WikiLeaks and the Matter of Private Manning

Hal Berghel,
University of Nevada, Las Vegas

The release of significant documents by WikiLeaks, the international online not-for-profit organization, has become front-page news that has significant implications for computing professionals.

What a time for WikiLeaks. This story has taken wing.

In 2010, WikiLeaks.org, the self-proclaimed not-for-profit online repository of anonymous leaks, posted some politically charged and embarrassing digital content dealing with the Afghanistan war (the "Afghan War Diary"), gunsight footage of an airstrike in Baghdad ("Collateral Murder"), and thousands of purportedly secret US State department diplomatic cables ("Cablegate"). In addition to attracting the ire of US government officials and politicians, these leaks embarrassed several foreign governments. All three of these leaks were allegedly the work of Bradley Manning, a socially awkward, somewhat unstable US Army private serving in Iraq.

We add to the mix Julian Assange, a nonconformist former computer hacker who refers to himself as the founder and editor in chief of WikiLeaks, and Adrian Lamo, a convicted computer hacker/snitch with both Asperger's syndrome and other alleged personal issues. The prevailing media perspective at this writing holds that the WikiLeaks EiC somehow got secret—and very embarrassing—documents from the Army private, and then had them posted on the WikiLeaks website.

In a weaker moment, the private then discussed his involvement in this derring-do with Lamo. The latter then shared the information with US government officials and a reporter for *Wired Magazine*. At that point the plot thickens, fingers point wildly (and, of course, outward), and seemingly everyone with even the slightest bit of egg-on-face takes a self-serving position that takes dead aim at the EiC and the private.

Beyond this, things begin to get murky.

KNOWN KNOWNS

The constituencies affected by the three leaks are slightly different but overlapping—there's plenty of embarrassment to go around. The Department of Defense and military were embarrassed by the Collateral Murder video because some of the victims were Reuters' war correspondents and children. Defense officials and the military were also embarrassed by the 75,000 documents (most of which were classified "secret") that were released as the Afghan War Diary, but for different reasons. These documents included intelligence intercepts, internal military incident reports, speculative assessments, and reports from informants, some of which referred to other informants by name, much to the chagrin and alarm of the US and sympathetic foreign governments.

But the holy grail of embarrassment was Cablegate: approximately 250,000 diplomatic cables between the US State Department and nearly 300 embassies, consulates, and diplomatic missions around the world. Of these cables, about one-half were unclassified, one-third were labeled "confidential," and approximately 15,000 were labeled "secret." WikiLeaks has released only a small fraction of the cables thus far; a larger

 Published by the IEEE Computer Society 0018-9162/12/$31.00 © 2012 IEEE

portion has been shared with major newspapers, including *The Guardian*, *The New York Times*, *Der Spiegel*, *El País*, and *Le Monde*. By the time of the Cablegate leaks, the battle lines were drawn, and the strongly opinionated among us began choosing sides and taking aim.

Cablegate and its predecessors produced a veritable feeding frenzy of accusations from Western politicians, most of which were directed toward Julian Assange. Mike Huckabee, a former US presidential aspirant, is said to have called for Assange's execution for treason (Assange, it should be noted, is not a US citizen). Australia's Prime Minister Julia Gillard called Assange a criminal and recommended revoking his Australian passport (which was nullified when Australia's Attorney General opined that Assange had broken no Australian law). US Vice President Joe Biden labeled Assange a "high-tech terrorist." Presidential contender Newt Gingrich recommended that Assange be treated as an "enemy combatant." Conversely, Republican presidential contender Ron Paul suggested that Private Manning might be a "political hero … a true patriot who reveals what is going on in government."

Meanwhile the homeless (and close to being stateless) Assange took refuge in the historic English country estate of a wealthy journalist, documentarian, and restauranteur. So 2012 begins.

KNOWN UNKNOWNS

The prevailing, but not singular, view of the leaks falls under the rubric of "stolen and leaked documents." On this account, the documents were government property that was downloaded from government servers and subsequently uploaded to WikiLeaks without permission: stolen, pure and simple. Free speech advocates tend to view these leaks as a natural byproduct of a free press in a democracy and are sympathetic to Manning and WikiLeaks. Bureaucrats and politicians tend to view the leaks as threatening and subversive and are hostile to Manning and WikiLeaks. The majority of observers seem to accept the stolen and leaked documents explanation.

However, to add complexity to the story, there is the "conspiracy" account, promulgated by Zbigniew Brzezinski, former National Security Advisor to President Carter: the leaked documents might be background noise that overshadows the more important and damaging "seeded" documents that were added to the mix. In Brzezinski's view, these WikiLeaks should not be taken at face value. According to him, it is quite possible, if not probable, that Assange and WikiLeaks were duped by "special intelligence interests" specifically to embarrass the US and weaken its relationship with friendly allies.

Rather than being the channel for a toxic data dump of secret material, Assange actually might be the useful idiot for foreign intelligence services: WikiLeaks might be an instrument of information warfare rather than the purveyor of blown whistles.

At this writing, it remains to be determined whether Assange, working under an assumed alias, actually encouraged Manning to provide the files to WikiLeaks. This is a critical determination for Assange, as an active role might lead to his prosecution under the US Espionage Act.

And yet, to some extent, the most interesting part of this story has so far gone largely unnoticed.

HOT LINKS

The complete list of countries with extradition treaties with the US is available at www.state.gov/documents/organization/71600.pdf.

For Zbigniew Brzezinski's views of the leaks, see www.pbs.org/newshour/bb/government_programs/july-dec10/weakileaks2_11-29.html.

Several threads of Wired Magazine's coverage of Bradley Manning's Article 32 hearing are linked to www.wired.com/threatlevel/2011/12/adrian-lamo-bradley-manning.

FIPS 199 can be found online at http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf. EO 13292 is online at www.archives.gov/isoo/policy-documents/eo-12958-amendment.html. The earlier EO 12958 is at www.archives.gov/isoo/policy-documents/eo-12958-amendment.html.

www.WikiLeaks.org and www.bradleymanning.org are relevant to this discussion.

THE COMPUTING AND IT DIMENSION

There's no shortage of drama in this tale. Enter US Senator Joe Lieberman and Amazon CEO Jeff Bezos. According to published reports, Lieberman or his staff asked Bezos or his staff to stop hosting WikiLeaks on Amazon Web Services—at the time the primary host of WikiLeaks content in North America. Mind you, this was after the three leaks had already gone viral. When I saw the media reports of this story, my first thought was, "What part of 'the toothpaste is out of the tube' don't they understand?" In any event, Amazon Web Services did pull WikiLeaks.org content from its server cluster.

Of course Amazon Web Services wasn't the sole hosting service for WikiLeaks. No one who knew how the Internet worked thought that it was. When Amazon pulled its content, it had no effect on content elsewhere. Nor did it seem to have any effect on the continued migration of the documents through cyberspace.

Similarly, when EveryDNS pulled the DNS entry for the WikiLeaks.org IP address record for North America (after an alleged 100 gigabit/second distributed denial-of-service attack directed against WikiLeaks.org was threatening its service to other subscribers), the DNS records for other WikiLeak hosts began to proliferate. As networkers worldwide watched this unfold, they saw it as nothing beyond the level of minor inconvenience to curious Internet surfers.

That government officials and their staffs acted as if they actually thought they could magically end the embarrassment by pulling the plug on a hosting service is symptomatic of our cyberdeficiencies. This entire episode will live on as a paradigm case of cyber silliness.

I'm confident that Bezos and his Amazon leadership team knew quite well that pulling the hosting service served no useful purpose. My hunch is that this was viewed as purely a business decision—they didn't need the distractions from congressional complainers and watchdogs, and they certainly wanted to avoid guilt by association with the controversial WikiLeaks.

Within a few hours after EveryDNS removed the authoritative DNS records for the WikiLeaks.org site hosted by Amazon Web Services, WikiLeaks defiantly announced on Twitter the creation of WikiLeaks.ch. That domain resolved to an IP address that is part of a small class-B network cluster, not in Switzerland but in Sweden, where, ironically, Julian Assange had an outstanding arrest warrant for alleged sex offenses. (You can't make this stuff up, folks!)

The Swedish server in turn redirected traffic to a French host, which assigned an IP address that was part of a 16-address server cluster located in France but registered in Melbourne, Australia. Of course, the WikiLeaks team was parallel processing all the while, so there were multiple threads operating simultaneously. If you're beginning to feel that getting hold of WikiLeaks content on the Internet is like trying to shovel smoke into a bucket, you're getting the big picture.

Meanwhile, back in Congress, US Senator Dianne Feinstein, chair of the Select Committee on Intelligence, and vice-chair Christopher Bond requested that Attorney General Eric Holder prosecute Julian Assange (to my knowledge, the justification was somewhat hazy). At about the same time, Swedish authorities issued an arrest warrant and sought to extradite Assange on the sex charge. Assange considered requesting asylum in Switzerland, but the Swiss authorities balked under US pressure, in part because Switzerland has an extradition treaty with the US.

Ecuador's Deputy Foreign Minister discussed the possibility of Assange taking residence there, but the country's president puts the kibosh on that idea for the same reason. Unfortunately, there aren't many asylum candidates among the dozen or so countries that don't have extradition treaties with the US.

Security clearances were never intended to be issued carte blanche.

But the computing and IT component is just a small part of this story. The part of the story that has been underreported so far has to do with the rest of the people involved—the many nameless who remain in the shadows, an ensemble of colorful actors cast against the background of a much larger group of powerful politicians and military brass who, by most accounts, aren't the sharpest knives in the drawer.

THE UNTOLD STORY

At this writing, Julian Assange is fighting extradition to Sweden, living in an English manor, and soliciting donations on the WikiLeaks site to help with his legal defense. Private Manning has been detained since May 2010 in military jails in Kuwait and Quantico, Virginia, under conditions that have drawn criticism from a variety of sympathizers, including Amnesty International. He is currently incarcerated at Fort Leavenworth, Kansas, awaiting trial facing a courts marshal under Article 32 of the Uniform Code of Military Justice.

Let's assume that Private Manning did in fact upload the documents to WikiLeaks by using his access to the Secret Internet Protocol Router Network (SIPRNet) as Adrian Lamo testified. In 2009, Manning would have been 21 or 22 years old. Unless the insignia chart has been revised significantly since I served, the military brass doesn't consider a private, most especially one barely beyond his teenage years, to be a bulwark of reliability and sound judgment.

The operative question is, "By what authority were Manning and his cohorts given access to sensitive, classified government documents?" I've asked this question of every senior military officer that I know, and have yet to find anyone who even claims to know the answer. In my day, a military security clearance wasn't a hunting permit for curiosity seekers.

One relevant data point is Donald Rumsfeld's desire to encourage information sharing between and within military agencies while he was Secretary of Defense under George W. Bush. It's likely that this created the climate that made it possible for low-level enlisted military personnel like Manning to access sensitive information that was either beyond the scope of his job or, under the most charitable interpretation, marginally related.

This is a good time for everyone to be reminded that security clearances are like college diplomas—they affirm that the individual has satisfied some minimal standards appropriate to the imprimatur. Neither attests to an individual's sagacity or capacity to contribute anything important to the world. They are best thought of as one filter among many.

Security clearances were never intended to be issued carte blanche. Standard operating procedures always circumscribe their use on a need-to-know basis. The fact that an individual has been deemed trustworthy by a vetting process is just the first step in a reasonable authorization process. Having the requisite

clearance should not entitle the holder to access all information classified at a level commensurate with the clearance. The second step determines whether the holder has a "need to know" based on his military occupational specialty code and rank. In this context, the "impact of disclosure" is always taken as a critical consideration in this determination.

At the time Manning is alleged to have leaked this information, protocols for determining confidentiality levels, data integrity levels, and availability level had already become law in the E-Government Act of 2002. Title III of this act, The Federal Information Security Management Act (FISMA), mandated that the National Institute of Standards and Technology create such standards, which became Federal Information Processing Standard (FIPS) 199 in February 2004—five years before the WikiLeaks disclosures. President Bush's Executive Order (EO) 13292 specifically included military plans, weapons systems, operations, foreign government information, intelligence activities (including special activities), intelligence sources or methods, and foreign relations.

If Manning's case goes to trial, his attorneys will have a field day with the issue of why the US government didn't follow its own information security guidelines when it allowed him to rummage through secret information.

There's another issue involved as well—admittedly a social issue rather than a legal one. Why would any reasonable authority put a disputatious Army private in front of a computer terminal that can access controversial, contentious, embarrassing, or libelous information with international implications?

There's a familiar staple in case law called the attractive nuisance doctrine that holds that a landowner who presents curiosities to those who aren't fully capable of understanding the risks involved may be held liable for damages. There's a perfectly reasonable sense in which the secret documents were an attractive nuisance to someone like Private Manning.

While I agree that someone should take responsibility for the WikiLeaks fiasco, it's someone much farther up in the organization chart than Manning. Here's a news flash for our military: kids and young adults sometimes do dumb things. Don't trust them with the keys to the kingdom.

DID THIS WIKILEAKS STORY TEACH US ANYTHING?

There are so many characters, subplots, and scene changes at this point that it will take years to really appreciate this security drama.

But what, if anything, have we learned?

- It's easy to steal information—especially when it's electronic. Hadn't anyone in the military chain of command heard of Napster? They should have seen this one coming.
- Innocuous "little people"' can create real problems for governments: Daniel Ellsberg, David Koresh, Osama bin Laden—no big shake-up here.
- It's easier to steal something than to detect that it's being stolen? That one was easy.
- It's hard to keep secrets. Ben Franklin said it all: "Two people can keep a secret if one of them is dead."
- Be careful whom you trust. Consider Judas, Guy Fawkes, Benedict Arnold, Gavrilo Princip, Kim Philby, Aldrich Ames, Robert Hanssen, ….
- Be careful what information you retain and share. Think Enron, Arthur Anderson, and the shredding party that ensued in the midst of a recent US Justice Department investigation. The cat has been out of this bag since the invention of the bag.
- Perhaps access to internationally sensitive diplomatic information should be reserved to policymakers and diplomats who actually have a need to know this information. There's a news flash.
- Information security policy has to make sense and be enforced. Maybe WikiLeaks and Private Manning should be considered change agents?

In plain terms, any reasonable, security-aware person either already knew or should have known everything this lesson has taught us. This is really a confirming instance of policymakers and government officials who were asleep at the wheel. If there's anyone who deserved to sit in a jail cell over this, it's someone further up in the food chain than an Army private.

Unfortunately, our military leadership doesn't seem to be very quick on the uptake. As this column goes to press, the Army has placed an entire 100-member company from the 4th Stryker Brigade at Joint Base Lewis-McChord, Washington, under lockdown because of the apparent theft of expensive military equipment—another example of closing the corral after the cattle have escaped. Is it possible that the real problem behind this theft was attractive temptation without adequate oversight—in the same spirit as WikiLeaks and the matter of Private Manning? C

Acknowledgment: Many thanks to Jim Earl for his insights.

***Hal Berghel**, Out of Band column editor, is a professor of computer science at the University of Nevada, Las Vegas, where he is the director of the Identity Theft and Financial Fraud Research and Operations Center (itffroc.org). Contact him at hlb@berghel.net.*