The Most Powerful of Adversaries: NSA Programs and Techniques Provide Lessons in Data Privacy and Managing Enterprise Collaboration

intralinks.com

Protecting your data in the age of the NSA and PRISM

Soon after Edward Snowden released a cache of top-secret documents detailing the far-ranging data collection activities of the U.S. National Security Agency (NSA) in the summer of 2013, the Federal Bureau of Investigation (FBI) approached the secure email provider Lavabit with a demand to turn over the encryption keys to its communications. Their target was, allegedly, none other than Snowden himself, who had been posting his @lavabit.com address and inviting human rights activists around the world to contact him. Ladar Levison, the owner of Lavabit, refused the Bureau's request. Levison was concerned that turning over his private encryption key would allow the government to decrypt not only Snowden's communications but also those of all of Lavabit's nearly 400,000 customers, many of whom are activists and had chosen Lavabit for its security. Facing a contempt of court charge, Levison eventually turned over the encryption key. However, he simultaneously shut down his service, thus preventing the authorities from gaining access to his customers' communications.

Few companies have the ability to act like Lavabit and shut down in the face of such a demand. Lavabit was a very small organization with no shareholders and few employees to answer to for their actions. As organizations become more decentralized and their employees more mobile, they naturally need to share more information, raising concerns about how to adequately protect that information from NSA-like government actors. Most organizations have no plan in place for reacting to a government request for data. How should companies prepare to deal with this issue? What steps can be taken to protect data? We'll explore these questions in this report, place the NSA threat in perspective, and suggest steps most companies can take to preserve data privacy.

The NSA in Perspective

The NSA is not unique in its use of the Internet for intelligence gathering. Most other major industrialized nations contribute to or have some surveillance footprint on the Internet. Some of these nations even engage in economic espionage and sabotage efforts, a serious concern for businesses worried about intellectual property and their global competitiveness.[1] However, because of the NSA's aggressiveness and scope, organizations should consider to what degree they need to protect against such an agency and other only slightly less capable state actors. The NSA can be thwarted, as their frustration with breaking[2] the Tor network[3] demonstrates. Though, as is often the case, hardening one security weakness inevitably leads to the adversary exploiting that weakness.

Risk assessments by corporations and individuals are critical in this context. To perform a risk assessment, one has to understand the capabilities of those who are trying to infiltrate their information systems, and place these risks in context. Many organizations face security and data privacy threats from many sources – malicious hackers, insiders, or weak security systems and process. In reality, the most dangerous threat for most organizations is unintended mistakes and errors by employees – losing a laptop, or sending a confidential file to the wrong people. An analysis of recently revealed NSA strategy and techniques can help provide perspective as well as give insights into the methodologies of other state actors. Many of the NSA's techniques involve accessing metadata, so we'll explore that distinction first. Next, we'll identity the major NSA programs revealed as of today, and some suggested countermeasures.

Metadata Versus Data

The FBI wasn't actually after the content of Snowden's emails. After all, the former NSA contractor knew the NSA's capabilities and was using messages encrypted with the widely used Pretty Good Privacy (PGP) encryption software to communicate with people. The Bureau initially requested that Lavabit install a pen register (a term borrowed from the old telephony days, a pen register is a device used to capture all calls made to and from a particular phone). In this case, the FBI wanted to know with whom Snowden was communicating.

At the time, many backers of government surveillance emphasized the distinction between communications data and metadata (data about data), insisting the majority of information collected, such as the Verizon phone records, were metadata, and thus didn't warrant the negative reaction. Even President Obama chimed in. This implied that because the NSA wasn't listening in directly on phone conversations, the information they gathered wasn't as sensitive as the actual communications.

However, this isn't the case. For decades the NSA has been surveilling foreign countries that encrypted their communications data or monitoring electronic signals that weren't sending communications data, i.e. "electronic intelligence." This can provide valuable intelligence such as identity information, location information, and proof of connections between entities. If, for instance, every time a call is made from a specific number in Columbia to a phone in Mexico and there is a drug-related killing in Mexico near the receiving phone, then that would suggest someone in Columbia is ordering the killings. Or, another example, provided by the NSA itself, suggests that when a phone signal only comes on to place a call, then goes off, that user is probably using a disposable phone and trying to elude capture, thus warranting closer scrutiny.

Similarly, the leaked NSA documents suggest the agency tracks phones used outside the United States that then appear in the country where the owner of record hasn't come through a known border crossing. This indicates the bearer has crossed the border illegally. If the phone's owner only communicated with his mother about recipes, the metadata (when and where the phone connected to the telephone network) could be much more valuable than the conversations.

Major Covert Surveillance Programs of the NSA

Founded in the 1950s, the NSA was once referred to as No Such Agency because of continued government denial of its existence. Steeped in secrecy, the NSA has a long history in "signal intelligence," gathering communications information worldwide for national security purposes. Banned by law from domestic surveillance, it has been increasingly using domestic sources for its foreign intelligence-gathering mission. They use domestic sources because a large amount of the world's telecommunication traffic traverses the United States, as well as the widespread use of U.S.-based service providers.

Since a large amount of the world's telecommunications traffic travels through the U.S., this puts the U.S. and, in particular, the NSA, in a unique position to monitor much of the world's communications. While other countries certainly do this within their own borders, they have limited capabilities to surveil foreigners and may be totally reliant on information shared through treaties or mutual cooperation with foreign agencies. The U.S. government uses a number of techniques to access data. Some, such as the court order presented to Lavabit, remain within the scope of legal authority. Others, such as the tapping of transatlantic fiber-optic cables and hacking of Internet routers, are of less clear legal justification. As the following chart demonstrates, organizations can work around or outwit NSA programs.

Major NSA Surveillance Programs

Program	Description	Countermeasures
PRISM	Originally thought to be a program that allowed NSA analysts direct access to the servers of major Internet companies, PRISM is software that facilitates the transfer of data about targeted non-U.S. persons. While still working within the legal framework of the Foreign Intelligence Surveillance Act (FISA), PRISM is a technical system for providing access to data requested by the government under FISA. Responding to FISA requests is mandatory but supporting PRISM is voluntary.	While still complying with their legal obligations, Twitter avoided the public backlash faced by other major providers who supported PRISM. Twitter simply refused to implement the technology to ease the burden of surveilling their customers.
Tailored Access Operations (TAO)	TAO is an NSA group of hackers that uses computer network exploits to grab control of network routers. Once the routers are controlled, TAO personnel can inject exploits or software to take advantage of vulnerability.	If the NSA wants to target an organization, there probably isn't much you can do about it. However, companies must take appropriate security measures: keep systems patched and updated, be aware of newly released threats and vulnerabilities, etc. If the NSA can do it today, someone else can attack you tomorrow.
Muscular	This program tapped the internal fiber-optic cables between servers at Google and those inside Yahoo. This traffic, which didn't pass through the public Internet, was thought to be safe and wasn't encrypted.	After learning about the program, major Internet services have moved to encrypt all traffic, even between their internal operations.
XKeyscore	Dubbed the "Google" of the NSA, XKeyscore is one of a host of programs that allow agents to search broad swaths of Internet communications in order to identify targets. XKeyscore pulls in data from a myriad of sources, including: phone and email communications, website visits, Facebook chats and private messages, searched terms, and much more.	Not much information exists about the source of the XKeyscore data. Since it's primarily Internet-related, using end-to-end encryption and not leaking information in the URL string are important first steps.

Major NSA Surveillance Programs

Program	Description	Countermeasures
Dishfire	Dishfire pulls in hundreds of millions of SMS (text) messages a day from mobile phone users. Using an analytic tool called Prefer, the NSA is able to discern such information as geocoordinates, SIM card changes, travel itineraries, financial transactions, border crossings, contact chaining, and some passwords.	Many people are lulled into using SMS as a private communication medium, sending an email with an encrypted file and then sending the password to the file via SMS. Always avoid using unsecure communications mediums for sensitive data. Be aware of the metadata your communications channels might be leaking.
Bullrun	Bullrun is an NSA program to retain encrypted Internet traffic with the presumption that it can be decrypted at a later date. Alternatively, Bullrun refers to the intentional weakening of encryption standards.	Make sure your services use things such as forward secrecy and avoid using uncompromised but weak encryption standards such as RC4.

Advanced Persistent Threat

With billions of dollars at its disposal, the NSA's cutting edge information-gathering exploits should come as no surprise. In a December 2013 blog post, Brad Smith, Microsoft's general counsel and executive vice president for legal and corporate affairs, labeled the government's actions as an "advanced persistent threat" because they undermined confidence in online security and the privacy of technology services.[4] The label, typically used for sophisticated cyber criminals, was meant to convey the idea that instead of being a partner with industry in trying to secure the world's communications, the U.S. government was now an adversary. By allowing known vulnerabilities to go unpatched or introducing vulnerabilities for their own purposes, the NSA was weakening the very structure of the Internet.

Key Takeaways

Microsoft's assessment of the situation has implications for all businesses. Regardless of intent, the U.S. government's use of its superior capabilities speaks volumes. Any techniques they utilize today may find their way into the hands of less-noble agents tomorrow, be they government actors or cyber-criminals. The lesson is clear. If you can secure against the most powerful of adversaries, then the others will not be of much concern.

- **Make a plan for how your organization would react to a data request.** Very few organizations have a prepared plan for how they would react to a government request for data or metadata. Assembling a legal, technical, and senior management team to prepare a strategy and approach will ensure you can react quickly and appropriately.
- **Know your customers, partners, and suppliers and understand their information privacy needs.** Often data requests will be for third-party information. Not every customer has a state actor actively pursuing them and not every customer who does is a terrorist or criminal. Human rights activists, political dissidents, lawyers representing foreign governments, and legitimate business people might have a need to hide information from governments around the world.
- **Be metadata aware.** Metadata is often an Achilles' heel. Organizations are often so focused on protecting data that they don't realize how vulnerable they are to metadata analysis. The breach at Target, when hackers accessed the financial information of many of the famous retailer's customers, could have been facilitated by their leaving metadata bread crumbs about their network on their public-facing documentation.[5]
- **Consider all attack vectors.** Encryption is an extremely powerful tool for securing data, but it's only as good as an understanding of all the attack vectors. Passive attacks rely either on holding encrypted data until some future date when one can brute force decrypt it or on obtaining the decryption key through alternative measures. Periphery attacks rely on security vulnerabilities at endpoints to thwart security of data in transit. Side channel attacks go to weakness in specific implementations of encryption techniques. Having personnel who are knowledgeable about these attacks review your specific system is imperative.

- **Anticipate legal requirements in system design.** Levison of Lavabit, and his customers, learned the hard way. Had his technology supported the legal requirements of tapping only Snowden's communications without jeopardizing his other customers, he could have complied with the court order in full. Alternatively, if his technology didn't allow him access to any of the data (including the metadata), he could not have been compelled to provide what he didn't have. His choice in design, however, led him to the problematic situation in which he ultimately found himself.
- **Understand where to house your data.** The ability of governments to legally – or covertly – access files and metadata often hinges on specific legal frameworks in different jurisdictions. For more details, read our paper *Where to HouseYour Data*.
- **Put the threat of government data access in perspective.** Organizations face numerous threats to the security and privacy of their data, as well as the data of their customers and partners that is in their trust. Recent data from Facebook, LinkedIn, Microsoft, and others shows that US FISA requests were rare, and affected only a small fraction of one percent of customer accounts. The threat from hackers or from other malicious actors may be a much more prevalent and pressing concern than the threat posed by NSA-like government agencies.

[1] *Australia spied on communications between Indonesia and attorneys in the United States representing them in trade talks with the U.S. http://www.nytimes.com/2014/02/16/us/eavesdropping-ensnared-american-law-firm.html?_r=3*

[2] *Tor users were attacked through local exploits on their computers rather than the Tor network. See documents relating to NSA program, code name EgotisticalGiraffe at http://www.theguardian.com/world/interactive/2013/oct/04/egotistical-giraffe-nsa-tor-document.*

[3] *"Tor (previously an acronym for The Onion Router) is free software for enabling online anonymity and censorship resistance. Tor directs Internet traffic through a free, worldwide, volunteer network consisting of more than five thousand relays to conceal a user's location or usage from anyone conducting network surveillance or traffic analysis." http://en.wikipedia.org/wiki/Tor_(anonymity_network)*

[4] *http://blogs.technet.com/b/microsoft_blog/archive/2013/12/04/protecting-customer-data-from-government-snooping.aspx*

[5] *http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/*

intralinks.com

Intralinks

(NYSE: IL): The leading, global technology provider of inter-enterprise content management and collaboration solutions designed to enable the exchange, management control of documents and content between organizations securely and compliantly when working through the firewall. Thousands of companies and more than two million professionals use Intralinks for everything from ad hoc collaborations to complex, multi-business partnerships in financial services, life sciences, manufacturing, technology, and a wide range of other industries worldwide.