Realtime publishers

Preventing Data Loss through Unsecure Browsers

The Essentials Series

Understanding Data Loss and the Threat of Unsecure Browsers

sponsored by

QUARRI™

Dan Sullivan

Introduction to Realtime Publishers

by Don Jones, Series Editor

For several years now, Realtime has produced dozens and dozens of high-quality books that just happen to be delivered in electronic format—at no cost to you, the reader. We've made this unique publishing model work through the generous support and cooperation of our sponsors, who agree to bear each book's production expenses for the benefit of our readers.

Although we've always offered our publications to you for free, don't think for a moment that quality is anything less than our top priority. My job is to make sure that our books are as good as—and in most cases better than—any printed book that would cost you $40 or more. Our electronic publishing model offers several advantages over printed books: You receive chapters literally as fast as our authors produce them (hence the "realtime" aspect of our model), and we can update chapters to reflect the latest changes in technology.

I want to point out that our books are by no means paid advertisements or white papers. We're an independent publishing company, and an important aspect of my job is to make sure that our authors are free to voice their expertise and opinions without reservation or restriction. We maintain complete editorial control of our publications, and I'm proud that we've produced so many quality books over the past years.

I want to extend an invitation to visit us at http://nexus.realtimepublishers.com, especially if you've received this publication from a friend or colleague. We have a wide variety of additional books on a range of topics, and you're sure to find something that's of interest to you—and it won't cost you a thing. We hope you'll continue to come to Realtime for your educational needs far into the future.

Until then, enjoy.

Don Jones

Copyright Statement

© 2011 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.

Understanding Data Loss and the Threat of Unsecure Browsers

Advances in information technology have reduced the cost of doing business, formed opportunities to create new products, and reduced barriers to interacting with customers. These advances have come with a downside, though. Businesses face a virtually constant risk of data loss, in large part because of the way information flows in distributed systems. In the past, information might have flowed from a mainframe to a terminal hardwired to the mainframe. Anyone who wanted access to information needed both physical access to a terminal and logical access to data on the centralized repository. Today's information infrastructure is much less centralized, and as a result, the flow of data is much less centralized.

Information is easily transferred from reasonably secure corporate servers and networks to client devices that may harbor key loggers, video frame grabbers, and other malware. One of the advantages of contemporary application design is that it is possible to share information with large numbers of users at a relatively low marginal cost. However, this sharing ability brings with it potential threats. Authorized users can maliciously or unintentionally steal or leak confidential or private information. Both your systems and the people that use them can become conduits for the loss of private and confidential data.

Preventing data loss requires a multi-pronged strategy. Users must be made aware of information security policies and procedures. Servers should be secured by removing unnecessary applications, closing unused network ports, and keeping the operating system (OS) patched. Data that is transmitted beyond the trusted corporate network should be encrypted. Unfortunately, these data loss prevention measures are not enough. In fact, you could invest more in securing application servers and network infrastructures and still not address a significant risk for data loss: the user browser.

The user browser is typically a weak link in what might otherwise be a strong chain of security. Fortunately, technologies are available to provide on-demand, session-based browser security. This three part series outlines the threats of unsecure browsers to data loss and describes methods for protecting Web applications from client-side data loss due to malware or malicious user activity.

This first article in the series examines ways in which data loss occurs and countermeasures for reducing the risk of data loss. The second article describes techniques for preventing data leaks from Web applications. The final article examines the challenge of preventing data leaks from malicious and unintentional user activities.

Challenges to Protecting Confidentiality and Privacy

Data must be accessible for legitimate business functions. This means data about customer accounts, patient records, banking transactions, and other sensitive information will be stored, transmitted, and analyzed in different ways and at different times in the course of normal business operations. Protecting something is much easier if it is contained in a limited space accessible to only a few trusted employees.

Imagine a thief who desperately wants to rob a bank. One option is to break in; bypass multiple locks, alarms, and vaults; and steal cash and valuables from a central vault. The plan is difficult and there is high probability of being detected and caught, if not in the act then shortly thereafter. Another option is to wait for customers to leave the bank and pick pocket them one at a time. This method is less complex than breaking into a central vault and less likely to lead to arrest—although the victim will eventually realize money is missing, there will be no obvious indicators about when or where it happened. Similar strategies can be applied to stealing corporate data: attack the well-secured central infrastructure or wait until the valuables leave the secure area to steal them. Often data moves beyond the boundaries of secured corporate networks through distributed systems and Web applications in particular.

Web Applications: An Increasingly Common Platform for Data Access

Web applications are popular platforms for new application development. Leveraging commonly deployed communication protocols as well as server and client software, Web applications can allow access to information servers from virtually anywhere with Internet access.

Many Web applications are used for internal purposes within a business. Back-office functions, such as finance, inventory, and logistics, are important to the day-to-day operations of a business. The primary users are likely employees or business partners with closely linked operations. In many ways, the data flowing through these applications have the best protection. The data only moves between the business' servers, on the business' network, or to the business' client devices (or those of a trusted business partner). Client devices in these environments may be subject to well-defined and enforced policies and procedures, but the browsers that run on these devices may still be vulnerable to tampering and potentially data loss.

> **Cross Reference**
>
> Common security threats to browsers are discussed in more detail later.

Web applications do not always reside within secure corporate networks. The advent of cloud computing introduced the concept of platforms as a service and software as a service. Sometimes the most cost-effective way to deploy a Web application is by hosting it with a cloud provider. Doing so adds another dimension of complexity and security risks with regard to potential data loss. Whether a Web application is hosted internally or by a cloud provider, there are several types of security measures that can help to mitigate the risk of data loss, including security measures for servers, data in transit, and data on client devices.

Securing Web Applications: Start with Servers

Sensitive information is stored and controlled by application and database servers, so it is reasonable to start there with mitigating the risk of data loss. Well-established methods include:

- Securing servers
- Applying authentication and authorization controls
- Employing application firewalls
- Performing vulnerability scanning

Securing, or hardening, a server is a process of reducing the capabilities of a server to just those needed to perform business functions. This process requires removing unnecessary software, such as compilers that might be used to compile code that has been tampered with; shutting down processes that are not needed, especially vulnerable applications such as ftp servers; and enabling logging and monitoring services to trigger alerts in the event of unexpected activities on the server.

Authentication is used to ensure users are who they claim to be. Authorization controls are used to enforce limits on what an authenticated user can do. These two controls work to prevent unauthorized access to data by conventional means, such as by copying a file from a directory or using an application to look up information in a database.

Application firewalls are gatekeepers that protect an application from malicious input from anyone trying to compromise the system, such as injection attacks, buffer overruns, and stack manipulations. For example, in an injection attack an attacker may try to send a malformed command to an application in what is known as an injection attack. For example, a database application may prompt a user for a username and password. A poorly designed application interface might be susceptible to SQL injection attacks that cause the application to return large amounts of data to the attacker. An application firewall, like network firewalls, can block disallowed types of communications and help reduce the threat of injection attacks and other forms of unwanted interactions with a Web application.

Another method for securing servers is vulnerability scanning. These specialized applications interact with applications, middleware, and OSs to detect known vulnerabilities in the systems. Vulnerability scanners can be valuable tools for application and systems administrators because these scanners point out the kinds of flaws that attackers may try to exploit. Problems can be corrected by applying patches, updating application firewall rules, or redesigning part of an application to reduce the impact of the vulnerability.

Securing Web Applications: Data in Transit

Private or confidential data that is transmitted across an untrusted network, such as the Internet, should be encrypted. Modern strong encryption algorithms, such as AES, when used with sufficiently-long encryption keys can provide sufficient protection for most business requirements. In theory, any encryption could be broken by brute force with enough time and computing resources. Therefore, from a pragmatic perspective, you want to encrypt your data well enough that the cost of decrypting a message without the key outweighs the value of the information. It is analogous to storing your valuables in a vault. As long as the time and expense of breaking into the vault exceeds the value of the items in the vault, you can be reasonably confident no one would invest the effort to break in to the vault.

Like the bank vault analogy discussed earlier, attackers may decide to wait until the valuables have left the vault before making their move. In this case, attackers may wait until the data has been decrypted on the client before stealing the data.

Securing Web Applications: Data on Client Devices

Client devices—such as desktop computers, laptops, and smartphones—can and should be secured as much as possible. Best practices include:

- Running local anti-malware and local firewalls
- Teaching users to avoid Web sites that may potentially host malicious applications
- Using secure practices with regards to browsing, such as clearing the browser cache and navigation history at the end of a session

The problem with such practices is that even in well-managed corporate environments, these practices can break down. Anti-malware might be out of date, firewalls might be misconfigured, legitimate Web sites may be compromised and host malicious software, and users might forget to clear sensitive information or may intentionally save passwords in a browser or save data on a local disk.

Protecting confidential and private information is more difficult today with the widespread use of Web applications. These systems are composed of a number of component types, each with its own security requirements and vulnerabilities. Many of the risks of data loss with servers and network infrastructure can be mitigated through sound IT security practices. Until recently, it has been difficult, if not essentially impossible, to adequately protect sensitive information on client devices that were not under the direct control of IT departments.

Security Vulnerabilities in Browsers

There is no single class of threats with Web browsers; there are many ways browsers can be exploited for data loss:

- Malicious software on the client device, such as keyloggers and video frame grabbers, compromises the browser
- A malicious insider who uses the browser to access a Web application to steal intellectual property
- Careless activity by users, such as leaving sensitive information in a browser cache on a shared workstation

There have long been limits to how much you can do to protect information in a browser. Web application administrators have limited knowledge about the security state of a client device. This is especially true of devices used by customers, clients, patients, or others outside the management control of the business. In addition, many of the protocols still used in Web applications are inherently unsecure. A user-agent header in an HTTP message can be forged to make it appear that it came from a legitimate user's browser when in fact it originated with an attacker.

A security model that depends on securing devices is inherently limited. Well-secured servers and corporate networks can transmit encrypted data across the Internet. Once the data reaches the client device and is decrypted, you have to depend on the security of the client to protect that information. Hoping clients are secure is a poor strategy for protecting sensitive information.

Securing Information, Not Just Devices

As you increasingly depend on Web applications as well as on data that moves in and out of trusted networks to untrusted devices, it becomes more important to secure information and not just devices. To do so, you need to pursue a three-point approach.

First, you should understand the data access life cycle:

- Where does data reside?
- Who has access to it when the data is at rest?
- How is it transmitted?
- Is the encryption appropriate for protecting the information transmitted?
- Perhaps most importantly, where does it go?
- How long does it stay where it goes?
- Who has access to it when it goes to these places?

The last two questions are especially problematic when you are talking about client devices that are not under management control of the business.

Second, you need to eliminate vulnerable points in the information flow. Security best practices for mitigating risks to servers, networks, and other infrastructure play an important role here. Traditional measures are limited when reducing vulnerabilities in Web browsers, so a third tactic is needed.

That third tactic is to deploy session-based security controls in the browsers prior to launching a Web application. Returning to the bank robber and pickpocket analogy, this third tactic is equivalent to clearing the street for bank customers and blocking access to them from anyone else who might be in the area.

Sensitive information can be protected from internal servers to external browsers. The articles that follow will discuss how to do just that.