Evaluating Common Privacy Vulnerabilities in Internet Service Providers

Panayiotis Kotzanikolaou, Sotirios Maniatis, Eugenia Nikolouzou, and Vassilios Stathopoulos

Hellenic Authority for Communications Privacy (ADAE)
{p.kotzanikolaou,s.maniatis,e.nikolouzou,v.stathopoulos}@adae.gr

Abstract. Privacy in electronic communications receives increased attention in both research and industry forums, stemming from both the users' needs and from legal and regulatory requirements in national or international context. Privacy in internet-based communications heavily relies on the level of security of the Internet Service Providers (ISPs), as well as on the security awareness of the end users. This paper discusses the role of the ISP in the privacy of the communications. Based on real security audits performed in national-wide ISPs, we illustrate privacy-specific threats and vulnerabilities that many providers fail to address when implementing their security policies. We subsequently provide and discuss specific security measures that the ISPs can implement, in order to fine-tune their security policies in the context of privacy protection.

Keywords: Internet Service Provider, Privacy, Vulnerabilities, Security Measures.

1 Introduction

Due to the social impact of privacy [1,2], the legislation in many countries explicitly recognizes privacy in electronic communications as a fundamental human right. In this context, the European Union has issued Directives concerning the privacy in electronic communications [3], while the EU member states are responsible to harmonize their legislation with the related Directives. Moreover, in several countries Independent Authorities are responsible to regulate and audit the proper implementation of privacy protection in electronic communications, see for example the Hellenic Authority for Communications Privacy (ADAE) [4].

Privacy in electronic communications refers to the right to communicate in private with others through a publicly available communication network or service. An electronic communications network may be a fixed line telephone network (such as PSTN or ISDN), a mobile network (such as GSM or UMTS), a wireless network (such as WiFi, Wimax, or Satellite), or a packet-based communication network such as the Internet or an add-on service, such as e-mail and voice over the Internet protocol (VOIP) services. Communication privacy involves the protection of all the communication data that are processed, stored and traversed through a public communication network or during the provision of an electronic communications service. Communications data can be distinguished in two broad categories [5]:

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 161–170, 2010.

- *Content data*, which comprise the actual content of the communication, and
- *Context data*, which are the external data of a communication, used for the establishment and provision of a communication.

The disclosure of the context data will in most cases affect the anonymity of the communicating parties. In some cases it may also affect the privacy of the actual content. For example, the context data during a web-surfing will also leak information concerning the actual content of a communication, since the IP address of the destination can easily be resolved to the related URL, which in turn can be accessed in order to describe, at least partially, the content of the communication.

Although privacy assurance requires the active involvement of both the user and the ISP, in this paper, we only focus on the role of the provider. Assuring the privacy from the ISP side requires a combination of technical, procedural and regulatory measures, based on ISP-specific security risks and security standards, either generic (e.g. ISO 27001:2005 [6]) or telecommunication specific (e.g. ITU-T X.1051 and ISO/IEC 27011 [7]). However, our experience has shown that although the vast majority of the ISPs have implemented security management programs, several common vulnerabilities exist, which can be exploited in order to violate the privacy of communications.

In this paper, we describe common security vulnerabilities of the Internet Service Providers (ISPs), which may lead to breach of communication privacy for their users. The results presented in this paper have emerged from a preliminary round of external security audits performed in a number of Internet Service Providers, operating in Greece. Moreover, we describe possible security measures to thwart these vulnerabilities. The rest of the paper is structured as follows. Section 2 describes the basic systems within the ISP environment, which are critical for the assurance of privacy in communications. Then it describes privacy-specific security threats that can endanger communications privacy. Section 3 points out common vulnerabilities that have been identified within the ISP environment and which may be exploited by privacy-specific threats in order to reveal communication data of the users. Also, it describes possible security measures that should be applied, in order to minimize the identified vulnerabilities and prevent privacy breaches. Finally, Section 4 concludes this paper.

2 Privacy Related Critical Systems and Threats

Most of the systems that are within the ISP's responsibility, handle communication data. For example, network elements such as routers and switches are used to enable the connectivity of a communication, and IT systems such as mediation devices and billing systems process communication data.

To start with, active network elements, such as wired or wireless access (layer-2) devices, switches, soft-switches, and routers, among others, are the primary systems that have to be protected, since they handle both user communication data (both content and context data), as well as signaling data, which still can reveal a lot of information about the user. If such a system is compromised, then a simple traffic analysis will reveal the actual communication, e.g. by extracting the contents of an email out of the TCP packets captured.

Table 1. Critical systems in relation to privacy

Category of System	Specific system	Criticality level in relation to privacy
Active Network Elements	Layer-2 access devices	Medium to High
	Routers	High
	Switches	Medium to High
	Soft-switches	High
IT Systems	E-mail servers	Very High
	Media gateways	High to Very high
	VoIP servers	High
	Web proxies	High
	P2P proxies	High
Passive Network Elements	Monitoring devices	Medium to High
	Management Devices	Medium to High
	Software tools & computers	High
	Data storage devices	High
Specialized Systems	Call Data Record systems	Very High
	Lawful Interception systems	Very High
	Data Retention systems	Very High
	Call Center systems	Very High

Apart from active network elements, IT systems that are related to specific communication services, like email servers, media gateways, Voice over IP (VoIP) servers, web proxies, peer-to-peer (P2P) proxies, etc., comprise an even more significant factor, since they contain the actual content and context of a user's communication (emails, visited web pages, voice sessions, etc).

Another type of critical systems from a privacy perspective is the passive network elements, such as monitoring and management devices, software tools and computers, and communication data storage devices. Such systems are important not only because they may allow direct access to communication data, but also because they can reveal accountability-related information, such as logical access to systems, administrative actions, and security-related incidents, among others.

Last but not least, there are specialized systems that may provide direct access to communication data due to operational or law enforcement requirements. The most imperative systems of this kind are systems that handle Call Data Records (CDRs), Lawful Interception systems and Data Retention systems.

2.1 Privacy-Specific Threats

Based on audit results performed on ISPs in Greece, we have identified the most commonly found privacy threats and we have mapped these threats to specific systems that are subject to these threats.

To ensure that the reproduction of your illustrations is of a reasonable quality, we advise against the use of shading. The contrast should be as pronounced as possible.

If screenshots are necessary, please make sure that you are happy with the print quality before you send the files.

1. **Masquerading by internal users.** This involves an internal user accessing a system by using an existing identity belonging to another internal user. In the environment of ISPs it has been found that it is common practice to use loose authentication and authorization policies for the internal users, despite the fact they are very strong for the external users. For example, the administrators of network elements or IT systems may share common usernames and passwords.
2. **Unauthorized use of data/systems/applications.** In addition to the above, it is quite common to find internal users with access privileges to sensitive applications and systems, although these users do not have official authorization, according to the security policy of the organization. This may involve systems managing CDR files and Call Center calls, which usually give access to sensitive communication data. Unauthorized use can be intentional or unintentional e.g. by misconfiguring access procedures and access rights.
3. **Embedding of malicious software.** Embedding of malicious software in systems like email servers or proxy servers may lead to loss of privacy for hundreds of users, if this is not noticed in time. A simple example is the installation of a passive interception tool which may monitor all the traffic in promiscuous mode.
4. **Communication infiltration/manipulation.** These threats mainly concern active network elements. Communication infiltration/manipulation may be the result of unauthorized use or of malicious software installed in an active network element. This will then put at risk the privacy of all the communications routed through the compromised network element.

3 Common Privacy Related Vulnerabilities and Possible Measures

Most of the systems that are within the ISP's responsibility, handle communication data. For example, network elements such as routers and switches are used to enable the connectivity of a communication, and IT systems such as mediation devices and billing systems process communication data.

3.1 User Account Management

User account management is a common area of user-related vulnerabilities in many systems with a large number of users. Concerning user account management, the following vulnerabilities have been identified:

1. ***Lack of personalized access and lack of accountability.*** The results from our security audits in various ISPs showed that within the ISP environment, it is quite common that the administrators share the same username/password, especially for systems such as edge routers in PoPs, proxy servers and WCS. This is also the case in remote management through dial-up. The modem is usually configured only with a single username/password shared among different administrators. Obviously this makes hard to ensure the accountability of the users and makes

the internal systems vulnerable to masquerading attacks by insiders, despite the fact that administrators are usually highly skilled and trusted users. Although the use of unique, personalized passwords introduces increased password management costs, these costs should be accepted by the providers it order to minimize possible impersonation attacks and lack of accountability.

2. ***Authorization control.*** Although the security policies of the ISPs involve periodic audits of user authorization privileges, this is rarely the case in the real environment. In several providers, accounts belonging to former employees have been found active, even in critical systems which are expected to be audited in short periods, such as the CRM. The lack of periodic audits has also lead to the existence of accounts with more privileges than the authorized ones. Such inconsistencies can be minimized if the security officer centrally maintains the personnel privilege management, by maintaining lists with the personnel access privileges as well as the possible changes to those privileges. On the other hand, the internal auditor should perform internal audits in critical systems, by matching the authorized user privilege lists against the actual user accounts.
3. ***Separation of duties.*** Most critical systems do not support the separation of duties between different kinds of users. For example, the system root/administrator can perform both the administrative and auditing action. This separation can be enforced by applying role-based access control (RBAC) systems. However, most versions of the widely used operating systems cannot support RBAC. This enables the system administrator to have access to the system logs, even if he may not formally be authorized to act as the system auditor.
4. ***Password management.*** Password management weaknesses have been identified in several systems within the ISPs. A commonly found security weakness is the use of unencrypted passwords for the initialization of user email accounts. Although these passwords are only used for the initialization of the account and this should not be considered as an important weakness, in some providers there is no automated policy in place to enforce password change after the first user connection to the e-mail service. The lack of password change enforcement policy is more common in web-based e-mail services. Another weakness found in the ISP environment related with password management is the use of admin accounts for ordinary purposes, despite the fact that the system administrators usually have different accounts for administrative purposes and for common purposes.

3.2 Logging and Auditing

System logging and auditing are the most valuable controls for the detection of security breaches, policy mis-configurations and system vulnerabilities.

1. ***Secure logging mechanisms.*** In most cases the ISPs maintain logging information that concerns system miss-configurations, erroneous operations or system performance evaluation, such as syslog information. In terms of security, user access logs are the most valuable log traces that are used by them. This information is not enough for guarantying the acceptable level of information privacy within the ISP premises. Indeed, system (network or IT) configuration files, application configuration files and executed commands (accounting) all consist of useful

security resources for preventing security breaches. More specifically regarding the network systems logging should also include the administrators' commands, as well as events retrieved from the AAA server including authorization, authentication and accounting logging. Regarding the IT systems, the transactions involving critical systems such as the Billing system, the CDRs and the e-mail servers should also be logged. A log file storing architecture should be also considered as an important security requirement. Experience shows that a centralized storage architecture with supportive distributed storing points is the most security effective method, since it provides a centralized control to the logging information, while the distributed storing points may support communication failures or achieve load balancing of log data when that is necessary. For information that is usually stored temporary in local memory (e.g. command history in IT systems) it should be transferred to permanent files at the earliest convenience. Also, the distributed storage points may be used in order to verify the integrity of the centralized log files. Since the logged events may contain context communication data of end-users, the confidentiality and the integrity of the logged data should be protected. Secure logging can be based on well-defined architectures and cryptographic techniques (e.g. [8,9]). The integrity of the log files can also be supported by applying immutable storage devices, such as WORM (Write Once Read Many) media.

2. ***Internal auditing controls.*** In most of the examined ISPs the already maintained log files can provide useful information for the identification and correction of possible security flaws and system mis-configurations. This however requires effective internal auditing procedures to be in place, in order to process and correlate the existing logging information. An ISP that uses secure logging for preventing security breaches should combine logging with effective auditing procedures. Auditing techniques can be continuous or periodic. Its aim is to identify the cause of a security incident and sometimes it gives evidences for identifying a security incident.

3.3 Contractors and Third Parties

A significant set of vulnerabilities discovered during our preliminary audits is related with the implicit trust assumptions between the ISP and its subcontractors or collaborating third-parties.

1. ***Trust Relationship between ISP and manufacturer.*** There is a substantial relation of dependence between the ISP and the various manufacturers of the systems used within the ISP. A manufacturer usually participates in all phases of a system's lifecycle within an ISP: from installation and configuration to support and maintenance. Thus, the manufacturers may gain knowledge of the network architecture and/or the configuration of various systems within the ISP. Moreover, in several cases the system/software manufacturers may have access to internal systems for maintenance reasons, which may lead to intended or unintended actions against users' privacy. Providers usually use state of the art technical and procedural measures to protect themselves from the potential harm of unauthorized use by the manufacturers, such as access controls, logging of operations performed

by the manufacturer, and control of components or patches to be installed through e.g. digital signatures, among others. We observed however that not all ISPs had similar levels of protection. Moreover, we observed that sometimes even ISPs with the strictest measures, in case of an emergency, could neglect formal access control procedures. Nevertheless, these measures are not a panacea. A manufacturer's expert, taking advantage of his explicit knowledge of the system, is potentially able to perform some actions that could pass over all the technical measures set by the ISP and therefore threaten communications privacy without being perceived. Unfortunately trust cannot be based on technical measures only. Trust is built over time and is further related with non-technical issues such as organizational reputation. It can also be based on strict bilateral agreements. However, the accurate enforcement of state of the art measures, frequent control of the system and reporting to technical managers, and frequent and in depth training of ISP's employees to gain good knowledge of the system, can eliminate the risks, although they demand additional resources (manpower, time, money).

2. ***Interconnection through other providers.*** The networks of the ISPs need to be inter-connected, in order ot provide world-wide connectivity to their subscribers. For example the communication data from a tier-3 ISP is forwarded between two regions through a tier-2 ISP interconnection. Data is usually not encrypted during transmission, so there is no technical guarantee that the interconnecting provider will maintain the same levels of protection. In case of a privacy incident, it is not always easy to technically discriminate the responsibility in case of interconnected providers. Trust comes into play again. Organizational reputation and bilateral agreements are the common measures followed by providers. For relatively low bandwidth interconnections, encryption or some kind of a VPN tunnel could provide a technical mean to overcome this vulnerability. For high bandwidth interconnections, the risk to analyze transmitted communication data is low because of the intrinsic difficulty to accomplish that and therefore current business models based on trust seem adequate. Regulatory controls can also provide a level of protection, by legally enforcing a common level of security for all the providers.
3. ***Provision of value-added services through third parties.*** The ISPs usually rely on third parties to provide some individual services. This is very common with billing services and value-added services (e.g. email). Of course such a provisioning increases the privacy related risks for the processed communication data. As in the case of interconnections, regulatory controls may legally enforce a common level of security controls for all the involved third parties, under the supervision and responsibility of the ISP. Enforcement of this rule however is not always straightforward, especially in the case of a third party organization residing in a foreign country where regulations may impose different security and privacy levels. Additionally, the ISP or the home regulator is difficult (or even impossible) to control the security level of the third party.
4. ***Co-location of systems.*** It is quite common that systems of various providers are physically co-located in the (shared) premises of a third provider. This makes easy for the administrators of one provider to physically access the systems of another provider. Moreover, in several cases it has been found that contractors of

providers or other third parties gain unattended physical access to the systems. In these cases, physical access control must be strengthened and vigorously enforced, in addition to existing logical access control measures, which may protect the systems from unauthorized use.

3.4 Perimeter and Network Security

This part of the auditing procedure was focused on the perimeter security of the provider's network, and specifically with well known-entities: firewall, intrusion detection and/or prevention systems, anti-virus/anti-spam software. The basic outcome is that providers are well-informed of the importance of those systems; however the actual implementation and proper monitoring reveals many weak points. A common practice found was the operation of network security systems under the initial default settings, without examining their suitability to the providers needs and without regular inspection of the produced results (e.g. log files).

Another major report was the inadequate antivirus/anti-spamming protection of internal networks. In some cases it has been found that the internal network of the ISPs is not adequately protected against virus and malware. Although in all cases anti-virus programs are used, in some cases no central antivirus administration is used, which may lead to outdated antivirus. Moreover, solutions that eliminate spam, phishing attacks, spyware are rudimentary operating without adequately protecting the internal users.

It is also worth reporting some issues concerning remote management of the network elements. It would be advisable to generally deny remote management and exceptionally allow under specific security restrictions; for certain cases and for certain users. For example, router management in many cases is performed using telnet over the insecure Internet. SHH2 is a secure replacement of telnet and the r-utilities, which provides strong authentication and encrypted communication over the Internet.

In case of a line-down event, modems are reported to be used for remote connection to routers, where the username/password pair is the only security measure. It would be advisable to restrict remote access from specific remote locations (e.g. IP addresses) using access lists and additionally to lock users after a certain number of unsuccessful login attempts.

3.5 System and Network Maintenance

The main report was the lack of systematic recording of the maintenance/installation/repair actions planned or performed on systems/networks, e.g. in a powerful ticketing system. This should be also coupled with a well maintained inventory of systems/networks, e.g. to allow for searching all actions performed in a certain device for a certain period of time. The above would be beneficial also in an auditing procedure.

Usually, installation, maintenance, and repair actions are performed either on site or remotely without a predefined procedure and recording of the specific actions. This would stimulate malicious users to install malicious code as part of the official software in order to gain access to internal resources.

The above example attains significant weight if one considers the same situation with critical systems, like Lawful Interception and Data Retention System. The installation of

an unwanted software module, e.g. passive monitoring tool may lead to the disclosure of sensitive information of thousands of subscribers.

The providers could ensure the authenticity and integrity of the system software, as well as its updates and patches by enforcing that each piece of software installed in the system is signed by means of a recognized electronic signature by its manufacturer. Moreover, key splitting could be used for any software changes together with electronic signatures. In this case, more than one authorized persons could cooperate to initiate the procedure of new or updated software installation.

4 Conclusion

The ISPs play a significant role in the protection of communications privacy. Even though most of the ISPs already employ a number of technical security measures to protect users communications privacy, the results from our external security audits report that a more effective and thorough application of technical, procedural and regulatory measures is required.

The importance of communications privacy mandates a thorough analysis and design of security policies to detect and prevent unauthorized and malicious actions by both insiders and outsiders. As it is shown by our preliminary auditing results, most ISPs do not always adequately apply the security measures set by their security policies in specific areas, such as user account management, logging and auditing, third party agreements, perimeter and network security, and system and network maintenance. Complementing an ISP's security policy with the proper handling of the aforementioned issues can provide a good level of guarantees on the protection of the communications privacy. We are going to further extend those preliminary security results and provide a framework, which will guide ISPs to perform self-audits and strengthen their network defense in support of communications privacy.

References

1. Warren, S.D., Brandeis, L.D.: The Right to Privacy. Harvard Law Review IV(5), 193–220 (1890)
2. The European Opinion Research Group: European Union citizens' views about privacy, Special Eurobarometer 196 (December 2003)
3. Directive 2002/58/EC of the European Parliament and of the Council: On Privacy and Electronic Communications, Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector. Official J. European Union, July 12 (2002)
4. The Hellenic Authority for Communications Privacy (ADAE), `http://www.adae.gr/adae/index.html?langid=en`
5. Zugenmaier, A., Claessens, J.: Privacy in Electronic Communications. In: Douligeris, C., Serpanos, D.N. (eds.) Network Security: Current Status and Future Directions, pp. 419–440. IEEE-Wiley (2007)
6. ISO/IEC 27001:2005 Information technology – Security techniques – Specification for an Information Security Management System (2005)

7. ISO/IEC 27011 Information technology – Security techniques – Information security management guidelines for telecommunications (draft), will be published jointly as ITU-T X.1051 and ISO/IEC 27011
8. Stathopoulos, V., Kotzanikolaou, P., Magkos, E.: A Framework for Secure and Verifiable Logging in Public Communication Networks. In: López, J. (ed.) CRITIS 2006. LNCS, vol. 4347, pp. 273–284. Springer, Heidelberg (2006)
9. Stathopoulos, V., Kotzanikolaou, P., Magkos, E.: Secure Log Management for Privacy Assurance in Electronic Communications. Elsevier Computers & Security 27(7-8), 298–308 (2008)