The following paper was originally published in the
Proceedings of the 7th USENIX Security Symposium
San Antonio, Texas, January 26-29, 1998

Securing ‘Classical IP over ATM Networks’

Carsten Benecke and Uwe Ellermann
Universitat Hamburg

For more information about USENIX Association contact:

1. Phone: 510 528-8649
2. FAX: 510 548-5738
3. Email: office@usenix.org
4. WWW URL: http://www.usenix.org/

Securing 'Classical IP over ATM Networks'

Carsten Benecke Uwe Ellermann
*DFN-FWL**
Firewall-Laboratory for High-Speed Networks
Fachbereich Informatik, Universität Hamburg
Vogt-Kölln-Str. 30
D-22527 Hamburg
Phone: +49-40-5494-2262
Fax: +49-40-5494-2241
{*Benecke,Ellermann*}*@fwl.dfn.de*

Abstract

This paper discusses some security issues of 'Classical IP over ATM' networks. After analyzing new threats to IP networks based on ATM, security mechanisms to protect these networks are introduced. The integration of firewalls into ATM networks requires additional considerations. We conclude that careful configuration of ATM switches and ATM services can provide some level of protection against spoofing and denial of service attacks. Our solutions are intended to be applied to current IP over ATM networks and do not require any changes to these protocols or additions to current switch capabilities.

1 Introduction

The trend towards ATM networks requires a reexamination of network security issues. ATM is based on the concepts of switched virtual connections and fixed length cells, this contrasts with the connectionless, shared medium, broadcast networks frequently referred to as "legacy networks". These conceptual differences required the development of new protocols like 'Integrated Local Management Interface' (ILMI) [14] and 'Private Network-Network Interface' (P-NNI) [15]. These specifications have not yet been subjected to a thorough security analysis.

[0]This work was funded by the DFN-Verein (Association for the promotion of a German Research Network) and Deutsche Telekom under project number: DT10.

In order to make the use of IP in ATM networks, additional services, such as the ATMARP server[1], had to be introduced. This also introduced new risks, which must be investigated before "Classical IP over ATM networks" can be used in critical environments.

Typically cryptography is used in networks to provide authentication, integrity, and confidentiality. Integration of cryptographic mechanisms into ATM networks is currently a research topic [7, 16], but none of these mechanisms have been standardized.

We provide solutions for most identified security problems. Other security flaws can be mitigated. Many improvements are possible by manual configuration of ATM hardware and changes to the bahaviour of the ATMARP server. Thus there is no need to provide proprietary protocol extensions and security can be achieved within the current standards for IP over ATM. Moreover the solutions do not require additions to current switch capabilities like cryptographic authentication for signaling.

2 Attacks on "Classical IP over ATM Networks"

The model for the following security analysis of a "Classical IP over ATM" (CLIP) LAN consists of

[1]The ATMARP (ATM Address Resolution Protocol) as specified in [10] is required for resolving IP addresses into ATM addresses and vice versa. Unlike ARP [11] which uses broadcasts to resolve addresses a server is required in non broadcast multiple access networks such as ATM.

two logical IP subnets (LIS) connected to each other by a firewall. The firewall is used to divide the LAN into a critical subnet containing valuable data called the "internal network" (192.168.15.0) and a public subnet connected to the world called the "external network" (192.168.16.0). The TCP/IP traffic between the networks is examined by the firewall. The type of services provided and the access control policy enforced by the firewall will not be discussed here. Currently no "native ATM" applications need to be supported, but the concept must not prohibit extensibility.

One possible setup for the above requirements is shown in figure 1. This configuration has two major drawbacks. Firstly, it does not allow for the possibility of running a "native ATM" application using both of the networks, as the firewall only provides TCP/IP services. Secondly, as this configuration requires the use of two ATM switches, expensive equipment is wasted.

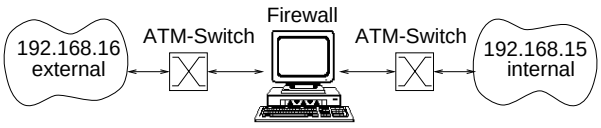

Figure 1: Gateway-Firewall in an ATM Network

As ATM allows for multiple *virtual networks* on the same physical network (i.e. on the same ATM switch) a similar setup can be built with just one ATM switch (see fig. 2).

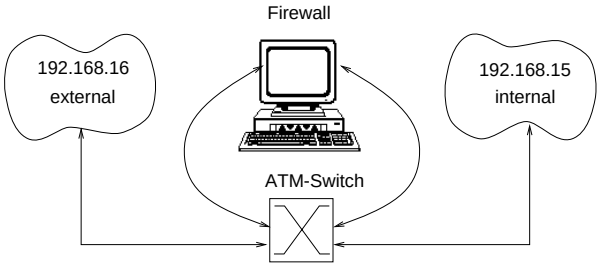

Figure 2: Gateway Firewall with one ATM Switch

The configuration of multiple virtual networks using one ATM switch is a simple task, but configuring this setup in a secure mode requires a deep analysis of the associated risks. The configuration with one ATM switch allows "native ATM" traffic to bypass the TCP/IP firewall. Unfortunately, "native ATM" connections can also be used to send IP datagrams. By circumventing the local Classical IP stack an attacker can send IP datagrams to systems in the other virtual network without traversing the firewall. The associated security risks and possible solutions are discussed in the following sections.

2.1 IP Spoofing over ATM Connections

IP spoofing attacks have been well understood for many years [2]. Essentially, IP spoofing means sending IP packets with faked IP source addresses. Services that use IP source addresses for authentication can be easily exploited by this attack.

IP spoofing is possible in 'Classical IP over ATM' (CLIP) networks. Whenever the ATM address of a server is known, an attacker can establish a direct ATM connection[2] to that host. The attacker can now register with the IP address of a trusted host by sending a carefully crafted 'InATMARP-Reply' message over this connection. After successful registration, spoofed IP packets can be sent over this connection. Moreover, due to the "ATMARP-Cache poisoning", the attacked server will send reply packets back to the attacker on the same ATM connection.

This kind of attack is possible, because the peers do not authenticate each other in a reliable manner. Moreover section *6.4 ATMARP Client Operational Requirements* of RFC 1577 [10] explicitly requires, that CLIP clients process 'InATMARP-Requests' and 'InATMARP-Replies' in order to update their local address resolution tables.

In contrast to legacy LANs (e.g. Ethernets) there is no need to attack the host whose address has been used[3]. Because the server sends its segments over the virtual connection to the attacker, the trusted host will not notice that its address has been used by another system.

Furthermore there is no need for the attacker to guess the TCP sequence number of the server. The server will use the established virtual connection to

[2] Note that the number of intermediate switches is irrelevant as long as a virtual connection between attacker and server can be established.

[3] In the case of a routed broadcast LAN the attacker also has to make sure that the host, whose IP address the attacker uses for spoofing, will not reset the spoofed connection. This can be done by flooding it with communication prior to the spoofing attack, so that the client is too busy to respond to the packets from the server.

send its segments to the attacker. So all other packets destined to the trusted host will also be sent to the attacker (see also section 2.3).

In summary, IP spoofing is easier to accomplish in ATM based networks and harder to detect. It can also be considered more dangerous, as simple countermeasures, for example requiring an IDENT [9] query before access is granted, can be spoofed more easily than in "legacy networks".

The figure 3 shows the time-sequence diagram of a successful simulated attack in a test environment. The attacker (A) pretends to be the host (192.168.15.A) and registers itself by sending an 'InATMARP-Reply' to host (B). In order to verify that the spoofing is successful, an 'ICMP-ECHO-Request' is used to test the established connection.

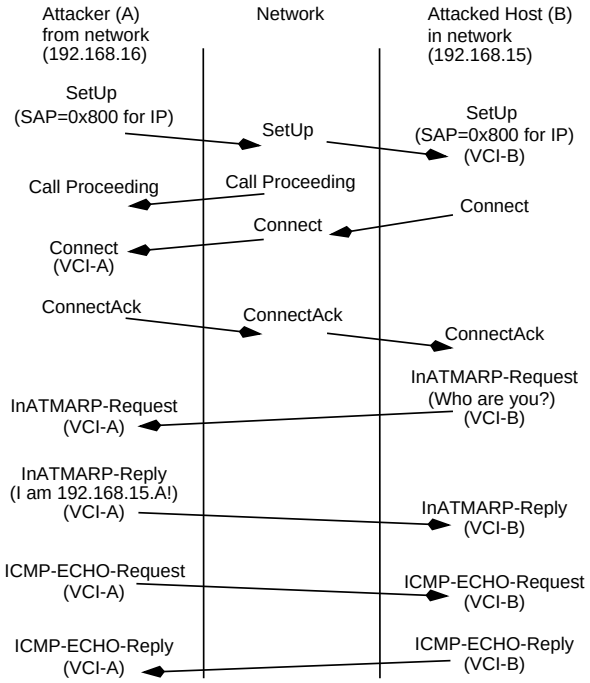

Figure 3: ATM based Spoofing Attack

It should be noticed that the attack is not detectable unless the host (B) verifies the 'InATMARP-Reply' by contacting a trusted ATMARP server (see section 3.1 for a discussion on securing the ATMARP server).

This attack is not restricted to hosts in the same LIS. Any host to which a direct ATM connection can be opened can be attacked. Routers that connect different LISs can be bypassed if the underlying ATM network allows for a direct ATM connection between hosts in different LISs. It is therefore important to point out that filters in these routers cannot be used to protect against this type of IP spoofing attacks. Neither a firewall nor an inter LIS router will have access to the datagrams because all hosts of the same LIS always use direct (non routed) connections. Moreover if the attacked host subsequentially wants to open TCP connections to the host (e.g. an IDENT query [9]), the address of which has been used for spoofing, a typical implementation will use the established virtual connection to the attacker. This would also enable the attacker to perpetrate 'Man in the Middle' attacks.

2.2 'Denial of Service' by Allocating IP Addresses of a LIS

The knowledge of the ATM address of an ATMARP server enables an attacker to scan the whole LIS IP address range. The attacker establishes a virtual connection to the ATMARP server and queries all IP addresses of interest. The server either replies with *'ATMARP_NAK'* or with the corresponding *<IP address,ATM address>* binding, providing all information an attacker needs for the denial of service attacks described below.

The attacker may now register itself with any unused IP address of the LIS. As every IP address can only be registered once, this will prevent hosts that were temporarily offline from registering themselves, if the attacker succeeds in allocating their IP address. The LIS member will be unable to use CLIP services as long as its IP address is registered with the attacker. Moreover the attacker may wait for clients to go offline by periodically verifying if a learned binding is still in the ATMARP servers cache.

Instead of reserving a random IP address in the subnet, the attacker only reserves the addresses of those LIS clients which are known to be temporarily offline. This puts the attacker in the position of being able to perpetrate very efficient attacks. Some additional aspects of ATMARP server based denial of service attacks are discussed in [1].

This kind of attack is possible, because any host that is able to establish an ATM connection to the ATMARP server, may register various *<IP address,ATM address>* bindings without authentication. An at-

tacker only needs the ATM address of an ATMARP server in order to establish a virtual connection. Since the ATM address of the attacker is not used for path finding during signaling, the attacker may select any ATM address during connection establishment[4] with the ATMARP server. This makes it even harder to trace the origin of an attack, as the address information in the ATMARP server cannot be trusted.

2.3 'Man in the Middle' Attacks

Whenever a LIS member queries the ATMARP server for the corresponding ATM address of an IP address that has been allocated by an attacker, the ATMARP server will reply with an *<IP address,ATM address>* binding which has been supplied by the attacker. This enables the attacker to carry out various 'Man in the Middle' attacks, since the LIS member will connect to the attacker if the attacker has supplied his own[5] ATM address.

2.4 'Denial of Service' due to Bandwidth Allocation

Another problem arises from "native ATM" applications. These applications can use ATM specific services, e.g. allocating a constant bit rate (CBR) for their virtual connections. Since CLIP usually uses the 'best effort' service of ATM (unspecified bit rate connections) any CBR based communication has higher priority than CLIP traffic. These "native ATM" applications could accidentaly allocate the whole bandwidth of an intermediate switch. This results in an denial of service for IP based applications.

If an attacker uses bandwidth reservation, it suffices to signal the desired CBR rate. After establishing the connection there is no need to send any data over the virtual channel. All intermediate switches have agreed to the bandwidth allocation, so they cannot offer this bandwidth to other connections. From the attacker's point of view, this attack is very inexpensive, as there is no need to send (dummy) data with the allocated rate. Other traffic classes, such as variable bit rate (VBR), can also be used for this attack.

Moreover this kind of attack is hard to trace. The reservation of resources is a common procedure in ATM networks so that each intermediate switch may have to refuse the establishment of a connection due to insufficient resources. If a switch refuses the establishment of a CBR or VBR CLIP connection, the client host cannot detect whether this is due to normal protocol processing or vicious bandwidth allocation. There is also no way to deduce an attack by bad performance over an unspecified bit rate (UBR) connection since the throughput of an UBR connection may degrade at any time due to normal resource allocation in an ATM network.

2.5 'Denial of Service' due to Excessive Connection Establishment

Another kind of ATM based denial of service attack reserves all available virtual connection identifiers of CLIP hosts by establishing many connections to one machine. If this host tries to allocate an identifier for a CLIP connection there may be none left. Again this attack is ATM specific, because there is no way to send any datagrams unless an ATM connection has been established to the destination or a router. If this connection cannot be established due to insufficient virtual connection identifiers (VCID) it is not possible to access the desired CLIP service. The UNI 3.1 interface limits the maximum number of connections[6] to 2^{24}. It seems that this huge number of simultaneous connections is enough even for a big server but a typical client implementation of an ATM device driver limits the number of VCIDs to a considerable smaller number of 1024 or 2048. This limit of 2048 connections can be reached by an attacker trying to block a host from communication.

[4] RFC 1577 [10] section 5 "Overview of Call Establishment Message Content" requires the originator to supply a "Calling Party Number" Information Element (IE). It is expected to be an ATM address that really belongs to the calling system, but of course this IE can be faked like any other unauthenticated information.

[5] This will not necessarily identify the attacker's host because he may have registered an additional ATM address at his local switch (see also section 2.6).

[6] The ATM cells at the 'User to Network Interface' have 8 bits for virtual path identification and 16 bits for virtual channels. This allows for a theoretical total of 2^{24} different virtual connections at any time between host and switch.

2.6 ILMI based Attacks

The 'Integrated Local Management Interface' (ILMI, [14]) is used at the interface between switch and workstation. The protocol is based on the 'Simple Network Management Protocol' (SNMP). Whenever a workstation boots, it may automatically configure its ATM address by contacting the switch with ILMI messages. The switch usually supplies a 13 octet address prefix which is common to all hosts that are connected to the switch.

A problem arises by the fact that ILMI does not provide a mechanism for the authentication because the underlaying SNMP only uses clear text pass phrases[7] as a weak authentication mechanism. Moreover the community name to access the ILMI management information base (MIB) is specified as 'ILMI' [13, p. 147]. An attacker who does not need to authenticate himself can use the ILMI to register additional ATM addresses for his workstation. By using the additional registered address the attacker can bypass address filters which have been configured at the switch. The attacker could also try to register himself with the ATM address of an offline workstation. This is similar to the attack described in section 2.2. ILMI can also be used to automatically configure the interface type of an ATM switchport. An attacker may use ILMI to pretend that he is a switch by setting the interface type to "NNI" (Network to Network Interface).

In order to attack the switch the UNI signaling has to be changed to NNI[8] signaling. This has to be done prior to attacks on the switch to make sure, that the switch will recognize the P-NNI protocol as this will be used by the attacker.

Example: Simulating an ATM Switch

We will briefly discuss a possible strategy an attacker could use in order to prepare for the attack on a switch (see the following section). In typical "Plug and Play" installations it is likely that the attacker's host is connected to an ATM switch that uses the ILMI protocol for automatic configuration. The host has already been detected by the switch and the interface (port) of the switch is configured for UNI[9] signaling. In order to change the interface from UNI to NNI it is sufficient to use the following ILMI mechanisms:

- Send a *cold start trap* (SNMP) message to the switch. The switch will now assume that the peer interface management entity (IME) is reinitialized. The switch will clear all previously cached MIB information for this IME.
- Perform the ILMI connectivity procedures. The peer IMEs convince each other that they are connected.
- Perform the ILMI automatic configuration procedures. The switch will try to determine the type of the peer IME by querying the following MIB objects:
  - *atmfAtmLayerDeviceType* object. The attacker could answer with a value of 2, thus pretending to be a network node.
  - *atmfAtmLayerNniSigVersion* object. The attacker could answer with a value of 3, thus pretending to use the P-NNI routing protocol.

  The switch will now assume a symmetric[10] setup, and the attacker can use the P-NNI routing protocol to confuse the switch as described below.

2.7 Attacks on ATM Switches

The manipulation of a switch in an ATM network is very similar to attacking a router in a "legacy network" and presents a serious problem. An attacker might use the P-NNI protocol in order to manipulate a switch. He could inject incorrect information in the peer group[11] database or even try to configure routing loops into the hierarchic structure. He might block the communication of whole peer groups or even redirect communication over his

[7] RFC1157[3] denotes them as 'community names'.

[8] 'Network to Network Interface' (NNI) describes the appropriate interface for switch to switch interconnection.

[9] 'User Network Interface' (UNI) describes a protocol to be used for connection management between host and private ATM switches.

[10] If the P-NNI protocol is used at the NNI, the setup is called *"symmetric"* because there are two network nodes (switches). The UNI protocols are not symmetric because they are used for different kinds of peers (between an end system (host) and a network node (switch)).

[11] A number of switches that share a common addressing scheme, e.g. the same address prefix, are grouped together. They belong to a 'peer group'.

workstation. The blocking of a peer group is very similar to the manipulation of routers with incorrect 'ICMP-Host/Net- unreachable' messages.

Attacks based on the P-NNI protocol can use replies to 'HELLO' messages of a peer group leader to inject malicious information about 'link states'. The peer group leader in turn will broadcast these changes to its group members. Peer group members that have updated their link state information with faked information are likely to make the wrong routing decision.

3 Solutions

Attacks on the ARP service and the ATM based IP spoofing can be prevented, if the ATM switch or, more generally, the ATM network supports mechanisms for access control. Most other discussed attacks can be prevented or mitigated by careful configuration of the ATM switch.

In ATM networks the control on access[12] to the network is shared between hosts and switches. On the other hand in "legacy LANs" like Ethernet the access to the network is only controlled by the nodes themselves (CSMA/CD)[13]. This fundamental difference between ATM and "legacy LANs" can be used for securing the networks against malicious attacks by providing a controlled access to network resources.

A major part of securing an ATM network relies on the ATM switch. It can be used for filtering certain addresses and to support monitoring of the network. The next sections will show how an ATM network can be secured against the attacks described before.

3.1 Securing the ATMARP Service

CLIP requires one ATMARP server for each LIS [10]. The ATM address of this server has to be configured on every node in the same LIS. The protection of the ATMARP service requires three steps:

- Configuration of the ATMARP server on one node in the LIS
- Configuration of static ARP entries for each known node in the LIS
- Auditing of all ATMARP queries coming from hosts that were not configured with a static ARP entry.

Configuration of an ATMARP Server An ATMARP server can be installed on a host in the LIS or on an ATM switch. From the security point of view installing an ATMARP server on a host is preferable for multiple reasons. The access to the ATMARP server on a host can be controlled more easily than on an ATM switch. As an ATMARP server on a host is implemented in software, it is easier to expand the ATMARP server with security enhancements for access control and auditing. ATMARP server on ATM switches depend on the firmware of the switch and are therefore difficult to expand. Moreover even though it is convenient to use the ATMARP server of the switch for multiple LISs, this makes it impossible to restrict the access according to the security policy of one LIS.

Configuring static ARP Entries In the second step the ATMARP server is configured with static ARP entries for every node in the LIS. Each entry consists of the tuple *<ATM address, IP address>*. This renders the described attack of malicious registration of an address of another node impossible, as static entries cannot be overwritten.

To gain additional security the ATMARP server should be configured to reject registration requests for unknown tuples of *<ATM address, IP address>*. This can be achieved by turning off the dynamic learning of new *<ATM address, IP address>* tuples. By these simple measures hostile registration of ARP entries can be prevented.

It has to be noted however that adding new nodes to this network will require manual configuration of the ARP entry.

Auditing of ATMARP Queries Attempts to register new ARP entries can be identified as either attacks or newly installed machines and should be audited. Also queries for unregistered ARP entries

[12] During signaling for connection establishment any node (both peers) and any intermediate switch may disagree to the SETUP request. ATM networks therefore offer some kind of "shared control" in contrast to legacy LANs which usually offer only a "shared access".

[13] Carrier Sense Multiple Access with Collision Detection

should be audited as this can be an attempt to scan the address-space for possible victims.

Open Issue In RFC1577 [10] it is required that every LIS client opens an ATM connection to the ATMARP server and registers its address binding. The ATMARP server will reject the registration if the same binding is already registered for another ATM connection. This attack will also succeed for statically configured *<ATM address, IP address>* bindings, as the ATMARP server will accept the malicious registration because a valid binding has been supplied. In consequence even with statically configured bindings a client may be blocked from registering after reboot. A solution to this problem is provided in the next section.

3.2 Integration of the Switch into a Firewall Concept

As described before, an attacker could try to open an ATM connection from an external host to an internal host thereby circumventing a firewall. A firewall concept for an ATM network needs to integrate the switch to prevent these attacks from succeeding. The configuration of the ATM switch has to make sure that connections can only be established between hosts of the same subnetwork (external or internal network). This can be done either by configuring PVCs only[14] or by restricting the signaling of new SVCs with access control list. The configuration of PVCs between all hosts of the same subnetwork yields a very secure configuration, but is hard to administer as adding a host will require the configuration of PVCs to *every* host in the same subnet. The definition of access lists on the other hand is more flexible and efficient as only few simple rules can restrict the creation of new SVCs. Even adding and removing hosts may not require reconfiguration if the subnets are identified in the access control lists by the use of wildcards.

The following sections describes the secure separation of two subnets – an internal and an external subnet – using access control lists on the signaling protocol. The firewall has two ATM interfaces: one "fwext" with the external network and one "fwint" with the internal network (see fig. 4).

[14] Beside configuring the PVCs the signaling of SVCs must be disabled.

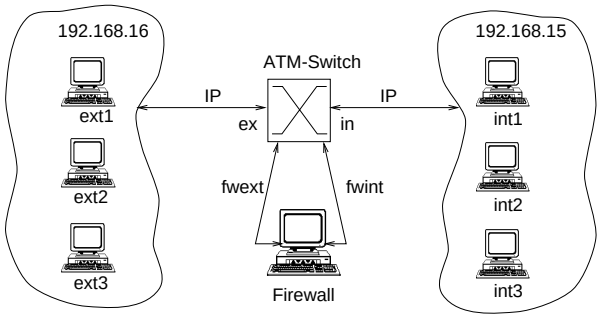

Figure 4: Firewall in an ATM Environment

3.2.1 Access Control on Signaling

Switches take an active part in opening ATM connections. Therefore ATM switches can be used to increase security by restricting the hosts ability to open connections to other hosts. The filters are similar to the rules that can be defined in packet screens. But these two filters differ in two important aspects: packet screens filter every packet whereas ATM switches restrict the creation of new ATM connections — no filtering occurs after successful setup of a connection. Rules in packet screens can be formulated on hosts (IP addresses) and services (TCP/UDP ports) whereas ATM switches only have access to the ATM addresses of the communicating hosts. The ATM switches have no control over type of IP-based service that will be accessed by the hosts. The filters on ATM addresses are sufficient for the intended use, as hosts will be grouped together by their ATM addresses and a firewall will be used for additional filters depending on the type of service.

As the filters on the switch rely on ATM addresses only, both the internal and the external network may have complex topologies (e.g. multiple interconnected switches). It is sufficient to configure the filters on the switch that is connected to the firewall. Figure 4 shows a simplified setup with only one switch.

The following restrictions have to be imposed by the ATM switch:

- Connections between hosts on the internal network should not be restricted.
- No connections should be opened from an internal to an external host.

- No connections should be opened from an external to an internal host.
- Connections between hosts on the external network should not be restricted.

With this configuration all communication between the internal and the external network must cross the firewall.

3.2.2 Sample Configuration for a Cisco LS 1010 Switch

The advantages of filter rules in ATM switches are described with the following example. The example network consist of three hosts on the internal network ("int1-3"), three hosts on the external network ("ext1-3"), one firewall with two interfaces ("fwint" and "fwext") and one ATM switch ("atmsw").

Definition of Symbolic Names for ATM Addresses Symbolic names are easier to comprehend and therefore reduce the risks of misconfigurations:

```
atm template-alias fwint
       4700918100000000e0f7df1901080020827e6100
atm template-alias fwext
       4700918100000000e0f7df1901080020827c5100
atm template-alias int1
       4700918100000000e0f7df1901080020827b8100
atm template-alias int2
       4700918100000000e0f7df1901080020825ca100
atm template-alias int3
       4700918100000000e0f7df190108002082a9f100
atm template-alias atmsw
       4700918100000000e0f7df1901f9f9f9f9f9f900
atm template-alias ext1
       4700918100000000e0f7df1901080020827be100
atm template-alias ext2
       4700918100000000e0f7df190108002082564100
atm template-alias ext3
       4700918100000000e0f7df19010800208254d100
```

In this example we choose to explicitly list all hosts in the filter rules. For larger networks wildcards should be used to select groups of hosts with just one rule.

Definition of Simple Access Control Lists The keywords `permit` and `deny` can be used to describe which hosts are allowed to use the signaling protocol to open a connection:

```
# internal hosts are allowed to reach
#                other internal hosts
atm filter-set inHosts permit fwint
atm filter-set inHosts permit int1
atm filter-set inHosts permit int2
atm filter-set inHosts permit int3
atm filter-set inHosts permit atmsw
atm filter-set inHosts deny default

# Hosts not listed (external hosts)
# are not allowed to reach internal hosts
atm filter-set exHosts deny  fwint
atm filter-set exHosts deny  int1
atm filter-set exHosts deny  int2
atm filter-set exHosts deny  int3
atm filter-set exHosts deny  atmsw
atm filter-set exHosts permit default

atm filter-exp intern inHosts
atm filter-exp extern exHosts
```

Unknown hosts will be treated like external hosts and cannot reach internal hosts. As only internal ATM addresses are necessary for the configuration the solution is applicable to both LANs and WANs.

If the ATMARP server has been configured as internal host, the address filters are sufficient to prevent an external attacker from directly connecting to the ATMARP server (see section 3.1). The combination of a secure ATMARP server and the use of address filters on switches to direct the access to the network through a firewall is a good choice for defending against the denial of service attacks discussed in sections 2.2 and 2.5.

Applying Filters to Interfaces The filters must be applied to the interfaces[15]. On an interface connected to an internal host the following commands must be applied:

```
atm access-group intern in
atm access-group intern out
```

On all external interfaces these two commands must be applied:

[15] Filters are not in use unless they are applied to a port of the switch.

```
atm access-group extern in
atm access-group extern out
```

3.2.3 Extension of the Concept

The above configuration separates the ATM network into two virtual networks the internal and the external network. This concept can be extended to separate multiple virtual networks. To which network a host belongs is simply a matter of configuration. A host may therefore belong to a virtual network depending on its communication and security requirements rather than depending on its physical location.

This feature of ATM networks makes it easier to structure networks depending on security requirements. If all these subnets are connected by one or multiple central firewalls, this concept will allow for very secure networks in the future.

3.3 Mitigation of Bandwidth Allocation Attacks

The combination of firewall, access control lists for signaling on the switch, and the secure ATMARP server is sufficient to establish a secure 'Classical IP over ATM' network. Figure 5 shows an extension to the setup discussed in section 4. The switch used for access control to the secure network is also used to connect other LISs ("external") to the Internet. As there is only one physical wire to the Internet access point (connected to the "ex" interface of the switch) it is still possible that the available bandwidth over this wire is allocated by an attacker (visualized with a dashed line between H1 and H2). The internal hosts will not be able to connect to the Internet or will perform at least very poorly.

There are two solutions that can address this problem. Both solutions require a careful configuration of the switch.

3.3.1 Limiting the available Bandwidth for each Traffic Class

Modern switches support the configuration of bandwidth resources for different traffic classes. Thus it may be possible to configure the "fwext" interface of the switch (figure 5) so that only a certain amount of bandwidth is available for CBR or VBR traffic. In essence this will not prevent the described attack but will reduce the impact, as the administrator can make sure that there is always enough bandwidth available for connections to the Internet.

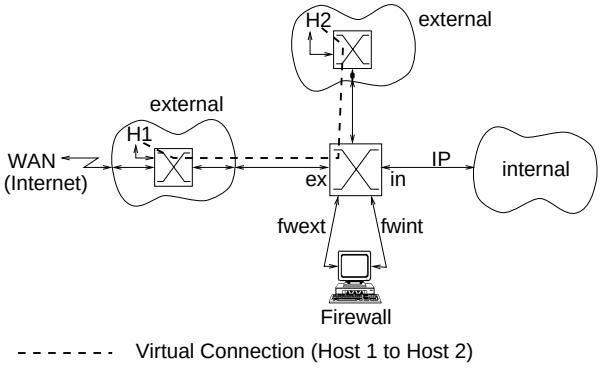

Figure 5: Bandwidth Allocation for SVC between two External Hosts

3.3.2 Configure a Permanent Virtual Connection

Another way to make sure that the internal network is always able to connect to the Internet is to configure a permanent virtual connection between switch and the Internet access point (router or switch). Typical switches provide a way to assign quality of service to PVCs. This is sufficient to allocate a certain amount of bandwidth to the PVC so that an attacker can only compete for the remaining bandwidth.

The main drawback of both solutions is that the administrator must have access to all intermediate switches in order to configure either a PVC to the Internet access point or limit the available bandwidth for demanding traffic classes (CBR/VBR). This may be impossible if the switches belong to different administration domains. Moreover the access to all the intermediate switches must be restricted to prevent reconfiguration by an attacker.

3.4 Static Switch Configuration

Both the ILMI based attacks and the attacks on the switch (see section 2.6 and 2.7) can be prevented by

static switch configuration. For example the administrator may configure individual ports of a switch as UNI ports. This prohibits changes to the port settings by a peer as described in section 2.6. It should be noted that this is a local configuration that needs to be applied to one switch only. This configuration will prevent a workstation which is connected to a port of the switch to use the P-NNI protocol for attacks on the switch.

Since there is still the chance that malicious routing information is propagated by other switches over a NNI link the switch is still vulnerable. One (interim) solution to this problem is the use of the 'Interim Inter-switch Signaling Protocol' (IISP) instead of P-NNI at the NNI interface unless the authentication has been addressed by the P-NNI designers. The IISP only supports statically configured routes, thus making it impossible to insert malicious information by sending messages to the switch. The major drawback of this solution is the burden of managing the static routing tables for fast scaling networks. IISP networks are also very error prone. If an intermediate switch goes offline all static routes through this switch are no longer usable.

A switch may also support the configuration of static ATM addresses at individual ports. This can prevent the registration of additional (unexpected) addresses at a switch port. This also makes sure that a workstation will only be able to register with a predefined address that matches a desired filter rule on the switch (see section 3.2).

4 Conclusions

This article describes some vulnerabilities present in "Classical IP over ATM" networks and introduces a switch based configuration and extensions to the ATMARP service as a countermeasure.

The use of IP in ATM networks leads to some interesting security problems. The risks of IP spoofing attacks are still high in ATM networks and need to be addressed by appropriate security mechanisms. In addition to these well known risks ATM features some new protocols whose security implications are not yet fully understood. Some possible attacks based on ILMI and P-NNI have been introduced in sections 2.6 and 2.7.

Section 3.1 discusses methods on how to secure an ATMARP server. ATMARP is a critical service for CLIP networks that must be secured. Another important result is that the ATM switches are very important for securing 'Classical IP over ATM' networks. ATM offers a "shared control" to network resources (see section 3). This feature is the basis for access control mechanisms in ATM switches (section 3.2.1). As an example we have shown how to setup ATM address filters for guarding the access to secure networks.

As ATM address filters are not sufficient to enforce typical security policies, firewalls will have to be used in combination with ATM address filters. The integration of a firewall into an ATM network was discussed for a gateway firewall. The concept can easily be expanded for a combination of packet screen with bastion host. This would require the configuration of three subnets (internal, external and DMZ[16]) instead of two subnets (internal and external). The switch can enforce the separation of these three virtual subnets with the same mechanisms that have been described before.

Section 3.3 shows how switches can be used to prevent some denial of service attacks by static configuration. This is necessary unless the ATM based protocols such as P-NNI and ILMI offer some kind of authentication.

Many of the problems discussed here originate from "Plug and Play" configurations. Vendors tend to supply their switches with automatic configuration tools (such as ILMI) which enable easy network setups. But a secure network requires a careful manual configuration of switches, protocols, and devices (e.g. firewalls) that control access to the network.

References

[1] Armintage, G. 1997: "Security Issues for ION protocols", Internet-Draft `draft-armitage-ion-security-00`, work in progress, Lucent Technologies 1997

[2] Bellovin, S.M. 1989: "Security Problems in the TCP/IP Protocol Suite" in Computer Communication Review, Vol. 19, No. 2, pp. 32–48, April 1989

[16] A bastion host is usually installed on its own subnet, frequently called "Demilitarized Zone" (DMZ) [4, 5].

[3] Case, J. et al 1990: "Request for Comments 1157: A Simple Network Management Protocol (SNMP)", Network Working Group, May 1990

[4] Chapman, D. B.; Zwicky, E. D. 1995: "Building Internet Firewalls", O'Reilly & Associates, September 1995.

[5] Cheswick, W. R.; Bellovin, S. M. 1994: "Firewalls and Internet Security: Repelling the wily Hacker", Addison-Wesley, 1994.

[6] Danthine, A.; Bonaventure, O. 1995: "Is ATM a Continuity or a Discontinuity for the LAN Environment?" in Effelsberg, W.; Spaniol, O.; Danthine, A. (eds.) Proceedings: HSN for Multimedia Applications, Dagstuhl, June 1995

[7] Deng, H.; Gong, L.; Lazar, A. 1995: "Secure Data Transfer in Asynchronous Transfer Mode Networks". *In: Proceedings of IEEE Globecom '95, Singapore*, November 1995.

[8] Heinanen, J. 1993: "Request for Comments 1483: Multiprotocol Encapsulation over ATM Adaptation Layer 5", Network Working Group, July 1993

[9] Johns, M. St. 1993: "Request for Comments 1413: Identification Protocol", Network Working Group, February 1993

[10] Laubach, M. 1994: "Request for Comments 1577: Classical IP and ARP over ATM", Network Working Group, January 1994

[11] Plummer, D. C. 1982: "Request For Comments 826: An Ethernet Address Resolution Protocol", Network Working Group, November 1982

[12] ATM Forum 1994: "Interim Inter-switch Signaling Protocol (IISP) Specification Version 1.0", ATM Forum 1994

[13] ATM Forum 1994: "ATM User-Network Interface (UNI) Specification Version 3.1", ATM Forum 1994

[14] ATM Forum 1996: "Integrated Local Management Interface (ILMI) Specification Version 4.0", ATM Forum 1996

[15] ATM Forum 1996: "Private Network-Network Interface Specification Version 1.0", ATM Forum 1996

[16] Varadharajan, V; Shankaran, R.; Hitchens, M. 1997: "Security Issues in Asynchronous Transfer Mode". *Proceedings of Second Australasian Conference, ACISP'97, Sydney July 1997*, Springer, 1997.