How to Cooperatively Improve Broadband Security

T. Cruz[1], T. Leite[1], P. Baptista[1], R. Vilão[1], P. Simões[1], F. Bastos[2], E. Monteiro[1]
[1] CISUC - DEI, University of Coimbra, Portugal
[2] PT Inovação – Aveiro, Portugal
tjcruz@dei.uc.pt
thiago@student.dei.uc.pt
pmbento@student.dei.uc.pt
rpvilao@student.dei.uc.pt
psimoes@dei.uc.pt
fbastos@ptinovacao.pt
edmundo@dei.uc.pt

Abstract: The growth in the number of domestic and Small Office/Home Office (SOHO) environments served by broadband connections (cable, xDSL), together with the emergence of a *digital convergence* paradigm, with the integration of services over a single medium, created a new set of security concerns . These concerns arise from the specific characteristics of the broadband medium itself, in the form of potential security threats, for ISPs, customers and third parties, due to three factors: high bandwidth, availability to a very large customer basis and the permanent nature of the connections. The traditional segmentation between the ISP and customer networks, relying on the customer technical skills to effectively manage its own network, is no longer effective, since nowadays each ISP serves a large number of customers that lack the required expertise. On the other hand, these customers own powerful network and computational resources which can be used, with or without their knowledge, to launch massive attacks to third parties.

The security model currently adopted by ISPs is based in a relatively reduced number of traffic barriers deployed in strategic places of their own backbone networks. However, the amount of network traffic these barriers need to process is substantially increasing over time, as a consequence of the ever growing customer base served by broadband, raising both severe cost and scalability constraints that might turn this approach unsuitable at all in the future. In response to this problem, we propose a new security architecture for broadband services, which takes advantage of the specific role and location of "home gateways" – as devices standing between the ISP and the customer network – to build a distributed IDS/IPS ("Intrusion Detection System/Intrusion Protection System"). This solution changes the current paradigm, presenting a novel approach to security in broadband service environments by redefining the frontier between Internet Service Providers and their customers. Close cooperation between ISPs and customer resources provides a shared security framework with improved scalability, granularity, flexibility and efficiency while shifting the frontier between ISP and customer networks and, thus, raising a number of ethical and technical issues.

The proposed distributed IDS/IPS is based on a hierarchic architecture, with a central orchestrator at the ISP level managing each gateway's behaviour in a coordinated way. Besides performing monitoring and attack prevention/detection functions autonomously, each gateway can also notify the central IDS of relevant events. Selected events generated by each gateway are sent to the central IDS in order to provide a macroscopic perspective of the whole network, thus identifying threat patterns whose detection would be impossible for a standalone device. This approach allows the ISP to deploy sophisticated, granular and scalable security mechanisms directly at the gateway level, which becomes the first defense layer of its own network.

While developing the solution, the ethical issues raised by the approach were also a matter of concern carefully discussed, concluding that the controlled transference of some security functions from the ISP to the client's own equipment brings considerable advantages to both, without significant ethical risks.

1. Introduction

Broadband access networks, in their present incarnation, pose a significant security threat for Internet Service Providers (ISPs), as a consequence of four factors: high bandwidth available to customers, widespread availability of these access technologies to a increasingly large customer basis served by a single ISP; the permanent nature of the connections (xDSL, Cable); and the lack of adequate technical knowledge required to enable each customer to guarantee his own network security needs. Even if some of the risks already existed before the emergence of broadband access networks, the transient nature of classic dial-up connections and the reduced amount of available bandwidth helped ISPs, making it easier for them to detect and control potential security threats or incidents affecting their own network, customers or third-parties.

The recent trend towards aggregation of voice, television and data services in the same communications access channel (*triple play*) and the diversity of services and applications (P2P, instant messaging, among others) contributed to aggravate security concerns in what refers to broadband environments. First, most of the customer base does not have enough technical skills and sensibility in order to effectively manage the security of their own networks, making them vulnerable to external threats and even potentially compromising the security of the provider network. The growth in the number of supported services and applications only contribute to add complexity, therefore hampering the detection and response to security threats and events - even more if this task is to be performed by centralized systems on the ISP network, with reduced scalability. Last, and since the customer expects voice and television services delivered over broadband to have equal, if not better, performance and reliability when compared to their conventional counterparts, the impact resulting of service interruptions will be bigger.

Traditionally, ISPs consider the security of the customer's network to be something out of their scope of influence, assuming that such responsibility must be assured by the clients themselves, autonomously. ISPs clearly define their security perimeter to end at their borderline equipment, with the customer being responsible for his own borderline equipment (such as *home gateways*) and everything beyond that. This attitude is culturally accepted by the users/customers which traditionally look at any kind of provider-conducted interference (either implicit or explicit) within their own private networks as a privacy matter.

Slowly, triple play networks started to change this scenario: it became accepted that some operations affecting the customer network could be performed by the provider in order to configure and remotely administer devices such as *set-top boxes* (STBs) and voice gateways. Even beyond this scope, the emergence of new services (e.g., IPTV, VoD, VoIP) and devices in SOHO networks along with the shift in the predominant network traffic models (with an ever increasing significance of P2P-related traffic), created the need for some kind of action to be taken in order to accommodate this new scenario.

Presently, the security model in use by ISPs is based in the existence of a relatively reduced number of traffic barriers deployed by the ISP in strategic places in its own network. As a direct consequence of the increasing diversity of services and applications supported over broadband, the amount of network traffic these barriers need to deal with is substantially increasing over time, causing scalability and cost issues. However, we believe it is possible to rethink, and therefore revise the established security model in broadband networks in order to better integrate the existing security mechanisms at the ISP and customer levels, without compromising user privacy or freedom.

As an alternative to the traditional ISP security model, we propose a solution that takes advantage from the specific role and position home gateways fulfill in the scope of broadband network architectures – as devices responsible for the exchange of information between the boundaries of the provider and customer networks – to develop a distributed IDS/IPS (*Intrusion Detection System/Intrusion Protection System*). This allows the ISP to deploy sophisticated, granular and scalable security mechanisms at the gateway level allowing it to become the first defense layer of its own network. As an added benefit from this *shared management* model, users without technical skills will get a better level of protection for their own networks. This is the underlying philosophy of the S3P project (*Security in Triple Play Environments*), which will be presented in this document.

S3P is a research project developed by the Communications and Telematics group at the Centre of Informatics and Systems of the University of Coimbra and funded by PT Inovação, Portugal Telecom's R&D company. It aims to provide the definition, implementation and evaluation of a security architecture with a stronger articulation between customer and ISP network security mechanisms in mind, establishing the home gateway as an useful device to both ISP and customer, from a security standpoint. In this paper we present the main aspects of the S3P architecture, in the following order: Section 2 details the scope of the project (triple play environments and industry trends), Section 3 discusses the ethical aspects of the proposed approach. Section 4 discuses the main aspects of the proposed solution, Sections 5 and 6 expose the S3P architecture with detail (from the home gateway and ISP standpoints). Section 7 summarizes previous work in similar projects. Section 8, presents the conclusions we have drawn and develops some insights into what future directions the project might take.

2. Motivation

As previously mentioned in Section 1, it is commonly accepted in broadband environments that the management of the customer's network security is a matter of his own responsibility. Even considering this premise to be acceptable to customers with technical knowledge, it poses considerable security risks for the large majority of the customer base, usually unskilled for this kind of task, being total of partially incapable of adequately configure and manage any kind of security mechanisms. This scenario affects not only the customer himself, but also the ISP who stands in a delicate situation of having a potentially unsatisfied customer (service quality degradation, security incidents) whose network can be used to attack other customers, the ISP itself or even third-parties. In these situations, the increasingly available bandwidth, combined with P2P applications and *everything-over-IP* convergence scenarios (voice, television) only contribute to substantially aggravate the potential risks involved either for the customer (possibility of network intrusion and stealing of sensitive data) or the ISP, itself more vulnerable to orchestrated DoS (Denial of Service) attacks and abusive uses of its network infrastructure.

This tendency has had repercussions at the industry level, with the introduction of ISP-provided equipments in the customer network (especially set-top boxes) and the trend towards standardization and convergence. Initiatives such as HGI (HGI 2006) and Broadband Forum (Broadband-Forum 1994) and products such as Windows Home Server (WHS 2007) make possible to deploy a extensive and coherent set of remote management and security services in the customer network, capable of monitoring his internal network (if desired) and the traffic flowing between it and the provider network. Either Broadband Forum and HGI have developed technical standards and recommendations in order to define a set of interfaces for security and remote management (HGI 2006; Broadband-forum 2006; Broadband-forum 2007) operations of devices located at the customer network (CPE, Customer Premises Equipments).

As a whole, those trends created the ideal conditions for rethinking the problem of security in SOHO and access networks. The emergence of a new scenario demands the identification and characterization of a set of new security threats associated with it, using the opportunity to research and develop a new approach onto how to deal with the customer network.

3. Security models and ethical issues: the *dos* and *don'ts* of broadband security

Albeit designed to protect the ISP and/or the customer, almost every security measure has some kind of drawback affecting one or both sides – bandwidth limiting and traffic shaping, for instance, have been the subject of much discussion because of ethical and legal concerns. Such collateral effects make it difficult to achieve the right balance between security and privacy in broadband environments.

In the traditional security model, the ISP has a limited reach (its influence perimeter is limited at the access network level), using traffic barriers and probes placed at strategic locations to detect and contain potential attacks. A simple analysis of this model shows that it is based on two simple premises:

- customers are fond of their privacy and they do not tolerate external interference with their own equipments and networks – therefore, they are responsible for their own infrastructure
- ISPs must assure adequate levels of security in their infrastructures while restricting their scope of influence at the access networks

In a modern broadband scenario, these two premises are mostly incompatible because most threats arise from compromised customer networks and equipments. Typical DDoS (*Distributed Denial of Service*) attacks come from *botnets* formed by swarms of compromised hosts attacking in a coordinated way - spammers use similar techniques to flood mail servers worldwide. In the past, such attacks could be mitigated by limiting traffic in the barriers deployed inside the ISP network but nowadays these measures are ineffective because the nature of the attacks has changed: instead of using a small number of compromised nodes to flood a target at high rates, now there is a much higher number of compromised nodes (spread among several ISPs and countries) generating directed network traffic at almost insignificant rates. If ISPs are to do something about these situations they must be able to extend their scope of influence farther than they currently do.

However, the commonplace vision about broadband access services, in which basically the customer is responsible for his own network management and the ISP for its own, tends to fade out gradually with the introduction of triple play and other value-added services whose operation depends on specific devices placed in the customer network. Frequently, these services require the installation of specific equipment provided (e.g., set-top boxes, IP phones) by the provider, either for the purpose of guaranteeing compatibility or for commercial strategic decisions (minimum DRM levels adequate for multimedia content). The increasing acceptance of such equipments creates the opportunity for rethinking the role of the borderline between the ISP and customer networks, allowing a better articulation between both without restricting or compromising the customer's freedom or privacy.

3.1 A new security model in a new scenario

With customers voluntarily accepting some degree of ISP interference in their networks, the cornerstone premises of the old model lose some of their importance. Simultaneously, the limitations of the traditional security model, make it incapable of adequately benefit from the increased customer tolerance. These circumstances call for a different approach to security in broadband environments.

To benefit the most of the increased user tolerance to external ISP interference, we propose the introduction of the concept of *operator-assisted home LAN security* which is based in a shared management model, where the ISP extends its reach to the customer gateway (CPE in the context of this project, despite the fact that the term CPE has got a broader meaning) and optionally even further (to the customers LAN), if allowed to do so:

- allowing the ISP to reach the CPE alone creates the conditions to implement a new security model, based on a distributed approach where "intelligent" security and monitoring mechanisms can be deployed at the CPE level (in the strategic border between the ISP and the customer networks instead of being centralized in the ISP infrastructure, with added scalability benefits) without interfering with the customer LAN. Because the CPE mechanisms are being exclusively used to monitor the traffic between the ISP and the client, the client's privacy is not compromised: the ISP could always do a similar monitoring inside its network, yet with significantly higher costs.
- if the user allows the ISP to do so, the CPE can extend its reach to the internal LAN, probing for a wide range of vulnerabilities via optional customer monitoring mechanisms, interfacing with operating system integrated resources to gather information about installed updates and active security parameters.

To a certain degree, what we propose is a paradigm shift in terms of network security models, moving from a non-scalable centralized model to a distributed, *shared management* architecture (Table 1).

Table 1: Security model paradigm shift

Traditional	Shared management
ISP restricted to its own network	Users define the ISP's scope of influence. Minimum ISP reach extended to CPE boundaries. Customer LAN can be monitored by the CPE, if the user allows it
Static barriers inside the ISP infrastructure traffic/bandwidth limiting and/or shaping	CPE-level mechanisms allow granular traffic control
CPE has limited capabilities, security effectiveness heavily depends on customer knowledge	CPE integrated into the security infrastructure, shared management between the ISP and customer
Traffic monitoring is possible at the ISP infrastructure, with scalability limitations	Traffic monitoring at the CPE level
Available detection and contention mechanisms in case of distributed attack are limited, slow and mostly ineffective	Capable of detecting attack in progress before it spreads further, via local CPE probes. CPE-embedded capabilities allow for deployment of countermeasures in a fast, effective way.

4. Proposed Approach

4.1 Management model

In response to the increasing difficulty to scale conventional ISP-level security solutions, the S3P project proposes a distributed security model taking advantage of the processing and remote management capabilities of *home gateways,* in a way that allows some of the security functions to be transferred to the client's equipment. Nowadays, *home gateways* are devices with a reasonable computational capability, which are available with no additional costs and are located at a privileged point of the network (between the network of a single client and the ISP network).This way they can be used to filter network traffic (in both ways), send important information to the provider and/or to the client (e.g., security alarms, usage patterns) and implement protection measures (like selectively filtering network traffic in response to possible attacks).

This way, the S3P Project proposes the creation of a decentralized structure in which *domestic gateways* act at the frontline of the internal network protection mechanisms, in order to deter the effects of an eventual attack to a domestic or to the ISP's network, or even to completely avoid it. Figure 1 presents this approach. In the S3P architecture, those *gateways* will start working in a coordinated way. Besides performing monitoring and attack prevention functions by their own means (based in configurations predefined by the provider) they can also notify the ISP's IDS of certain events and they can control the traffic based on the central IDS instructions.

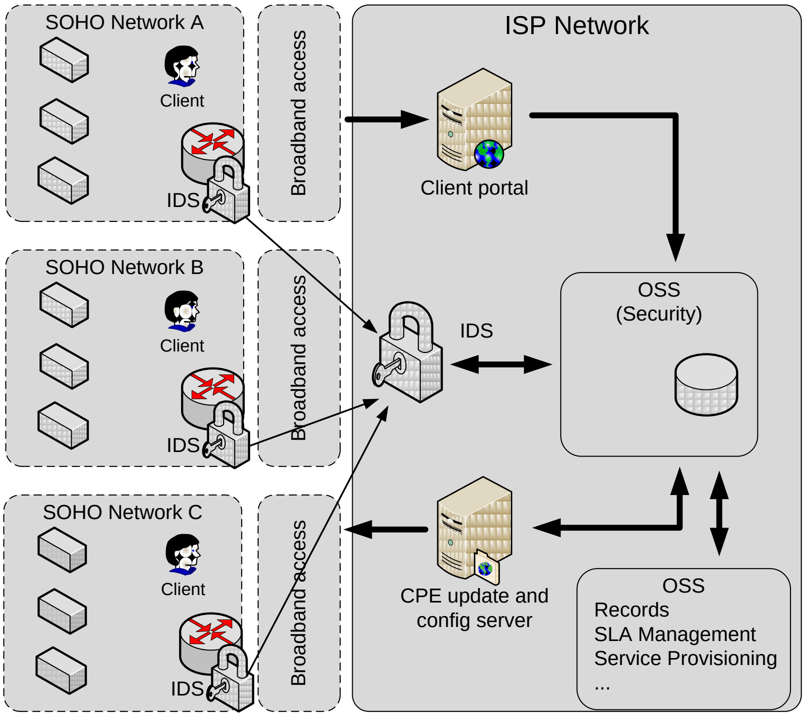

Figure 1: Generic Model of the Proposed Solution.

Since there will always be clients whose *gateways* will not cooperate with the IDS of the ISP and there will always be a risk of having compromised *gateways* inside the structure, consequently the confidence given by the ISP to each domestic *gateway* can never be absolute. The provider's platform must have enough flexibility to simultaneously deal with clients with cooperating *gateways*, clients with compromised gateways and clients without integrated *gateways*. In spite of that, and from a global standpoint, the potential benefits in terms of granularity and scale are considerable.
The proposed architecture is not only concerned with the idea of using the CPE to extend the reach of the provider's IDS, but it also tries to effectively improve the articulation between the client and the ISP networks. To achieve this the security policies adopted by the distributed IDS take the user's profile into account (e.g., user records, subscribed services) and they also concede the user a certain grade of customization, by means of a client's portal where one can, for example ask for explicit support for some of the applications or specify more detailed usage profiles that can have effects on the way the system works (e.g., parental control of Web contents).

The architecture foresees the use of entities (agents) present at the ISP and CPE levels (Figure 2). These entities will act based on the analysis of the data flow, besides other information that can be obtained from the databases of the ISP.

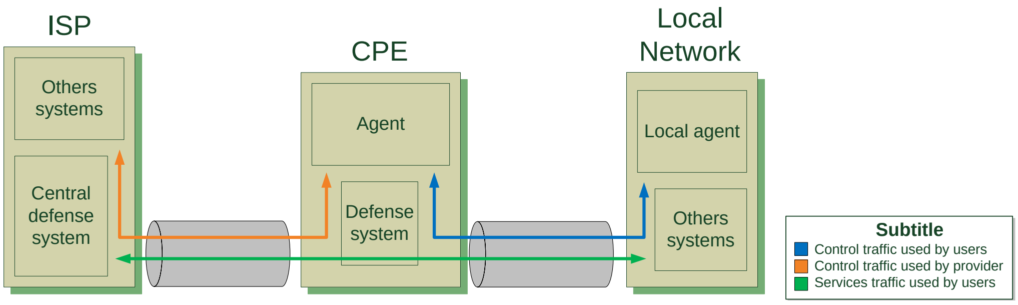

Figure 2: Scopes of influence in the S3P architecture.

As it can be seen in Figure 1, the proposed operation model is not fully distributed. A management infrastructure will be kept on the provider's side to coordinate the various intervenients on this process, orchestrating its operation based on the correlation of the pieces of information collected from the ISP network and from the different CPEs.

The existence of a profile management backend makes it relatively simple to the provider to deploy new rules or configurations for extended users groups, taking on account the specific profiles and of the installed equipments. Configuration management (Figure 3) is done by a configuration server (ACS, *Auto Configuration Server*), that makes the distribution of CPE software updates and the addition of new services. The communication between the CPE and ACS is assured by a in-house developed protocol stack that implements the TR-069 (or CWMP – CPE WAN Management Protocol) specification (Broadband-forum 2007), for the purpose of enabling secure communications between the provider and managed CPEs.

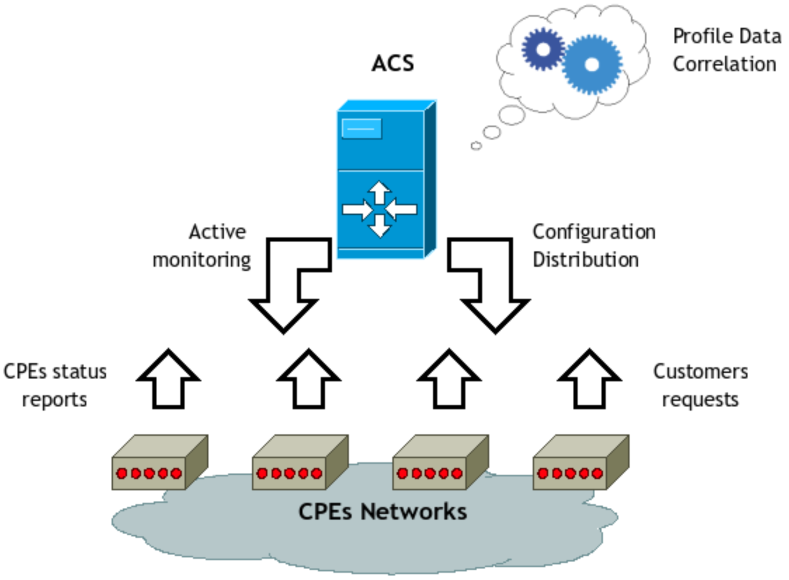

Figure 3: Relation between the ACS and CPEs

4.2 Security mechanisms and event treatment in the S3P architecture

The idea of assigning a more active role to *domestic gateways* is not new. *Firewalls* and *QoS* management capabilities are nowadays standard features in most of these equipments and they can be configured by users through Web interfaces. However, this approach is limited by a set of factors:

- The user has the responsibility to configure these tools, and he often doesn't have the adequate technical preparation.
- The gateway works standalone. There is no correlation of attacks with other users of the same ISP or with specific provider or LAN services.
- The capabilities of these tools are relatively limited, and they may not be robust enough for dealing with attack patterns which are getting more and more sophisticated each day.

In the S3P Project, these three weaknesses are addressed in several ways:

- Because of the higher sophistication of local security mechanisms, including packet filters, proxies, intrusion detection and prevention, *portscan* detection and many other mechanisms that usually are reserved for or found in bigger networks

- Sophisticated event management allows the system to correlate incidents that occurred on different clients and activate response mechanisms coordinated at the level of its network and of all its clients.

- Because the security configurations of each CPE are managed by the provider, even if the client's preferences have to be taken into account

The detection and the correct treatment of security incidents (that we will generically call events) is a key element in the proposed architecture. The generation and the treatment of events occur at two different levels:

- At the ISP level. The events received from the various CPEs are processed by the event correlation engine existing at the ISP level, allowing, for example, the detection of combined attacks either affecting or coming from several customers of the ISP. The provider can react to these events taking preventive measures on its own network and/or changing the CPEs' configurations (Figure 4).

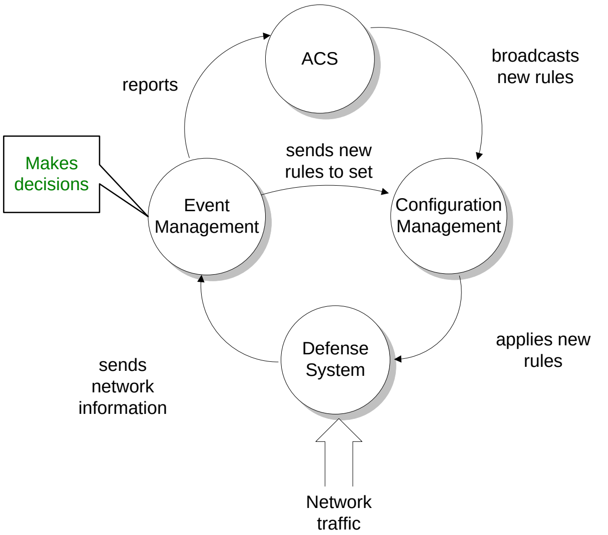

Figure 4: Operational model of the decision making process in the S3P architecture.

- At the local level (CPE), for efficiency and scalability reasons, and in order to allow a high granularity in the monitoring process, the CPE has a local event correlation engine (fed by events captured by traffic analysis tools, namely the intrusion detection system or the *portscan* detector and log records of the behavior of other tools, such as traffic flows filtered by the *firewall*, *proxy* and/or intrusion prevention system). All events are processed by the internal CPE correlation engine, being possible to activate counter-measures at the local level, based on the application of rules and procedures belonging to the security mechanisms of the CPE itself and/or with notification to the ISP level.

In general, the proposed platform works like a distributed intruder detection and prevention system with a broad scope covering the provider's network and the entrance/exit points of the clients' network, being capable of dealing with two levels of operation: CPE/microscopic and ISP/macroscopic. As an example, lets consider a group of customer networks that have just been attacked and infected by a *Trojan* and are taking part in a synchronized DDoS attack. Once the CPEs detect an abnormal activity pattern, they alert the provider through an event. On the provider's side, when the correlation mechanism detects a global pattern, it makes the distribution of new security rules (e.g., to restrict the usage of specific TCP/IP ports at the CPE level) to prevent the propagation of the attack to other clients. This example shows why the distributed event management system is of such a big relevance in the context of the S3P project architecture.

5. The S3P architecture at the CPE level

Figure 5 presents the architecture of the S3P platform, from the CPE perspective. The three main CPE modules are: the Defense System, the Event Management and the Configuration Management system. The CPE support system also includes the Failure Management and the optional Customer Network Monitoring module.

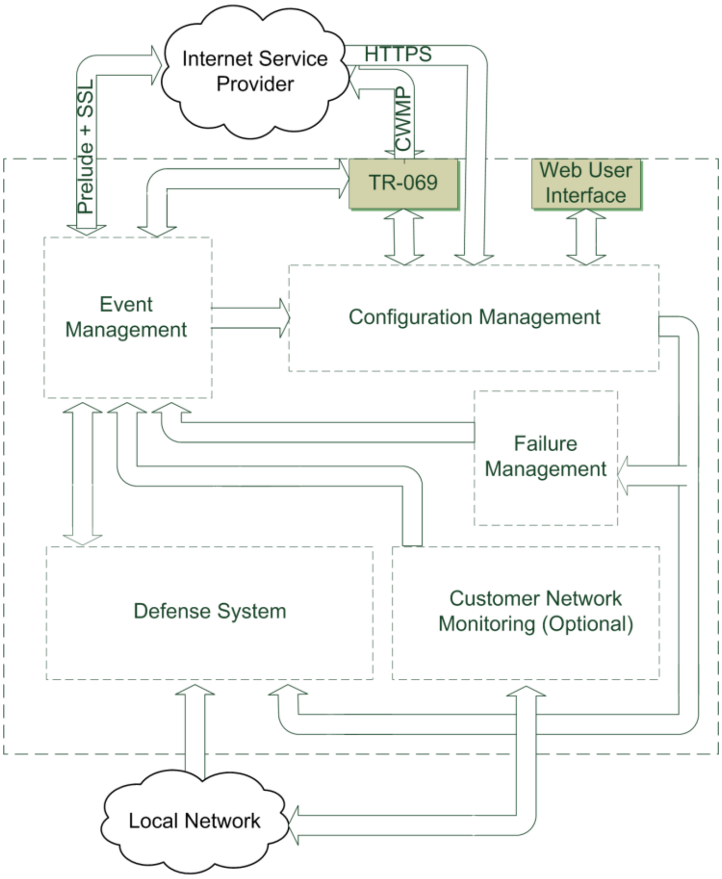

Figure 5: S3P architecture (CPE)

The Defense System aggregates the environmental active defense mechanisms and passive network traffic that flows through the CPE. Its configuration (rules, ACLs) is controlled by the ISP using the previously mentioned mechanisms. The Defense System includes a firewall, web filtering mechanisms (proxy and parental controls), intrusion defense/protection system, portscan detector, among others. Some of these components will play a passive role (portscan detectors, IDS), only generating events to feed the local event management engine. Others will play an active role, its configuration being dynamically modifiable by local or ISP decision, as a reaction to security incidents.

The Event Management System is based on the Prelude IDS platform (Vandoorselaere 2008) and includes sophisticated programmable event processing and correlation mechanisms (Chifflier 2008). From the event management perspective, events are originated from sensors (small agents) capable of collecting information from several sources and generating messages which, by their turn, are sent to the event management module through a secure connection in the form of IDMEF (*Intrusion Detection Message Exchange Format*) (Debar 2007) messages and kept on a local database.

The Configuration Management system is responsible for managing the CPE configurations (installed services, active configuration profiles). Configuration updates can be distributed remotely by the ISP or by the CPE itself (as a reaction to a security incident dealt locally by the CPE)

6. The S3P architecture from the ISP standpoint

Figure 6 presents the S3P architecture, from the ISP standpoint. The main components are the profile, security event and CPE management systems.

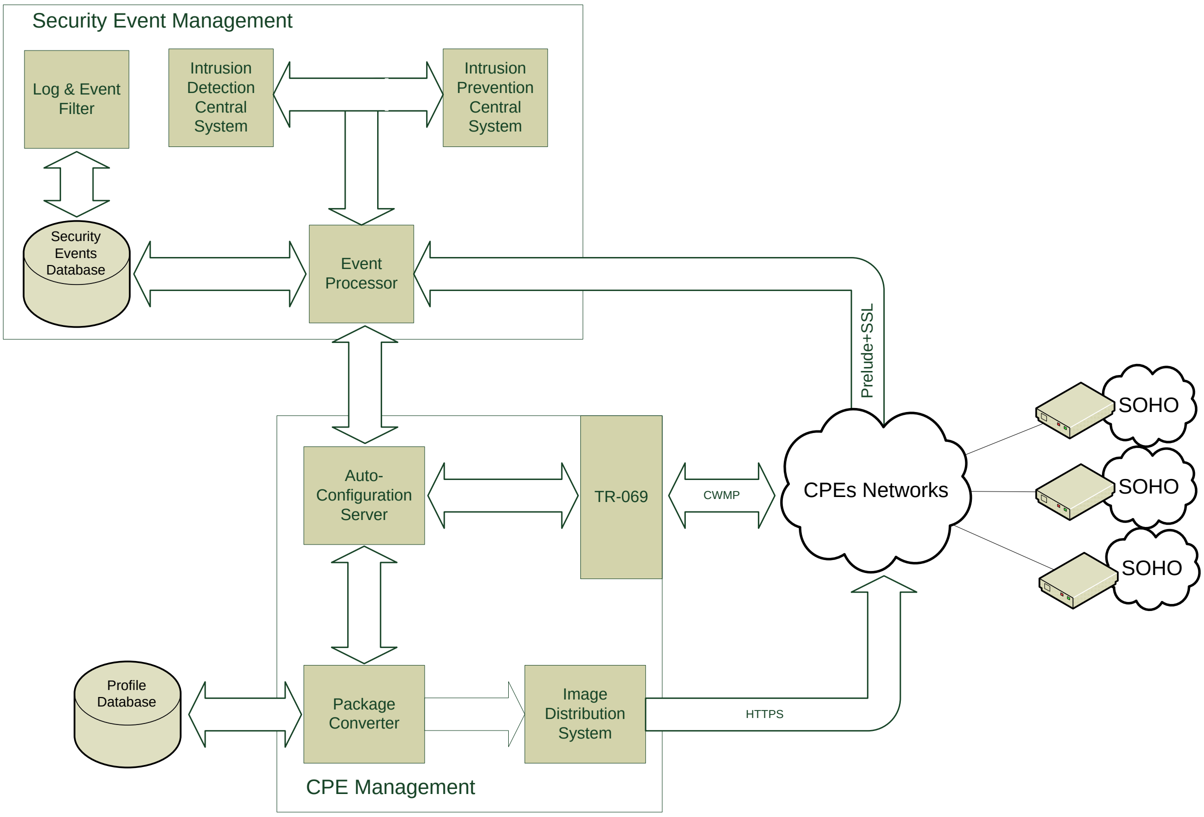

Figure 6: S3P architecture (ISP)

The security event management module is a security event correlation system – fed by the local event management modules of each CPE and also by events detected by sensors positioned in the ISPs own network – which allows for correlations of events detected by sensors installed on several points dispersed across the ISP's own network and activate the adequate orchestrated actions (traffic filtering at the ISP's own network level and/or local CPE firewall configuration updates).

The CPE Management system deals with the remote configuration of the CPE units (distribution of the applications and configurations to be used at each CPE) and monitoring of the operation of each one (detecting and reacting to operation failures). These tools are also used to manage configurations in a broader, generic perspective (e.g., updates, inventory) and also are used as a mechanism of remote intervention by the ISP in order to dynamically update/change the way CPE units work in response to security incidents.

The profile management subsystem ensures the maintenance of a database with equipment (CPE manufacturers, models and versions installed in each client) and user profiles (e.g., services subscribed to the ISP, preferences defined in the client portal). These profiles are essential to define which configurations must be sent to each CPE.

7. Related Work

Koutepas *et al.* (Koutepas 2004) and Wan (Wan 2001; Wan 2002) present a set of approaches against DDoS attacks based on local detection systems placed at various strategic locations in the entire Internet, constituting a distributed attack detection system. Attack alerts are communicated within the Distributed IDS using a flooding mechanism with messages formed in IDMEF - once attack detection has been established they install rate-limiting filters to fight.

Ioannidis et al (Ioannidis 2002) propose a solution against DDoS attacks using routers both for attack detection and response. Once a DDoS attack has been detected, the system uses custom filters to block traffic at the routers level. Events are communicated between cooperating routers using the special Pushback protocol - attacks are traced step-by-step closer to their sources and their bandwidth allocation controlled.

8. Conclusion

This architecture we have presented distinguishes itself by taking advantage of the domestic gateway – as a borderline device between the access network and the domestic network to create a security distributed platform, with benefits for the provider and for the client. Even if this approach seems to go against the traditional vision of the internet service – with the borderline boundaries on the ISP access network – it is adequate in face of recent developments like the introduction of *Triple Play* networks and with the growing adoption of standards for the remote management of the CPEs.

The next step will be the validation phase of the prototype with real users, in a testbed network, so that we can then go on with a more extended work of validation of platform scalability, by means of experimental measurements and analytical methods.

Acknowledgments

This investigation work has been partially sponsored by the Fundação para a Ciência e Tecnologia, by means of the DOMUS Project (reference POSC/EIA/61076/2004) and by the PT Inovação, by means of the S3P Project.

References

Broadband-forum (1994), Broadband Forum (online), http://www.broadband-forum.org

Broadband-forum (2006), “Functional Requirements for Broadband Residential Gateway Devices (TR-124) issue 1.0” (online), Broadband Forum, http://www.broadband-forum.org/technical/ download/TR-124.pdf, December 2006

Broadband-forum (2007), “CPE WAN Management Protocol (TR-069) specification v1.1” (online), Broadband Forum, http://www.broadband-forum.org/technical/download/TR-069Amendment2.pdf, December 2007

Chifflier, Pierre and Tricaud, Sébastien (2008), “Intrusion Detection Systems Correlation: a Weapon of Mass Investigation” (online), CanSecWest 2008, http://www.prelude-ids.com/fileadmin/templates/pdf/ correlation-womi-cansec2008.pdf, Vancouver, Canada, March 2008

Debar, H. et al (2007), “The Intrusion Detection Message Exchange Format (IDMEF)”, RFC 4765, March 2007

HGI (2006), “Home Gateway Technical Requirements: Release 1, Version 1.0”, Home Gateway Initiative (online), http://www.homegatewayinitiative.org/publis/HGI_V1.0.pdf, July 2006.

Ioannidis, J. and Bellovin S., “Implementing pushback: Router-based defense against DDoS attacks”, Network and Distributed System Security Symposium 2002, San Diego, California, February 2002.

Koutepas, G., Stamatelopoulos. F. ,Maglaris, B., “Distributed Management Architecture for Cooperative Detection and Reaction to DDoS Attacks”, Journal of Network and Systems Management, Vol. 12, No. 1, March 2004

Vandoorselaere, Yoann (2008), “Prelude Universal SIM: State of the Art” (online), *Libre Software Meeting* 2008, http://www.prelude-ids.com/fileadmin/templates/pdf/ RMLL_2008.pdf, Mont-de-Marsan , France, July 2008

Wan, K. and Chang R., “Engineering of a global defense infrastructure for DDoS attacks”, Proc. of IEEE International Conference on Networking, August 2002.

Wan, K., “An infrastructure to defend against distributed denial-of-service attack”, M.Sc. Thesis, Hong Kong Polytechnic University, June 2001.

WHS (2007), “Windows Home Server” (online), Microsoft Corporation, http://www.microsoft .com/windows/products/winfamily/windowshomeserver