Security Aspects and Future Trends of Social Networks

Anchises M. G. de Paula, iDefense

Abstract— **Social networks represent a new opportunity to online uses and a challenging scenario to security community. They bring new opportunities to users interact and socialize; however, the overwhelming amount of information generated, exchanged and redistributed by users demands the adoption of new tools and techniques, which are the object of this paper. The understanding of all implications of social network to human social interaction and society overall, will bring new ideas and challenges to consumers, businesses and governments worldwide. This report will analyze the social network phenomenon, focusing on its security implications and perspectives in the near future.**

Index Terms—**Social Network, Security, Predictions, Trends**

I. Introduction

THE last few years have seen the rise of a new trend on the Internet: online social networks. Social network is the grouping of individuals into specific groups, like small rural communities or a neighborhood subdivision [1]. Such networks quickly became a global and cultural phenomenon by adapting the concept of real-life social groups and interactions to cyber space. Web 2.0 technologies have been empowering social network platforms by making them more interactive, and the majority of online users are already attached to one or more social networks. From the personal spaces of Facebook, MySpace, Orkut and Windows Live to more interactive platforms like wikis, blogs, Twitter and online worlds (such as Second Life and World of Warcraft), hundreds of millions of users are building online communities and connecting to each other. Social networks are changing the way users interact, share information (personal data, opinions and news) and do business online, turning the communication-focused Internet that we know into a new social Web platform.

Social networks have their drawbacks. Despite the specific security risks related to their normal usage (such as information disclosure and privacy issues), they have become an attack vector for phishers, fraudsters and sexual predators. Cyber criminals are adapting their strategies and tools to target social network users and are improving their attack technologies to target Web 2.0 applications. Traditional offline criminals are also adopting the social networks to run their activities online, and offline crimes are moving to cyber space. From the user perspective, trust and privacy on the social Web remains a hot, yet unresolved topic.

II. Current State of Social Networking

A. Main Purpose and Characteristics

Social network sites allow individuals to present themselves in an online profile and establish or maintain connections with others (usually known as “friends”), building their social networks. A social network consists of two fundamental elements: nodes (users) and connections (their relationships). This is similar to the real world, where a circle of friends in a social group consists of people connected by friendships.

Participants use social network 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, medical interest or sexual orientation. Users can join virtual groups and search for people with similar characteristics, based on their profiles’ information. People usually belong to several social groups at the same time, sharing different personal facets with members of each group.

What makes social network sites unique is that they enable users to articulate and make their social networks visible, so the public display of connections is a crucial component of these services. The “friends list” contains links to each friend’s profile, enabling viewers to browse users’ networks. Features usually include groups, communities and message boards, albums, comments (also known as “scrapbooks”), ranks and private messaging. Many providers also offer music or video-sharing capabilities, built-in blogging (such as MySpace) and instant messaging technology (such as Orkut, which has an embedded GTalk interface).

Social networking benefits strongly from large-scale coverage; users have greater interest in social networking services as more of their friends use them.

History

SixDegrees.com was the first recognizable social networking site, launched in 1997. It allowed users to create profiles, list their friends, surf the friends’ lists and send messages, representing the first provider to combine the most popular social networking features. While SixDegrees attracted millions of users, it failed to become a sustainable business; in 2000, the service closed.

From 1997 to 2001, a number of community tools began

Anchises M. G. de Paula is with the iDefense Security Intelligence Services, a VeriSign company, Brazil (e-mail: adepaula@verisign.com).

supporting various combinations of profiles and publicly articulated friends, such as AsianAvenue, BlackPlanet, MiGente and LiveJournal (see Exhibit 2-1) [2]. The first business-oriented network site, Ryze.com, launched in 2001, was followed by Tribe.net, LinkedIn and Friendster. Friendster gained traction among early adopters and grew to 300,000 users through word of mouth before gaining attention from traditional press media, building the road to MySpace and Facebook. From 2003 on, several social networking sites launched and became popular, proliferating worldwide.

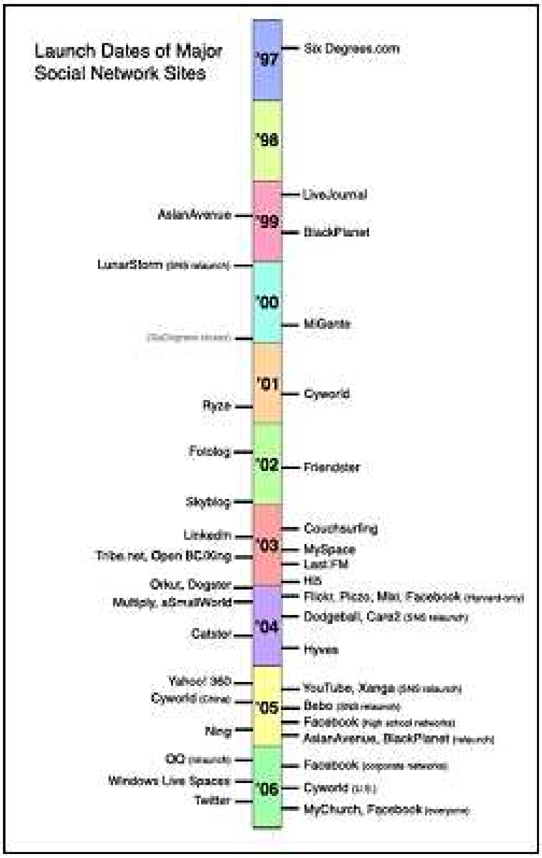


Exhibit 2-1: Social Networking Timeline

B. Social Network Folksonomy and Theorical Models

Social networking phenomenon represented a shift in online communities' organization, since they are primarily organized around people, instead of interests. Early online communities such as Usenet and current public discussion forums were structured by topics or had their interactions following topical hierarchies, but social networking sites are structured as personal networks with individuals at the center of their own communities, in an "egocentric" approach. Online social networks introduced a new organizational framework for online communities, and a vibrant new research context.

Web 2.0 applications and folksonomies[1] have led to new user experiences and yielded rich materials that are demanding appropriate representations to be efficiently studied and mapped. Folksonomy is present in the current social networking sites and applications by the adoption of collaborative tagging capabilities. Social network analysis (SNA) forms a family of methodologies to map and evaluate relationships and data flows between people, groups, communities or any type of social structures. This includes theories and abstract models as the "small world property," social graphs and semantic Web.

Digital Identities

Social identities are the names, nicknames, or aliases that users create to identify themselves on online social networking sites. Users adopt different nicknames or aliases in groups they belong to and usually each one of these groups has different privacy concerns; there are public profiles (like artistic or professional profiles) and private or closed profiles (with friends or family, for example). The possibility of having different social information listed on different groups is one of the key characteristics of social identities.

Depending on the nature and scope of a social network, users' identities have different purposes and might not be associated with a user's real identity. In a MySpace music profile, users might present their artistic names to serve promotional purposes and often do not link to people's real names. On the other hand, users from professional networks such as LinkedIn share their entire curriculum vitae.

The anonymity of the Internet makes it possible for users to decide which personal information they want to share and allows them to promote fake or exalted attributes. Users even create fake identities to trick someone else, which represents the phenomenon known as "Fakesters," which are profiles that are not linked to their owners' real identities. Fake profiles can represent anything from an idol, a movie character, a politician or a famous brand. As an example, research has shown that a man plays about one out of every two female characters in World of Warcraft [3]. Unfortunately, several malicious activities rely on the use of fake profiles, such as fraudsters and sexual predators looking for victims, worms spreading across social networks, and people looking for revenge.

Six Degrees of Separation Theory

Social networks have a so-called "small world" property, more widely known as the "Six Degrees of Separation" theory. [4] This is both an anecdotal and scientific observation that anyone on the planet can connect to any other person by no more than six people. It happens because people build human networks as dense clusters interconnected by shortcuts (the "friends of a friend" groups). Inside of a traditional group of friends, everyone knows each other; if at least one person in a group meets someone from a remote part of the world, it creates a connection between the two groups.

[1] Folksonomy, also known as collaborative tagging, social classification, social indexing and social tagging, is the practice and method of collaboratively creating and managing tags to annotate and categorize content. More info at http://en.wikipedia.org/wiki/Folksonomy

Social Graphs

A social graph (see Exhibit 2-2 [5]) is a social structure made of nodes, also known as “profiles”, which are generally attached to individuals or organizations. One or more specific types of interdependencies link these nodes, and might represent generic levels of relationships as a friend, a co-worker or family member.

Social network analysis, powered by social graphs, provides a visual and a mathematical analysis of relationships, helping to identify the various roles (who are the connectors, leaders, bridges or isolates) and groups characteristics of a social network. It helps determine the structure's key elements: where are the clusters, who is in the core and who are on the networks' peripheries. By comparing social graphs from different social networks, it is possible to build node equivalence when the same person belongs to different social networks.

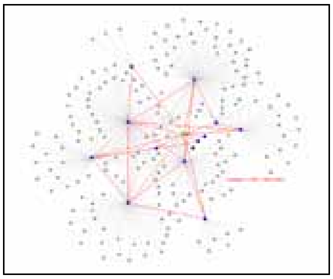


Exhibit 2-2: Social Graph Example

Representing Social Data with Semantic Web

Research in Semantic Web has provided models to leverage the richness of the online social interactions that the social networks represent. As the Web is becoming more and more social, we are now generating, exchanging and collecting a huge amount of knowledge online. Semantic Web researchers provide models to capture such activities and turn the information into collective intelligence.

Researchers see social data as a two-fold structure: data that describes the social network and data that describes what their members produce. There are several ontologies that are well suited for linking together data across various social networks include Friend of a Friend (FOAF)[2] and Semantically-Interlinked Online Communities (SIOC).[3] FOAF represents a profile about an individual and links data from one social network to another. SIOC aggregates data from various Web-based media (including wikis, and blogs) and presents information to users in the most appropriate representation. [6]

In addition, the Simple Knowledge Organization System (SKOS)[4] offers a way to organize manipulated concepts and to link them to SIOC descriptions. SKOS is an area of work developing specifications and standards to support the use of knowledge organization systems such as thesauri, classification schemes, subject heading systems and taxonomies within the framework of Semantic Web. SKOS provides a standard way to represent knowledge organization systems using the Resource Description Framework (RDF).[5] Encoding information in RDF allows it to pass between computer applications in an interoperable way. An RDF-based description of social data forms a rich-typed graph and offers a powerful way to represent online social networks.

Semantic Web technologies are appropriate means for modeling and formalizing to extract the knowledge produced by online social interactions (see Exhibit 2-3). Indeed, by connecting social networks to FOAF and social activities such as blog comments to SIOC, Semantic Web provides a complete interlinked graph on top of existing networks.

Dunbar's Number

British anthropologist Robin Dunbar first proposed Dunbar's number [7], which is the supposed cognitive limit to the number of individuals with whom any one person can maintain stable social relationships, the kind of relationships that people know each other and how every person relates socially. Group sizes larger than this generally require rules, laws and enforced policies and restrict regulations to maintain a stable cohesion. There is no precise value for Dunbar's number, but a commonly cited approximate figure is 150.

Demographics

Social networking sites are primarily organized around people, with individuals at the center of their own communities managing their personal connections. While social networks are often designed to be widely accessible, many attract homogeneous populations, so it is common to find groups using sites to segregate themselves by nationality, age, educational level, or other factors that typically segment the offline society.

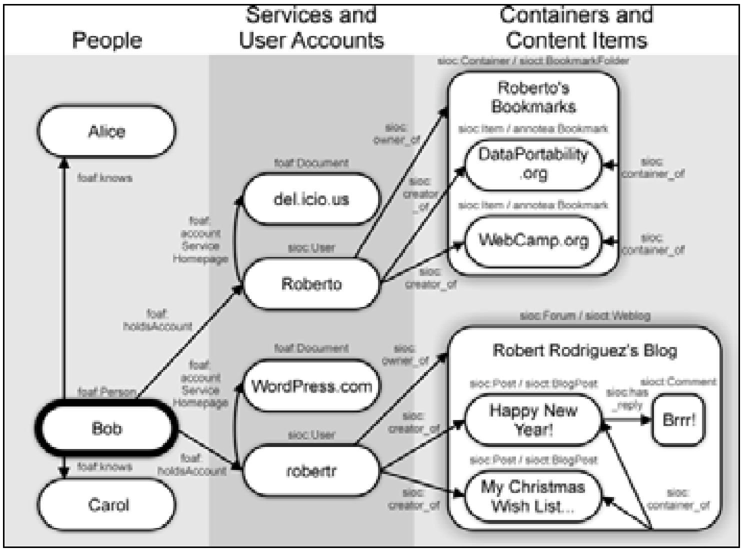


Exhibit 2-3: Social Graph Representation Using Semantic Web

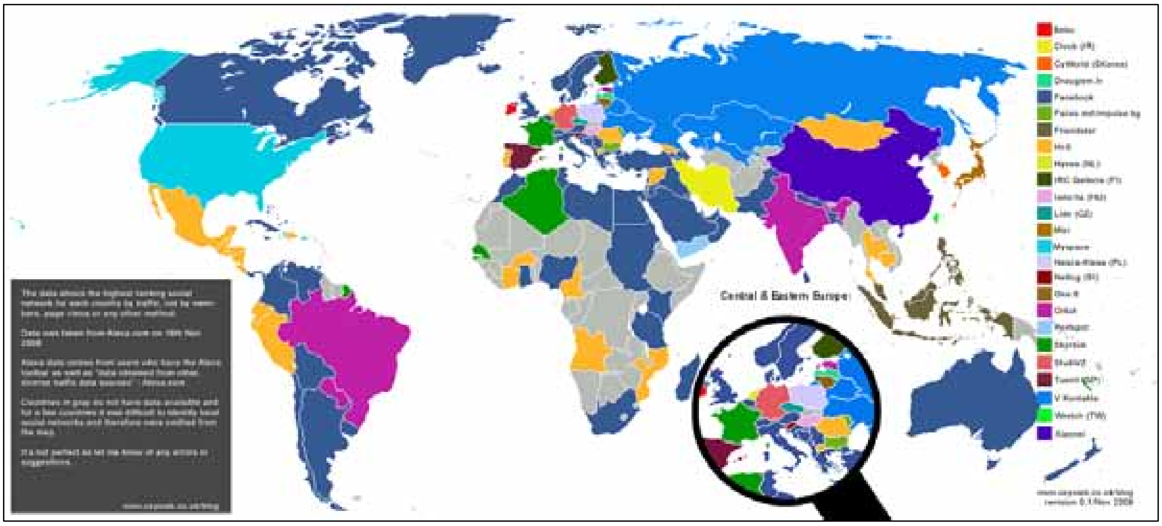
[2] http://foaf-project.org

[3] http://sioc-project.org

[4] http://www.w3.org/2004/02/skos

[5] http://www.w3.org/RDF

Since social networking sites enable users to get in contact with real-life friends, such connections (friends, family members, colleagues or professional acquaintances) usually make up the majority of the online connections between individuals. Figure bellow displays the dominant social networks by country [8] and how most popular social networks vary greatly between different geographic regions.



A dominant social network can hold off the local competition since it is the default service to these populations, so people will choose the same social networking site their friends use. A fundamental success factor of social networking sites is cultural relevance to a specific population.

C. *Current Problems*

Decentralization and Interoperability

Most of social networking sites provide very little interaction with external online services. They operate as "walled gardens," where the users' content is exclusive to the site and there is no way to share it with outside Internet applications. The reason for this lays behind the fact that sites' business models center on having the largest possible user base, and user lock-in is a major part of that strategy.

There is a great desire by many users to have an interoperable format that allows them to transport their social interactions across different sites. In addition, as a user struggles to gain reputation within one site, he or she wants to take that reputation to another world. As things are now, in order to switch to a new social networking site, a user would have to start from scratch, making new contacts and creating their online identity. Many people are currently willing join more than one social networking site; nonetheless, social networks could make this transition (or interoperability) easier in order to gain new subscribers.

Managing Social Identities

In the scenario described above, a user has no way to transport his or her data from one social network to another, so a single person usually has to subscribe to multiple social networks, keeping many profiles and connections — one for each site. By having different logins for different social networking sites, users have no chance to prove their identity across several platforms.

In addition, social networking sites have a very limited set of features for protecting digital identity and restricting the sharing of profile information. Most of them use simple password protection and have a three-level access control system (similar to UNIX): a user can keep his or her work for oneself, share with friends (group) or keep it public (available to all). In addition, most of social networking sites restrict profiles access only to internal users (no one else could access a profile without authenticating as a community member).

Trust and Reputation Management

Trust is a key concept to determine when to establish relationships with profiles from known people or strangers, much like in the real world. To build new relationships, users must be confident that are connecting to whom they expect. Reputation management and tagging technologies help users to assess trustworthiness of third-party information online.

The battle over reputation management is to have more positive comments than negative ones attached to a user profile. To build up an online reputation, a user needs to be in as many places as possible, posting, making friends, building relationships, staying active in forums and sharing information online with other users. In parallel, Web 2.0 applications made social tagging popular, where users can tag Web content as pictures, videos or blog posts to rank and categorize them. A set of tags built from the use of such applications form a folksonomy that can be seen as a shared vocabulary originated by, and familiar to, its primary users. Global tagging and aggregation is a great way to build trust on the Web and to find resources within a trusted social network.

Privacy

Privacy means that user profiles should never give out any information not explicitly slated to be publicly available. People tend to publish personal information on the Web, be it pictures (e.g., on popular sites like Flickr, Facebook, etc.), opinions (e.g.,blogs and forums), videos (e.g., YouTube), or personal home pages, comprising sensitive information such as birth dates, home addresses and personal phone numbers.

Since online users are usually querying and searching profiles, groups and forums about other users' information, protection needs are always on the side of everyone's personal privacy.

As in real-life relationships, people engage online networks with different levels of confidentiality, so users must be in control of what they disclose and should be able to define disclosure rules (e.g., "nobody," "friends," "friends of friends" and "everyone"). Most users have public profiles that are visible to everyone, so it is easy for skillful attackers to use sensitive personal data to perform social engineering attacks. Another relevant trend is the use of microblogging websites, such as Twitter, that provide a straightforward and ubiquitous way to create life streams, allowing users to disclosure their geographic locations and personal habits, for instance. Blogging about meetings is another big issue in terms of not only privacy loss, but also of violations of corporate policies. Competitors can freely read and exploit this information.

Content Overload

The proliferation of Web 2.0 applications (such as blogs, wikis, forums and social networks) eased the process of information publishing to an extent that overwhelms its consumers. With an extremely low barrier of entry and almost no expense, Web 2.0 allows anyone with a computer to become an independent publisher. As a result, users are publishing duplicated or reused content; and popular feeds may become hard to track since they still provide a tremendous amount of information within a short period of time.

It is very time consuming to track and read many of online publications, blogs and forums, so people have to choose what to read and what to avoid. In this scenario, it is incredibly easy to aggregate information; however, it is almost impossible to process, analyze, validate and contextualize them, offering a unique perspective of the facts behind the stories. There will be more information to manage in the future, so online relationship management and data-mining tools are needed.

Legal problems

Most of the known issues in social networks link to the need to protect user's personality and image. This encompasses social concepts like reputation, false allegations, the right to one's image, privacy, insult and discriminations of all sorts. From a legal point of view, social networking risks include the violation on user's data-protection rights and identity fraud.

Since Web 2.0 services host user-generated content, the service providers must establish a detailed "Terms of Service" statement that covers the users' rights versus the ability of the provider to police that content. Social networking and Web 2.0 service providers are often under pressure to intervene in inappropriate user-generated content. These interventions may be requested by other users (the copyright holder or a victim of online harassment), or may be initiated by the service provider itself. Similarly, some of these actions are acceptable while others might violate users' rights, which pose a difficult dilemma to several providers. Usually, service providers may intervene on user-generated content when a user has posted inappropriate, illegal or copyrighted material, or has defamed or published private information about another person.

Fundamentally, with regard to legal and awareness requirements, social networking providers should be familiar with compliance and governance mandates and security frameworks. Unfortunately, there is no set of international, uniform regulation to guarantees the privacy rights and personal data protection across the Internet.

People's Usage Problems

Social attacks include slander through identity theft, defamation, stalking, injuries to personal dignity and cyber bullying. People create fake profiles mimicking personalities or brands or to slander people who are well known within a particular network of friends (e.g., a celebrity or a member of a school class). While this is also possible using conventional Web pages, social networks can be extra damaging because they make it easier to target victims within social groups that know the victims. In addition, the victim of an attack may take too long to realize that he or she is a victim and may not be able to access the profile since access to it may be restricted to the group ridiculing that victim. As more teenagers go online, they face a growing risk of abuse, including cyber bullying[6] or grooming by adults who intend to commit sexual abuse. In addition, most teenagers have never received proper orientations on how to avoid such risks or how to not be involved in these activities.

Cyber bullying on social networks include harassment, denigration, outing (sharing someone's secrets, embarrassing information or images), trickery (talking someone into revealing secrets and then sharing it online), flaming (an angry, critical or disparaging electronic message or discussion), exclusion, stalking and threatening behavior. Another problem is stalking, which typically involves threatening behavior in which the perpetrator repeatedly seeks contact with a victim through physical proximity and/or phone calls (offline stalking) but also by electronic means such as e-mail, instant messaging and social networking sites (this is also known as "cyber stalking"). Social networks encourage the publication of personal information, including data that can reveal an individual's location and schedule (for instance, home address and home phone, schedule of classes and so on).

An additional social threat is the exposure to problematic content on the Internet. This covers a broad spectrum of undesirable or illegal material, as violent media (movies, music, and images), hate speech, adult pornography and obscene content. Self-harm-related websites (sites dedicated to enabling self-injury and suicide, or those that encourage anorexic and bulimic lifestyles) introduce another element of problematic content.

Teens sending sexual messages or nude or suggestive photos of themselves over their mobile phones are

[6] Cyber bullying is a term used to describe repeated and purposeful acts of harm that are carried out using technology, particularly mobile phones and the Internet.

representing a new threat. "Sexting,"[7] has become a concern for parents with the proliferation of mobile phones with cameras and social networking sites. The issue has gained international attention following multiple incidents in the US in which teens face child pornography charges for sending nude or scantily clad images to other teens. These images or sexually explicit text messages can be posted on the Internet or forwarded to others, which can end in harassment or even sexual assault charges. In the US, a survey revealed that one in five teenagers said they had sent or posted online nude or semi-nude pictures of themselves [9].

III. Future of Social Networking

Social networking sites are a relatively new phenomenon, and as with any other technological innovation, they will continue to have a long period of both technical and social adjustments and improvements to fit in people's needs and behaviors. People will also adjust their online practices in the light of the new social networking technologies.

A. Meta-Social Networks and User-Centric Social Universes

With users occupying multiple roles and having dynamic social networks that can grow and shrink, an important aspect in the future of social networks is that users will be able to manage their profiles and connections using meta-social network tools. Such tools, such as Explode [10], will be able to manage users' profiles and the trust networks that exist across distinct social networks, using Semantic Web, data portability and shared-authentication technologies. In this scenario, the user will become the center of his or her social network, adding a cross-network friendship in its virtual-centralized profile.

Tools for managing a distributed presence on the Web and for checking others' views of the user's Web presence are likely to be necessary to support effective social network use in a distributed set of networks.

B. Metaverse: Convergence and Integrating Social Networks and Virtual Worlds

Internet and social network evolution are based on an open, distributed environment. Multi-user online environments[8] usage is growing, since nowadays gaming is not as important as their social networking aspect. These environments connect many simultaneous Internet users and differ from regular computer games because their environments are perpetual and are often referred to as virtual, persistent worlds. Users log on, join the game, build relationships and leave whenever they wish, but the game continues with other players in a hyper-real, richly rendered, three-dimensional space. Players control "avatars," which are in-game characters that have attributes and interact with other avatars and the game's environment.

Most MOEs have some of the same characteristics as the popular social networking sites of today. All of them promote users' social interaction with other members and the social nature of social networks and MOEs depends largely on the ability of users to interact with other members inside the communities. Heavyweight research organizations, like IBM and Linden Labs, are trying to make it possible to move MOE avatars between virtual worlds seamlessly, maintaining the avatar's identity in terms of appearance, personal information and banking status. In the future, these virtual environments may converge into one metaverse.

Integrating Social Networks and Data Portability

Integrating data from different networks, moving information and social graphs across diverse sites or finding all related content about a particular topic are generally complex tasks that require specific standards and technologies and require that social network providers support these functionalities. Many Web 2.0 services today already have their own application programming interfaces (APIs) to promote their integration with third-party applications. Furthermore, many services already have basic features to allow users to import and export their data using standard tools like VCard.[9]

Recent years have seen an explosion in the number of open protocols designed for or usable by social networking platforms. A social network provider theoretically has the opportunity to use or compose with a non-exhaustive and still growing list of open protocols and providers, such as the ones listed below (a detailed overview of these protocols is out of the scope of this paper):

--Authentication: OpenID, CardSpace, i-card, Liberty Alliance, Facebook Connect

--Authorization: Oauth, CardSpace, i-card, OpenSocial

--Semantic Markup and Description: RDF, MicroFormats

--Network Description: FOAF, XFN, OpenSocial, DiSo

--Network Visualization: TouchGraph, WPS

--Remote Manipulation of Data and their Relations: REST, SOAP, XML-RPC, DiSo

--Service Description: XRDS, UDDP

--Service Execution: OpenSocial, Facebook Applications

--Message Transport: REST, SOAP, XMPP, SMTP

--Application Hosting: OpenSocial

--Indexation and Search: Google Social Graph

Recently, Facebook, Google and MySpace announced their own technologies topermit user data portability between social websites, representing a new stage in the social networking services competition. Google's Friend Connect and MySpaceID are built with open-source code, based on the OpenID, OAuth and OpenSocial standards. It makes social identity sharing easier across the broader Internet, not just on a

[7] The phrase combines the words "sex" and "texting" and refers to potentially prurient messages and images send over electronic devices, like cellular phones or laptop computers. Source: http://sexoffenderresearch.blogspot.com

[8] Multi-user online environments (MOEs) refer to the entire set of persistent online environments that range from massive multiplayer online role-playing games (MMORPGs) such as World of Warcraft or City Of Heroes, to virtual worlds, like Habbo Hotel and Second Life.

[9] vCard is a file format standard for electronic business cards. Source: http://en.wikipedia.org/wiki/Vcard

few partner websites. "Facebook Connect" was the first interoperability protocol. Along with an easy logon, the user has the option of re-broadcasting whatever they do on the third-party site to all of their friends within Facebook and matching existing friend relationships on Facebook with those on the third-party site. Facebook Connect allows any developer to let users log onto their websites using their Facebook credentials and integrate other key Facebook features, like a friends list, into third-party applications, which can in turn send data back into Facebook and the news feed.

In addition, currently existing authentication services such as OpenID[10] extend the concept of single sign-on to social network users by making existing user IDs portable to other sites.

C. *Social Web Bill of Rights*

As a response to the endless discussion on data and privacy rights, on September 2007, Open Social Web group[11] promoted the "Bill of Rights for the Social Web,"[12] a straightforward document put out by four Web 2.0 pioneers. It outlines how companies should treat the data they collect from users of social network sites, as personal data, who the user is connected to, and users' content. Such discussion turned out to be a hot topic after the February 2009 Facebook users' rebellion that upended Facebook's attempt to change its terms of service to grant itself a perpetual license to all photos, videos and copyrighted material posted by its members. [11]

The "Bill of Rights" promoted the discussion about users' rights on their own information usages. Its main goal is to promote the idea that users should be able to assert three basic rights over their data: ownership, control (the right to share, keep private, or completely revoke the data at user's discretion) and freedom.

D. *Virtual Currency*

Wikipedia defines virtual economy as the emergent economy existing in virtual worlds, usually by the exchanging of virtual goods in the context of an Internet game [12]. Each virtual world has its own virtual economy and virtual currency based on the exchange of virtual goods (weapons, spells, clothes, food, houses and so on). Sometimes, these virtual currencies are tied to the real world since they might be purchased from the game provider and some people do interact with virtual economies for "real" economic benefit. In addition, people can sell their characters, virtual money or goods on online auction websites for real money.

Games are one of the newest and most popular types of online applications on several social networking sites. Since monetization is an important aspect of games, Social Network providers are starting to deploy virtual currency, such as hi5's "Coins." Users are able to spend their Coins to purchase premium content, advanced features and status upgrades. Many publishers of Facebook games are doing the same, in the hopes that a unified virtual currency will engage more gamers and, ultimately, make them spend more money on games.

The use of money (real or virtual) on social networks, however, has the side effect of attracting fraudsters and cyber criminals, who will target online users to steal their social networking credential and their online money.

E. *Mobile Social Networking*

Essentially, since both social networking and mobile usage are ubiquitous and growing, the overlapping demographics will generate plenty of new opportunities to mobile social networking in the coming years. Due to mobile phones limitations (such as small screens, limited keyboards and often poor network connectivity), the native sophisticated interfaces and rich media content offered by social networks cannot be entirely duplicated on mobile devices. However, the so-called "smart-phones" have become quite sophisticated in the features they provide and offer serious processing power to software applications. They may include global positioning system (GPS) tracking devices and music players, and could supply valuable user information to social networks, such as geographical location coordinates or listening habits. As these devices add features, phones become a more-complete repository for personal data linked to a single individual.

The benefits that mobile social networking can bring in terms of enhanced location awareness and availability need to be balanced with the responsibility inherent of these features and the specific user's requirements for personal privacy.

F. *Sensor Networks*

By combining social network and Web-connected devices, applications can provide an extension of social activities through sensors, as user activity is modeled not by voluntary user input but can be automatically generated by sensors. Other sources of social data available on the Web could be used as sensors to minimize the required user input, aggregating the online activities and footprints of users to their social profiles. By using semantic representations of information from sensors, people could connect through shared activities and interests. More importantly, we can send alerts based on abnormal activity patterns.

An increasing amount of portable devices are supporting sensor-based interactions, from peripherals (Nike and iPod) to integrated sensors (the iPhone's accelerometer). Sensors are becoming more prevalent in mobile devices in recent years. By supporting Bluetooth and WiFi communication, mobile phones have now become sensor gateways for individuals. A wide range of Bluetooth sensors, such as heart monitors and environmental monitors, can be associated with these mobile phones, enabling a new paradigm—the personal sensor network—in which the individual becomes the sensor hub.

[10] OpenID is a universal ID technology in which a user registers with a website (also known as "OpenID Provider"), which assigns the user a URL as his or her personal identifier. The user then uses that unique URL on any site that supports OpenID, and the logon process is handled through the site that assigned the URL (the "OpenID Provider"). Source: http://openid.net

[11] http://opensocialweb.org

[12] http://opensocialweb.org/2007/09/05/bill-of-rights

G. Social TV

Internet protocol television (IPTV) comes up in the market as next generation for television, where users are able to watch television wherever they are. Social networking brings many favorable social services to television watchers based on IPTV technology and the ability of people to share their experiences and opinions. The main features of social TV include the online sharing of TV-watching experiences, the interaction between TV watchers (via chat, e-mail, forums, video-conferencing), community-watching TV (watching together by presence service or by online sharing) and recommendation sharing (social networks, personal broadcasts).

H. Social e-Government

A new generation of politicians is emerging, and they are increasingly adopting social media tools to interact with the citizens. The recent election campaign of US President Barack Obama is perhaps the best example of this. There are three broad areas of interaction for which the state can gain benefits from social networks:

--Government to Citizen, by promoting online public services and disseminating information, as "official" advice and support, and making information more transparent.

--Second, Citizen to Government, where citizens could use the Web to express their views, highlight politicians' work, engage with the government and influence policy makers.

--Citizen to Citizen interactions are helping each other to handle public service outcomes (ranging from healthcare information to sharing advice about tax matters).

I. Corporate use

For the corporate sector, social networks can create great opportunities to develop closer relationships with customers since current Internet consumer are no longer mere buyers and now use all opportunities to view, inquire, communicate about, and analyze products and services. They are willing to share their feedback and complaints about their favorite products and brands. Web 2.0 is useful to develop products, establish commercial relationships and learn more about consumers. Business opportunities for social networks include:

--Social advertising, which represents ad formats that engage the social context of the viewer, where the ad is targeted based on what it knows about individual users.

--Micro-payment for social networks to enable the exchange of goods and services on the platform, which also apply to developers who provide social software applications.

--Platforms for micro-niches could charge a subscription or access fee.

--Reselling of marketing and business intelligence based on information collected on the network.

--Buying clubs offering coupons and driving demand for people interested in the same type of products

--Interacting with "real world" small and medium commerce by connecting social platforms with established boutiques, coffee shops, restaurants and bars.

Enterprises need to adapt their business models for the social Web. This includes large social networks (like Facebook) and small or focused social networks; which will represent a opportunity to reach a niche or group of customers.

J. E-Learning through Networking

Schools and higher education foundations are increasingly using social networking as a communications and collaboration tool of choice. As such, in the near future, it would be beneficial for schools to promote online interaction through social networking sites, in order to prepare students to adult life with the skills they need to succeed. Safety policies remain important, as does teaching students about online safety and responsible online expression; however, students may learn these lessons better while they are actually using social networking tools.

IV. Security aspects of Social Networking

A new paradigm provides a lot of opportunities, but when it is done without the necessary security requirements kept in mind, it serves as a deterrent to growing and user adoption. In addition, since social networks attract thousands of users who might represent potential victims, social networks represent a very desirable target to mass attackers.

A. Actors and Motivation

There are several actors and groups targeting social networks for fun and profit. Malicious actors might adopt several categories of attacks and tools to target social networks' users; the following are a few examples:

--Spammers and phishers use social networks' compromised accounts to send fraudulent messages to victims' friends.

--Fraudsters and cyber criminals might use social networks to capture user data and run social engineering attacks.

--Hacktivists and offline terrorist groups create communities to spread their words and to promote their causes; recruitment is also common

--Sexual predators use social networks to share illicit content and to recruit victims.

Social networks are popular communication mediums for many communities, including malicious ones. Several hacking groups have been creating hacker-themed online communities to promote their malicious activities and tools. Many others

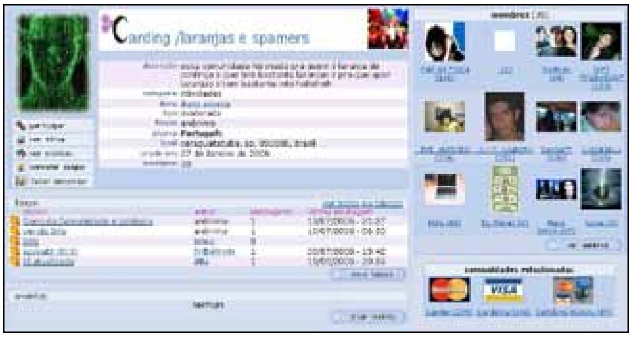


Exhibit 3-1: Example of a Carding Forum on Orkut (no longer available), Advertising "Trustworthy" Mules and Spammers

offer hacking tutorials, news articles, tools or exploits. Several communities run as marketplaces to encourage the abuse of stolen credit card information and attacks against high profile targets such as banks or e-Commerce sites (see Exhibit 3-1). Hacking communities in social networking sites also offer hacking services, which include paid hacking services.

Many of the attackers' profiles on social networks seem from unsophisticated users, since they may use these communication mediums only on the initiation phase.

B. Current Security Threats

As the popularity of social networks started to increase, hackers, fraudsters and malicious users started using them to run illegal activities, either by using the social networks as attack vectors to traditional cyber crimes, by creating specific threats to social networking users or by running direct attacks to disrupt social networking sites.

Social networks have by nature some intrinsic properties that make them ideal to be exploited by an online criminal: a huge and highly distributed user-base made of clusters of users sharing the same social interests, thus developing trust with each other.

Privacy

The availability of personal information on social networks provides ideal conditions for actors to abuse such information and leverage it. The inappropriate exposure of sensitive information might represent a good opportunity for criminals and terrorists to conduct "criminal data mining."

Bad actors could use unflattering material or personal information from social networks to select their targets, profile their victims, and plan and execute their activities. Also described as "knowledge discovery," data mining and predictive analytics give fraudsters and terrorists an opportunity to manage and make sense of the myriad of information coming from their targets, ranging from social network profiles, personal conversations on scrapbooks, blog and Twitter posts, and personal photos on online albums

Identity/Password Theft

Identity theft has been with us in various forms for a very long time. Thieves who assumed the identities of unsuspecting consumers in an effort to commit fraud have ruined the financial lives of their victims. Searches of existing online information could flag social security numbers, birth dates, addresses and any sort of personal data that might help a criminal steal someone's identity or create a false identity. Criminals can easily obtain false credentials necessary to move throughout the many systems that require identification.

Attackers use compromised social network accounts to launch attacks because they can spread more easily from one account to the next. The inherent trust relationships improve attackers' chances of convincing their victims that they are legitimate, through social engineering. Once an attacker gains access to an important individual within a community, it increases the risk of attack for anyone connected to that individual. Social network credentials can be stolen by using traditional key loggers, by running brute-force attacks or by social engineering (usually based on the information available on users' profiles).

iDefense observed attackers abusing a Security Focus Jobs site in December 2007, whereby attackers were able to freely register as a recruiter and obtain resumes and business information about 2,471 individuals who registered with the site. Subsequently, the attackers sent fraudulent e-mail messages to each of the individuals.

Malicious Code, Viruses and Worms

Malicious code utilizes infected users' social network accounts to collect friend information and use it to proliferate. In addition, many attackers use social networks to create fake profiles and publish fake links that lead to sites infected with malicious code.

Banner ads, video content and fake social network profiles have become a pipeline for stealing personal information as more consumers jump online. There are malicious codes distributed through pop-up ads, and not all of them require a click by the user.

In some cases, social engineering is not necessary to carry out attacks. For example, an early MySpace worm, also known as the Samy Worm, used JavaScript commands to add friends to a particular account automatically. Such a worm spreads automatically to new accounts because the content is automatically embedded on the profile pages of new victims.

In January 2009, iDefense investigated attackers utilizing the my.barackobama.com website, a social network for President Obama supporters, to spread malicious code. The attack utilized fake images trying to convince users to install a malicious executable file through fake Flash codec errors. Attackers injected the same URLs into many different websites and forums, suggesting that attackers utilized automatic forum crawling and account creation programs.

Spam, Phishing and Financial Fraud

Phishers usually collect user information from compromised social network accounts to send spam and phishing messages. Similar to phishing that targets banks, phishing that targets social networks can have financial impacts and cause monetary losses. There are cases in which attackers set up fake social network profiles and then establish connections with friends on "buddy lists" to gain more information and potential targets to phishing attacks.

Several malicious codes target online gamers. These attacks will typically allow hackers to take over compromised accounts from subscription-only gaming, so that they will access the virtual property deposited in these accounts, sold to them through the digital underground. Second Life is one example of a social network for which a compromised account allows successful attackers to extract real money. According to the official Second Life blog in November 2006, various phishers target Second Life to steal in-game money (Linden dollars) by claiming that the user could use a hack to create free money. [13] Afterwards, attackers can convert in-game money directly into real money.

The increasing use of social networks and virtual worlds as social and business platforms, including the use of virtual money in social environments, are attracting cyber criminals. Financial fraud has already been affecting online games' users for many years by the theft of online goods (weapon, objects or virtual money) or "gold farming,"[13] which created an underground economy based on the selling of virtual goods and the transfer of virtual money.

Data Loss

Data leakage incidents include the loss of personal, corporate, confidential or customer information, inappropriate public statements about the company, using corporate resources for personal uses and harassment of or inappropriate behavior toward a customer or another employee. Social networking sites are another mean through which those things can occur, however, and they create a broader impact upon a company's reputation.

Data loss prevention is currently one of the problems that many companies are experiencing most. Companies are looking for ways to prevent confidential and proprietary information from leaving the company and being accessed by outsiders and unauthorized people. Most incidents occur via e-mail or file transfers, but instant messaging chat tools, blog posts, Twitter messages and even online resume content could also disclose proprietary company information.

Information Control and Censorship

In many ways, it is unrealistic for administrators to manage the huge amount of information available on social networking sites effectively. It is improbable that social networking sites will ensure accuracy, legality or usefulness of content before users publish it. For this reason, it is difficult to prevent actors from posting unwanted information; however, communities that use self-policing mechanisms or moderation are generally more successful. As an example, rating systems allow users to remove erroneous content by popular vote.

Thresholds for new users and self-moderating social networks should be the goal going into the future since users are often aware of these problems first. Security teams that watch social networks are an effective reactionary approach to limiting malicious content, but decentralized social networks may not have the resources to devote to such problems.

Offense, Hate and Discrimination

Typical attacks in this category are cyber stalking and cyber bullying, a repeated contact to a victim and purposeful acts of harm, including harassment and humiliation. Cyber bullying victimization can lead to negative effects similar to offline bullying such as depression, anxiety and low self-esteem.

Hate speech is a specific type of online content designed to threaten certain groups publicly and act as propaganda for offline organizations. These hate groups use websites to propagate, share ideology, recruit new converts, link to similar sites, advocate violence and threaten others. Offline groups are using online techniques to accomplish their goals and improve communication. In addition, there is also concern that a small number of youths converted online may start conducting offline hate crimes.

Sexual Crimes and Child Safety

Social networking environments represent a serious risk to teenagers and younger children, as they can be victims of several threats as cyber bullying, online harassment and sexual predators. Usually, children who are at risk online are those who are also at risk offline. The most frequent threats to children on social networking sites in general come from their peers, young adults and predatory older adults.

Child pornography is a particularly horrific crime because it involves pictures and movies that depict minors in suggestive poses or explicit sex acts. An additional issue is the presence of youth-generated sexual content (photographs and videos) intended for view by other minors (usually, friends and partners). Though not intended for adult consumption, the Internet may play an unexpected role in spreading such content, potentially putting the children on embarrassing situations.

Social network providers have a hard time keeping their sites entirely clear of sex offenders, given the huge number of users and the fact that not all of them use their real identities.

Social Networks under Attack

Social network providers, as with any other Web application, might be vulnerable and become the target of a direct attack. Security vulnerabilities could provide hackers with a means to attack providers and cause service failures (such as a denial of service), unauthorized access to users' credentials (followed by disclosure of private information) or could be used by a virus to be spread amongst user accounts. Cross-site scripting (XSS) or SQL injection vulnerabilities on social network applications could cause huge problems to millions of users.

Malicious users could take control of the visitors of social sites by remotely manipulating their browsers through legitimate Web control functionality such as image-loading HTML tags or JavaScript instructions. [14]

Home, a virtual world for PlayStation 3 users to interact with other gamers, was hacked in December 2008. [15] Crackers were able to access the Home server so that they could upload, download or delete any file within the server, leading to identity theft and the spread of malicious code. Facebook was also vulnerable to XSS attacks. [16] On March 2009, Koobface[14] worm targeted users of the social networking websites Facebook, MySpace, hi5, Bebo, Friendster and Twitter. Koobface spreads through invitations

[13] http://en.wikipedia.org/wiki/Gold_farming

[14] http://en.wikipedia.org/wiki/Koobface

from a user's contact that include a link to view a video. It ultimately attempts to gather sensitive information from the victims such as credit card numbers.

C. Predictions on Future Security Aspects of Social Networks

Technological evolution of social network services and their global adoption will bring security risks that might represent opportunities to malicious actors exploring such services. Information security professionals and law enforcement agencies must adapt to the approaching threats.

Exploit of Social Network Gadgets

Web widgets are those graphic little applications that bring third-party tools and games (like clocks and calculators) to the social networking site. They have experienced a rapid adoption rate in desktops, mobile devices and Web applications because they are easy to create and implement.

Since widgets have become popular, they have become targets for malicious actors, who looked to use them as spyware, for virus dispersal and hijacking. Social network providers release their widgets' software developers kit (SDK) so developers can create their own SDKs to run in the social networking site. The downside of an SDK is that it is available to everyone, including those with malicious intent, who will have access to the system and a roadmap of how to manipulate the widget.

Widgets are vulnerable to exploits by hackers and criminals due to inadequate security models, which allow malicious code to run freely and spread easily. They bring similar vulnerabilities as those found on the Web but with a higher risk since they share a much broader connectivity with an underlying application or operating system. This enables a powerful attack vector capable of gaining privileged access to local resources by default.

Social Network Worms and Phishing Powered by Semantic Web

All social networking sites identify "circles of friends" based on existing relationships or common interests in a group or community. A malicious actor could use such characteristics to harvest large amounts of reliable social networking information.

The FOAF project provides a machine-readable Semantic Web format specification describing the links between people. Even if such sources of information were not so readily available yet, one could infer social connections from mining Web content and links. Worms built with support from Semantic Web attributes would be able to easily identify users' connections and quickly spread across social graphs.

Terrorism Using Social Networks and Online Communities

Terrorist organizations are start using social networks and virtual worlds in their daily activities. Terrorists could use virtual worlds to create an exact replica of their targets to plan and simulate an entire attack, so that they no longer need to travel to the target to carry out reconnaissance. Instead of sending potential jihadists to train in military camps in Pakistan, Afghanistan and Southeast Asia, organizations such as al-Qaeda and Jemaah Islamiah could turn to the virtual world and use online training camps to evade detection and avoid prosecution. In such scenarios, Second Life could easily become a terrorist classroom.

Social networks and online communities also help terrorists to recruit new members and could be used as places to meet up and discuss their plans. Once these groups and communities are built, it is easy for them to start spreading propaganda, recruiting and instructing like minds on how to start terrorist cells and carry out jihad. On October 2008, authorities arrested two white supremacists men who were planning to kill Senator Barack Obama and more than 100 African-Americans; they had met online through a mutual friend.

In addition, microblogging communities, such as Twitter, could be used as an effective communication tool for coordinating terrorist attacks and track the news in real time. One of the most useful tools available is the opportunity to transfer virtual money between avatars, money that can then be translated into real currency to support criminal activities.

On the dark side of virtual words, there is one radical terrorist group in Second Life, called the "Second Life Liberation Army,"[15] that has been responsible for some computer-coded atomic bombings of virtual world stores in the past, using weapons and armories in Second Life. Attacks in Second Life include blowing up the Australian Broadcasting Commission's (ABC) island, attacking Reebok and American Apparel stores and storming the stage at the January 2007 meeting of the World Economic Forum in Second Life.

Social Network Forensics

The explosion of social networking sites and Web 2.0 technologies by cyber criminals will demand a specific effort from law enforcement agencies to investigate crimes in such sites. Effective forensic investigation of social networking threats requires evidence gathered from social network sites and any technology that tracks what happened, who did it, and when. Social network forensics represents the need of specific investigation skills covering the social networking universe.

Information security professionals will need to develop specific tools and process to detect and investigate malicious activities on social networks and ensure that the information has been secured and examined in the correct manner and all evidence has been recovered. Information discovery demands the ability to search for information as soon as a user creates or distributes it. It also demands the ability to measure search quality, to run a dynamic classification of the search results, and to have a proper visualization tool for reading the data according to many different criteria and contexts.

A new social networking forensic framework must focus on the analysis of an online actor (profile) and its activities. It will have to include the investigation of the suspect or victim relationships and online communities, the usage pattern on a

[15] http://secondlla.googlepages.com

social networking site, uncovering past relationships and forensic analysis of intra-social networking applications [17].

V. Conclusion

Social networks are growing rapidly and functioning far beyond the "list of friends" concept. Users want to express their identities and share information in restricted virtual communities. Social networks are driving the evolution of the Internet from a "flat" Web model toward a number of socially interconnected, user-centric websites. The "way of communicating" has evolved from point-to-point message exchanges between isolated users to group-oriented activities.

Social networking sites must recognize this basic aspect of human social interaction and find strong and intuitive methods for implementing it on a software level while providing the necessary level of protection, privacy and trust. Several hacking groups are attacking social networks, spreading keyloggers, Trojans and other malicious tools.

Governments and intelligence agencies will have to adopt new paradigms and technologies to use and manipulate the amount of information and interaction in a social Web.

References

[1] Website "What is Social Networking", Available: http://www.whatissocialnetworking.com

[2] Source: http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html

[3] The Daedalus Project, "WoW Gender-Bending", Available: http://www.nickyee.com/daedalus/archives/001369.php

[4] WikiPedia, http://en.wikipedia.org/wiki/Six_degrees_of_separation

[5] http://www.thenetworkthinker.com

[6] "Leveraging Social data with Semantics", Available: http://www.w3.org/2008/09/msnws/papers/ereteo_et_al_2008_leveraging.html

[7] WikiPedia, http://en.wikipedia.org/wiki/Dunbar's_number

[8] http://www.oxyweb.co.uk/blog/socialnetworkmapoftheworld.php

[9] By Reuters, "Sexting: The new, dangerous trend among teens." IBN Live. May 04, 2009. Available: http://ibnlive.in.com/news/sexting-the-new-dangerous-trend-among-teens/91732-19.html

[10] http://blogs.zdnet.com/social/?p=97

[11] JD Lasica, "Toward a Facebook bill of rights." SocialMedia.biz. Feb. 27, 2009. Available: http://www.socialmedia.biz/2009/02/27/toward-a-facebook-bill-of-rights.

[12] WikiPedia, http://en.wikipedia.org/wiki/Virtual_economy

[13] http://blog.secondlife.com/2006/11/07/important-free-money-hack-dont-fall-for-it

[14] Elias Athanasopoulos, A. Makridakis, D. Antoniades S. Antonatos, Sotiris Ioannidis, K. G. Anagnostakis and Evangelos P. Markatos, "Antisocial Networks: Turning a Social Network into a Botnet", 2008, Available: http://blogs.zdnet.com/security/images/facebotisc08.pdf

[15] Ryan Naraine, "PlayStation Home virtual world hacked", ZDNET. Dec. 22, 2008. Available: http://blogs.zdnet.com/security/?p=2330

[16] Dancho Danchev, "Four XSS flaws hit Facebook", ZDNET. Dec. 15, 2008. Available: http://blogs.zdnet.com/security/?p=2308

[17] Jeff Bryner, "Facebook Forensics", SANS, June 11, 2009, Available: https://blogs.sans.org/computer-forensics/2009/06/11/facebook-forensics

Anchises M. G. de Paula (CISSP) works as Global Threat Intelligence Analyst at iDefense, a VeriSign company, and is President of ISSA Chapter Brazil. He has more than 10 years of strong experience in Computer Security, had been worked as Security Officer in Brazilian telecom companies and also Security Consultant on local resellers and consulting firms. He owns a Computer Science Bachelor degree from Universidade de São Paulo (USP) and a master degree in Marketing from ESPM and is CISSP, GIAC (Cutting Edge Hacking Techniques) and ITIL Foundations certified