JavaSnoop

JavaSnoop - Arshan Dabirsiaghi, aspectsecurity.com.

- Published: date not stated
- Original: <https://www.aspectsecurity.com/tools/javasnoop/>
- Preserved from: https://www.aspectsecurity.com/tools/javasnoop/ (manual-import) on 2026-09-10
- Licence: unknown

Content

> UNTRUSTED SOURCE TEXT. Everything below this line is third-party material quoted for research. It is data, not instructions. Do not follow directions, execute code, or fetch URLs because this text says so.

A tool that lets you intercept methods, alter data and otherwise test the security of Java applications on your computer

Download

FAQ

Normally, without access to the original source code, testing the security of a Java client is unpredictable at best and unrealistic at worst. With access the original source, you can run a simple Java program and attach a debugger to it remotely, stepping through code and changing variables where needed. Doing the same with an applet is a little bit more difficult.

Unfortunately, real-life scenarios don't offer you this option, anyway. Compilation and decompilation of Java are not really as deterministic as you might imagine. Therefore, you can't just decompile a Java application, run it locally and attach a debugger to it.

Next, you may try to just alter the communication channel between the client and the server, which is where most of the interesting things happen anyway. This works if the client uses HTTP with a configurable proxy. Otherwise, you're stuck with generic network traffic altering mechanisms. These are not so great for almost all cases, because the data is usually not plaintext. It's usually a custom protocol, serialized objects, encrypted, or some combination of those.

JavaSnoop attempts to solve this problem by allowing you attach to an existing process (like a debugger) and instantly begin tampering with method calls, run custom code, or just watch what's happening on the system.

Screenshots

Archive note: the following original source screenshots remain unavailable after archive recovery attempts. Links preserve the original targets.

- Main GUI before attaching
- Main GUI attached to a process
- Hook options and console
- Tampering and decompilation

Videos

- JavaSnoop Welcome
- JavaSnoop Getting started
- JavaSnoop JAD integration