Realtime publishers

Preventing Data Loss through Unsecure Browsers

The Essentials Series

Preventing Data Leaks from Malicious and Unintentional User Activities

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

Preventing Data Leaks from Malicious and Unintentional User Activities

The term data leak is something of a euphemism. Comparing data loss to the kinds of leaks that occur with plumbing captures the idea of a potentially slow but persistent loss, but it misses the potential role of human actions. The focus in this third and final article in this series focuses on the role of malicious and unintentional user activities in data loss and its prevention.

Risk of Loss of Enterprise Information by User Activities

Companies and other organizations can lose data because authorized users intentionally copy or capture data with the intent of using it in ways they are not authorized to do so. These organizations can also lose data because of mistakes, oversights, and other unintentional acts that leave information vulnerable to theft or tampering. The two types of user-related data loss are so different, they warrant separate discussions.

Data Loss from Malicious User Activities

Web application users are granted access to data because they need that access to perform their jobs. Ideally, your authorization schemes are designed to grant all access that is needed to perform a task but not more than that. Even when minimal access rights are granted, you can see there are still many cases where you have to trust employees or business partners to not misuse the data that they can access. Consider examples of confidential or sensitive information that must be available to a wide range of employees:

- In a bank, tellers, branch managers, customer service representatives, and fraud detection specialists may all require the ability to read detailed customer financial information.
- In a health care situation, receptionists, nurses, doctors , pharmacists, and insurance processing staff will require varying levels of details about a patient, including data that is regulated as protected healthcare information.
- In a law firm, lawyers, clerks, and paralegals may need to share confidential client information such as trade secrets, human resources case information, and litigation material.

This list is not meant to imply that any group of employees is untrustworthy; it is designed to show the breadth of opportunity available to employees who are motivated to commit information theft. Many current security controls still provide the opportunity for a crime when the motivation is there.

Potential for Information Theft

Stealing information from an employer is not a new story. What is a more contemporary phenomenon is stealing intangible assets. As more and more company value is based on such assets, it is not surprising that thieves would turn their attention to them. Prime targets include:

- Trade secrets
- Confidential negotiation documents
- Customer lists
- Marketing and sales strategy documents
- Personal, health, or financial information about well-known, public figures
- Personally identifying information for use in identity theft

A disgruntled salesperson leaving one company to work for a competitor might decide to impress his new employer by bringing detailed information about potential new clients. This may not be difficult at all. While the employee is traveling for business, he uses a computer in a hotel business center to access a company Web application. He runs a report listing customers and sales activity in his region. The employee knows that if he runs the print command in the application, the application will record that action in the audit log. Instead, he simply uses a series of screen shots that he pastes to a file and emails it using his personal email. The data is effectively stolen without an electronic trace because the Web application could not control or even monitor activities on the unmanaged client device. Web applications can limit what data a user sees but not how that data is used. Information theft is not the only threat that a disgruntled employee poses.

Potential for Information Sabotage

Not all disgruntled employees want to steal from their employers. Some just might want revenge for a perceived injustice they suffered. In that case, information sabotage is a risk. Building on the previous examples, consider the types of data at risk:

- In a bank, a disgruntled employee may not tamper with account balances because those actions would be readily detected. Unstructured data, such as notes about a client account may be changed with malicious intent.
- In a healthcare situation, a vindictive employee might tamper with data in the record of a patient who was unusually troublesome to the employee.
- In a law firm, a misguided new employee might try to change or delete information in a case file that is detrimental to her client.

Both information theft and information sabotage can occur when Web applications do not sufficiently control user actions on the client browser. Another type of data loss risk stems from human error.

Unintentional Threats to Data Loss

We all make mistakes. Sometimes those mistakes can result in a loss of private or confidential data. Web applications are complex, and average users understandably don't know the details of their application's implementation. For example:

- A user may not realize that data is written to a local device in the form of cookies, and that applications should only be used on trusted networks.
- The antivirus software on a client device may not be up to date (even up-to-date antivirus software can miss malware). As a result, the device has become infected with malware capable of copying files, capturing keystrokes, and stealing data in other ways.
- A user may download a sensitive file on a shared device with the intention of deleting it after printing but forgets and leaves the file.

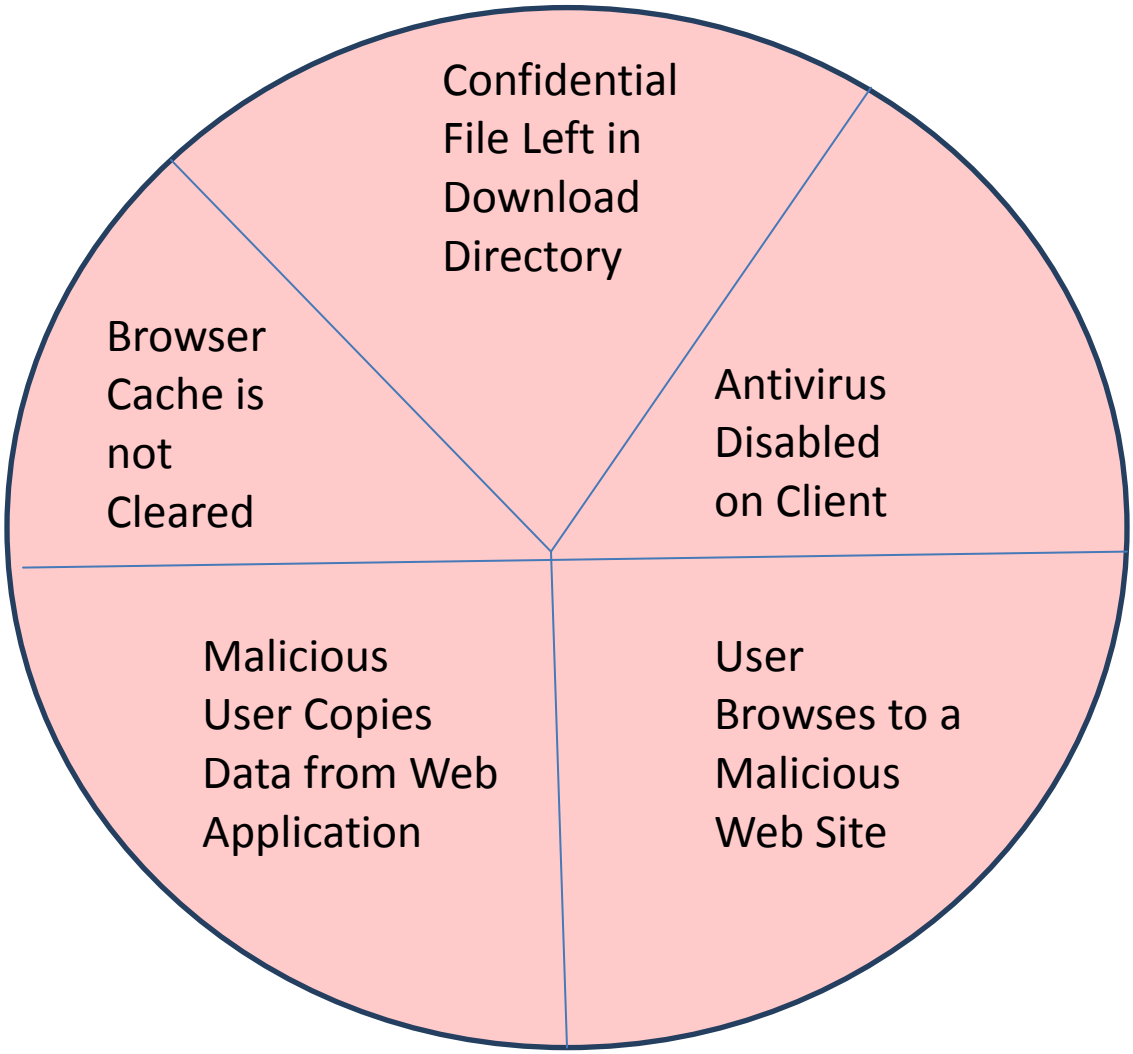

Figure 1:. Web browsers are subject to a variety of data loss threats.

Even situations that many IT professionals would recognize as potential data leaks, an average user may not. Consider a CFO traveling offsite for a corporate meeting. As soon as she lands, she realizes she has run down her laptop battery. On her way out of the airport, she stops in at an airline lounge and uses a computer the airline provides for its members. She logs into her corporate email account and opens spreadsheets with the latest financial reports. This may seem like reasonable behavior to most users, but there are significant risks:

- The spreadsheet data may be left behind in clear text in a temporary file
- The CFO could accidently save the file locally
- The CFO could forget to log out of her Webmail session
- Malware in the browser could be recording the session, collecting the spreadsheet content, zipping the content, and sending it to a collection server

As you can see from these scenarios, there is no shortage of ways data loss or information tampering can occur. Both intentional and unintentional user actions pose a risk to protecting the confidentiality and integrity of sensitive information.

Mitigating the Risk of Data Loss from User Activities

Businesses are not at the mercy of employees, business partners, and publicly shared devices around the globe. There are ways to mitigate the threats associated with user actions:

- Controlling browser capabilities
- Blocking potentially threatening Web sites
- Securing browsers on demand

All of these mitigating strategies can be implemented using on-demand browser-based security controls.

Control Browser Capabilities

An earlier example illustrated how a disgruntled or malicious employee could avoid Web application monitoring and control by using a client function such as the print screen feature. When accessing sensitive data, Web application users should be prevented from copying, pasting, printing, or saving such sensitive data to local files. By default, browsers do not do so. Web applications can be designed to download a session-based security mechanism to client devices before starting the Web application client. It is through these on-demand controls that features can be blocked while the Web application is running. Of course, when the session ends, the on-demand security controls are removed, and client functionality is restored.

In addition to blocking operations related to copying sensitive data, it is important to log activities in a browser running a Web application. If the history of computer security has taught us anything, it is that it is difficult to anticipate all the ways a determined attacker can compromise an application. Logging events may not immediately prevent a malicious activity but could prove crucial to identifying such an event and containing the damage as soon as possible.

Block Access to Potentially Threatening Web Sites

Another control that can be implemented with on-demand browser-based security controls is blocking access to threatening sites. In the past, you could be reasonably confident that avoiding illegal music download sites, pirate sharing sites, and other questionable sites was sufficient to avoid Web-based malware. Those days are gone. Now even legitimate sites can be hacked, resulting in the sites hosting malicious code without the knowledge of Web administrators at those sites.

It is so difficult to know whether a Web site may be compromised (for example, if it is suffering from cross-site scripting attacks) that it is reasonable to enforce a "no browsing" policy while Web applications are open and working with sensitive information. This setup can be implemented by blocking access to all domains other than the one hosting the Web application and perhaps other known and trusted Web sites, such as those run by subsidiaries or business partners.

Provide Browser Security On-Demand

Hoping client devices are secure is not a reasonable strategy. In fact, a more conservative assessment is more reasonable: Assume they are insecure. With that assumption, you need to deploy on-demand browser security controls that can control user actions and block access to potentially threatening Web sites.

You might trust most of your users, but even the best-intentioned employees can make mistakes or do things that undermine the confidentiality of sensitive information. On-demand security is essential to mitigating the risks associated with both malicious and unintentional acts.

Summary

The Web browser continues to be a weak point in Web application security. Malicious users can take advantages of Web applications to access to a wide array of data that may be valuable to third parties. Users can unintentionally leave valuable information subject to theft. Web application designers now have options for mitigating data loss risks in the browser. By deploying on-demand browser-based security controls, Web application developers can start to exercise comparable controls at the browser that they now have at the server.