Social Networks: Security and Privacy

Laerte Peotta de Melo, Edna Dias Canedo, Robson de Oliveira Albuquerque and Rafael Timóteo de Sousa Júnior

***Abstract*— This paper presents a study on social networks services and a survey of the attacks and malicious use of this interaction mechanism whose utilization is continuously growing. Increasingly, social networks sites are investing in security mechanisms, which are dependent on the understanding and awareness of the users to follow the security models provided by the service providers. This paper proposes a model of security and privacy on social networks to improve security and reduce the risks associated with them. This model is designed as referential for evaluating security and privacy indicators over actual social networks services.**

***Index Terms*—Social networks, security, privacy, attacks, defense measures and security model.**

I. Introduction

Nowadays the increasing utilization of social networks is becoming a strong tendency in the Internet, mainly due to the possibility of expression of ideas and socialization by means of communication mediated by computer (CMC) tools. Such tools provide the actors in the network to build, interact and communicate with other actors, leaving on the Internet traces that allow the recognition of their connection patterns and their social networks through these connections. Social networks have become a global and cultural phenomenon by adapting the concepts of real life interactions from social groups to the cyber space.

Social network sites (SNS) allow individuals to present themselves with an online profile and to establish or maintain links and connections with other actors, building what is commonly referred as their social network profile. Moreover social networks enable the grouping of individuals into specific virtual groups. A social network presents two basic elements: actors (users that can be represented by a weblog, a fotolog, etc.), and connections (relationships, which are the interactions or social ties). The connections of a social network can be perceived in different ways, being dynamically formed through social interaction between actors. This way, the actors and their social connections are similar to the real world, where a circle of friends in a social group is composed of people linked by friendships. The participants use social networking sites to interact with people they already know in the real world or to meet new people, based on common interests, such as friendship, business, hobbies, sexual orientation, etc. Actors may join virtual groups in search of people with similar characteristics, based on information showed in their profiles. Normally an actor belongs to various social groups, at the same time, sharing different personal characteristics with each group. Social networks in the Internet have specific features, either to allow the networks to be perceived as a comprehensive tool by the user and also to allow the information about the network behavior to be apprehended by this user.

Social networks can be analyzed from different points of view. For instance, the work described in [1] presents a study based on a social vision and an economic vision. The focus of this paper is the security and privacy aspects of social networks. Therefore, we first review common attacks in these networks, and then we present some defensive measures. At last, we propose a security evaluation model for social networks systems.

A. Attacks in Social Networks

Providers of social networks, like any other web application, are vulnerable and may become a target of direct attacks. Security vulnerabilities can provide (to attackers) ways to attack and cause failure of service providers (ex, denial of service), unauthorized access to accredited users data (followed by disclosure of confidential information) or be used to spread a virus among user accounts. Vulnerabilities such as cross-site scripting (XSS) or SQL injection in social networking applications can affect millions of users. Malicious users can use XSS vulnerabilities to steal cookies, accounts, run applications in flash, inducing users to download malware, etc. [4]. Moreover, the attacker can take control of visitor´s browsers by inoculating infected images, HTML tags or JavaScript instructions, allowing the spreading of keyloggers, trojans and other malicious tools.

Social networks are growing rapidly and their operation is beyond the concept of a simple buddy list. Social networking sites must recognize some fundamental aspects of human social interaction and put forward strong and intuitive methods for their implementation in the software level, so as to provide the necessary level of protection, privacy and trust, in terms understandable by humans.

Reference [2] presents a study on the future of social networks and their security aspects, specifically current threats against these networks.

B. Paper Organization

The rest of this paper is organized as follows. The next section is a description of the main forms of social network services.

Section 3 contains a survey of main attacks and malicious behavior in social networks. Section 4 presents defense measures used in social networks. Section 5 presents the proposed model of social safety in social networks. Finally, we present our conclusions about the subject.

II. Social Networks

An important element in the study of social networks is to understand the differences among social networking sites. These SNS are spaces employed by users to express their social habilities on internet. Such SNS are systems that allow the construction of an individual virtual personality by means of a profile or a personal page. This page is used for interaction with other actors through comments and the public exposition of the network of friends of each actor. The SNS are also a category of social grouping software, which are systems with direct application to computer-mediated communication. A contextualization of the main SNS in the Internet is presented in next sections, while a more detailed study of these SNS is presented in [3].

A. Orkut

It is a SNS that has become very popular among Brazilian Internet users and in India since 2006. Orkut combines several features such as the definition of profiles focusing on the users interests, the creation of communities and visualization of members that belong to the social network of each actor. It basically works based on the concepts of profiles and communities. The profiles are created by the actors after sign up, indicating who their friends are. The user is able to publish multimedia content linked to his profile and can write comments in other users scrapbooks. Communities are created by actors and allow the joining of users, thus serving as forums, with topics and messages.

B. Fotolog

Fotologs are publishing systems that allow the actor to publish photos accompanied by short texts and receive comments. In general, a fotolog interface is quite simple. Each fotolog has a private address where the user publishes his photos. This address acts as a personal page, as it identifies the actor or the group that uploads the photos. Moreover, the actors can publish their friend lists and links to other content.

C. Flickr

Flickr is a site that allows the publication of photos, texts that accompany them, comments and video. Furthermore, it allows images to be tagged with keywords for searches and classifications. At Flickr, it is necessary to have a personal or a professional account.

D. Facebook

Facebook works through profiles and communities. In each profile the user can add modules for gaming applications, tools, etc. It is often perceived as more private than other social networking sites because only the actors who belong to the same network can see the profile of each other. Facebook allows the actors to make their own applications, turning the profile a more personalized one.

E. MySpace

MySpace allows the display of social networks and interaction with other users, building profiles, blogs, groups, photos, music and videos.

F. Twitter

Twitter is a site commonly known as microblogging, because it allows short texts to be written with up to 140 characters. It is structured with the concept of followers and people to follow, where each user can choose who you want to follow and be followed by others. You can send private messages to other twitters and pages can be customized by twitter, building a small profile.

G. Utilization Map

Figure 1 shows a map of the use of social networks in the world, as presented in Patsakis *et al* [7]. Recent researches show that SNS are increasingly becoming part of everyday life of people. The sites that are most widely used are Facebook, MySpace, Bebo and Hi5, being Facebook the most popular site among the English-speaking countries [7]. Orkut is the SNS most used in Brazil.

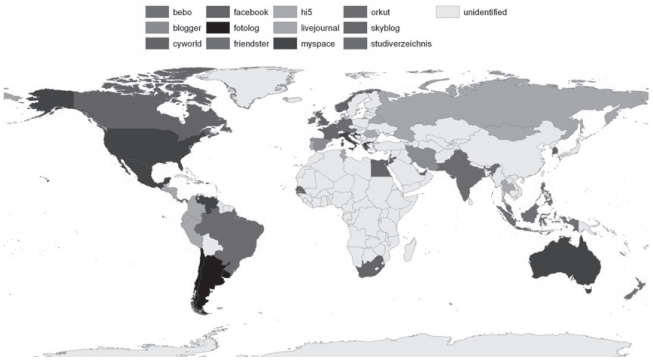

Figure 1: The world map of Social Networking [7]

III. Major Attacks and Malicious Use

With the increasing use of SNS, security problems multiply as well because several personal information are exposed to all kinds of actors / users, so this information can be published and used in an unwarranted way by any attacker.

The access to social networks is commonly done through a web application, so vulnerabilities may be intrinsic to the service. However some attacks seek to overcome the security barriers a web site and explore techniques such as social engineering and trust among users.

Each attacker has his own motivations, being interested in specific targets or not, either trying to obtain financial gain or just playing around, but trying to basically obtain and disseminate information of the other users. Below there is a review on the main attacks and malicious use of social networks.

A. Credentials robbery

The credentials robbery is directly associated to identity robbery. In this case, information regarding a user of a social network is employed in order to defraud or deceive other users who belong to the same relationship environment.

Many countries already have specific laws to treat cases of identity robbery, as the Act of 1998 that defines it as crime in the U.S.A., expressing that it is a crime to use in a conscious way, without express authorization, any means of identification of another person illicitly [5].

The most common form of this type of attack is to obtain the user login information through an active system, such as a keyloger or a spyware. However, recent reviews of trojans found software codes that capture the information in a transparent way, simply by analyzing the network traffic between the infected machine and the social network servers.

These methods of attack are effective when the victim presents some involuntary collaborative behavior. In other words, they are based on social engineering, which basically compels the user to execute some application or click on a received link inducing him to download and execute malicious code. This method is inoperative when the user follows security rules often provided by the server of social networks. Therefore some attacks employ hacker techniques to compromise a system where user information can be collected.

B. Fake Identity

In this case a new identity is created with information from a person that is not a user of social networks. The fake personality is profiled either seeking to obtain trust from a network of users or, in some extreme cases, just to denigrate the image of a user. This kind of attack is becoming more common in situations where an attacker first assumes a fake identity and then tries to impersonate another user.

To obtain a successful fake identity the attacker has to induce some degree of trust to other users, so information from the victim should be consistent and convince other people. Therefore various techniques are used in obtaining the information, including:

a) Research information about the victim in search sites;
b) Direct access to information through other people;
c) Recovery of documents from recycle bin (dumpster diving);
d) Theft or robbery of documents;
e) Deviations of postal correspondence;
f) Social engineering techniques.

It is possible that in some cases the fake identity is modified to make hard its association to a real person. In this case the attacker does not want to pretend to be someone else, but just hide his real identity informing data that composes another identity that seams to be from a real person.

C. Exploitation of Trust

This mode of operation can be done automatically or manually. In manual mode, the attacker seeks to enter into a community and behave as trustworthy user. In normal situations it takes some time until all users start to trust this user. After that he is able to perform some kind of attack as social engineering, using techniques that are based on behavior and observation.

The automatic mode is related to identity robbery, given that using proper tools and in possession of a trusted identity it is possible to perform some attacks, such as providing a link that takes a user who relies on another user through a chain of trust to install some type of malware, such as a trojan, keyloger or even a botnet client.

D. Bulling and Cyberbulling

This term that was first used in Great Britain refers to a form of cruelty that occurs in relationships among children and teenagers who are bullied or harassed in a violent way, making the victims unable to defend themselves. It is closely related to attitudes of intentional aggression, which causes distress to the victims, but it consists of making an aggression by means of an obsessive joke.

The basic difference between bullying and cyberbulling is the presence of the aggressor, that is not necessary in cyberbulling, but also the extent of this attack that is larger than bullying [6].

The interesting psychological aspect of this attack is that in cyberbulling the attacker does not visualize the reaction of the victim, thus eliminating some common human reactions such as remorse.

Moreover the identity robbery that allows the attacker to present a fake identity can be used either to hide the localization of the aggressor, or in some cases, to make the victim to blame other innocent users.

E. Phishing

This kind of attack uses techniques to compel a victim to report some information directly to the attacker. Basically, data is collected from responses coming from the victim user after this user receives some request through spam, either by email or exchange systems (such as P2P). The attacker is also able to diffuse this data to other attacker by means of messages through their own social networks.

To be successful, phishing combines the described techniques of identity robbery, fake identity and trust

exploitation. This way, phishing has evolved significantly. In some cases, when a computer is inoculated by the phishing malware, the user identity information is captured and employed for automatically sending email and other messages through message exchange programs. Also, links are inserted in the user profile pertaining to a community in social networks, inducing a higher level of trust to whom is receiving this type of message. In other words, a victim user receive messages from multiple channels and these messages are sent by someone who is part of the user's relationship network (i.e. which is already part of the user's chain of trust). That makes it really difficult, from the point of view of defensive screening, the identification of the origin of the attack.

Furthermore, it is possible for the attacker to exploit the number of participants and followers on social networks. Automated systems are able to transfer user bases for participants who seek recognition by the amount of associated followers and are also used to sending messages to self-promotion, or simply sending spam.

IV. DEFENSE MEASURES

SNS are intensively investing in security. However users should be aware of the available protections and follow the security models that these sites offer to them, but the major responsibility should be over the companies that provide this type of service.

As some attacks described in this paper are based on social engineering techniques, it becomes very difficult to detect that some type of corruption has occurred. Basically the identification of incidents is performed through denunciations coming from the virtual community participants. Therefore, the human factor is preponderant in security systems on social networks, thus making a strictly technological security model completely utopian.

In general, security models depend on how a user deals with his information. In other words, it does not matter how much strong the security is, if the user is careless with his information [9]. Because users employ easily deductive passwords, accept invitations from other users indiscriminately, use public computers with few or no control, click links received in email from strangers, etc., it is very difficult to implement defensive measures.

Conversely, providers of social networking services must not completely transfer the security responsibilities to their users. Indeed these providers must follow procedures to identify and manage any type of security incident, keeping users safe and protected, as well as respecting the privacy and guaranteeing the terms of use of the information provided by the users.

Table I presents a summary of attacks and security measures that can be used as prevention or reaction mechanisms. It also indicates the stages in the security model proposed in this paper.

Table I: Summary of attacks and security measures

Attack	Description	Stage	Security measures
Credentials robbery	Associated directly to identity robbery. In this way, information of users of social networks is used in order to defraud or deceive other users who belong to the same ambience relationship.	1, 2 and 3	– Mutual Authentication Model
Fake Identity	A user employs some means to impersonate another.	1	– Data mining Analysis Models
Exploitation of Trust	In manual mode, the attacker seeks to enter into a community and behave as a trustworthy user, but it takes some time until all users start to trust this user. In automatic mode, to the attack is based on identity robbery, and using proper tools to diffuse the false idea of a trusted identity.	3	– Model Trust and Reputation
Bulling and Cyberbulling	Bulling is a form of cruelty in relationships among children and teenagers who are aggressed or harassed in a violent way, making the victims unable to defend themselves. Cyberbulling is similar but without the presence of the aggressor.	2 and 3	– Data mining Analysis Models
Phishing	Capturing information from careless users.	1, 2 and 3	– Intrusion Detection System (IDS) and monitoring data from site. – Model Trust

V. Proposal of a Model for Social Safety Networks

Security models seek to find an aggregate structure of protections that allow the improvement of the safety to their users. However the weakest point in the case of a SNS security model would be the user of social networks himself. Therefore the proposed model described hereafter tries not to transfer or to be based in the user's security system.

Given this context, Figure 2 shows a security model that relies on the SNS, thus making them responsible for the security. The model is divided into three stages, which are explained below.

A. Stage 1

At this stage the model tries to identify the action of automated attack processes, commonly known as robots, avoiding that these actions take effect without the necessity of human interaction, thus preventing such attacks. The authenticated user interacts with the system, but it is possible to identify whether it is a human or computer, based on the entropy of this interaction. For this reason, it must be requested that the interaction is analyzed by means of the Turing test. Completely automated public Turing tests are able to tear apart computers from humans. These tests, commonly abbreviated to Captcha, in the case they identify the human user, allow this user to access the system.

B. Stage 2

At this stage it is possible to identify changes in user behavior through activities and other variables that can be mapped and used. If distortions occur regarding the behavior of the user it might be requested to obtain user confirmation by means of positive identification, assuming user has some other secrets, or other information that is only known by the user and assuming that the attacker is unable to know it. However it is necessary to employ a second model of authentication and identification (not just user and password).

C. Stage 3

Being a little more complex, this stage can seek to identify the malicious utilization by seemly legitimate users, ghosts (created just to exploit the system), or even other users who have compromised the credentials of other users. In this case, one of the most common attacks would be sending links and information that could be used to trick a user of a trusted community, using the reputation acquired earlier, as already discussed in section III.

In this case it is necessary to the service provider to establish a policy of minimal use, being necessary to have controls to what can be done and in what amounts it can be done.

If the utilization policy is violated or even if there is an effort do it, users must have their accounts blocked, from a few minutes to several days, depending on the security policy, or even be banned from the social network community.

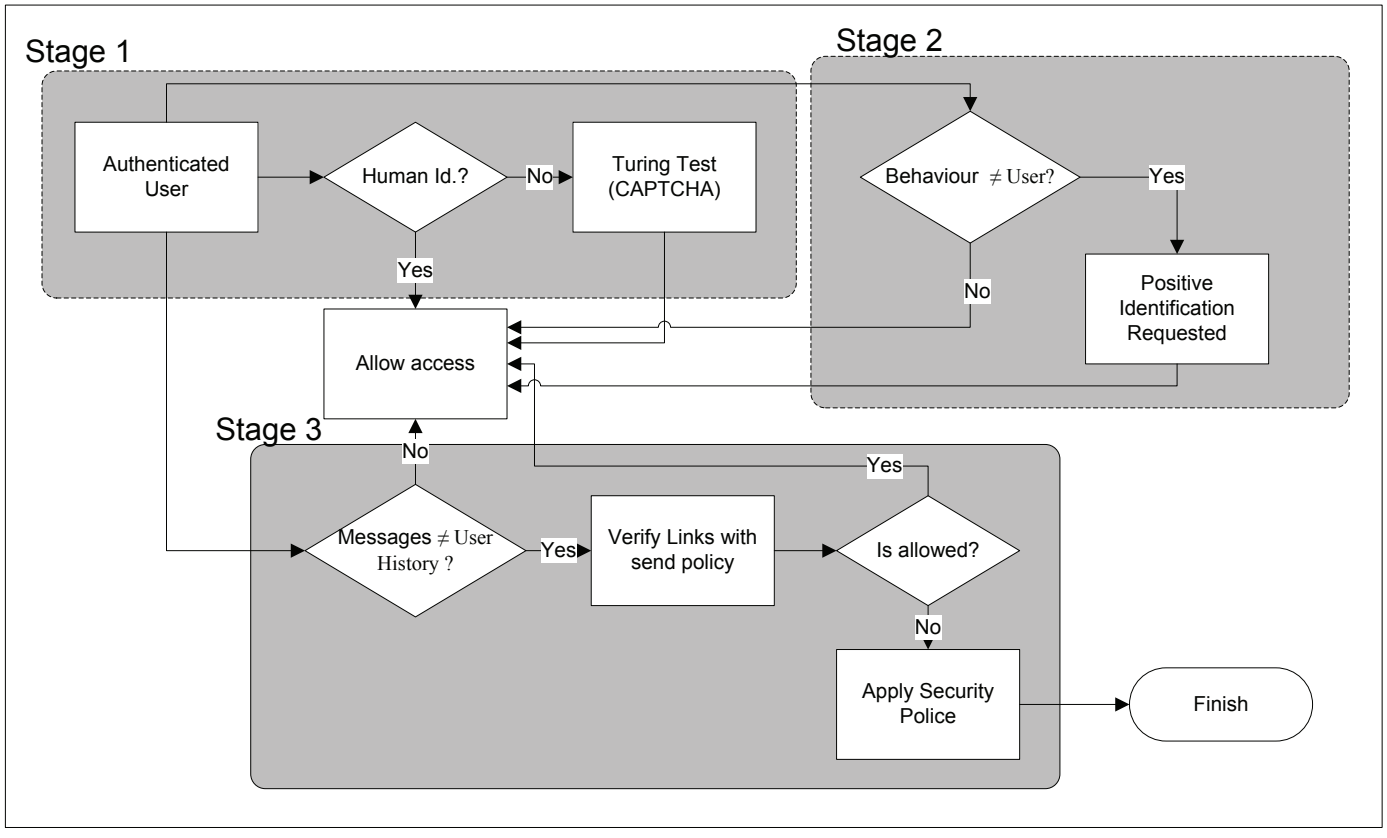

Figure 2: Model of Social Networks Security.

VI. Conclusions

The growth of social networks in recent years turned these networks a nowadays reality for companies that are entering in this environment previously dominated by ordinary users. Thus the security of social networks becomes a critical factor to business, as well as to the common user.

Considering the attacks that already exist in social networks, there are security measures intended to improve safety and reduce risks, thus making the environment safer to the users.

The model proposed in this paper has the minimum requirements to address the attacks reviewed and assess the presented defense measures. It is important to note that the proposed model in this paper seeks to remove the security responsibility from the user. Also a critical success factor for this model is the identification of the incidents in time to be able to avoid or counter the subsequent attack. This consideration requires the model to identify the origin of the attacks and their targets, then allowing identifying the taxonomy of the attack and the attacker's motives.

The complexity of social networks is constantly increasing once it creates new interfaces with greater interaction between users. As example of such new interfaces there are the cooperative and online games, collaborative works and online data, and tracking of mobile users.

Regarding the legislation subject, it is pretty scary what security and forensic specialists faces when analyzing social networks. Issues of digital crime are daily reported because there is not yet a global consensus about laws in these environments. As a global effect it occurs that what can be considered a crime in one country is not necessarily is the same in another. Therefore it would be reasonably to think of an adaptive model so the collaboration work of law enforcement could be achieved.

Also, there is the problem of identifying and associating the criminal to the crime, in many cases it can derail an investigation based on fully digital environment. In many situations, some forensic techniques may be required, but many social networks are based in distributed systems, thus the evidence collection procedure is hard and requires interactions with Internet Service Providers, companies themselves and even with users. In many cases they are in different cities and even in different countries, which can generate international incidents. In such cases the interaction with international law enforcement is totally necessary and beyond the scope of a security model for a social network site.

References

[1] Donald Steiny, "Unsocial Networks - Restoring the Social in Social Networks". Proceedings of the 42nd Hawaii International Conference on System Sciences - 2009: pp.1-10.

[2] Anchises M.G. de Paula, "Security Aspects and Future Trends of Social Networks". Proceedings of The Fourth International Conference on Forensic Computer Science (ICOFCS). Pp.66-74.

[3] Recuero Raquel, "Redes Sociais na Internet". Porto Alegre: Sulina, 2009. 191p.

[4] Weimin Luo, Jingbo Liu, Jing Liu, Chengyu Fan, "An Analysis of Security in Social Networks," dasc, pp.648-651, 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009.

[5] Paget, François. Roubo de identidade, McAfee Avert Labs, 2007. Acessível em www.mcafee.com/us/local.../wp_id_theft_br.pdf

[6] Morais, Tito. Bullings e Cyberbullings. 2007.

[7] Patsakis, Constantinos and Asthenidis, Alexandros and Chatzidimitriou, Abraham. Social Networks as an Attack Platform: Facebook Case Study. ICN '09: Proceedings of the 2009 Eighth International Conference on Networks. 2009, pp: 245—247. IEEE Computer Society Washington, DC, USA.

[8] Grzegorz Kolaczek. "Trust Modeling in Virtual Communities Using Social Network Metrics". Proceedings of 2008 3rd International Conference on Intelligent System and Knowledge Engineering.

[9] Centro de atendimento a incidentes de segurança – CAIS/RNP. Segurança em redes sociais: Recomendações Gerais, 2009. Acessível em http://www.rnp.br/_arquivo/disi2009/rnp-disi-2009-cartilha.pdf.

[10] Social Networks - Problems of Security and Data Privacy (Background Paper). The Council of European Professional Informatics Societies (CEPIS), 2008.

Edna Dias Canedo is graduated in Systems Analysis by Universidade Salgado de Oliveira; Goiás (1999). Master degree by Universidade Federal da Paraíba UFPB in the domain of software engineering (2002). She is currently following her PhD program at Universidade de Brasília (UNB) and is professor of the Software Engineer Course in the Gama Institute, of the Universidade de Brasília – UNB.

Laerte Peotta de Melo is graduated in Electrical Engineering with emphasis in Electronics by Universidade Presbiteriana Mackenzie-SP (1996), Specialization in security of computer networks by Universidade Católica de Brasília (2004), Specialization in computer forensics by Universidade Federal do Ceará (2007), Master degree in Electrical Engineering by Universidade de Brasília (2008). He is currently following his PhD program at the Universidade de Brasília (2008).

Robson de Oliveira Albuquerque is graduated in Computer Science by Universidade Católica de Brasília (1999). Specialization in Computer network by União Educacional de Brasília (2000). master's degree by Universidade de Brasília (2003). Master degree (DEA) in computer systems and programming by Universidade Complutense de Madri (2007). Doctorate in Electrical Engineering by Universidade de Brasília (2008). Presently he is a federal public employee, researcher at Department of Electrical Engineering of UnB, researcher associated to the Grupo de Análisis, Seguridad y Sistemas (GASS) at Universidade Complutense de Madri and he is following a doctorate degree program at Universidade Complutense de Madri.

Rafael Timóteo de Sousa Jr. is graduated in Electrical Engineering by Universidade Federal da Paraíba, Campina Grande (Brazil, 1984), Master degree (DEA) in Telematics and Information Systems by École Supérieure d'Electricité - SUPELEC (France, 1985) and Doctorate degree in Signal Processing and Telecommunications by Université de Rennes I (France, 1988). He performed his sabbatical year research on computational trust in ad hoc networks at Ecole Supérieure d'Electricité - SUPELEC (2006-2007). He is an associate professor of the Universidade de Brasília in the domains of Computer Networks Engineering, Information Technology and Information Security.