Realtime publishers

The Evolving Threat Landscape and New Best Practices for SSL

sponsored by

Dan Sullivan

Chapter 3: Preparing for Tomorrow: Future Considerations and Risks 31
Application of SSL Technologies and Responses to Security Threats 32
Organized Crime and Cybersecurity 32
State-Sponsored Attackers 33
Politically Motivated Attacks 34
Insider Attacks 35
Emerging Best Practices 37
Industry Standards Related to SSL 37
Implementation Standards: Elliptic Curve Cryptography 37
The Need for End to End SSL Encryption 38
Security In Depth and Internal Network Traffic 39
Risk of Insider Abuse 39
Concerns about SSL and Performance 39
Undermining Trust in the Internet 40
Snowden Revelations 40
Heartbleed Vulnerability 41
Breaches of Security and Privacy 41
Restoring Trust 43
Summary 44

Copyright Statement

© 2015 Realtime Publishers. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtime Publishers (the "Materials") and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtime Publishers its web site sponsors. In no event shall Realtime Publishers or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtime Publishers and the Realtime Publishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtime Publishers, please contact us via e-mail at info@realtimepublishers.com.

Chapter 3: Preparing for Tomorrow: Future Considerations and Risks

If there were any doubts about the sophistication of today's cyberthreats, the 2014 attacks on Sony Corporation put them to rest. On November 22, 2014, attackers hacked the Sony network and left at least some employees with compromised computers displaying skulls on their screens along with threats to expose information stolen from the company. The scope of the attack forced employees to work with pen, paper, and fax machines while others dealt with the repercussions of the release of embarrassing emails. Avivah Litan of Gartner said "This attack went to the heart and core of Sony's business and succeeded," and "We haven't seen any attack like this in the annals of U.S. breach history." According to Joseph Demarest, assistant director of the U.S. FBI's cyberdivision "the malware that was used would have slipped or probably gotten past 90% of Net defenses that are out there today in private industry and [likely] challenged even state government." To summarize: Sony was the subject of an advanced, persistent attack using exploits that would have compromised the majority of security access controls.

The future of cybercrime and security risks is not looking favorable for those trying to do business with and on the Internet. Take for example, the comments of Bryan Sartin, Director of the Risk Team, Verizon Enterprise Solutions, quoted in the Wall Street Journal:

> Cyberattacks are all around us. It's not just about stealing data; it can be about extortion, data destruction, combinations of demonstrated denial of service [DDoS] attacks, and data theft.

And Eric Friedberg, Executive Chairman of Stroz Friedberg speculates in the same Wall Street Journal article:

> On the state-sponsored side, I think 2014 has shown that cyberattacks can be an effective tool for state-sponsored agents and intelligence programs. I don't see that abating in the least. A bigger theme for 2015 and beyond is that we're getting to the point where hacktivists and state-sponsored groups with extreme agendas are committing attacks really on that border of cyber warfare.

The coverage around the Sony attack and projects from security experts may rightly leave many in business wondering whether their networks are sufficiently protected and, of particular interest here, can comprehensive use of SSL help avoid some of the worst impacts of a Sony-type breach? Clearly, there is no panacea and the threat landscape appears to becoming more, not less, dangerous. In spite of these dismal projections, there are practices that can be put in place that help business to function while providing protections for their systems and data.

No single tool can prevent sophisticated attacks, and SSL is no exception. It is not "the" solution to cybercrime, but it is part of solutions that mitigate the risk to businesses and other organizations. There are many factors to consider going forward as you adapt and improve your security controls:

- Application of SSL technologies continue to improve and change in response to security threats
- Best practices are emerging
- Restoration of trust in the Internet
- Capture of best security practices and sound management principles in policies
- Benefits of advances in cryptography

Let's start with the variety of actors threatening business operations on the Internet.

Application of SSL Technologies and Responses to Security Threats

The set of actors threatening business and government operations has evolved over the decades. What started as online vandalism and minor disruptions, such as the Morris Worm in 1988, has evolved to levels of significant threats to even major businesses and national governments. The major actors in cyberthreats are:

- Organized crime
- State-sponsored attacks
- Politically motivated attacks (hacktivists)
- Insiders within victim organizations

Organized Crime and Cybersecurity

Organized cybercrime is an evolving concept. It typically includes for-profit organizations using cyberattacks for financial gain or using information systems for some part of traditional crimes. Assessing the state of organized crime and its role in cybercrime is difficult, at least for those outside governments with access to wide ranging information on the subject.

Some researchers, such as Jonathan Lusthaus in How Organised is Organised Cybercrime? (Paywall), argues that we need to be careful how we classify "organized" cybercrime. Lusthaus argues that a group using a hierarchical control structure to organize cyberattacks for profit is not the functional equivalent of large, organized online mafias. However, others such as the European Union law enforcement agency EuroPol notes that cybercrime now includes well-defined and differentiated services available as "Crime as a Service" (Source "Organised Crime Groups Exploiting Hidden Internet in Online Criminal Service Industry").

One of the challenges in discussing cybercrime is distinguishing between different types of cybercrimes (see Figure 3.1). Many cases of interest to law enforcement involve the use of information technology to facilitate crimes that are not essentially computer-based, such as the illegal sale of weapons and drugs. For the purposes of the discussion here, the focus is on preventing or at least mitigating crimes against business' information assets and infrastructure.

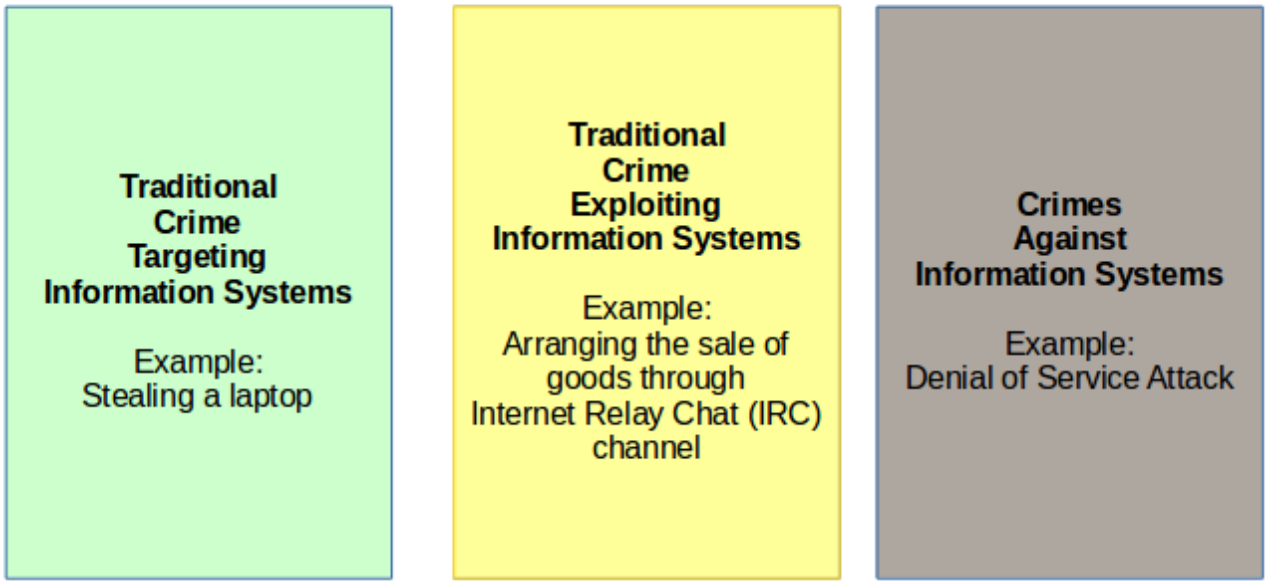

Figure 3.1: The term cybercrime encompasses three distinct modes of using information systems to commit criminal acts.

SSL technologies are particularly important for protecting information assets. Identity and payment card data is routinely sold on dark networks (not accessible through search engines). Businesses may not have the capabilities to disrupt or dismantle such sites but they can deny thieves information worth stealing by encrypting private and sensitive data. As noted earlier, encrypted data will appear like random strings of characters. Unless attackers are also able to steal the private key that was used to encrypt the stolen data, it will be useless to them.

State-Sponsored Attackers

Cyberattackers may be after more than personal information and credit card data. State-sponsored attacks add another dimension to the security space that businesses must address. Writing in *CSO* magazine, Maria Korolov points out significant differences in the methods, means, and motivations of state sponsors of cybercrime from organized crime:

- Targeting different types of data, such as intellectual property
- Disrupting services
- Focusing on targets for extended periods of time if necessary
- Developing and maintaining well-funded and well-organized organizations

We do not often see details of state-sponsored attacks in the press, but that has been changing recently. In May 2014, the U.S. Department of Justice charged five Chinese military hackers for "for computer hacking, economic espionage, and other offenses directed at six American victims in the U.S. nuclear power, metals, and solar products industries. " According to the indictment, the attackers tried to "maintain unauthorized access to their computers and to steal information from those entities that would be useful to their competitors in China, including state-owned enterprises (SOEs)."

Roderic Broadherst and colleagues writing in the *International Journal of Cyber Criminology* note the breadth of state-sponsored cyberactivities:

> Today, we find that numerous governments (or their proxies) are using Internet technologies to commit crime. Allegations that Russia has executed or encouraged distributed denial of service attacks, and that Chinese authorities are engaged in widespread economic and industrial espionage, have been matched by the disclosures of Edward Snowden that the United States Government has engaged in massive programs of cyber-surveillance. One might also note the offensive cyber operations against Iranian nuclear enrichment facilities (Sanger, 2012). Such activities may not be defined as criminal under the laws of the state that undertakes them, but are usually regarded as crimes by the state that is on the receiving end.

Another problem with state-sponsored cyberattacks is that they can introduce new techniques and methods that may not have been in general use. For example, the Stuxnet worm included a programmable logic controller rootkit for disrupting the operations on centrifuges. Although Stuxnet targeted specific devices (variable frequency drives from two particular vendors and operated between about 800Hz and 1200Hz), a functional rootkit for attacking industrial devices controlled by programmable logic controllers was now available.

The advent of malware that attacks non-information systems changes the threat landscape for many businesses and institutions. Although it was theoretically possible to attack industrial equipment, power grids, and other civil infrastructure, we now have demonstrated proof of it as well as produced a working example for others to learn from and build on.

Politically Motivated Attacks

Another source of cyberattacks is politically motivated actors, or hacktivists. Hacktivism started as a term describing the use of online resources for social change but has expanded to include malicious activities. The latter are the subject of this discussion.

Some of the best-known hacktivists are Anonymous and LuzSec. Operations by Anonymous include a 2008 denial of service attack against the Church of Scientology, "Operation Tunisia" in support of the Arab Spring that helped protesters avoid government surveillance, and "Operation Ferguson," which offered victims of police violence retaliation against the municipal services of the offending locality. LuzSec has claimed responsibility for a number of attacks, including the 2012 attack on Sony Pictures with a SQL injection attack and a denial of service attak on the CIA.gov public Web site.

Hactivist operations have occurred in support of social movements, such as the Arab Spring, and against organizations, particularly government agencies and companies that are opposed by group members. In such attacks, the goal may not be to steal data or intellectual property but to disrupt and embarrass the victims.

Insider Attacks

As the name implies, attacks by insiders are crimes committed by employees, contractors, or others who have some legitimate access to a business' information systems.

A 2012 study on fraud in the financial sector by the Software Engineering Institute found important features of insider attacks within financial institutions:

- The "low as slow" approach allowed attackers to steal more and avoid detection longer than did other methods
- Few inside attackers hold technical positions or have advanced technical skills
- Fraud by managers cost more and continued longer than fraud by non-mangers
- Few incidents involve collusion between insiders; 69% of insider attacks where collusion was involved entailed collusion with outsiders

According to a 2013 survey by the Software Engineering Institute, 53% of respondents found insider attacks more damaging than outsider attacks. The most common types of attacks included:

- Exposure of private or sensitive data (unintentional)
- Intellectual property theft
- Unauthorized use of or access to information resources
- Theft of proprietary information

The damage caused by insiders can be substantial. The BBC reported a UK-based supermarket chain suffered a breach due to an insider. Personal details of 100,000 employees was stolen and posted online. As large as that is, it appears minor next to the Sony 2015 attack, purportedly in response to a political comedy movie called "The Interview." The U.S. government has accused North Korea of involvement with the attack but non-government security experts suspect insiders may be responsible. Of course, it is possible for a state-sponsored attack to use insiders, so it may not be an either-or situation. Without sufficient details, it is impossible to know with reasonable certainty how the attack was executed (see Figure 3.2).

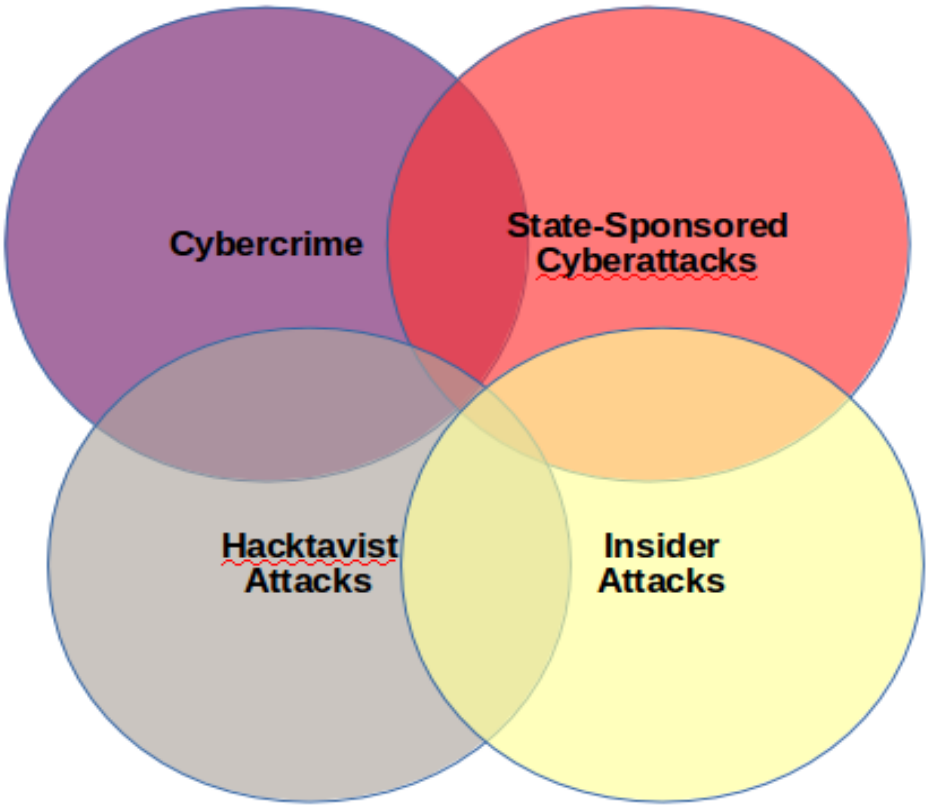

Figure 3.2: The forms of cyberthreats are not mutually exclusive and can overlap in ways opportunistic to multiple attackers.

The discussion around the 2015 Sony attack highlights the fact that categories of cyberthreats, such as organized crime, state-sponsored attacks, activism, and insider threats are not mutually exclusive. Any attack on a business or organization may involve one or more of these groups. A state sponsor may use the cover of a hacktivist group to mask its efforts to steal intellectual property for state-owned enterprises. Nationalist cybercriminals may collaborate with their governments to execute cyberattacks against perceived enemies of the country.

If we broadly categorize attacks into those designed to steal data and those with other intents (e.g., disruption of services and public embarrassment), we can focus on the former and the role of SSL technologies for mitigating the risk of data loss.

Emerging Best Practices

The IT community is constantly analyzing security controls, cryptography methods, and administration practices. The byproduct of this work is best practices that we can implement today to help improve the overall security posture of our systems and data. It is important to understand that best practices are not static. What was a best practice in the past (e.g., using the Digital Encryption Standard [DES] algorithm for encryption) may no longer be the case; however, some principles are still relevant despite rapid and significant changes in technology (e.g., applying the principle of least privilege).

With regards to SSL technologies, three practices are worth understanding and adopting:

- Adoption of industry standards related to SSL
- Implementing always-on SSL
- Employing practices that help restore trust in the Internet

Each of these contributes to advancing the ability of businesses to conduct operations on the Internet. Some, like using industry standards, have immediate benefits, while practices to restore trust in the Internet should be considered long-term projects.

Industry Standards Related to SSL

Industry standards are important for both the implementation of SSL and the application of SSL from a business perspective.

Implementation Standards: Elliptic Curve Cryptography

Encryption protects data by mapping it from an easily understood form, commonly called "clear text," to an apparently random sequence of characters, called "cypher text." Encryption works from a practical perspective when it is difficult to derive the clear text from a cypher text without decryption key. As computing power increases, it becomes more feasible to map from cypher text to clear text.

There are two ways to counter increasing ability to crack encryption with greater computing power: increase key length or change algorithms. Increasing key length is the easier of the two options to implement, but this approach eventually succumbs to either the increasing computing capacity or the discovery of an inherent weakness in the algorithm. The DES, for example, was a standard algorithm in the past, but extending key lengths and applying DES multiple times, for example using Triple DES (3DES), no longer provides sufficient protection. The Advanced Encryption Standard (AES) and other strong encryption algorithms have largely replaced DES.

The AES algorithm is considered strong because it is unlikely that someone has the computing resources to crack its encryption unless there is a theoretical weakness in the algorithm that could be exploited. AES encryption exploits the fact that it is difficult to factor large integers into prime numbers. This technique works well but has the disadvantage of requiring longer keys than other algorithms for the same level of protection.

Elliptic Curve Cryptography (ECC) algorithms use a different kind of math problem, involving logarithms and elliptic curves. ECC algorithms using a 256-bit key can provide equivalent protection to the RSA algorithm using a 3,072-bit key (see Figure 3.3).

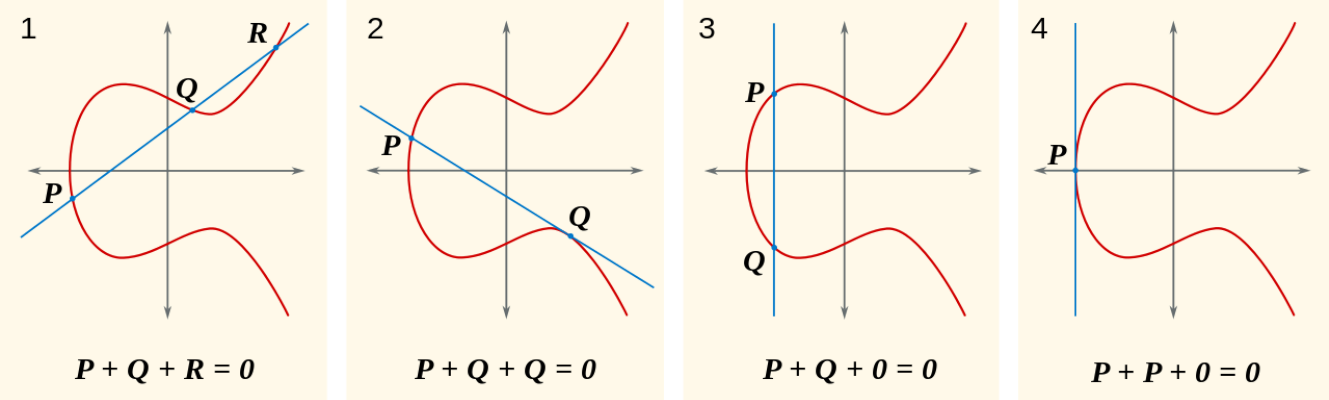

Figure 3.3: Solving problems involving elliptic curves is computationally intractable (Source: By SuperManu [GFDL (http://www.gnu.org/copyleft/fdl.html) or CC BY-SA 3.0 (http://creativecommons.org/licenses/by-sa/3.0)], via Wikimedia Commons).

A number of standards have been defined related to elliptic curve cryptography, including:

- BrainPool
- NSA Suite B
- ANSSI FRP256VI
- SafeCurves

As with any cryptographic system, decisions about parameters of the implementation, such as selected curves and constants, can impact the overall effectiveness of the encryption. As researchers study ECC implementations, they may find some are more secure than others, either because of parameters selected or because of weaknesses in coding that render encrypted data vulnerable to attack. Businesses depend on security researchers and industry practitioners to implement secure algorithms and advise users on the soundness of particular standards and implementation.

The Need for End to End SSL Encryption

Another suggested practice is to use SSL for all data transfers, both within and outside your organization's network. This approach may sound like an over use of SSL, but there are two factors to keep in mind: the need for security in depth and the risk of insider attacks.

Security In Depth and Internal Network Traffic

With the practice of security in depth, we assume that some of our security controls will fail. Vulnerabilities will be exploited. Users with legitimate access will perform unauthorized operations. Systems administrators will make mistakes. By employing multiple mechanisms to protect systems and data, we improve the chances of protecting in spite of failures with some security measures. For example, if an attacker were able to compromise perimeter defenses and gain access to internal network traffic, the attacker could collect and analyze network packets. If the payload of those packets were not encrypted, the attacker would have access to that data. Using encryption even for internal network traffic helps reduce the risk of compromising the confidentiality of your internal communications and data transfers.

Risk of Insider Abuse

By definition, insiders have privileged access to data and applications. They have devices that have access to internal networks, servers, and other devices. Encrypting data provides an additional layer of protection for confidential and private data. For example, if data were encrypted on a file server and an insider gained access to sensitive files, the attacker would find nothing of value to steal or exploit.

Concerns about SSL and Performance

There may be some concern that SSL encryption will adversely affect application performance, but SSL does not place any significant demand on system resources. Perhaps some of the best evidence for this statement comes from Google's switch to encrypting email by default. According to a blog post describing the Google experience:

> In January this year (2010), Gmail switched to using HTTPS for everything by default. Previously, it had been introduced as an option, but now all of our users use HTTPS to secure their email between their browsers and Google, all the time. In order to do this we had to deploy no additional machines and no special hardware. On our production frontend machines, SSL/TLS accounts for less than 1% of the CPU load, less than 10KB of memory per connection and less than 2% of network overhead. Many people believe that SSL takes a lot of CPU time and we hope the above numbers (public for the first time) will help to dispel that.

The substantial benefits of SSL outweigh the marginal costs in terms of additional CPU demand and memory overhead.

Undermining Trust in the Internet

A long-term goal for many in the IT profession should be to help restore trust in the Internet. Businesses, health care delivery, education, government, and many other functions of modern society are leveraging the advantages of ubiquitous, low-cost communication and information sharing. During the past few years, we have witnessed a number of incidents that have undermined trust in the Internet:

- Snowden revelations
- Heartbleed vulnerability
- Breaches of security and privacy

These three examples highlight three distinct challenges to protecting the confidentiality and integrity of data and services on the Internet.

Snowden Revelations

In June 2013, Edward Snowden, a former contractor to the U.S. National Security Agency (NSA), began a series of leaks disclosing classified documents about government surveillance by the United States and allied nations. Some of the surveillance was conducted with the cooperation of telecommunication companies. It is not clear how many documents were released but official estimates by government officials are as high as 1.7 million documents.

A number of surveillance programs and operations were disclosed:

- Prism, which provided access to email accounts
- Tempora, a British surveillance program
- Boundless Informant, a database of phone call metadata
- Xkeyscore, a tool for analyzing Internet data collected by the NSA

The consequences of Snowden's revelations are far reaching. Some herald the disclosures as important events from a public policy perspective. Daniel Ellsberg, author of the Pentagon Papers, said "Edward Snowden has done more for our Constitution in terms of the Fourth and First Amendments than anyone I know." James R. Clapper, Director of National Intelligence, argues that "We've been clear that these leaks have been unnecessarily and extremely damaging to the United States and the intelligence community's national security efforts."

In addition to the civil rights and national security issues, there are indirect consequences on trust in the Internet and the possibility of maintaining privacy in the age of mass surveillance programs. The Wired article entitled "How the NSA Almost Killed the Internet" tries to describe the extent of the damage to trust in the Internet. But concerns about mass surveillance are just one of the factors undermining trust in the Internet.

Heartbleed Vulnerability

The Heartbleed vulnerability is a weakness in some versions of the widely used OpenSSL library. The vulnerability allows attackers to read up to 64K of memory at a time of systems running vulnerable versions of the OpenSSL library. Attackers could access memory and gain access to private keys used for encryption, username and passwords, and other data stored in memory. By one estimate, about half a million trusted Web sites were vulnerable to Heartbleed.

Heartbleed was a serious vulnerability. Security expert Bruce Schneier, who is not known for hyperbole, noted "On a scale of 1 to 10, this is an 11." This vulnerability was widespread and is now widely known. However, as bad as it was, it did not mean "the Internet is broken," as some proclaimed. It does, however, highlight the need for additional best practices. Solange Desc suggests several steps in her article "Dr. Strangebug, or How I Learned to Stop Worrying and Accept Heartbleed":

- Using a password vault to store passwords
- Using strong passwords or passphrases
- Not reusing passwords across Websites
- Using two-factor authentication when available

Heartbleed educated the public about facts IT professionals have long known: software has bugs and vulnerabilities, even widely used security tools.

Breaches of Security and Privacy

Users of the Internet are beginning to rethink the concept of privacy. A fairly steady stream of new stories about data breaches understandably could leave some people feeling that any of their data online is subject to compromise (see Figure 3.4). Even a major financial institution such as JPMorgan Chase can be breached; an attack in 2014 disclosed data about 76 million households and seven million small businesses, according to the New York Times.

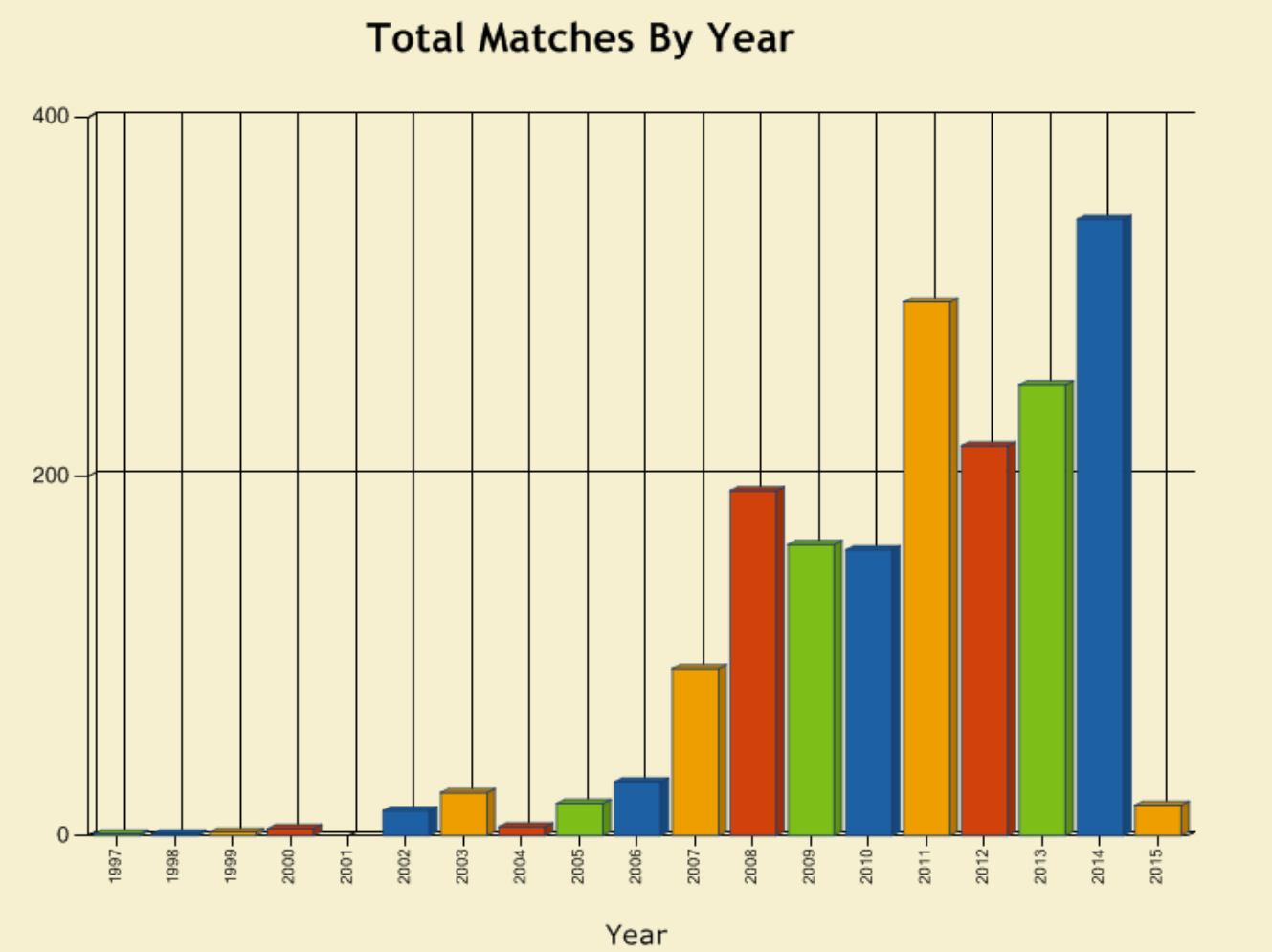

Figure 3.4: There has been an increasing trend in data disclosure and leak vulnerabilities according to data collected by the National Vulnerability Database (Image Source: https://web.nvd.nist.gov/view/vuln/statistics-results?adv_search=true&cves=on&cwe_id=CWE-200).

Our concepts of privacy extend beyond financial information to include details of personal lives, healthcare, education, and interactions with businesses, governments, and other institutions. A 2014 study by Accenture highlights current attitudes about privacy and the Internet:

- 87% believe adequate safeguards are not in place to protect their privacy
- 64% are concerned about Websites tracking their behavior
- 56% re-enter credit card data rather than store it online in an effort to protect their privacy
- 70% do not believe businesses are sufficiently transparent about how they use data collected about them
- 40% believe only about 10% of their personal data is private

The findings indicate that many believe they are being observed and to some degree their behavior analyzed online in ways they are not fully aware of—a direct confrontation to traditional views of privacy. Users do not feel in control of their information nor do they feel that they understand what is being done with their information. Perhaps most importantly for businesses trying to serve such customers is that a vast majority do not feel that adequate protections are in place.

Restoring Trust

Businesses cannot protect the entire Internet, but they can help secure their parts of the network. This begins by understanding the state of software security. Even best designed architectures and well-written applications may have vulnerabilities. Add to this that we function in an environment that includes attackers able and willing to launch advanced persistent attacks against businesses and governments. The range of malicious actors now includes organized cybercrime, hacktivists, nation states, and insiders. In spite of all these threats, there are measures we can take to address these risks:

- Assuming data will be leaked, and therefore we should be
- Encrypting data at rest as well as data in motion, and this requires
- Establishing a well-protected encryption infrastructure, including
- Managing encryption keys,
- Monitoring lifetimes on SSL certificates and replacing them prior to expiration, and
- Patching security systems and software.

These measures can help reduce some of the risks IT operations face, but by themselves, they might not promote a sense of trust. Many of these operations are done behind the scenes, at least from the perspective of a customer. Another practice to consider is sharing information about your security and privacy practices. These can include:

- Publicly sharing the breadth of security practices you employ described in terms easily understood by someone not familiar with IT and security terminology
- Publishing data use and privacy policies in summarized, easy to understand form
- Demonstrate the use of encryption and high levels of authentication with Extended Validation (EV) certificates

Also capture best security practices and sound management principles in security policies. Policies should be reviewed regularly and revised as needed. You should stay abreast of best practices and evolving threats. These will influence your policies and procedures as you develop responses to emerging threats. When there are data leaks, within your own organization or others, try to learn from them. For internal breaches, you may have access to forensic data that can help identify the methods used by attackers and lead you to vulnerabilities that can be corrected.

Cryptography continues to advance. Additional methods, such as perfect forward secrecy, which mitigates the risk of data loss even if parts of a message are compromised, can provide additional levels of protection to your data. Few organizations will have cryptographic experts on staff, but you can get the benefit of their knowledge by maintaining relationships with security experts and vendors with knowledge of advances in cryptography.

It is important to monitor the global threat landscape. Attackers are constantly refining attacks and developing new methods to compromise systems. A number of security vendors now maintain global intelligence networks to monitor the Internet for malicious content and activity. This kind of intelligence gathering can act as an early warning system to help understand the kinds of threats that may be emerging.

Finally, assume security controls will fail. SSL is both a first and last line of defense. Data in motion is protected even when it is outside a controlled network when it is encrypted. As a last line of defense, encrypted data at rest is protected in persistent storage even if network and server security controls are compromised.

Summary

Business face constant threats to their data, infrastructure, and applications. Attackers are increasingly varied in their tactics, motivation, and goals. Average users of the Internet are losing trust in organizations they depend on to protect their privacy. None of these factors helps you leverage the benefits of the Internet, in fact, the present potential detriments to fully exploiting the advantages of the Internet. No single business, government, or other organization can solve the problem we all face. There are measures individuals and business can take to help restore trust in the Internet. A first step is to improve data protections by using SSL encryption for all data in motion.