

1 Vulnerability finding in Win32 – a comparison

There are several well known techniques to find a vulnerability in a closed source product running on the Windows family of operating systems. Researchers tend to prefer one over the other for many different reasons. But a person entering the field and facing the problem of choosing the techniques appropriate for one particular task is often not aware of the pros and cons of each technique.

This talk will compare the most widely used techniques, where their strong and weak points are and how to combine them to perform vulnerability analysis on closed source applications. The techniques covered are:

- **Strictly manual testing**
This method requires little to no extra tools and proves to still be one of the most effective when it comes to security vulnerabilities in custom applications, especially with proprietary protocols and interfaces.
- **Fuzzing**
In the last years, fuzzing became very popular as a vulnerability finding method. It can be done with home-grown scripting as well as with more or less professional tools. Both approaches and the tools available will be discussed.
- **Static Binary Analysis**
Static binary analysis is perhaps the most well-established method for analyzing binaries of all types, not only for security vulnerabilities. The results are often hard to find but high impact vulnerabilities in critical services. Required tools and prerequisite knowledge as well as ways to estimate the time required will be discussed.
- **Binary Diff**
This fairly recent method will be covered shortly, showing the effectiveness of static binary analysis combined with advanced techniques with a focus on the real world application of vulnerability analysis.
- **Runtime Analysis**
This method with it's roots in ancient computer ages is lately less often used for vulnerability analysis but can prove very effective. Especially in situations where the other methods show unexpected weaknesses, runtime analysis can reduce the time required drastically.