Security of ISP Access Networks: practical experiments

Yann Bachy, Vincent Nicomette, Eric Alata, Mohamed Kaâniche,
Jean-Christophe Courrège

Security of ISP Access Networks: practical experiments

Yann Bachy*†§, Vincent Nicomette*†, Eric Alata*†,
Mohamed Kaâniche*‡ and Jean-Christophe Courrège§
*CNRS, LAAS, 7, Avenue du colonel Roche, F-31400 Toulouse, France
†Univ de Toulouse, INSA de Toulouse, LAAS F-31400 Toulouse, France
‡Univ de Toulouse, LAAS F-31400 Toulouse, France
§Thales Communications & Security, 3, avenue de l'Europe, 31400 Toulouse, France
* firstname.name@laas.fr, §¶ firstname.name@thalesgroup.com

***Abstract*—Home Internet connections are becoming more and more important in our every day life. Many Internet Service Providers (ISP) include an Integrated Access Device (IAD) in their offers allowing the customer to easily take advantage of all the included services. This IAD is connected to a local loop, most of the time based on the Public Switched Telephone Network (PSTN). The local loop and the IAD together constitute the access network of an ISP. To our knowledge, very few studies addressed the security of these access networks. This is the purpose of this paper. We first present a platform and a set of experiments aiming at capturing and analysing communications on the local loop. This platform allowed us to carry out a comparative study of the security of six IADs from different ISPs, by analysing the network protocols used during their boot-up process. The results of this first study revealed a security weakness for two of the six access networks, especially during the firmware update procedure of the IADs. A second platform and set of experiments are then presented, which allow us to experimentaly test the possible exploitation scenarios of the identified weakness. Finally, we show that the security issues pointed out above, dont only impact the IAD, but also any other home Internet connected device, implementing firmware updates.**

I. Introduction

Today, Internet connection at home has become more and more accessible, both economically and technically. Indeed, there is no need for advanced technical skills to access the Internet at home: all the ISPs supply installation guides or help lines in order to facilitate the set up of the Internet connection.

In order to renew the economic model of Internet, the ISPs introduced all-inclusive (Internet, Telephone and Television) offers, also known as "triple play" offers, exploitable by means of additional user equipment. These types of equipment, such as modems, routers, IP-phones, TV-decoders or even all-in-one devices, are all available off-the-shelf. To complete their offers, in some countries, the ISPs started to produce their own all-in-one devices to take advantage of all the features included in their offers, these are the so-called Integrated Access Devices (IAD), which are now installed in many homes. They provide the customer with an Internet connection, but they also include many more functions, such as a WiFi hotspot and a TV Decoder. The IADs are connected to a local loop, most of the time based on the Public Switched Telephone Network (PSTN). The local loop and the IAD together constitute the *access network* of the ISP. Setting up a home network becomes really easy as the IAD includes network address translation (NAT). As a consequence, all the computers and other smart-devices connected to the home network can automatically gain access to the Internet simultaneously. In addition, this led to the emergence of home network protocols such as DLNA[1], to the wide sharing of user data and to an increase of communication channels between domestic devices and the Internet.

Just like for other embedded computer devices [1], the security of these IADs, provided by the ISPs, has become a major concern [2]. Different studies have identified several vulnerabilities [3][4][5]. These works mainly present methods allowing one to compromise an IAD. In [3], the author investigates the risks related to a compromised IAD. Firstly, the author suggests the IAD could be used in a botnet or serve as a spam relay, thereby raising concerns about the information received or sent through the IAD. Secondly, it is suggested the IAD may allow the attacker to sniff any data corresponding to the target user, thereby raising a confidentiality issue. However, these studies take into account only 2 scenarios:

- The attacker is the user itself, and has a physical access to his IAD and can do whatever he wants with it;
- The attacker is at a remote location and attempts to reach an IAD through the Internet, or by deploying malicious software, such as a virus.

A third assumption should be considered, in which the attacker physically taps into the infrastructure connecting the customer to the ISP: the local loop. This paper explores this assumption by performing a security analysis on typical ISP access networks, combining the local loop and the IAD. Thereby, this paper provides two main contributions. The first one is the design of a platform dedicated to capture any communication on a local loop. We use this platform in order to observe communications and protocols used during the boot-up process of an IAD, between the IAD and the different servers of the ISP network. These communications are

[1] *Digital Living Network Alliance*

important because they characterize the configuration process of an IAD. The analysis performed on these communications allowed us to precisely identify and compare the protocols used by a selection of IADs from different ISPs and, in particular, to identify weaknesses in these communications for two IADs. The weaknesses are important because they betray design flaws in the configuration of the access networks of the corresponding ISP, and as consequence, may potentially endanger all the clients of this ISP. The second contribution of this paper is a method leading to exploit the weaknesses identified previously. Using this method allowed us to demonstrate a weakness in the firmware update procedure of the IADs concerned by the identified weaknesses. Since these update procedures are similar to those of any other Internet connected device, we conducted a second set of experiments testing the firmware update procedures on a panel of Smart-TVs, which are one of the most common type of smart-object in people homes today, and that present an important amount of features.

This paper is structured as follows. Section II summarizes some important characteristics of home Internet connections. Section III describes 1) a platform allowing to sniff all communications between any IAD and the ISP and 2) the main results from the first experiments we carried out using this platform. In particular, this section exhibits some interesting weaknesses in communication protocols used by some IADs during the boot-up process. Section IV describes 1) a second platform simulating an ISP, 2) an iterative method to configure this platform, and 3) the results we obtained by applying this method to the two IADs presenting security vulnerabilities in Section III. Section V then discusses how these methods can be used to similarily analyse other devices connected through an IAD. Finally, Section VI discusses some future work.

All the experiments described in this paper were carried out in France. Nevertheless, these techniques are applicable in any other country with analogous architectures. All the ISPs we have tested the access network, have been informed of our results. For ethical reasons we can not disclose their names. Moreover, for legal reasons, we cannot provide too much detailed technical information about our attacks. Our main objective is to raise awareness about some weaknesses affecting access networks considering in particular the local loop which has been seldom explored in related work.

II. Home Internet access network

A. Network address translation

On the Internet, every device (cellphone, IAD, etc.) is assigned a unique public IP address. With this address, everything connected to the Internet becomes accessible from any location on the Internet. This accessibility facilitates the hijacking of such equipment, by exploiting their potential vulnerabilities. Therefore, every equipment connected to the Internet must protect itself against any possible attacks.

The first version of IP to be widely deployed is version 4. This is still the most used version of IP today. This version of IP only allows a maximum of 4 billion IP addresses. To palliate this shortage, a network address translation (NAT) [6] technique was introduced, and is especially useful for home networks. Indeed, for all home networks connected to the Internet (IPv4) today, the only equipment which possesses a public IP address is the IAD. All the other equipment, such as computers, smart-TVs, connected DVD readers, alarm systems, etc., are assigned a so-called "private" address and they must pass through a translation by the IAD in order to reach Internet services. Using this technique has several advantages. From a security point of view, the main advantage is that the IAD is the only device directly "visible" to the Internet. The other devices behind the IAD, which have private IP addresses, are not directly connected to the Internet network, and thus not directly accessible by a foreign host on Internet.

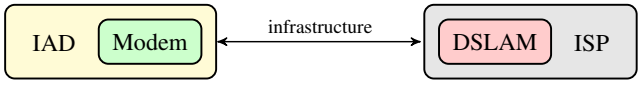

Fig. 1. Local loop

Since the deployment of IADs, with NAT installed by default, the security of home-networked devices mainly relies on this feature. Considering all this, the IAD has become a critical part of the infrastructure connecting the ISP to the customer. Therefore, it is essential to analyze the security on this part of the network.

B. The local loop

All ISPs are generally organized in the same way. They have their own core network which is physically connected to all the customers. The overall infrastructure is designed in order to cover an entire country. This segment, between the customer and the ISP's infrastructure, is also known as the local loop (cf. Fig. 1). There are 4 main physical supports used for the local loop: copper pair, coaxial, fiber optics and radio waves. To quickly satisfy the demand, the infrastructure of the ISP mostly relies on the infrastructure of the historical phone company or on the infrastructure of an existing cable-TV provider, to reach the customer. This segment may have been designed a long time ago, without considering its future use or any security aspects. Our case-study was carried out in France, where copper pair is by far the most used kind of local loop. Therefore, we will hereinafter, only consider ADSL (Asymmetric Digital Subscriber Line) IADs. The method developed in our study can be applied to any kind of local loop by using analogous hardware[2].

This copper pair is terminated by a MoDem (*Modulator and Demodulator*) on the user's side, and by a DSLAM (*Digital subscriber Line Access Multiplexer*) on the ISP's side. These two equipment modulate and de-modulate a digital signal into high-frequency analog signals which are transmitted over the copper pair.

[2]Soldering fiber optics will require specific skills and hardware.

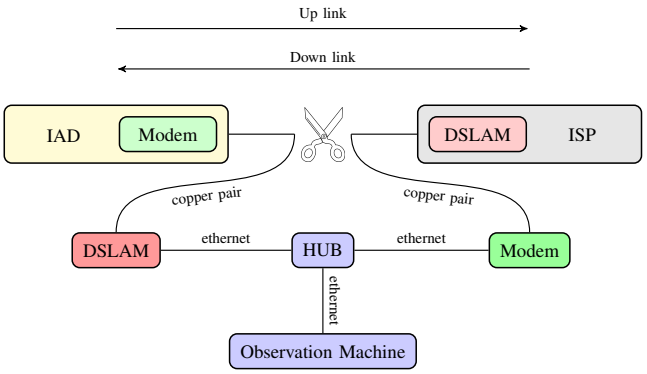

Fig. 2. Observing the local loop

In the following, we describe a platform designed to sniff any communication on a local loop. We will be using this platform in order to analyze the security of the communications between the ISP and an IAD on the local loop.

III. A LOCAL LOOP OBSERVATION PLATFORM

This platform is intended to observe any communication on the local loop. The method we use can be applied to any kind of local loop by using analogous hardware; hereinafter we detail our method for copper pair local loops. Our platform is composed of a DSLAM and an ADSL modem. We first describe this platform in subsection III-A. Then, subsection III-C is dedicated to a comparison of the boot sequence of different IADs, based on data collected with this platform. This comparison reveals the security measures enforced by the different ISPs on their access networks.

A. Method

To capture all the data flows on a pair of copper, several methods exist:

- *sniffing*: duplicate the signal and try to demodulate it without knowing any of the parameters used during the ADSL initialisation;
- *man-in-the-middle*: demodulate and re-modulate the signal, by taking part of the ADSL initialisation.

The first solution needs to deal with problems related to signal processing. It leads to the development of a tool able to passively synchronize itself according to the negotiation between the DSLAM and the IAD. Not only these specific problems are beyond the scope of our work, they also imply tools that are not freely available. The second solution, however, can be accomplished with easily available devices. In our platform we have adopted this second solution (cf. Figure 2).

The DSLAM and modem at each end of the copper pair fulfill the exact opposite operation of each other. Indeed, the modulation used on the up-stream differs from the one used on the down-stream. Therefore, it is possible to physically cut the line and insert a new DSLAM and a new ADSL modem, while preserving the connectivity between the customer and the ISP. In fact, this modification changes the way the IAD communicates with the ISP's DSLAM: it synchronizes and communicates with the inserted DSLAM; the inserted DSLAM communicates with the inserted ADSL modem which, in turn, synchronizes and communicates with the ISP's DSLAM. As the local network interface included in both modems and DSLAM are most of the time Ethernet, this manipulation finally consists in transforming one copper line into two copper lines interconnected by an Ethernet LAN (see Figure 2). As sniffing on an Ethernet LAN is very easy, any communication over the local loop can be observed.

This configuration allowed us to carry out a comparative study on all the different protocols used during the boot-up sequence of a selection of IADs we had the opportunity to test. We present the most interesting points of this comparison in the following subsection.

B. Equipment and Configuration

As mentioned before, this platform requires several pieces of hardware that are available "off the shelf". We used a `Zyxel IES-612-51` DSLAM, a `D-Link DSL-320B` Modem and a "left over" HUB. For the observation machine, any PC capable of running Wireshark is sufficient.

Both the DSLAM and the Modem must be configured with the same ATM settings as those used by the target ISP. When these values are not published by the ISP, we try standard values, and derivates of those, such as 8/35 LLC, 8/35 VC, 8/36 LLC, 8/36 VC. Most modems, like the one we used, include classic IAD functions such as NAT and DHCP. For this platform, these functions must be deactivated and the modem should function in the so-called "bridge-mode". Neither the Hub nor the PC require any specific configuration.

C. IAD Comparison

We used our platform to observe the boot-up sequence of several IADs provided by different ISPs. Globally, all the IADs we have observed, use PPP, IPv4 and standard UDP and TCP protocols, such as DNS, SIP, NTP and HTTP. Most ISPs also use encrypted communications based on SSL. Moreover, we have noticed that every request to a specific server is preceded by a DNS query in order to obtain the IP address corresponding to the URL of this server. This behavior is systematic, even if the server has been contacted previously. We have observed that the boot-up sequence is generally composed of four steps (detailed below): 1) ATM, 2) PPP, 3) Configuration and 4) SIP.

The results of this study are summarized in Table I. The first column contains the IAD identifier (anonymously). The second column of this table shows the main parameters used by the IAD for the ATM negotiation. The third column indicates if the ISP uses PPP, and if it does, which authentication protocol is used. The fourth column indicates if the ISP uses DHCP to assign an IP address to the IAD. The fifth column shows the hash algorithm that is used during the SIP registration process. The penultimate column shows the protocols that are used during the configuration process. Finally, the last column shows the protocols used during the firmware version update process.

TABLE I
CHARACTERISTICS OF THE DIFFERENT IADS

BOX	ATM	PPP	DHCP	SIP	Configuration	Update
A	8/35/LLC	chap	no	MD5	HTTP, FTP, SSL	-
B	8/35/LLC	chap	yes	MD5	HTTP, SSL	SSL
C	8/36/VC	no	yes	MD5	SSL	-
D	8/35/LLC	chap	yes	MD5	HTTP	HTTP
E	8/35/LLC	chap	yes	MD5	HTTP	HTTP
F	8/35/LLC	chap	no	MD5	SSL	-

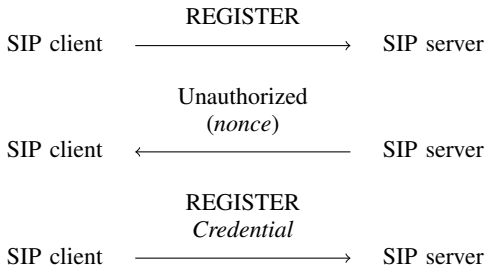

Fig. 3. SIP registration

1) ATM: We can notice that most ISPs use very similar parameters for the ATM protocol. These parameters are often published by the ISP allowing the customer to use an IAD available off-the-shelf with manual configuration, instead of using the IAD supplied by the ISP. In this study, we have observed only 2 different configurations. Therefore, and as long as the ISP uses parameters close to the ones we have observed, configuring our platform in order to sniff the communications through the copper pair remains relatively easy. Even non-standard parameters can be retrieved using reverse engineering techniques.

2) PPP: This protocol is frequently used when ISPs are constrained to share the local loop [7] with the phone line company. We can notice that for one of the ISPs that we observed, this protocol has been totally abandoned. Other ISPs implement the protocol but on a different virtual interface. In most cases this interface is not used to transfer any data. Doing so allows the ISP to reduce the overhead when transmitting data without loosing compatibility in situations where PPP is still required.

3) SIP: The most frequently used protocol for telephony over IP, and thus over Internet, is SIP. A SIP client, which in most cases is included in the IAD, uses a username and a password to connect to the SIP server. Different ways exist to secure the establishment of a SIP session. By observing the negotiation more precisely, we have noticed that all the IADs in our study use the same protocol as shown in Figure 3.

- An empty registration request is sent by the SIP client;
- This request is refused by the server which returns an "Authentication Required" message, including a "nonce";
- The SIP client then authenticates itself by supplying to the SIP server a MD5 checksum calculated mainly from the nonce and the SIP password (that the SIP client knows or is able to calculate).

All the IADs we have observed use MD5 to hash their reply. The use of the MD5 hash algorithm has been disadvised [8] for several years already, due to proven weaknesses. However, considering that the nonce rotates [9], an MD5 hash can be sufficiently secure, if the password is long enough to resist brute force attacks, and sufficiently unpredictable to be considered as quasi-random.

4) Configuration: IADs are designed to allow the final user to take benefit of all the provided services such as TV and telephone. To allow these services performing correctly, a specific configuration is necessary, which moreover may vary frequently. Hence, the configuration of an IAD is a critical phase of the boot-up sequence. As a consequence, most of the time, this phase uses cryptographic methods either to authenticate the box with the ISP or to protect the content of the messages. So, without prior knowledge on the infrastructure of the ISP, it is difficult to identify these connections and to characterize them.

However, as stated in the introduction of this section, before accessing a server, a DNS request is sent to obtain the IP address of the server. This is confirmed by our observations. Moreover, the DNS request reveals important information about the exchange. For instance, if the request sent to the domain name server contains the term TR69, or similar, which is known to be a commonly used configuration protocol, we can suppose that the exchange concerns the configuration phase.

The protocols used to transport the configuration are presented in the penultimate column of table I. We can see that the different ISPs do not use the same protocols to configure their IADs. Most ISPs use the protected HTTPS protocol to transfer the configuration. For IAD A, the SSL exchange is preceded by the non-protected HTTP protocol which is used to declare the presence of the IAD on the network. Taking a deeper look at the implementation of the SSL protocol we have observed the use of two different exchange algorithms, **TLS_RSA_WITH_RC4_128_SHA** and **TLS_RSA_WITH_AES_256_CBC_SHA**. Both of these are compliant with the recommendations issued by the French Network and Information Security Agency (ANSSI) [10]. Other countries may adopt stronger recommendations. However, if we take a look at the two IADs D and E, we can see that only the non-protected HTTP protocol is used. Thus, we were able to extract the configuration for these two IADs, which are very similar.

5) Firmware updates: Some of the IADs we have analyzed in this work allow the end-user to check the availability of a new firmware, and in case one exists, to launch the firmware upgrade of the IAD. We analyzed different exchanges that were initiated during this process. The results show that if this functionality exists, the same protocols as during the configuration process are used. This implies that the update process of IADs D and E is not secure. Just like during the configuration process, we were able to extract the entire firmware during our experiments.

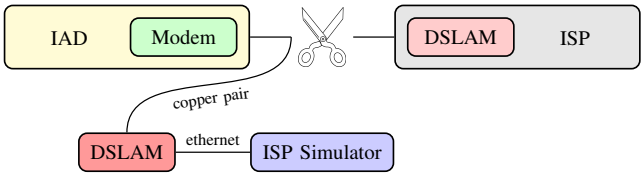

Fig. 4. Emulating an ISP

To summarize these experiments, except for a few details, all the IADs we have studied, seem to function the same way. However, the IADs D and E differ significantly from the others on one point: the protection during the configuration and update procedure. The protocol used does not authentify the servers of the ISP from the IAD point of view and vice-versa. This reveals some security weaknesses in the design of the access network of the corresponding ISPs. In the remainder of this paper, we present our second platform, intended to simulate an ISP. We'll be using the results of our first platform and an iterative method in order to explore possible exploitation scenarios of the identified weaknesses.

IV. ISP SIMULATION PLATFORM

This section describes the second platform we have set up to analyze local loop and IAD security aspects. This platform simulates an ISP based on the knowledge acquired using the local loop observation platform. Here, instead of connecting our DSLAM to the ISP's network using a modem, we connect it to a computer capable of simulating the behavior of an ISP (cf. Figure 4). This step is accomplished step by step following an iterative method. In the following we describe our iterative method as well as a few examples, finally we discuss the results we obtained.

A. Iterative method

This method can be assimilated to a grey-box approach. We don't have any precise information about the internal functions of the IAD. Nevertheless, the information we've gathered using the observation platform, during the first part of this case-study, gives us some precious information about the system. Our method is composed of 4 steps repeated cyclically.

- **Observe**: During the boot-up, we observe all the outgoing traffic of the system on the network;
- **Analyze**: We analyze the next request to which we can not yet answer, often such a request is repeated regularly waiting for an answer;
- **Build response**: We install and configure the necessary software allowing to answer the last request, which is blocking the boot-up process;
- **Reboot**: We reboot the system in order to proceed to a new boot-up process.

These four steps are repeated manually until we reach the process we want to test. Our first goal is to cover the entire boot-up process of the IAD. The second one is to reach an update sequence. Once we are able to simulate the ISP's behavior during the boot-up process, it becomes interesting to be able to modify the firmware to suit our own needs. Reverse engineering techniques and open source software allowed us to do so. Having done so, we can infect any vulnerable IAD with a malicious firmware.

B. Implemented services

Several services are required by an IAD to function at the customer's home. However, during this study, we realized that all these services aren't necessarily functional when the IAD announces to be ready. The two services we installed on our ISP simulator, in order to achieve this stage, are:

- **PPP**
  At boot time, for ISPs using PPP, the IAD attempts to authenticate itself with the ISP using the PPP protocol.
- **DNS**
  Embedded devices, such as IADs, rarely know the server's IP addresses with whom they need to communicate. Therefore, it is necessary to provide a DNS service allowing the IAD to satisfy these requests.

In order to analyze the firmware update procedure of an IAD, we need one more service. This service varies from one ISP to another and here we only analyze IADs using the non-secure HTTP protocol.

- **HTTP** Several protocols exist to transfer data from one device to another. In this study we found two IADs using the non-secure HTTP protocol. Therefore we need an HTTP server, which allows us to simulate the ISP during the firmware update procedure.

Globally, after only 4 reboots, we were able to compromise the update procedure of the corresponding IAD.

C. Equipment and Configuration

For this second platform we have used the same DSLAM as the one use for the observation platform. Its configuration also remained unchanged. For the ISP simulator, we used a PC with a `Intel Pentium 4 2,8Ghz` processor, `2GB` of memory and the `Debian` operating system. The different services discussed in the previous section were installed with the following configuration:

- For PPP, we used the Debian `pppoe` package together with `freeradius` configured in such a way to accept any login/password combination.
- For DNS, we used the Debian `bind9` package together with `dnsmasq` in order to redirect any DNS from the IAD to our ISP Simulator.
- For HTTP, we used the Debian `apache2` package without any specific configuration apart from creation of the same directory structure as the one available on the legitimate firmware update server.

D. Experimental results

We particularly analyzed the firmware update procedure. As long as secured protocols are used, such as HTTPS, and as long as they are well implemented, it is not possible to simulate the ISP's update-server. Since we are not in

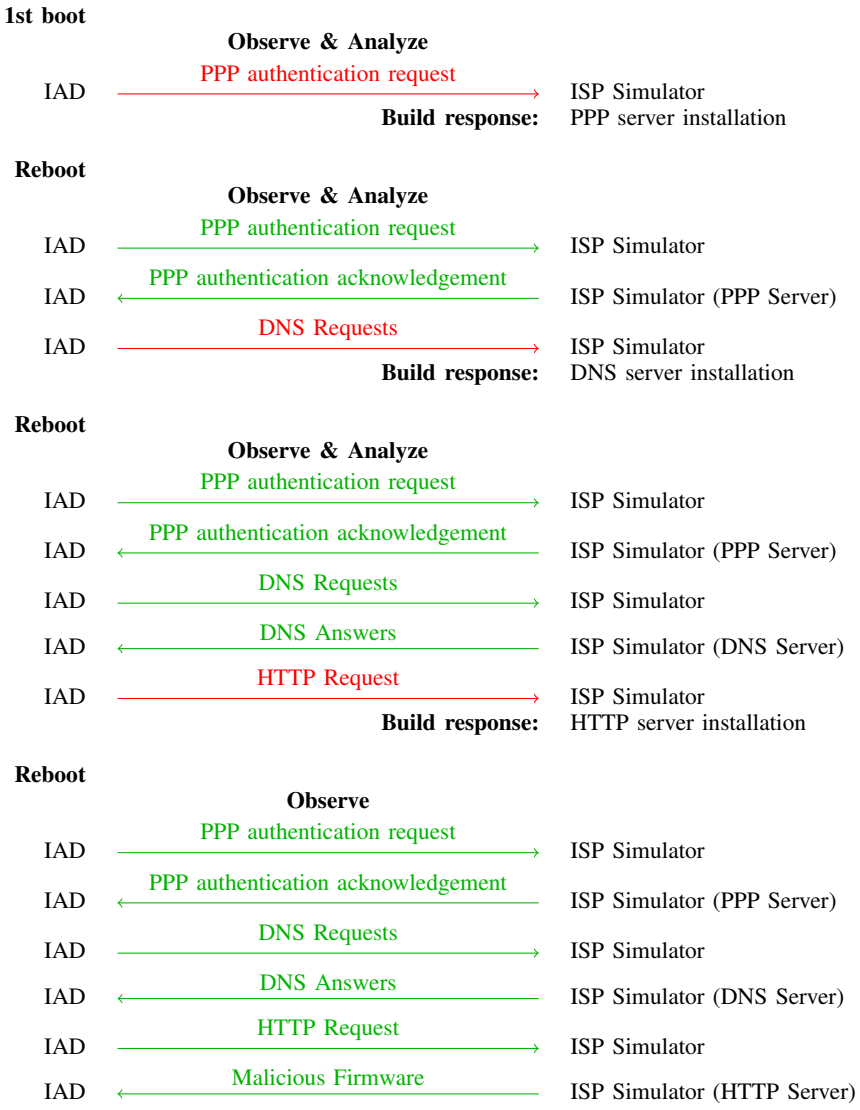

Fig. 5. Boot-up and firmware update sequence

possession of the encryption-keys that are used, the IAD systematically refuses to establish any connection based on the HTTPS protocol with our platform. This problem, of course, does not exist with the non-secure HTTP protocol. Using the information we obtained during our observation experiments, we were able to create our own firmware and install it on the IAD using this platform. This firmware is identical to the one installed originally by the ISP except for a few details:

- We de-activated the firewall, this allows us to access the SSH service using the WAN-interface.
- We de-activated the update procedure, which ensures our firmware will remain on the IAD.
- We installed a soft-phone, which allows us to set up, possibly premium-rated, phone-calls using the modified IAD.

This implies that the original firmware is not signed or encrypted in any way. To extract and modify the contents of the original firmware, we have only used open-source software. The entire sequence of our experiment is described in Fig. 5. These three modifications allow one to entirely control an IAD from a remote site. The subscriber won't notice any difference of functionality. Indeed, all the services (Internet, TV and telephone) remain entirely functional. The impact of this attack will be visible to the subscriber on his bill at the end of the month on which all the premium-rated phone-calls will be charged. The three modifications we have made to the original firmware only serve as examples. We could imagine many more attacks, using these weaknesses. Considering the firmware of an IAD is most of the time based on Linux, once the attacker obtains a shell-access, almost any modification can be made. For instance, an attacker may open ports to a specific device inside the network, and therefore expose it to the entire Internet.

V. Impact on other smart-devices

Considering the IAD security issues related to ISP access networks, we question the impact on other home Internet connected devices. Indeed, the firmware update procedure of the devices may be very similar to those of the IAD and is performed thanks to their Internet connection. Just as we were able to modify the firmware of some IADs thanks to our simulation platform, it is feasible to modify the firmware of other devices through this same plateform and methodology. We have addressed this question in [11] considering the specific context of smart-TVs. In particular, we have experimentally analyzed the firmware update procedures of four major brand smart-TVs and we were able observe and identify the communication protocols between the Smart-TVs and their smart-content provider. An example of results is provided in table II were the smart-TVs are anonymously referenced as A, B, C and D.

		A	B	C	D
Negotiation	protocol	HTTP	HTTP + HTTPS	HTTPS	HTTP
	content	unknown	XML + –	–	XML
Transfer	protocol	HTTP	n/a	HTTP	HTTP
	content	Binary	n/a	Binary	Binary

TABLE II
Smart-TV firmware update procedures

In each firmware update procedure, two phases are distinguished: 1) a "negotiation" phase that checks if a more recent firmware version is available for this Smart-TV, and 2) if a newer version is available, a "transfer" phase wherein the actual firmware is transferred. For each phase, we observed the protocols that are used, and the type of content. Negotiation phases of A, B and C are very similar, they either use the secured HTTPS protocol, in which case the content is ciphered, or, when a non-secured protocol such as HTTP is used, the content uses an unknown encoding and is therefore also ciphered. The negotiation phase of D uses the non-secured HTTP protocol and its content is human readable XML. This allows a classic "man-in-the-middle" attack to substitute the URL leading to the new firmware and force the TV to download a different firmware.
All observed firmware transfer phases use the non-secured HTTP protocol. For each of these TVs, we carried out a "man-in-the-middle" attack simulating the update server during this phase, proposing legitimate but outdated firmware[3]. Smart-TVs A and B refused our outdated firmware without specifying any reason. It is likely that some signature is exchanged during the negotiation phase. Smart-TV D on the contrary accepted our outdated firmware. This security breach allows any attacker to exploit previously corrected security flaws on this TV.

This example clearly highlights the fact that security weaknesses of a specific access network may impact any other device connected to a home computer network. This problem is even more concerning knowing that the amount of Internet connected home devices is increasing constantly.

The European commission estimates, after a consultation that started in 2012 [12], an average user will possess 7 Internet connected devices in 2015. All these devices will possibly use the Internet to obtain firmware updates using similar methods as those observed during the experiments described in this paper, and therefore present similar vulnerabilities, which can be detected with the platforms described in this paper.

[3]We downloaded and archived legitimate firmware from the constructors Web sites.

VI. Conclusion

Government organizations such as the ANSSI, in France, are worried about the level of security of the different IADs and other home Internet-connected devices. Many of these devices run minimalist operating systems, which due to production constraints are often out-dated compared to every day security standards. To our knowledge, only very few scientific studies address this problem, and especially the configuration of the IADs relative to the protocols aiming at communicating with the servers of the ISP, for upgrading the firmware for instance.

In this paper, we have proposed and described a novel method to analyze the security of the ISP's last mile, i.e., the ISP access network. Two main contributions can be highlighted in this study:

- A first platform allowing to observe all the communications between any IAD and the servers of the ISP through the local loop. We used this platform in a case-study in order to observe the configuration and firmware update process implemented in 6 different IADs. These observations allowed us to compare the different protocols used during this process and, in particular, allowed us to identify weaknesses on access networks of two ISPs.
- A second platform allowing us to simulate an ISP or any other online service provider. This platform allowed us to exploit the weaknesses detected using the first platform.

The attacks presented in this paper require physical access to the local loop connecting the target to its ISP. They correspond to targeted attacks against a specific end-user. Indeed, it seems that the presented platforms can hardly be used to carry out massive attacks but rather specific enhanced attacks, which can be performed by organizations with financial resources and ambition. Clearly, such attacks enter the APT category (Advanced Persistent Threat), which is one of the most dangerous threat category and one of most difficult to detect and eradicate.

Several countermeasures to address the weaknesses pointed out in this paper deserve to be analyzed:

- Generalization of cryptographic methods during critical exchanges. In this study, we can see that many ISPs have already chosen to use the secure HTTPS protocol.
- Measuring variation of the attenuation on the ADSL line, since this value should drastically change when one inserts our platform on the local loop. Detecting plateform like the one presented in this paper is important as it may serve to observe any non-protected, and perhaps

sensitive, exchanges initiated by the end-user. Moreover, this technique can be an interesting way to ensure that a third-party infrastructure is not being tampered.
- Generalization of firmware signing and encryption. If we consider the IAD as an end-point of the ISP's network, the content of the firmware must be guaranteed.

As future work, we plan to generalize our experiments with many other connected devices, as our platform is generic enough to be used for any kind of connected devices performing firmware update thanks to an Internet connection.

Acknowledgement

We are very grateful to the late Yves Deswarte for his significant contribution to this work.

REFERENCES

[1] A. Cui, M. Costello, and S. J. Stolfo, "When firmware modifications attack: A case study of embedded exploitation," in *proc. of Network and Distributed System Security Symposium (NDSS)*, San Diego, USA, April 23rd 2008.

[2] "Défense et sécurité nationale." Paris, France http://www.elysee.fr/assets/pdf/Livre-Blanc.pdf: Direction de l'information légale et administrative, 2013, pp. 44–45.

[3] N. Ruff, "Sécurité de l'ADSL en France," in *proc. of Symposium sur la sécurité des technologies de l'information et des communications (SSTIC)*, Rennes, France, June 1st 2006.

[4] F. Raynal and G. Campana, "An attack path to jailbreaking your home router," in *proc. of Hack In The Box (HITB)*, Kuala Lumpur, Malaysia, October 11th 2012.

[5] P. Geissler and S. Ketelaar, "How I met your modem: Advanced exploitation & trojan development for consumer dsl devices," in *proc. of Hack In The Box (HITB)*, Amsterdam, The Netherlands, April 11th 2013.

[6] L. Zhang, "A retrospective view of network address translation," *Network, IEEE*, vol. 22, no. 5, pp. 8–12, 2008.

[7] Vivien, "Le retour du combat pppoa / pppoe vs ipoa / ipoe." http://lafibre.info/techno-du-web/pppoa-pppoe-ipoa-ipoe/: lafibre.info.

[8] X. Wang and H. Yu, "How to break md5 and other hash functions," in *Advances in Cryptology–EUROCRYPT 2005*, Aarhus, Denmark, May 23rd 2005, pp. 19–35.

[9] "SIP password security - how much is yours worth?" http://www.sipsorcery.com/mainsite/Help/SIPPasswordSecurity: SIPSorcery.

[10] O. Levillain, "Ssl/tls: état des lieux et recommandations," in *proc. of Symposium sur la sécurité des technologies de l'information et des communications (SSTIC)*, Rennes, France, June 6th 2012.

[11] Y. Bachy, F. Basse, V. Nicomette, E. Alata, M. Kaâniche, J.-C. Courrège, and P. Lukjanenko, "Smart-tv security analysis: practical experiments," in *LAAS Technical Report*, Accepted for publication at DSN 2015.

[12] Commission européenne, "Stratégie numérique : la commission lance une consultation sur les règles concernant les dispositifs connectés intelligents - l'"internet des objets"," 2012. [Online]. Available: http://europa.eu/rapid/press-release_IP-12-360_fr.htm