IJoFCS (2010) 1, 60-79

e-forensic PRESS

The International Journal of
FORENSIC COMPUTER SCIENCE

www.IJoFCS.org

Security Aspects and Future Trends of Social Networks

Anchises M. G. de Paula

Abstract - Social networks represent a new range of online uses that pose a series of challenges to the security community. While these networks provide new opportunities for interaction and socialization among users, the overwhelming amount of information generated, exchanged, and redistributed by users demands the adoption of new tools and techniques to search, analyze and secure online data, which are the subject of this paper. An understanding of the implications of online social networking to human social interaction and societal structure will bring new ideas and challenges to consumers, businesses, and governments worldwide. This report analyzes the social network phenomenon, focusing on its security implications and perspectives on potential future development paths.

Keywords - Social Network, Security, Predictions, Trends

1. Introduction

ONLINE social networks have become increasingly popular in recent years. These networks join individuals into groups that, in many ways, resemble small rural communities or neighborhood subdivisions [1]. Such networks quickly became a global cultural phenomenon by adapting the concept of real-life social groups and interactions to cyberspace. Web 2.0 technologies have empowered social-network platforms by increasing interactivity; as a result, the majority of online users is currently attached to one or more social networks. From the personal spaces of Facebook, MySpace, Orkut, and Windows Live to more interactive platforms, such as wikis, blogs, Twitter, and online worlds (e.g., Second Life, World of Warcraft), hundreds of millions of users are connecting with each other and building online communities. Social networks have changed the ways in which users interact, share information (personal data, opinions, news), and conduct business online, transforming the familiar communication-focused Internet into a new social platform.

Several drawbacks are associated with social networks. In addition to security risks related to improper usage (e.g., information disclosure, privacy issues), these networks have become an at-

tack vector for phishers, online fraudsters, and sexual predators. Cyber-criminals have adapted their strategies and tools to target social-network users and have improved attack technologies to target Web 2.0 applications. Traditional offline criminals also use social networks to plan criminal activities or are targeting their activities to online victims; offline criminal activity is thus migrating to cyberspace. From the user perspective, issues of trust and privacy within online social networks remain unresolved.

2. Current State of Social Networks

2.1. Main Purpose and Characteristics

Social-networking sites allow individuals to present themselves in an online profile and to establish or maintain connections with others (usually known as "friends"). Social networks consist of two fundamental elements: nodes (users) and connections (relationships between users). This structure is similar to real-world interactions, wherein a circle of friends in a social group consists of people connected by friendships.

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, including friendship, business, hobbies, medical interest, or sexual orientation. Users can join virtual groups and search for people with similar characteristics using the information contained in online profiles. Individuals usually belong to several social groups simultaneously and share different personal facets with the members of each group.

Because social-networking sites enable users to articulate and make visible their social networks, the public display of connections is a crucial component of these services. Each user's "friends list" contains links to each friend's online profile, enabling viewers to browse users' networks. Additional features usually include groups, communities, message boards, photo albums, comments ("scrapbooks"), tagging, and private messaging. Many providers also offer music- or video-sharing capabilities, built-in blogging (e.g., on MySpace) and instant-messaging technology (e.g., the embedded GTalk interface of Orkut).

Social networking benefits strongly from large-scale coverage; users develop greater interest in social-networking services as they are used by more of their friends.

2.2. History

The first recognizable social-networking site, SixDegrees.com, was launched in 1997. It allowed users to create profiles, list their friends, surf friends' lists, and send messages, representing the first provider to combine the most popular social- networking features. Although SixDegrees.com attracted millions of users, it

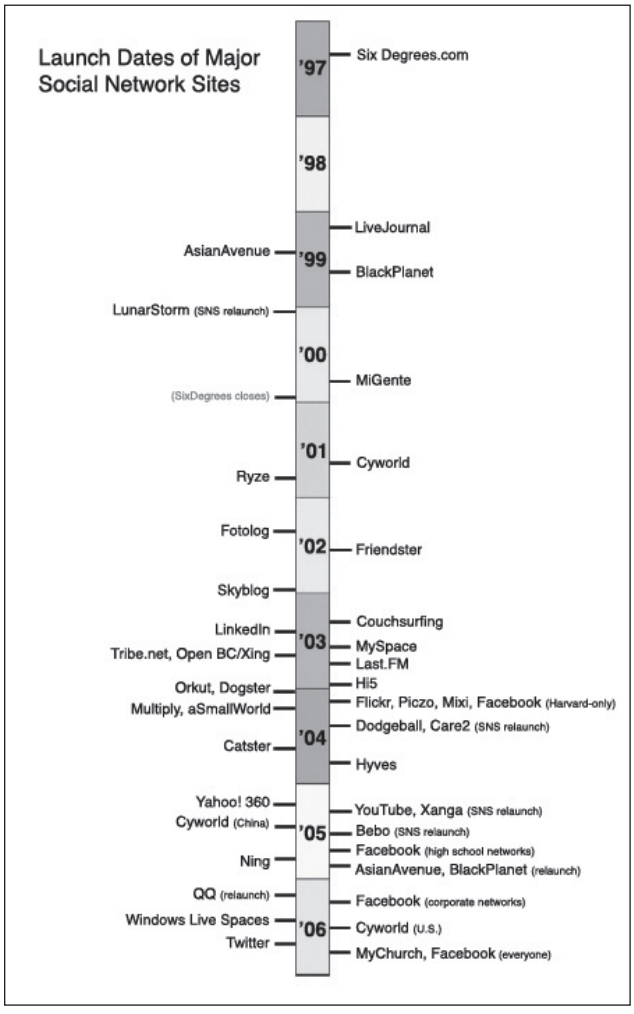

Figure 2-1: Timeline of Social-Networking Sites

failed to become a sustainable business and the service was discontinued in 2000.

From 1997 to 2001, several online community tools (e.g., AsianAvenue, BlackPlanet, MiGente, LiveJournal) began supporting various combinations of profiles and publicly articulated friends (Fig. 2-1) [2]. The first business-oriented network site, Ryze.com, was launched in 2001, followed by Tribe.net, LinkedIn, and Friendster. Friendster gained traction among early adopters and acquired 300,000 users through word of mouth before attracting the attention of traditional press media, paving the road for MySpace and Facebook. Since 2003, several social-networking sites have been launched and have proliferated worldwide.

In April 2008, Facebook exceeded MySpace to become the social-networking website with the highest number of unique monthly worldwide visitors. Facebook has since become the social network of choice in most countries. On July 21, 2010, Facebook announced that it had more than 500 million active users.

2.3. Social Network Folksonomy and Theoretical Models

The social-networking phenomenon represents a shift in online communities' organization from interest-oriented to people-oriented. Early online communities (e.g., Usenet) and current public-discussion forums have been structured topically, with interactions following topical hierarchies. In contrast, social-networking sites are structured egocentrically through personal networks, with each individual at the center of his or her community. Online social networks have thus introduced a new organizational framework for online communities that represent a vibrant new research context.

Web 2.0 applications and their relative folksonomies[1] have led to new user experiences and have yielded rich materials that must be appropriately represented to enable efficient mapping and research. Folksonomy is manifested in current social-networking sites and applications by the adoption of collaborative tagging capabilities. Social-network analysis (SNA) employs a family of methodologies to map and evaluate relationships and data flows between people, groups, communities, and other social structures. SNA utilizes theories and abstract models, such as the "small world property," social graphs, and Semantic Web.

Digital Identities

Social identities are designated by the names, nicknames, or aliases that users create to identify themselves on online social-networking sites. Users may adopt different nicknames or aliases in each group to which they belong; profiles may be public (e.g., artistic or professional profiles) or private (e.g., restricted between friends or family members), and each of these is associated with different privacy concerns. The ability to share different social information with different groups is a key characteristic of social identities.

The purposes of users' identities differ, depending on the nature and scope of social networks, and may not be associated with real identities. For example, users may present their artistic names in a MySpace music profile for promotional purposes, and these aliases are often not linked to real names. In contrast, users of professional networks (e.g., LinkedIn) share their entire curriculum vitae using real names and identities.

The anonymity of the Internet allows users to choose the personal information they want to share and helps them to promote false or exaggerated attributes. "Fakester" users create false identities to trick others and do not link these profiles to their real identities. False profiles often emulate users' idols or movie characters, or are associated with the use of famous brands. For example, researchers have found that about half of the female characters in

[1] Folksonomy (or collaborative tagging, social classification, social indexing, social tagging), is the practice and method of collaboratively creating and managing tags to annotate and categorize content.

World of Warcraft are associated with male users [3]. Unfortunately, several malicious activities rely on the use of false profiles by fraudsters and sexual predators looking for victims, individuals seeking revenge, and those who create worms that spread across social networks.

Six Degrees of Separation Theory

Social networks have a "small world property," known more widely as the "six degrees of separation" theory [4]. This theory describes the anecdotal and scientific observation that anyone on the planet can be connected to any other person through no more than six people. Such connectivity is due to the structure of human networks, which are dense clusters interconnected by shortcuts ("friends of a friend" groups). Every individual within a traditional group of friends knows everyone else in the group; if at least one person in a group meets someone from a remote part of the world, a connection is created between two groups.

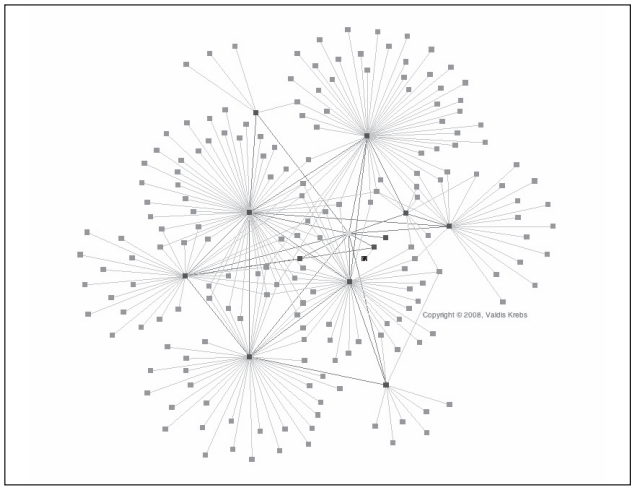

Figure 2-2: Social Graph Example

Social Graphs

Social graphs (Fig. 2-2) [5] depict social structures comprised of nodes (user profiles) that represent individuals or organizations. Nodes are linked by one or more specific interdependencies representing generic levels of relationships, such as friends, co-workers, or family members.

SNA uses social graphs to visually and mathematically analyze relationships, facilitating the identification of various roles held by group members (connectors, leaders, bridges, isolates) and the characterization of social-network groups. In this way, key structural elements can be defined through the identification of clusters, as well as core and peripheral members. The comparison of social graphs depicting different social networks allows researchers to define node equivalence when the same person belongs to different social networks.

Dunbar's Number

British anthropologist Robin Dunbar first proposed Dunbar's number [6], which places a cognitive limit on the number of stable social relationships that any individual can maintain. Stable relationships are defined as those in which people know each other and through which every person relates socially. Group sizes exceeding Dunbar's number generally require rules, laws, enforced policies, and restrictive regulations to maintain stable cohesion. Dunbar's number is not defined by a precise value, but is commonly estimated to be 150 individuals.

Dunbar's number suggests that there is a limit to the number of peers with whom a social-networking member can actively interact and build strong ties. On the other hand, the use of modern online social-networking resources may help people to engage in a number of active connections that exceeds this theoretical limit.

Representing Social Data with Semantic Web

The application of Semantic Web has provided models that represent the richness of online social interactions. As the Web becomes more social, a vast amount of knowledge is generated, exchanged, and collected online. Researchers have used Semantic Web to construct models that capture such activities and track the transformation of information into collective intelligence.

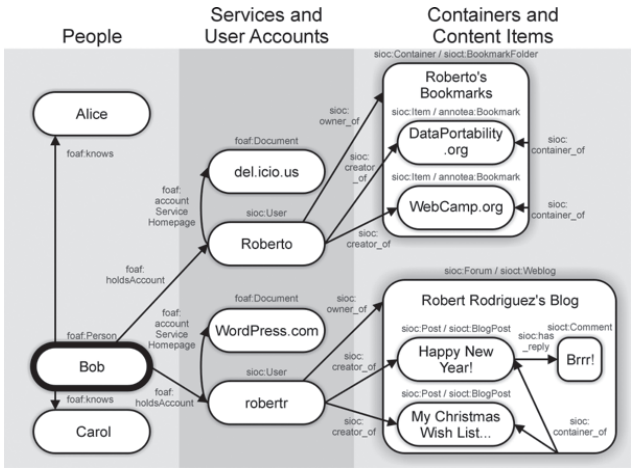

Figure 2-3: Social Graph Representation Using Semantic Web

Researchers see social data within a two-fold structure that includes data describing the social network and those that represent what members produce. Several ontologies can be used to link data across various social networks, including Friend of a Friend (FOAF)[2] and Semantically Interlinked Online Communities (SIOC).[3] FOAF represents individual profiles and links data among social networks. SIOC aggregates data from various Web-based media (including wikis and blogs) and presents information to users in the most appropriate manner [7].

Existing concepts can be organized and linked to SIOC descriptions using the Simple Knowledge Organization System (SKOS).[4] SKOS develops 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 represents knowledge-organization systems using the Resource Description Framework (RDF).[5] RDF-encoded information can be passed interoperable between computer applications. An RDF-based description of social data forms a rich-typed graph and offers a powerful way to represent online social networks.

[2] http://foaf-project.org
[3] http://sioc-project.org
[4] http://www.w3.org/2004/02/skos
[5] http://www.w3.org/RDF

Semantic Web technologies construct formal models that are useful for the extraction of knowledge produced by online social interactions (Fig. 2-3). By connecting social networks to FOAF and social activities (e.g., blog comments) to SIOC, Semantic Web provides a complete interlinked graph that supersedes existing networks.

Demographics

Social-networking sites are organized primarily around people, with each individual managing personal connections from the center of his or her community. Despite the fact that many social-networking services use designs that promote wide accessibility, various services attract homogenous populations where these groups commonly use the social networking sites to segregate themselves by nationality, age, educational level, or other factors that typically segment the offline society.

Because social-networking sites enable users to contact real-life friends, the majority of online connections are between friends, family members, colleagues, and professional acquaintances. A dominant social network can surmount local competition by providing the service of choice among existing groups of friends.

Figure 2-4 displays the dominant social networks by country in November 2008 [8], indicating pronounced regional variation in the most popular social networks. The success of social-networking sites relies fundamentally on their cultural relevance to a specific population.

2.4. Current Problems

Decentralization and Interoperability

Most social-networking sites provide very little interaction with external online services. They operate as "walled gardens," wherein user content is exclusive to the site and cannot be shared with other Internet applications. This limitation results from the sites' business

Figure 2-4: Adoption of Social Networks by Country (November 2008)

models, which employ user lock-in as a strategy for the acquisition of the largest possible user base.

Many users would prefer an interoperable format that would allow them to transport social interactions across different sites. Users who have struggled to gain a reputation within one site would like to transfer that reputation to other contexts. Currently, users who switch to a new social-networking site must begin anew, making new contacts and creating another online identity. Many users are currently willing to join more than one social-networking site; nonetheless, social networks could gain more new subscribers by facilitating interoperability.

Managing Social Identities

Because users cannot transport their data between social networks, individuals usually subscribe to multiple social networks and must thus maintain many profiles and connections. Distinct logins for each social-networking site prevent users from proving their identity across several platforms.

Further, social-networking sites have a very limited set of features for the protection of digital identity and the restriction of profile information sharing. Most sites use simple password protection and have a simple three-level access-control system similar to that of UNIX systems: users can choose to keep their information completely private, share it with a designated group of friends, or make it publicly available to all viewers. Most social-networking sites restrict profile access to internal users by requiring authentication as a community member.

Trust and Reputation Management

As in real-world interactions, trust is a key concept governing the establishment of relationships based on the online profiles of known people or strangers. To build new relationships, users must be confident that they are connecting with whom they expect. Reputation management and tagging technologies help users assess the trustworthiness of online third-party information.

Reputation management is based on a user profile's accumulation of more positive than negative comments. To build positive online reputations, users must be in as many places as possible, posting, making friends, building relationships, staying active in forums, and sharing information online with other users. The parallel development of Web 2.0 applications has popularized social tagging, by which users

can rank or categorize Web content, such as pictures, videos, and blog posts. A set of tags built from the use of such applications forms a folksonomy that can be seen as a shared vocabulary originated by, and familiar to, its primary users. Global tagging and aggregation build online trust and facilitate the identification of resources within a trusted social network.

Privacy

Privacy concerns demand that user profiles never distribute information that is not explicitly classified as publicly available. Many users publish personal information on the Web, including pictures (e.g., on Flickr, Facebook), opinions (e.g., on Twitter, blogs, forums), videos (e.g., on YouTube), and a variety of information on personal home pages. Such postings may contain sensitive information, such as birth dates, home addresses, and personal phone numbers. Because online users typically use query functions to search profiles, groups, and forums for information about other users, the protection of personal privacy is an inherent issue.

As in real-life relationships, people engage in online networks at different levels of confidentiality. Users must thus be in control of what they disclose and should be able to define disclosure rules (e.g., "nobody," "friends," "friends of friends," "everyone"). Most users have public profiles that are visible to everyone; these profiles often contain sensitive personal data that enable skillful attackers to use social-engineering strategies. The increasing use of microblogging services, such as Twitter, allows the creation of life streams in which users often disclose their geographic locations and personal habits. Blog entries about business meetings are another form of privacy risk, as well as a potential violation of corporate policies. Competitors can freely read and exploit such information.

Content Overload

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

Given the time-consuming nature of tracking and reading numerous online publications, blogs and forums, users must choose what to read and what to avoid. Although information is readily aggregated, it is almost impossible to process, analyze, validate, and contextualize in a manner that offers a coherent perspective on the facts behind the stories. As the amount of information continues to increase, users will require online relationship-management and data-mining tools.

Legal Concerns

Most of the known issues in social networks relate to the need to protect users' personalities and images. These social concepts encompass several factors, including reputation, false allegations, the right to one's image, privacy, insults, and discrimination of all sorts. From a legal point of view, social-network risks include the violation of users' data-protection rights and the perpetration of identity fraud.

Because Web 2.0 services host user-generated content, service providers must establish a detailed "Terms of Service" statement that covers users' rights and providers' ability to police existing content. Social-network 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 (e.g., copyright holders, victims of online harassment), law enforcement authorities or initiated by service providers. Some of these actions are acceptable, while others may violate users' rights; such situations have posed difficult dilemmas for several providers. Service providers may typically intervene when a user has posted

inappropriate, illegal, or copyrighted material, or has defamed or published private information about another person.

Given these legal and awareness requirements, social-network providers should be familiar with compliance and governance mandates and security frameworks. Unfortunately, we currently lack a framework for uniform international regulation that guarantees privacy rights and personal data protection across the Internet.

Usage Problems

Online social attacks include identity theft, defamation, stalking, injuries to personal dignity, and cyber-bullying. Attackers create false profiles to mimic personalities or brands, or to slander a known individual within a network of friends (e.g., a celebrity or a member of a school class). While such attacks may be carried out using conventional Web pages, they are particularly damaging within social networks because known victims may be targeted within social groups. Additionally, a victim's failure to immediately recognize a defamation attack may prevent him/her from accessing the offending content, due to the attacker's restriction of such access to the group ridiculing that victim. Teenagers' extensive use of online resources is associated with a growing risk of abuse, including cyber-bullying[6] and grooming by adults who intend to commit sexual abuse. Most teenagers have not received proper instruction on how to avoid such risks.

Cyber-bullying on social networks includes harassment, denigration, outing (sharing someone's secrets, embarrassing information, or images), trickery (talking someone into revealing secrets and then sharing it online), flaming (angry, critical, or disparaging electronic messages or discussions), exclusion, stalking, and threatening behavior. Stalking 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 through electronic means, such as e-mail, instant messaging, and social-networking sites (cyber-stalking). Social networks encourage the publication of personal information, including data that can reveal an individual's location and schedule (e.g., home address and phone number, schedule of classes).

Exposure to problematic content on the Internet constitutes an additional social threat. Problematic content includes a broad spectrum of undesirable or illegal material, such as violent media (movies, music, images) which promote hate speech, pornography, obscene content, and websites related to self-harm (sites dedicated to enabling self-injury and suicide, or those that encourage anorexic and bulimic lifestyles).

An increasingly prevalent threat is represented by sexual messages or nude or suggestive photographs sent by teenagers using mobile phones. With the proliferation of camera-equipped mobile phones and social-networking sites, "sexting"[7] has become a concern for parents. The issue has gained international attention following multiple incidents in the United States, in which teenagers have faced child pornography charges for sending nude or scantily clad images to other teenagers. Users can post on the Internet or forward these images or sexually explicit text messages, which can end in harassment or even sexual assault charges. A survey conducted in the United States [9] revealed that one in five teenagers said they had sent or posted online nude or semi-nude photographs of themselves.

3. Future of Social Networking

Social-networking sites are a relatively new phenomenon, and as with any other technological innovation, they will require a long period of

[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.

[7] This term combines the words "sex" and "texting" and refers to potentially prurient messages and images send over electronic devices, such as mobile phones or laptop computers. Source: http://sexoffenderresearch.blogspot.com

technical and social adjustment and improvement to fully meet users' needs and accommodate their behaviors. Users will also adjust online practices to adapt to new social-networking technologies.

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

Users currently play multiple roles within dynamic and fluctuating online social networks; thus, the further development of social networks must allow users to manage their profiles and connections using meta-social network tools. Such tools, such as Explode [10], will allow users to manage profiles and trust networks across distinct social networks using Semantic Web, data portability, and shared-authentication technologies. Users will thereby be able to maintain cross-network friendships using a centralized online profile.

Tools for the management of a user's distributed Web presence and others' ability to view that presence will likely be necessary to support effective social-network use within a distributed set of networks.

3.2. Metaverse: Convergence and Integration of Social Networks and Virtual Worlds

Internet and social-network evolution have occurred within an interactive and distributed environment. Increasing use of multi-user online environments (MOEs)[8] reflects the growing importance of social networking over gaming. Often characterized as virtual, persistent worlds, MOEs connect many simultaneous Internet users. The perpetual nature of these environments distinguishes them from those of typical computer gaming. Users may 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 with defined attributes that interact with other avatars and with the game's environment.

Most MOEs share some characteristics with popular social-networking sites and promote social interaction among users. The social nature of these environments depends largely on users' ability to interact within communities. Major research organizations [e.g., International Business Machines (IBM), Linden Labs] are working to enable the seamless movement of MOE avatars among virtual worlds while maintaining the avatar's identity in terms of appearance, personal information, and banking status. In the future, these virtual environments may converge to form a metaverse.

3.3. Integrating Social Networks and Data Portability

The integration of data from different networks, movement of information and social graphs across diverse sites, or identification of all content relevant to a particular topic are complex tasks that require specific standards and technologies supported by social-network providers. Although many Web 2.0 services currently employ application programming interfaces (APIs) to promote their integration with third-party applications, most social-network providers do not. However, some social-networking services have implemented basic features that allow users to import and export profiling information using standard tools, such as vCard.[9]

The number of open protocols designed for or usable by social-network platforms has increased exponentially in recent years. Social-network providers theoretically have the opportunity to use or compose with a growing number of open protocols and providers. Although a detailed overview of these protocols is beyond the scope of this paper, they include [11]:

[8] Multi-user online environments (MOEs) are a set of persistent online environments, ranging from massive multiplayer online role-playing games (MMORPGs; e.g.,World of Warcraft, City Of Heroes) to virtual worlds (e.g., Habbo Hotel, Second Life).

[9] vCard is a file format standard for electronic business cards.

--Authentication: OpenID, CardSpace, i-card, Liberty Alliance, Facebook Connect;
--Authorization: Open Authentication (Oauth), CardSpace, i-card, OpenSocial;
--Semantic markup and description: Resource Description Framework (RDF), MicroFormats;
--Network description: FOAF, XHTML Friends Network (XFN), OpenSocial, DiSo[10];
--Network visualization: TouchGraph, Web Positioning System (WPS);
--Remote manipulation of data and relationships: Representational State Transfer (REST), SOAP (Simple Object Access Protocol,), XML-RPC [a remote procedure call (RPC) protocol which uses Extensible Markup Language (XML) standard], DiSo;
--Service description: XRDS (eXtensible Resource Descriptor Sequence), UDDP (Unified Design and Development Platform);
--Service execution: OpenSocial, Facebook Applications;
--Message transport: REST, SOAP, Extensible Messaging and Presence Protocol (XMPP), and Simple Mail Transfer Protocol (SMTP);
--Application hosting: OpenSocial;
--Indexation and search: Google Social Graph.

Facebook, Google, and MySpace have announced technologies that permit user data portability among social websites, representing a new source of competition among social-networking services. Google's Friend Connect and MySpaceID use open-source code based on the OpenID, OAuth, and OpenSocial standards. These standards facilitate social-identity sharing across the Internet, not just among a few partner websites. Facebook Connect was the first interoperability protocol to be implemented; it features an easy logon, the option to rebroadcast activities on a third-party site to Facebook friends, and the matching of existing Facebook friend relationships with those on a third-party site. Facebook Connect allows third-party developers to let users log onto their websites using their Facebook credentials and to integrate other key Facebook features, such as friend lists, into third-party applications. The third-party sites can then send data back to Facebook and create news feed.

Existing authentication services (e.g., OpenID[11]) further extend interoperability and single sign-in functionality by making social-network user IDs portable to other sites.

3.4. Social Web Bill of Rights

In response to a lengthy public discussion of data and privacy rights, the Open Social Web group[12] presented the "Bill of Rights for the Social Web"[13] in September 2007. Composed by four Web 2.0 pioneers, this document outlined the appropriate treatment of data collected by companies from social-network site users, including personal data, data describing to whom users are connected, and user-generated content. The "Bill of Rights" defined three basic users' rights over their data: ownership, control (the right to share, keep private, or completely revoke data at user's discretion), and freedom.

These issues arose again following the February 2009 Facebook users' rebellion, which halted the company's attempt to change its terms of service to grant itself a perpetual license to all member-posted photos, videos, and copyrighted material [12].

3.5. Virtual Currency

Wikipedia defines virtual economy as the emergent economy existing in virtual worlds, usually characterized by the exchange of virtual goods within the context of an Internet game [13]. Virtual worlds have distinct virtual economies and currencies that are based on the exchange of virtual goods (e.g., weapons, spells,

[10] http://diso-project.org

[11] OpenID is a universal identification technology in which a user registered with a website (OpenID Provider) is assigned a URL that serves as a personal identifier. The user may then use the URL on any site that supports OpenID, and the logon process is handled through the provider site. Source: http://openid.net.

[12] http://opensocialweb.org

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

clothes, food, houses). Some virtual currencies are tied to the real world through purchase from game providers, and some people interact with virtual economies for real-world economic benefit. Users can also sell their characters, virtual money, and/or goods on online-auction websites for real money.

Games are one of the newest and most popular online application types on several social-networking sites. Because monetization is an important aspect of games, social-network providers have begun to distribute virtual currency (e.g., hi5's "coins"). For example, Hi5 users can spend virtual coins to purchase premium content, advanced features, and status upgrades. Many publishers of Facebook games are also using their own virtual currency, in the hope that a unified virtual currency will become universal and it will engage more gamers and, ultimately, encourage them to spend more money on games.

The use of money (real or virtual) on social networks, however, attracts fraudsters and cyber-criminals who attempt to steal users' social-networking credentials and online money.

3.6. Mobile Social Networking

Given the growing ubiquity of social networking and mobile-phone usage, the overlapping demographics will provide numerous opportunities for future mobile social-networking applications. Given the limitations of mobile phones (e.g., small screens, limited keyboards, often-poor network connectivity), the sophisticated native interfaces and rich media content offered by social networks cannot be fully duplicated on mobile devices. However, smartphones are increasingly been equipped with sophisticated features and sufficient processing power for software applications. Some devices already include a built-in interface or leading social networking sites. Mobile phones may include global positioning system (GPS) tracking devices and music players, and could supply valuable user information to social networks, such as locational coordinates or listening habits. As features are added to these devices, phones become a more complete repository for personal data linked to a single individual.

The benefits of mobile social networking, including enhanced location awareness and availability, must be balanced with users' requirements for personal privacy.

3.7. Sensor Networks

By combining social-network- and Web-connected devices, applications can extend social activities through sensors. 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 online activities and user footprints with their social profiles. Using semantic representations of information from sensors, users could connect through shared activities and interests. More importantly, alerts could be sent to users when abnormal activity patterns were detected.

An increasing number of portable devices support sensor-based interactions, from peripherals (e.g., Nike + iPod sport sensor[14]) to integrated sensors (e.g., iPhone's accelerometer). Sensors have recently become more prevalent in mobile devices. By supporting Bluetooth and WiFi communication, mobile phones have become sensor gateways for individuals. A wide range of Bluetooth sensors, such as heart 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.

3.8. Social Television

Internet protocol television (IPTV) is the next television market, allowing users to watch television programming wherever they are. Social

[14] http://www.apple.com/ipod/nike

networking through IPTV technology brings many favorable social services to television viewers, based on users' ability to share their experiences and opinions. The main features of social TV include online sharing of TV-watching experiences, interaction among TV viewers (via chat, e-mail, forums, video-conferencing), community-viewing of TV programming (watching together through a social television service or by online sharing), and recommendation sharing (via social networks, personal broadcasts).

3.9. Social e-Government

A new generation of politicians has increasingly adopted social-media tools to interact with citizens. The 2008 electoral campaign of Barack Obama, the President of the United States, provides an excellent example of such use. Governments can benefit from social networks through three broad areas of interaction:

--Government to Citizen: promotion of online public services and dissemination of information as "official" advice and support, increasing the transparency of information;
--Citizen to Government: citizen use of the Web to express views, highlight politicians' work, engage with the government, and influence policy makers;
--Citizen to Citizen: interactions that help fellow citizens handle public-service outcomes (e.g., healthcare information, advice about tax matters).

3.10. Political Use of Social Networks

Since the social-media-directed protests disputing the 2009 election results in Iran, Twitter and social-networking sites have emerged as powerful online tools for the organization and dissemination of virtual and real-world protests. People realized that they could effectively mobilize local protests and inform thousands of others worldwide through Internet resources, such as social networks and the Twitter microblogging service.

3.11. Corporate Use

Social networks allow the corporate sector to develop closer relationships with customers, since current Internet consumers are not merely buyers, but also use many opportunities to view, inquire, communicate about, and analyze products and services. Consumers readily share their feedback and complaints about their favorite products and brands. Web 2.0 applications are useful for product development and the establishment of commercial relationships, and allow companies to learn more about consumers. Business opportunities that incorporate social networks include:

--Social advertising: formats that engage the social context of the viewer and target advertising using user data;
--Micro-payment within social networks: enables the exchange of goods and services within the social-networking platform; also applies to developers of social software applications;
--Platforms for micro-niches: subscription or access fees could be charged;
--Resale of marketing and business intelligence based on information collected on the network;
--Buying clubs: to drive demand, users interested in similar product types could be offered coupons;
--Interaction with real-world commerce: social platforms could be connected with small- and medium-sized businesses, such as established boutiques, coffee shops, restaurants, and bars.

Companies must adapt their business models to take advantage of social Web features within large (e.g. Facebook) and small or focused social networks. Smaller networks present the opportunity to reach a niche or distinct group of customers.

3.12. E-Learning through Social Networking

Schools and higher-education foundations increasingly prefer to use social networking as

a communication and collaboration tool. In the near future, it would be beneficial for schools to promote online interaction through social-networking sites. Such interaction could be used to prepare students by providing them with the adult life-skills they need to succeed. Security policies remain important, as does instruction for students about online safety and responsible online expression. Students may learn these lessons best while using social-networking tools.

4. Security aspects of Social Networking

Although new paradigms provide many opportunities, their implementation without consideration for necessary security requirements can deter growth and user adoption. Because social networks attract thousands of users who represent potential victims, social-networking sites are desirable targets for mass attackers.

4.1. Actors and Motivation

Several actors and groups target social networks for fun and profit. Malicious actors may adopt several categories of attacks and tools to target social-network users; the following are a few examples:

--Spammers and phishers use compromised social-network accounts to send fraudulent messages to victims' friends;

--Fraudsters and cyber-criminals use social networks to capture user data and carry out social-engineering attacks;

--Hacktivists and offline terrorist groups create communities to spread their views, promote their causes, and frequently to conduct recruitment;

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

Social networks are popular communication media for many communities, including those with malicious intent. Several hacking groups have created hacker-themed online communities to promote their malicious activities and tools. Many others offer hacking tutorials, news articles, tools, or descriptions of exploitation techniques. Several communities function as marketplaces to encourage the abuse of stolen credit-card information and attacks against high-profile targets, such as banks or e-commerce sites (Fig. 4-1). Hacking communities within social-networking sites also offer hacking services, often for profit.

The majority of attackers' profiles on social networks appear to have been created by unso-

Figure 4-1: Example of a Carding Forum on Orkut (no longer available), Advertising "Trustworthy" Mules and Spammers

phisticated users, since attackers may use these communication media only in the initiation phase. Skilled malicious actors usually participate in underground forums and use secret communication channels.

4.2. Current Security Threats

With the increasing popularity of social networks, hackers, fraudsters, and malicious users began using these networks to conduct illegal activities. These activities have been undertaken by using social networks as attack vectors for traditional cyber crimes, by creating specific threats to social-network users, or by conducting direct attacks that disrupt social-networking sites.

The intrinsic properties of social networks make them ideal for exploitation by online criminals. These networks represent a huge and highly distributed user base comprised of clusters of users who share the same social interests and have thus developed trust with each other.

Privacy

The availability of personal information on social networks provides an ideal condition for the abuse and leveraging of such information. The inappropriate exposure of sensitive information allows criminals and terrorists to conduct "criminal data mining."

Malicious actors may use unflattering material or personal information from social networks to select targets, profile victims, and plan and execute criminal activities. Also described as "knowledge discovery," data mining and predictive analytics allow fraudsters and terrorists to manage the large amount of information produced by their targets, including social-network profiles, personal conversations on scrapbooks, blog and Twitter posts, and personal photos on online albums.

Identity/Password Theft

Various forms of identity theft have existed for a very long time. Thieves have assumed the identities of unsuspecting consumers in an effort to commit fraud, ruining the financial lives of their victims. Searches of existing online information may yield social-security numbers, birth dates, addresses, and other personal data that help criminals steal or create false identities. Criminals can easily obtain the necessary false credentials to move throughout the many systems that require identification.

Attackers use compromised social-network accounts to launch attacks because they can readily move from one account to the next. Inherent trust relationships among users 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, the risk of attack increases for anyone connected to that individual. Social-network credentials can be stolen using traditional key loggers, by running brute-force attacks, or by social engineering (usually based on the information available on users' profiles).

iDefense researchers observed attackers abusing a Security Focus Jobs site in December 2007. The attackers were able to freely register as a recruiter, obtain the resumes and business information of 2,471 registered users, and send fraudulent e-mail messages to all of those individuals.

Malicious Code, Viruses, and Worms

Malware authors have recently noticed that malicious code can be efficiently spread using social-networking sites, due to the ease of leveraging trust among socially connected users through social engineering. In this way, victims can be convinced to install the malicious code. Malicious actors target the most popular services, such as Facebook and Twitter, to take advantage of large user bases.

Malicious code is proliferated through friend information collected from infected users' social-network accounts. Many attackers also use social networks to create false profiles and

to publish false links that lead to sites infected with malicious code.

Banner advertisements, video content, and false social-network profiles have increasingly been used to steal personal information as the number of online consumers has risen. Malicious codes are distributed through pop-up advertisements, some of which do not require a click by the user.

In some cases, social engineering is not necessary to carry out attacks. For example, the early MySpace worm "Samy Worm" used JavaScript commands to add friends to targeted accounts automatically. Such worms spread 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 supporters of United States President Barack Obama, to spread malicious code. The attack utilized false images that aimed to convince users to install a malicious executable file through false Flash CODEC errors. Attackers injected the same URLs into many different websites and forums, suggesting that they utilized automatic forum-crawling and account-creation programs.

Malicious actors have employed increasingly innovative methods to control botnets[15], including the use of social-networking services. iDefense has cataloged hackers who adapted the protocols of many social-networking sites (e.g., Twitter, Google Groups) and URL-shortening services (e.g., bit.ly) to send action messages to zombie computers. In this way, their actions appeared as normal user activity and the likelihood of discovery was reduced.

Spam, Phishing, and Financial Fraud

Phishers usually collect user information from compromised social-network accounts to send spam and phishing messages. Like phishing that targets banks, phishing that targets social networks can have financial impacts and cause monetary losses. Attackers may set up false social-network profiles and then establish connections with friends on "buddy lists" to gain more information and identify potential targets for phishing attacks.

Several malicious codes target online gamers. Hackers typically use these codes to take over compromised subscription-only gaming accounts and access the virtual property deposited therein in order to sell the virtual goods through the digital underground. Successful attackers of some social gaming sites, such as Second Life, may extract real money from compromised accounts. According to a November 2006 entry in the official Second Life blog, various phishers have targeted Second Life to steal in-game money (Linden dollars) by claiming that the user could use a hack to create free money [14]. Attackers can convert the in-game money of compromised users directly into real money by reselling the virtual goods on public or underground forums or retrieving the existing credits.

The increasing use of social networks and virtual worlds as social and business platforms, including the use of virtual money in social environments, attracts cyber-criminals. Financial fraud has affected online gamers for many years, through the theft of online goods (weapons, objects, virtual money) or "gold farming,"[16] which created an underground economy based on the sale of virtual goods and the transfer of virtual money.

Data Loss

Incidents of data leakage include the loss of personal, corporate, confidential, or customer information, inappropriate public statements

[15] A botnet is a group of computers on the Internet that, although their owners are unaware of it, have been infected and set up to perform malicious activities to other computers on the Internet, including sending spam or running Distributed Denial of Service (DDoS) attacks. Any such computer is referred to as a "zombie," a "robot" or "bot."

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

about companies, the use of corporate resources for personal purposes, and harassment of or inappropriate behavior toward a customer or fellow employee. Social-networking sites are another platform through which data leakage may occur, and such incidents have a broader impact on corporate reputations.

Many companies are currently focused on preventing the loss of confidential and proprietary information and its access by unauthorized outsiders. Most data-loss incidents occur through e-mail or file transfers, but instant-messaging chat tools, blog posts, Twitter messages, and online resume content published on social networking sites may also disclose proprietary company information.

Information Control and Censorship

Administrators cannot realistically or effectively manage the huge amount of information available on social-networking sites. Social-networking sites are not likely to ensure the accuracy, legality, or usefulness of content before users publish it. For this reason, it is difficult to prevent actors from posting unwanted information; while communities that use self-policing mechanisms or moderation are generally more successful. For example, rating systems allow users to remove erroneous content by popular vote.

Future development of social-networking sites should employ thresholds for monitoring new content published by its users and self-moderation capabilities, once users are often the first to be aware of content problems. Security teams that monitor social networks are an effective reactionary approach to limiting malicious content, but decentralized social networks may not be able to devote sufficient resources to address such problems.

Offense, Hate, and Discrimination

Cyber-stalking and cyber-bullying involve repeated contact with victims and purposeful acts of harm, including harassment and humiliation. Like offline bullying, cyber-bullying can lead to 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 use online techniques to accomplish their goals and improve communication. Law-enforcement organizations are also concerned that a small number of youths converted online may begin to use social networks to promote offline hate crimes.

Sexual Crimes and Child Safety

Social-networking environments represent a serious risk to children and teenagers, who can become the victims of cyber-bullying, online harassment, and sexual predation. Children who are at risk online are usually those who are also at risk offline. The most frequent threats to children on social-networking sites come from peers, young adults, and predatory older adults.

Child pornography is a particularly horrific crime involving images and videos that depict minors in suggestive poses or explicit sex acts. Youth-generated sexual content (photographs and videos) intended for viewing by other minors (usually friends and partners) is a related serious issue. Although such content is not intended for adult consumption, it may unexpectedly spread through the Internet and potentially embarrass the children.

Social-network providers find it difficult to keep their sites entirely free of sex offenders, given the huge number of users and the ease of creating false identities.

Attacks on Social Networks

As with the providers of any other Web application, social-networking providers may represent vulnerable targets for direct attacks.

Security vulnerabilities may allow hackers to attack providers, causing service failures (e.g., denial of service) or unauthorized access to users' credentials followed by disclosure of private information. Such vulnerabilities may also be used to spread a virus among user accounts. Cross-site scripting (XSS) or SQL injection vulnerabilities on social-network applications could cause problems for millions of users. Furtnermore, malicious actors have debilitated social-networking sites through orchestrated Distributed Denial of Service (DDoS) attacks.

Malicious users may take control of visitors to social sites by remotely manipulating their browsers through legitimate Web-control functionality, such as image-loading HTML tags or JavaScript instructions [15].

Home, a virtual world wherein PlayStation 3 gamers interact, was hacked in December 2008 [16]. 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 has also been vulnerable to XSS attacks [17]. In March 2009, the Koobface[17] worm targeted users of Facebook, MySpace, hi5, Bebo, Friendster, and Twitter. Koobface spreads through invitations from a user's contact that include a link to view a video. It ultimately attempts to gather sensitive information from victims, such as credentials and credit-card numbers.

4.3. Future Security Threats for Social Networks

The technological evolution and global adoption of social-networking services will bring further security risks that may present opportunities for malicious actors exploring such services. Information-security professionals and law-enforcement agencies must adapt to these potential future threats.

Exploitation of Social-Networking Gadgets

The introduction of social-networking applications and web gadgets provides a potential vector of malicious attacks. Web widgets are small graphic applications that bring third-party tools and games (e.g., clocks, calculators) to social-networking sites. Such applications have a rapid adoption rate in desktops, mobile devices, and Web applications because they are easy to create and implement.

The rising popularity of widgets has led to increased targeting by malicious actors, who use them as spyware, for virus dispersal, for hijacking, and might explore existing software vulnerabilities. Social-network providers release widget software developers' kits (SDK) to allow developers to create widgets that run in the social-networking site. However, the availability of these SDKs provides system access to users with malicious intent, who gain a roadmap for widget manipulation.

Widgets may be vulnerable to exploitation by hackers and criminals due to inadequate security models, which may allow malicious code to run freely and spread readily. Vulnerabilities associated with widgets are similar to those found on the Web, but present a higher risk because 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.

Criminals may also create malicious applications to intentionally install malware on victims' systems. Legitimate applications, such as the CityFireDepartment Facebook application, can be modified to distribute malware. Attackers compromised this application and used injected IFrames to infect victims with rogue anti-virus applications [18].

In September 2009, a security researcher promoted the "Month of Facebook Bugs," an initiative that included the daily posting of security flaws in Facebook applications throughout the month of September. To promote

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

awareness of social-networking application security, the researcher reported bugs in third-party applications available on Facebook. Most of these bugs were XSS flaws in various social applications, including Facebook's 10 most popular, that potentially affected millions of users [19].

Social-Network Worms and Phishing Powered by Semantic Web

All social-networking sites identify "circles of friends" based on existing relationships or common interests within a group or community. Malicious actors may 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. In the absence of such sources of information, social connections can also be inferred by mining Web content and links. Worms that incorporated Semantic Web attributes could easily identify connection among users and quickly spread across social graphs.

Terrorism Using Social Networks and Online Communities

Terrorist organizations have begun to use social networks and virtual worlds in their daily activities. Terrorists may use virtual worlds to create exact replicas of targets for the planning and simulation of attacks, eliminating the 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 operate online training camps in virtual worlds to evade detection and avoid prosecution. Second Life could easily become a terrorist classroom.

Social networks and online communities also help terrorists recruit new members and may serve as meeting places for the discussion of plans. Once these groups and communities are built, terrorists may readily spread propaganda, and recruit and instruct converts in the construction of terrorist cells and the execution of jihad. In October 2008, authorities arrested two white supremacists who planned to kill Senator Barack Obama and more than 100 African-Americans; they had met online through a mutual friend.

Microblogging communities, such as Twitter, may also be used as an effective communication tool for coordinating terrorist attacks and tracking news in real time. The ability to transfer virtual money between avatars is also useful for criminal activities because that money can then be translated into real currency and it is very difficult to track.

Second Life currently contains a radical terrorist group called the "Second Life Liberation Army"[18] that has been responsible for computer-coded atomic bombings of virtual-world stores using Second Life weapons and armories. Previous Second Life attacks include the explosion of the Australian Broadcasting Commission's (ABC) island, attacks on Reebok and American Apparel stores, and storming the stage at the January 2007 virtual meeting of the World Economic Forum.

Social-Network Forensics

The rising use of social-networking sites and Web 2.0 technologies by cyber-criminals demands specific criminal investigation tool and procedures by law-enforcement agencies. Effective forensic investigation of social-networking threats requires evidence gathered from social-networking sites and the use of technologies that track activities, identify perpetrators, and specify the timing of online criminality. Social-network forensics is a set of specific investigation skills applied to the social-networking universe.

Information-security professionals must develop specific tools and techniques to detect

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

and investigate malicious activities on social networks, and to ensure that information has been properly secured and examined and that all evidence has been recovered. Information discovery requires the ability to search for information as soon as it is created or distributed by a user. It also demands the ability to measure search quality, dynamically classify search results, and properly visualize data according to numerous criteria and within numerous contexts.

A new social-networking forensic framework must focus on the analysis of online actors (profiles) and their activities. It must incorporate the investigation of suspects' or victims' online relationships (past and present), participation in online communities, and usage patterns on social-networking sites, and the forensic analysis of intra-social-networking applications [20].

5. Conclusion

Social networks are growing rapidly and incorporate functionality far beyond the initial "list of friends" concept. Users wish 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" online 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 levels of protection, privacy, and trust. Hacking groups continue to attack social networks, spreading key loggers, Trojan horses, and other malicious applications.

Governments and intelligence agencies must 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 at: http://www.whatissocialnetworking.com.

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

[3] The Daedalus Project, "WoW Gender-Bending". Available at: 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] WikiPedia, http://en.wikipedia.org/wiki/Dunbar's_number

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

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

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

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

[11] T. P. Anglade, O. Pekelman, L Montagne. "The Social Web: Small Businesses / Big Solutions." Nov. 20, 2008. Available at : http://www.w3.org/2008/09/msnws/papers/af83.pdf.

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

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

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

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

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

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

[18] R. Thompson, "Hacked Facebook applications reach out to exploit sites in Russia", AVG Blogs, Oct. 14, 2009. http://thompson.blog.avg.com/2009/10/hacked-facebook-applications-reach-out-to-exploit-sites-in-russia.html.

[19] theharmonyguy, "FAQs on FAXX and the 'Month of Facebook Bugs'", theharmonyguy blog, Sep. 3, 2009. http://theharmonyguy.com/2009/09/03/faqs-on-faxx-and-the-month-of-facebook-bugs.

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

Anchises M. G. de Paula works as International Cyber Intelligence Analyst at iDefense, a VeriSign company. He has more than 15 years of experience in the computer security industry, having worked as a Security Officer for Brazilian telecom companies and a Security Consultant for local resellers and consulting firms. He earned a bachelor's degree in Computer Science from the Universidade de São Paulo (USP) and a master's degree in Marketing from the Escola Superior de Propaganda e Marketing (ESPM). He is CISSP-, GIAC- (Cutting Edge Hacking Techniques) and ITIL-Foundations certified. As an active member of the Brazilian information-security community, Anchises served as President of the Brazilian chapter of the International Systems Security Association (ISSA) in 2008-2009 and Director of the Brazilian chapter of the Cloud Security Alliance (CSA) in 2010-2011.