2011

Embedded with Facebook: DoD Faces Risks from Social Media

Phillips, Kenneth N.; Pickett, Aaron; Garfinkel, Simson

Embedded with Facebook

DoD Faces Risks from Social Media

Capt. Kenneth N. Phillips, Marine Corps Tactical Systems Support Activity
LT Aaron Pickett, Navy Information Operations Command
Simson Garfinkel, Naval Postgraduate School

Abstract. U.S. service members are increasingly jeopardized by information posted on social network websites. While some of the most damaging information comes from spouses and other non-official sources, other information comes from the use of social media by the DoD because non-public, secure channels for questions and feedback do not exist. Other problems arise from the conflict between the DoD's desire to promote its mission by distributing information to a world-wide audience and the ability of adversaries to misuse that information. We have conducted a study of information posted on Facebook and other social media websites and have determined that it is relatively easy to correlate the DoD official records with online profiles, allowing the targeting of specific warfighters. We summarize several cases in which the public disclosure of information led to mission compromise and suggest ways for improving current policy and practice.

Introduction

U.S. service members are increasingly jeopardized by information posted online by the DoD, by friends and family, by other service members, and by themselves. Information posted online can be used to target service members and their families for crime, retribution, or terrorism. Online postings can also leak sensitive information about tactics or capabilities, and can even compromise specific operations.

These risks are not hypothetical: terrorist publications have advocated collection of information from Facebook [1]; in March 2010 an Israeli raid had to be canceled because a soldier posted the details of the raid to his Facebook page [2]; and there have been persistent reports of military members being targeted by identity theft rings [3].

It is not clear how the DoD should respond. Certainly DoD Operations Security prevents direct security compromises such as publishing the time and locations of planned attacks against our adversaries.[1] But much of the most damaging information published today does not come through official channels. Attempting to regulate a spouse posting to an online support forum the location of her husband in Afghanistan would pose obvious First Amendment issues.

The DoD is better positioned to limit the disclosure of personal information on DoD websites—for example, by limiting the posting of names and photographs. But such attempts to restrict the flow of information will have an adverse impact on recruitment, public affairs, and diplomatic efforts. Currently the trend has been to embrace openness, despite the risk.

There are also strong reasons within the DoD to encourage the use of social media. Social media allows easy communication between service members and their families, improving the morale of both. These websites and services also provide excellent platforms for the informal distribution of information—even from one official source to another. Indeed, services like Facebook and Twitter are now used by the DoD in an official capacity to supplement other public affairs activities.

We argue that there is a difference between using social media for carefully controlled publications and the uncontrolled disclosure of sensitive information. To this end, we conducted an investigation of vulnerabilities that result from the intentional and inadvertent release of information about service members to the Internet between September 2009 and September 2010. We found many previously undocumented cases in which information that could be considered sensitive but which was unclassified was routinely posted by DoD personnel and their families on publicly available websites. We also developed reliable techniques for cross-correlating and fusing information between multiple freely available information sources, amplifying the risk posed by the individual disclosures.

During the course of this investigation the DoD changed its policy on Facebook and other social network websites, and now allows them to be used from official computer systems and for both personal and professional purposes. This change makes the results of our study even more important.

We believe that the new, relaxed policy needs to be accompanied by a systematic examination of information that the DoD is publishing to the Internet through both official and informal channels. DoD personnel need to understand the ability of our adversaries to integrate multiple releases of apparently innocuous information into a form that can compromise operations and personnel. Finally, service members and their dependents need to understand risks and the need for appropriate conduct.

Embedded with Social Media

Today Facebook is the world's dominant social network site. Facebook boasts over 600 million active users, half of whom check the site on any given day. According to Facebook these users share more than 30 billion pieces of content and spend over 700 billion minutes on the site each month [4].

Facebook is also the most popular social network site for DoD personnel. Using our techniques for correlating official DoD records with directories on Facebook, MySpace, and LinkedIn, we determined that (at the time of the study) between 25% and 57% of DoD personnel had Facebook accounts, between 22% to 48% of DoD personnel had MySpace accounts and 11% to 18% had LinkedIn accounts [5]. These numbers have likely increased over the past year with the continued growth and acceptance of social media sites.

In February 2010, the DoD updated its policy regarding the use of social media sites [6], directing that the Non-classified Internet Protocol Router Network (NIPRNET) be configured to allow access to social media, e-mail, instant messaging, and other Internet-based applications not controlled by the DoD or Federal Government. The new policy also allows for official uses of social media sites that are not related to public affairs and directs that all external official presences on the Internet be registered on <http://www.defense.gov>.

The DoD itself maintains official sites on Facebook, Flickr, Google Buzz, Twitter, UStream, and YouTube, along with the DoDLive Blog. All of the DoD services, including the National Guard and Coast Guard, have an official presence on Facebook, Twitter, Flickr, and YouTube. Numerous high-ranking leaders within the DoD have their own Facebook pages and are aggressively using social media for recruiting, public relations, and information dissemination. For example, the Chairman of the Joint Chiefs of Staff's page[2] has over 15,000 individuals listed as "liking" the page.

The Army, Air Force, and Marine Corps have also published guidelines[3] for service members who choose to use social media sites in an unofficial or personal capacity. The Air Force and Marine Corps guidelines help service members understand what is and what is not appropriate to post online. They also provide general recommendations for the privacy settings that members use on social media sites and remind service members that content posted online can be seen by anyone. The Army guideline provides details on specific social media sites on which the Army maintains an official presence and encourages soldiers to participate in these sites as a way of spreading positive publicity about the Army.

Deployed units are using sites such as Facebook and Twitter to share photographs and newsletters and to release official information [7]. Individual service members use Facebook and other sites to stay in contact with loved ones during deployments. Family members use these sites to keep their deployed service members informed about happenings at home and to let friends and extended family know about what is happening with their service member.

In August 2010, the Navy released an All-Navy message specifically addressing the use of Internet-based capabilities, including social network sites such as Facebook. The guidance warns service members to be careful about using third-party applications on social network sites, encourages them to learn about and use the privacy settings available on social media sites, and reminds them to be thoughtful about who they allow to access their social media profiles. The ALNAV also warns service members about the potential for criminals to use personal information posted on the Internet for identity theft [8].

Social Media Risks and Exploitation

With all of the activity taking place on social network platforms, there are bound to be leaks of sensitive information. These leaks can occur in two ways. First, a specific sensitive item might be inadvertently posted in an online forum where an adversary exploits it. But information can also be released in small bits that are later collected and correlated. Adversaries can then fuse this data to develop a more complete profile.

Potentially harmful leaks include:

- **Locations and dates of deployments**
- **Details about pending operations**
- **Identifying photos of service members**
- **Identities and location of service members' families and friends**
- **Locations of sensitive facilities**
- **Impending policy changes**
- **Non-public details of military capabilities**

These risks are not theoretical. A post on a jihadist website instructs followers to gather intelligence about U.S. military units and the family members of U.S. service members, including "what state they are from, their family situation, and where their family members (wife and children) live," and to "monitor every website used by the personnel … and attempt to discover what is in these contacts" [1].

These risks to security do not come only from adversaries attempting to collect information, but also from inadvertent posts by one's own forces. Israeli Defense Forces (IDF) postponed an operation in March 2010 after a soldier posted the location and time of a planned raid on his Facebook page [2]. In a separate instance that took place in July 2010, it was revealed that Israeli soldiers who had served at a secret IDF base had set up a public Facebook group meant for veterans of the base. Members of the group had uploaded photos of themselves inside the base. A reporter inadvertently admitted to the group copied posts and photos from the group's "wall" to his own computer [9]; quotations from the posts were later published.

While not as directly revealing as the information distributed in Israel, the DoD routinely publishes personally identifying information of service members including high-resolution photographs, name, rank, promotion dates, occupational specialty, and unit affiliations. Until a recent policy change by the Office of the Secretary of Defense [10], the last four digits of a service member's Social Security Number could be posted on public webpages. The new policy, issued shortly after our research was distributed within the DoD, called attention to the problem and its implications. These details can be combined with other publicly available records to reveal more sensitive details.

Internet queries based on disclosed information can provide home address, family status, the identity of family members, and other sensitive information. Furthermore, identifying details provided by the DoD can be used to uniquely identify and target accounts belonging to service members. This can be accomplished by matching names and photographs, or by checking for membership in Facebook groups associated with military units or specialties. It may also be possible to deduce a service member's birth year from their date of rank (since most officers are commissioned soon after college, and promote at regular intervals), and match that with biographical information on a Facebook profile. We believe that this poses a risk to service members, their dependents, and operational capabilities.

During World War II, Americans were advised not to repeat military information that they might have learned due to association with friends and families—"loose lips sink ships." These lessons are now long forgotten, as Example 1 readily confirms.

High-resolution photographs available from DoD press releases and Facebook profiles pose a special risk to U.S. forces. For one, they can be used to build biometric databases used to covertly identify these individuals years after the original photograph is released. Location-based services and geo-tagging of photographs pose yet another risk. A photograph snapped with a cell phone camera and posted to a social networking website or e-mailed to a distribution list can also inadvertently reveal the graphical location of their homes, workplace, or even sensitive locations, since many cell phones now embed geographical location within digital photographs.

Example 1: Actual posts (anonymized) from Facebook pages belonging to DoD personnel, found with a simple search

"DEPRESSED....COUNT DOWN in 32 days my better half will deploy to Afghanistan. What to do now? "

"family and friends a moment of your time to pray for my nephew chris b******, he is leaving to Afghanistan for a year of duty with the army national guard. He will deploy on august the 10th. Thank-you all."

"Please keep our family in your prayers as both of my brother deploy to Afghanistan tomorrow at 11 am....."

"To all my friends and family. Tonight say a prayer for 1-66 armor 4th infantry. Tonight will be there last night state side, as they deploy to Afghanistan."

"Dear Lord, Please keep My Husband, My Son, & their fellow Soldiers safe- and give me & our Family strength these next (very long) 12 months! "

"I want to thank those that attended the Send-Off party for my husband MAJ Doug P***** and my son, SGT Mitchell S****** as they prepare to deploy to Afghanistan in 10 days! "

Many social network users leave their profile privacy settings open to the public, allowing any web user to view their personal information. This personal information can be even more damaging if combined with profile information from family members and friends. In February 2010, Pete Warden created a script that downloaded 215 million public profile pages from Facebook, including 120 million from U.S. users. He planned to make the profile data available to academic researchers, but deleted it after Facebook threatened a lawsuit [11]. Six months later, security researcher Ron Bowes wrote a script that downloaded the names and profile URLs of 171 million Facebook users; he then made the downloaded information freely available over the Internet [12] before Facebook could intervene.

Just as damaging as the content of the individual posts is the identifying information associated with them. When this information comes from Facebook it is frequently accompanied with the true name of the person who posted it–the use of fake names or aliases is a violation of Facebook's terms of service and can result in account termination. Facebook also frequently displays that individual's friends and in some cases, where that person lives, works, and spends their time.

All of this information can be used by adversaries to improve targeting of U.S. forces and their families. The targeting of service members and their families is not unprecedented: one year after the Vincennes accidentally shot down an Iranian civilian airliner in 1988, a van belonging to the ship's former commanding officer was fire bombed in an apparent retaliatory attack.

Being able to search for results like this also makes it easy for would-be identity thieves to find out when a service member will be away, making them more vulnerable to identity theft. It's difficult for warfighters to monitor their credit when they are in a warzone.

With the relaxation of the DoD's policy on social media, commands have started using Facebook and other social media sites to share information with members and their families. As such, the DoD should be specifically concerned with the use of Facebook as an open forum for personnel and family members to ask questions related to orders and personnel records.

It is frequently not obvious to users of these pages that information posted is visible to the world and not restricted to the intended audience. Such questions potentially reveal details about service members, families, and troop deployments. Individual postings might seem harmless, but they can be useful to adversaries if they are combined with other posts, the identities of the posters, and information gathered using other methods.

In our review of Facebook, we found specific examples on command-sponsored Facebook pages that raise concern; they are shown in Example 2.

Example 2: Facebook posts that show evidence of deployments

"About 3 weeks ago we received verbals to Lemoore. We are currently stationed in Atsugi, Japan. I am in need of a early family member return because our rotation date to leave here is in mid November and I am pregnant and due November 25th."

"I am also currently awaiting orders but to ECRC NFLK fwd Afghanistan and I am currently in Guam."

"I already have PCS orders for a GSA in Aghanistan, I report to NMPS in December when should I receive my Temadd orders for my assignment and training. I saw in my orders that they should be release along side my PCS orders. I was told 60 days before I transfer from a few people. Is this right?"

Even if a Facebook group could be restricted to vetted members of the command, their dependents, or close friends, it is important to realize that Facebook's servers are not operated by the DoD. Information stored in these servers is available within Facebook to various programmers, system administrators, and others–many of whom may not be U.S. citizens, and may not even reside within the United States. Unlike DoD servers, which rely on encryption to transmit sensitive information over the NIPRNET, Facebook is generally accessed without encryption.

Facebook and other social network sites do not require identity verification prior to creating an account, which makes it easy for an adversary to impersonate an account or create a fictitious account, then befriend unknowing targets. Security consultant

Thomas Ryan set up a Facebook profile for a fictitious 25-year-old woman working at the U.S. Navy's Network Warfare Command. Within a month, the profile had over 300 contacts from within the U.S. defense and intelligence communities, an invitation to speak at a security conference, and a request to review a technical paper by a NASA researcher [13]. One military contact of the fictitious female even revealed details of take-off times for military helicopter flights in Afghanistan [14]. Ryan was also able to gain access to e-mails and one person's bank account information by making use of details published on personal profile pages to guess the answers to "secret questions" that are used as back-up authentication when a user forgets a password [13].

Already enemy organizations have used social networks to obtain intelligence. In Israel, for example, military intelligence officers were ordered to close their Facebook accounts after it was discovered that some had been "friended" by Hizbullah operatives posing as Israeli women for the purpose of gaining access to personal information [9].

Another important security problem with Facebook is the use of so-called "cookie authentication," which allows an adversary to impersonate legitimate Facebook users and gain extended unauthorized access to a Facebook account by capturing a Facebook "cookie" from an unsecured wireless network or from a public computer. Software is now widely available that gives the attacker an easy-to-use web-based interface of the cookies that have been captured; simply clicking on a user name allows the attacker to compromise any of the linked Facebook accounts at will.

Facebook allows third-party developers to write applications that users can add to their Facebook profile. These applications frequently have unrestricted access to a user's personal data. When a user permits an application access to their profile, the application can also see the profile information of that user's friends with the same level of detail that the user can see, unless it has been specifically prohibited by the friends' privacy settings. The default settings permit this behavior.

The net result of the large membership groups, the access given to "friends," and Facebook's security model is that it is unwise to store any information on Facebook that is meant to have any form of restricted dissemination.

Recommendations

Even a casual analysis of Facebook indicates that a significant amount of information is being posted that could easily be used against U.S. interests. This a growing problem that needs to be addressed.

Social media such as Facebook increasingly plays an important role in personal communication, entertainment, political discussions, and even the dissemination of official information. The DoD has already decided that it makes more sense to embrace social media than to attempt a futile ban. Indeed, if the DoD were to abstain from the new media in an official capacity and ban its use, it is likely many of the conversations would remain active in unofficial capacities. But as our work shows, social media is creating real risks and vulnerabilities for the DoD. Given the scale of the problem, the most effective near-term solution we see is education.

Service members must be taught to understand the risks involved in posting personal information on the Internet, not only to themselves, but to their units and families. They need to be informed about the different levels of privacy available on social network sites and the implications of each level. They also need to understand that the privacy level they select is not a guarantee of privacy. There have been leaks of private information in the past and there are bound to be more leaks of private information in the future. The reality is that any information that is posted to a social media website may readily become available to the public at large–access controls are not effective.

The DoD needs to consider ways to make service members and their families as safe as possible when using social media. One way to do this is to provide specific guidelines of how individuals can use these services safely, as well as examples of how lax practices may make us vulnerable to Open Source Intelligence collection by our adversaries.

Recently there have been some efforts to educate the services. For example, the Department of the Navy Chief of Information produced a briefing with "Recommended Facebook Privacy Settings."[4] The briefing explains how Facebook makes money by showing targeted advertisements. The materials rightfully warn that anything stored in Facebook could be made public–manipulating the privacy settings is no guarantee of preserving privacy. Nevertheless, the briefing does give specific recommendations on how to set Facebook's complex privacy settings. Keeping materials such as this up-to-date will be a challenge given Facebook's tendency to make rapid and significant changes to both its user interface and its underlying privacy policy.

Other services are taking similar measures. The Marine Corps is incorporating education on social media use into annual operational security and information assurance training [15]. The Army Memorandum on the responsible use of Internet-based capabilities [16] warns that the use of social networking sites by Army personnel provides adversaries with the opportunity to gather personal information that can be used to directly target Army and DoD personnel.

Educating the service members is not enough. We have seen posts by spouses, children, parents, and friends that revealed details about the location or deployment dates of their service member. By itself, this information might seem harmless, but when it is put together with information from other posts and other sources, it can become dangerous. An adversary could easily determine the address of a service member's family based on their name and the location information in their profile. Then they can find out the location of the children's schools or daycares. An innocent post by a wife that her husband is halfway through his deployment in Afghanistan can alert an adversary that the family might be extra vulnerable to an attack. To this end, the Army directs that personnel discuss the proper use of social media with family members using a guide[5] specifically tailored to family members.

Technology can also be of help. For example, the website ReclaimPrivacy.org operates a "privacy scanner" that allows individuals to scan their own Facebook privacy settings. Google has a plug-in for its Gmail service that detects attempts to send e-mail that one might later regret. Similar technology could be developed by the DoD to protect privacy, strip location information from photographs, or scan messages and postings for sensitive information.

Nevertheless, one of the fundamental problems with today's social networks is the lack of authenticated identity. When a service member receives a "friend" request from an old friend or

classmate, it can be difficult, if not impossible, to authenticate that request. But such authentication is important with today's social networks that provide more information to "friends" and "followers" than to outsiders.

One way around this problem would be for the DoD to provide an alternate social network site for DoD members and their families. Such a site could allow family members to communicate with service members and with each other in a more secure setting that is not available to the general public. Membership to the site could be controlled and restricted to only service members and those they invite to the site. More stringent privacy settings could be provided and enforced so that profiles and posts are not visible outside of directly connected relationships.

ABOUT THE AUTHORS

Capt Kenneth Phillips is a recent graduate of the Naval Postgraduate School in Monterey, California where his master's thesis explored correlating public DoD records with social network websites. He currently serves as the SATCOM Project Support Officer at the Marine Corps Tactical Systems Support Activity.

Capt Kenneth Phillips
MCTSSA, Box 555171
Camp Pendleton, CA 92055-5171
E-mail: kenneth.n.phillips@usmc.mil

LT Aaron Pickett is a U.S. Navy Information Warfare Officer currently assigned to Navy Information Operations Command (NIOC) Suitland. He graduated from LeTourneau University in 2002 with a BS in Computer Science and Engineering, and from the Naval Postgraduate School in 2010 with a MS in Computer Science. His past assignments include NIOC Hawaii and instructor duty at Naval Nuclear Power Training Command.

LT Aaron Pickett
NIOC Suitland
4251 Suitland Road
Washington, DC 20395-5720
E-mail: aaron.pickett@navy.mil

Simson L. Garfinkel is an Associate Professor at the Naval Postgraduate School in Monterey, California. His research interests include computer forensics, the emerging field of usability and security, personal information management, privacy, information policy and terrorism.

Simson L. Garfinkel
Naval Postgraduate School
Monterey, CA
E-mail: slgarfin@nps.edu

REFERENCES

1. Phil Ewing. The terror threat at sea. Navy Times Scoop Deck Blog, December 31 2009. <http://militarytimes.com/blogs/scoopdeck/2009/12/31/the-terror-threat-at-sea/> Accessed April 23, 2011.
2. Yaakov Katz. Facebook details cancel IDF raid. The Jerusalem Post, March 2010. <http://www.jpost.com/Home/Article.aspx?id=170156>
3. Geoff Ziezulewicz. ID theft surges among US troops in UK. Stars and Stripes, November 18 2008. <http://www.military.com/features/0,15240,179476,00.html>
4. Facebook statistics. Facebook Press Room, 2010. <http://www.facebook.com/press/info.php?statistics> Accessed April 23, 2011.
5. Kenneth N. Phillips. Correlating personal information between DoD411, LinkedIn, Facebook, and Myspace with uncommon names. Master's thesis, Naval Postgraduate School, 2010.
6. DoD Directive-Type Memorandum 09-026 responsible and effective use of Internet-based capabilities, February 2010. <http://www.defense.gov/NEWS/DTM%2009-026.pdf>.
7. James Dao. Military announces new social media policy. New York Times At War Blog, February 2010. <http://atwar.blogs.nytimes.com/2010/02/26/military-announces-new-social-media-policy>. Accessed April 23, 2011.
8. ALNAV (All Navy) 057/10 Internet-based capabilities guidance, August 2010. <http://www.public.navy.mil/bupers-npc/reference/messages/Documents/ALNAVS/ALN2010/ALN10057.txt>
9. The Media Line. There are things we'll never know. The Jerusalem Post, July 2010. <http://www.jpost.com/Israel/Article.aspx?id=180838> Accessed April 23, 2011.
10. Office of the Secretary of Defense. Policy Memo 13798-10, "Social Security Numbers (SSN) Exposed on Public Facing and Open Government Websites." November 23 2010.
11. Jim Giles. Data sifted from Facebook wiped after legal threats, March 2010. <http://www.newscientist.com/article/dn18721-data-sifted-from-facebook-wiped-after-legal-threats.html> Accessed April 23, 2011.
12. Ron Bowes. Return of the Facebook snatchers. Internet Blog, July 2010. <http://www.skullsecurity.org/blog/2010/return-of-the-facebook-snatchers>. Accessed April 23, 2011.
13. Shaun Waterman. Fictitious femme fatale fooled cybersecurity. The Washington Times, July 2010. <http://www.washingtontimes.com/news/2010/jul/18/fictitious-femme-fatale-fooled-cybersecurity> Accessed April 23, 2011.
14. Michael Cosgrove. US military and security fooled by Internet 'friends' hoax. Digital Journal, July 2010. <http://www.digitaljournal.com/article/295079>. Accessed April 23, 2011.
15. MARADMIN (Marine Administrative Message) 181/10 responsible and effective use of Internet-based capabilities, March 2010.
16. SAIS-GKM (Assistant Secretary of the Army, Information Systems – Governance, Acquisition & Chief Knowledge Office Memorandum) Memorandum, responsible use of Internet-based capabilities, 2010. <http://www.slideshare.net/DepartmentofDefense/army-official-social-media-policy>

NOTES

1. The DoD Operations Security (OPSEC) Program Manual 5205.02-M (November 3, 2008) describes a step-by-step approach for identifing and mitigating OPSEC risks, much of which relies on education, training and general awareness.
2. http://www.facebook.com/admiralmikemullen
3. http://socialmedia.defense.gov
4. http://www.doncio.navy.mil/ContentView.aspx?ID=1818
5. https://www.us.army.mil/suite/page/589183