RESEARCH PROPOSAL

JOSEPH HALLETT

What do I want to do

Bytecode steganography is a novel technique for hiding run-time behaviour in compiled programs. It has been proposed as a potential solution against program exfiltration—an information security problem involving the removal of compiled code from secure computers.

The idea is that by making small changes to the architecture of a computer programs display different behaviour depending on whether they are being run on the original or modified machine. This steganographic approach has the advantages over DRM-based techniques: it isn't immediately obvious that there is any exfiltration protection present as any program featuring such techniques remains a valid program for the unmodified architecture—albeit with different behaviour. A further benefit is that the protection lies in the architecture the program is running on rather than inside the program itself: there is no code to decrypt or logic to circumvent inside the executable itself, only a widely altered behaviour when specific architectural modifications are made.

There has been relatively little research on the feasability of this or if whether the technique would offer any protection in practice. I want to explore the topic and assess the feasibility of such techniques. By developing a toolchain for finding the modifications and generating programs with this exfiltration protection an assesment can be made as to its effectiveness and any security it may provide.

Is it worth doing

Exfiltration is a growing problem for both companies and governments. Recent efforts by *Wikileaks* and articles about hacking have increased the public perception of the leakage problem.

Are we interested in this

Looking at steganographic architectures fits well with the cryptography group's interests. The implementation of a secure systems on top of small computer architectures is of particular interest. Verifying that such a steganographic provides information-security adds further value.