http://dx.doi.org/10.18243/eon/2016.9.11.4

Internet Security Concerns in Scholarly Publishing

By Tony Alves (ORCiD 0000-0001-7054-1732)
Director of Product Management
Aries Systems Corporation
talves@ariessys.com

Security should be a constant concern when working on the Internet. Every organization has mission-critical systems and processes that rely on the Internet in some way, such as membership services, e-commerce, inventory control, data exchange, email, etc. Keeping all of these systems safe from hackers and keeping them up and running without disruption is an essential part of any organization's IT operations. Publishers are no different, and in fact, many publishers rely on online systems for just about all aspects of their business, from content acquisition, to content preparation, to quality control processes, to distribution and e-commerce. Some of these systems are housed within a publisher's data center, and others are housed by vendors and by software-as-a-service providers. As the Director of Product Management at Aries Systems, I recognize that security and reliability are top priorities for our clients, and all software development projects consider security and reliability as a matter of course. This article is a very general overview of some of the issues that Editorial Offices should keep in mind when working online and when working with vendors who provide services over the Internet.

There are three general online threats faced by organizations with operations dependent on the Internet. A common but not widely known threat is a "denial-of-service" (DoS) attack, which is an attempt to slow down or take down a computer or network by overwhelming it with requests. It is somewhat analogous to people trying to crowd onto an elevator without first letting people off. A "distributed denial-of-service" (DDoS) is when an attack comes from many, often thousands, sometimes millions, of unique IP addresses. For example, the October 21, 2016 DDoS attack on the Internet services company Dyn included tens of millions of IP addresses flooding Dyn's servers, which made websites including Twitter, Reddit, Amazon, Netflix, and Spotify unreachable.[1] Protection from this sort of attack usually includes mechanisms for analyzing and identifying data packets before they enter the network, and then filtering those packets so that only legitimate traffic gets through. In many jurisdictions, DoS attacks are highly illegal, and in the United States and Europe perpetrators can be arrested and imprisoned.

A second and more well-known threat is the hacker. Hackers are generally trying to steal data, often valuable user data such as names, emails, Social Security numbers (in the United States), passwords, and credit card numbers, though sometimes hackers are just trying to cause mischief by disrupting workflow, deleting data, or revealing embarrassing information. Hackers access data by gaining unauthorized entry into computer networks and by watching unprotected data traverse the Internet. Some recent high-profile hacks include the 2013 theft of credit and debit card numbers from 40 million Target accounts, the theft of username and password data from 500 million Yahoo users (which happened in 2014, but wasn't revealed until September 2016), and the email hacks of Sony in 2015 by the North Korean government and the Democratic National Committee in 2016 by the Russian government.

[1] York K. Dyn statement on 10/21/2016 DDoS attack. http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack. Accessed November 13, 2016.

A strong and effective firewall is used to keep hackers from penetrating a network, and is also used to battle DoS attacks. A highly effective method of securing a network is to have a "default-deny" policy. This means that the firewall administrator identifies the allowed network services, and all other network services are denied both entry and exit to and from the network. A default-deny policy is used at Aries Systems, and though this adds significant overhead to network administration, it is far more secure than the "default-allow" approach where the administrator lists network services that are *not* allowed, and everything else is accepted.

Hackers also use viruses and malware to wreak havoc or steal data. One of the largest malware attacks took place in July of 2015, when a security hole in Adobe's Flash product, used heavily in advertising, allowed hackers to hijack computers and render them unusable until a ransom was paid. Virus detection software is an absolute necessity for any computer connected to the Internet, and virus detection software should always be kept up to date. Good antivirus software from reputable vendors try to keep up with new threats, and most will have automated ways to keep the software installed on your computer current. Antivirus software should be deployed in various places, such as on network servers, email servers, and on people's desktops. At Aries Systems, all manuscript files are scanned for viruses upon receipt on the Web server and any infected files are quarantined and reported. In addition, the submitting author is notified of the violation so that he/she can cleanse the virus at the source. To protect data as it moves across the Internet many websites and services use "Secure Sockets Layer" (SSL) protocol when transmitting data. When a user sees "https," this indicates that SSL is active and the user can be assured that best practices are being employed to protect their communications.

A third and often overlooked threat is the disgruntled staff member, especially someone who has access to computer systems, network administration, and proprietary data. This is perhaps the most difficult threat to combat, since it is really a threat from within the organization, and the tools for prevention will often impact people's productivity and even be perceived as a slight or an insult to some individuals. Although a disgruntled staff person can do a lot of damage to an organization's credibility, outright destruction and theft is less common since, unlike DoS attacks and hacking, the perpetrator is usually a known person.

Some best practices that can cut down on risk include facility access control and intrusion monitoring. Strict authorization protocols, such as limiting staff access, logging all access as it occurs, and routinely reviewing those logs, are basic strategies. There are of course high-tech ways to limit access, such as passcodes, keycards, and biometric recognition (such as eye or fingerprint scans). It is highly recommended that a "dual-factor" strategy be employed, for example, at Aries Systems both a passcode and a biometric scan is required to enter any data center, and this access is automatically logged. It may seem obvious, but all third parties and contractors should be escorted and shadowed whenever they enter data centers and places where sensitive data is stored. Also, limiting access to passwords and security settings, forcing regular changes to those codes, and limiting the ability for people to act on others' behalf are additional best-practice precautions.

Scholarly publishing is a global endeavor, requiring 24/7 access to services and data. People are working around the world, which means that people are working around the clock. With tight deadlines, with point-of-care services, with just-in-time inventory fulfillment, with print-on-demand, etc., it is no longer acceptable to have access limited to just business hours. All of this means that "continuity of service" isn't a convenience; it is a must-have. Some organizations, including Aries Systems, handle this by maintaining mirrored systems, often housed in geographically separate locations. Real-time mirroring or "hot mirrors," which means that that all data centers are operating as exact replicas of each other in real time, is an ideal way to ensure continual access to data and services. When planning this sort of dual hosting facility, it is good to consider having multiple standby power sources, such as multiple generators using different fuels, and multiple Internet service providers so that Internet connectivity is not dependent on just one or two carriers. Data backup of all systems is also an integral part of a continuity-of-service plan. A rigorous backup policy includes regular backups (continual, hourly, daily) to some sort of storage medium, like magnetic tape, hard disk, or optical storage. Sending the backup media off-site, or using a remote backup service over the Internet, keeps the data safe in case of data center destruction. An important consideration is to be sure you have the ability to actually extract the data in a usable format if necessary. Aries Systems sends backup media, which contains the system's software and customers' data, to a commercial storage facility, and maintains the capability to completely restore the system in a remote location if necessary.

Secure computer systems and data integrity are part of guaranteeing continuity of service, especially if the organization handles sensitive data like credit card information or patient data. Organizations should regularly test their security protocols, both on a systems level and on a physical-plant level. The most common network security test is the "penetration test," which is an attack on a computer network designed to gain access to the system, thus revealing security weaknesses. Although Aries Systems does not handle credit card data, there is plenty of valuable data housed on Aries' servers. Therefore, penetration tests are regularly undertaken, and the results are reviewed. This then allows the IT team to design strategies for reinforcing any identified weak points. If a vendor is handling financial information, it is important that the vendor conforms to the "Payment Card Industry Data Security Standard" (PCI DSS) also referred to as "PCI compliance". Details on this can be found at www.pcisecuritystandards.org.

As mentioned, security is not just about protecting computer networks, it also includes securing physical equipment and limiting access to data centers. It is also important to maintain written protocols, to review those protocols on a regular basis, and to find ways that those protocols and processes might be circumvented, either intentionally or by mistake.

Security is a broad topic with many nuances and varied approaches for mitigating risk. The preceding is just a cursory look at some of the considerations made by organizations that maintain computer networks and services that house data and provide essential services to customers. Publishers are particularly reliant on software systems and the Internet to conduct regular business. What's more, publishers are also handling huge amounts of data, which is often being sent or streamed across the Internet, and publishers are engaged in e-commerce at every level of the publishing process. This means that security and system reliability are absolutely essential to publishers. There are many dangers, traps, and outright attacks out there in the wilds of the Internet, and it is important that security be the number one priority of the publisher and the publisher's vendors and partners.

Ira Salkin Scholarship: Accepting Submissions 1 January 2017

The essay topic for 2017 is "Expectations of the Editorial Office to police publication ethics—how it has changed during the past 10 years."

The submission deadline for entries is 31 May 2017.

The author of the winning essay will receive:

- Complimentary registration at a meeting of his/her choice
- $1,500 USD toward travel/accommodation
- Essay published in *EON*

More information and submission instructions can be found online. Questions? Contact scholarships@ismte.org.