Long Term Cybersecurity research
Summaries of projects granted in the first NWO call for proposals (2012)

Project number	CYBSEC.12.014 / 628.001.006	
Main Applicant	Prof. dr. ir. H.J. Bos	Vrije Universiteit Amsterdam Faculteit der Exacte Wetenschappen Informatica
Project title	Re-Cover: The Power of Obfuscation	

Scientific summary

Software vendors and cybercriminals alike rely on obfuscation techniques to protect sensitive information from the prying eyes of reverse engineers. Obfuscators transform both the control flow and data layout of a program to make it practically infeasible to reverse them. A program's control flow can be hidden by a VM, while data layouts are hidden by splitting variables over multiple memory locations, or generating a string at runtime, rather than storing it explicitly in the binary, etc.
Over the years, much research was conducted in probing control obfuscations. Typically, it shows that most techniques are limited in the face of determined attackers.
Surprisingly, we do not know any such probing attempt for obfuscated data and memory. This is remarkable, because for reverse engineers there is great value in the data and its layout. So far, the tacit assumption is that data obfuscation is strong and cannot be automatically reversed in practice. The research question is whether this assumption is justified. Specifically, our hypothesis is that it is false for current data obfuscators and that it is feasible to recover the data structures in a semi-automated way.
To probe data obfuscators, we propose to use a combination of static and dynamic analysis. For instance, by observing the program's behavior, we identify strings that were not in the original binary, or accesses to different locations that always occur in close proximity (suggesting split variables), etc. If we are right, the research outcome will have far-reaching implications for software security. We will build on our analysis to improve existing obfuscation techniques.

Applicable NCSRA themes

- Malware
- Secure design & engineering

Applicable NCSRA theme

- Malware