CSEP564 : Computer Security : Reading 6

Karuna Sagar Krishna

November 8, 2024

Paper Title

Beware of Finer-Grained Origins

Paper Authors

Collin Jackson, Adam Barth

Problem

The authors find that many of the current and newly proposed security policies in browsers are not designed correctly. This is because they don't carefully consider the interaction with other existing browser functionalities. Such poor designs cause privilege elevation opening doors to more attack vectors. The authors point of few such features, briefly describe the problem and provide a solution.

Approach

The paper explores poorly designed features and provides solution approaches to avoid these problems. When granting privileges to a subset of documents in an origin, the browser is not able to effectively enforce that because the scripting policy is not aware of these sub-origin details. So the scripting policy lets any document from same origin inject scripts or content into any other documents in the same origin completely disregarding the privileges granted to a subset of the documents in that origin. This is origin contamination. Few examples of features that cause origin contamination - cookie paths, web server key enabled cookies, allowing mixed content from https and http, letting users accept certificate error, not enforcing Extended Validation (EV) certificates, Petname toolbar and serving signed JARs from malicious sites.

The paper explore another class of features that address the origin contamination problem by defining fine grained origins. However, these features don't work well with features that allow documents to import content and export data. A document can import content from different origin in multiple ways - using script, css stylesheets, images, video, applets and XMLHttpRequest (XHR). By importing these contents, the document is effectively endorsing the content to run in the same origin as the document. A document can export data via form submission and XHR to some network endpoint; abstractly this can be thought of as declassification of data from the document to some URL. In particular, use of relative URLs is problematic since the relative URLs are resolved relative to the current document. The paper lists few examples of new features that define fine grained origin - locked same origin policy, IP based origin and Passpet password manager.

Next, the paper provides solution to the problems described above. Browser security designers are required to carefully consider both implicit and explicit relationship with various existing browser functionality. The paper suggests 3 approaches - embrace, extend and

destroy. The first approach is to embrace the browsers existing policies, particularly the same origin policy. The paper provide 2 examples of features using the embrace approach - frame navigation privileges based on origin and phishing filters that mark entire origin as phishing or non-phishing. The second approach is to extend the URL to enable finer grained origins. HTTPEV uses a new scheme to enforce EV certificate and YURL adds public key to the host name that together with browser support prevent importing content or exporting data to different origin. The third approach is to destroy contaminated origins by refusing to display or execute content. ForceHTTPS, SafeLock and ForceCertificate use this approach.

Conclusions

The paper cautions about various poorly designed browser security features that are aimed to provide fine grained origin policy. The paper concludes that there are various features and proposals that interact poorly with existing browser functionality exposing users to more attack vectors. The paper provides solution approaches that can be used to avoid origin contamination and provide finer grained origin policy.

New Ideas

The authors generalize the concept of importing libraries and exporting data as endorsing and declassification. This generalization provides a more abstract way to model and think about the specific instances and hence I think this is a new idea.

Similarly, another new idea is that the authors generalize their solution approaches as embrace, extend and destroy. This is essentially a set of guidelines for designing browser security features.

Improvements

Though the paper explores poorly designed features, it doesn't provide any further explanation about why these are poorly designed. What was the miss in the design process that led to implementation of these features. This could provide valuable insights for future designers.

The authors could have also added references to any real world attacks that exploited the problems described in the paper. They could also have added information about how popular these features were. These information would help understand the seriousness of these problems.

New Directions

The paper is quite old (it references IE7, use of java applets); so it would be interesting to revise with the latest research and features in modern browsers related to origin policies. Also, more complex applications are designed and implemented as web application; eg. banks, stock brokerage, Google Docs, Powerpoint and Excel online. So it would be interesting to see what challenges are faced by these modern and complex applications.

The authors stop at providing solution approaches and not a full solution to fine grained origin policy. So the logical next steps would be propose concrete solution and evaluate it.