inefficiency. However, on my opinion, it appears interesting and useful to list all the theoretically possible attacks that may occur on ELANs because hardware's performance improvements will surely make those attacks feasible in the future.

This article does not aim at providing any protective means to secure ELANs. However a study is under way and aims at integrating security services - authentication, access control, confidentiality, integrity, etc - into ELANs architecture extending known models such as IEEE 802.10 (IEEE 802.10-A, 1989) (IEEE 802.10-B, 1990).

6 ACRONYMS

- ARP : Address Resolution Protocol
- BUS : Broadcast and Unknown Server
- ELAN : Emulated LAN
- LAN : Local Area Network
(LAN also designates a traditional LAN such as Ethernet and Token Ring)
- LE-ARP : LAN Emulation Address Resolution Protocol
- LEC : LAN Emulation Client
- LES : LAN Emulation Server
- LLC: Logical Link Control
- MAC : Media Access Control
- VCC : Virtual Channel Connection
- VCI : Virtual Channel Identifier
- VPI : Virtual Path Identifier.

7 REFERENCES

ATM Forum (1994) ATM User-Network Interface Specification, version 3.1.

Biagioni, E., Cooper, E. and Sansom, R. (1993) Designing a practical ATM LAN. *IEEE Network*, mars 1993, 32-39.

De Prycker, M. (1991) Asynchronous Transfer Mode: Solution for broadband ISDN. Ellis Horwood, New York.

Ellington (1995) LAN Emulation Over ATM, version 1.0, ATMFORUM/94-0021.

IEEE 802.10 (1989) Standard for Interoperable Local Area Network (LAN Security (SILS) - Part A - The Model, December 1989.

IEEE 802.10 (1990) Standard for Interoperable Local Area Network (LAN Security (SILS) - Part B- Secure Data Exchange", January 1990.

ITSEM (Information Technology Security Evaluation Manual) - Version 1.0 - September 1993.

ITSEC (Information Technology Security Evaluation Criteria) - Version 1.2, Luxembourg, June 1991.

JCSEC (Japanese Computer Security Evaluation Criteria) (1992) Functionality Requirement, Japan Electronic Industry Development Association, Draft Version 1.0, August 1992.

Jeffries, R. (1994) ATM LAN Emulation: the inside story. *Data communications*, September 1994.

Kaufman, C. Perlman, R. and Speciner, M. (1995) Network Security, Private communication in a public world, Prentice Hall, Englewood Cliffs NJ 07632.

Newman, P. (1994) ATM Local Area Networks, *IEEE Communications Magazine*, March 1994.

Pierson, L. G. and Tarman, T.D. (1995) ATM Forum / 95-0137 - Requirements for Security Signaling.

Stiller, B. (1995) A survey of UNI signaling systems and protocols for ATM networks, *ACM SIGCOM*, Vol 25 n° 2, 21-33.

Truong, H.L. Ellington, W.W. Jr., Le Boudec, J.Y. Meier, A.X. and Pace, J.W. (1995) LAN Emulation on an ATM network, *IEEE Communications Magazine*, May 1995.

UIT-T X.800 (1991) Data communication networks ; open systems interconnection (OSI) ; security, structure and applications. Security architecture for open systems interconnection for CCITT applications.

Vetter, R.J. (1995) ATM concepts, architectures, and protocols, *Communications of the ACM*, Vol. 38, n° 2, 30-38 109.

Voydock, V.L. and Kent, S.T. (1983) Security mechanisms in high-level network protocols, *ACM Computing Surveys*, Vol 15 n° 2, 135-171.

8 BIOGRAPHY

Maryline LAURENT obtained an engineering degree in electronics from the French graduate School ENSERB in 1993 and an advanced degree in Telecommunication Network Management from the Franco Polish School of New Information and Communication technology (EFP). Now she is a PhD student within the Networks and Multi-media Services Department (RSM) of Telecom Bretagne (a French Graduate School of Telecommunications Engineering), Rennes, France, since December 1994. She works on networks security, mainly in the ATM field, where her job consists in securing communications over ATM networks.