Finding and Exploiting Access Control Vulnerabilities in Graphical User Interfaces

Collin Mulliner
collin[at]mulliner.org

August 2014

This document is the accompanying white paper for the presentation *Finding and Exploiting Access Control Vulnerabilities in Graphical User Interfaces* at Black Hat USA 2014 in Las Vegas, NV, USA.

Graphical user interfaces (GUIs) contain a number of common visual elements or widgets such as labels, text fields, buttons, and lists. GUIs typically provide the ability to set attributes on these widgets to control their visibility, enabled status, and whether they are writable. While these attributes are extremely useful to provide visual cues to users to guide them through an application's GUI, they can also be misused for purposes they were not intended. In particular, in the context of GUI-based applications that include multiple privilege levels within the application, GUI element attributes can be misused as a mechanism for enforcing access control policies.

We introduce GEMs, or instances of GUI element misuse, as a novel class of access control vulnerabilities in GUI-based applications. We present a classification of different GEMs that can arise through misuse of widget attributes, and describe a general algorithm for identifying and confirming the presence of GEMs in vulnerable applications. We then present GEM Miner, an implementation of our GEM analysis for the Windows platform. We evaluate GEM Miner using real-world GUI-based applications that target the small business and enterprise markets, and demonstrate the efficacy of our analysis by finding numerous previously unknown access control vulnerabilities in these applications.

We further developed a set of tools called GEMTools. These tools are partially based on code written for GEM Miner and code developed independently of our GEM Miner efforts. These tools can be used to manually inspect, analyze, and exploit applications for GEM vulnerabilities.

We highly recommend reading our academic paper: *Hidden GEMs: Automated Discovery of Access Control Vulnerabilities in Graphical User Interfaces* (link at the end of this white paper).

GEMTools

With the GEMTools we provide some means to analyze and exploit applications that contain GEM vulnerabilities.

UnHide

The UnHide utility is a simple tool that will set every top level window of an application to visible. Besides the actual window all widgets that are inside the window will be also set to visible. Thus UnHide will show all hidden windows and widgets of a running application. If the application stores sensitive data in hidden windows the UnHide tool will find it. In addition to making all windows visible the UnHide tool further takes a screen shot of every window of the target application. The screen shots will be stored in the directory from where UnHide is launched. The screen shots provide an easy way to inspect all windows of the target application.

The UnHide tool has the following syntax: `GEMTools_unhide.exe <appname.exe>`.

Example: `GEMTools_unhide.exe Application.exe`

WinSpy++ GEM colors

The GEM colors tool is a small helper to easily find widgets (especially text edit fields) that are set to Read-Only. The GEM colors tool is an addition the the popular WinSpy++ tool. The GEM colors tool adds the functionality to color every widget inside a window with either red or green. Deepening if the widget is set to Read-Only (red) or to Read-Write (green).

To use the GEM colors functionality run `WinSpy_gemcolors.exe` select a window and click the `color` button.

Material

During our research on GEM vulnerabilities we created various tools and a detailed academic paper titled *Hidden GEMs*. The slides, tools, and paper are available on our website.

Full academic paper on GEM Vulnerabilities *Hidden GEMs: Automated Discovery of Access Control Vulnerabilities in Graphical User Interfaces* Collin Mulliner, William Robertson, Engin Kirda. In the Proceedings of the 35th IEEE Symposium on Security and Privacy (IEEESP) San Jose, CA, USA May 2014. `http://www.mulliner.org/collin/academic/publications/mulliner_oakland2014.pdf`

GUISEC website with updated slides and tools for download
`http://www.mulliner.org/security/guisec/`