A NetLogo plug-in to secure data using GNUs Pretty Good Privacy software suite

Doug Salt$^{\text{OrcID: 0000-0001-5186-9388}}$ Gary Polhill$^{\text{OrcID: 0000-0002-8596-0590}}$

Abstract

A description of a NetLogo plugin and the reasoning behind its design and implmentation. The plugin makes use of Gnu's Pretty Good Privacy software suite to encrypt arbitary data sources in Netlogo. This both secures the data to a reasonable degree and protects any sensitive data that might be in use for a publically available model.

Introduction

Cheap, publicly-accessible, distributed storage, colloquially known as the "cloud" is becoming increasingly prevalent [@] and is increasingly used for the storing of experimental data [@]. Storing experimental data in this way has several advantages, such as any access to the internet allows instant access to this data [@]. This means the data is effectively accessible anywhere. Data might be stored in a single location, or it might be distributed. The convenience is that from the point of view of the consumer of the data, it all appears to originate at a single web-based location [@]. Also such data is cloned and distributed in real space for the purposes of fault-tolerance [@] and thus can exist in many locations simultaneously [@]. Thus the chances of it being lost are remote [@].

It is reasonably easy to use such cloud hosted data in NetLogo models. This following list of providers is by no means meant to be comprehensive, and some institutions provide their own, cloud-based solutions, but it is our suspicion that some, non-technically aware NetLogo users are making use of the cloud without being aware of the ramifications of doing so, and doing so by using the cheap and often free provision of these cloud-storage hosts. This arises because each of the major cloud storage providers such as Dropbox [@], Microsoft's OneDrive [@] and Google Drive [@] provide tools that allow the invisible, local mounting of such resources. These exist for the most prevalent platforms such as all Microsoft Windows versions greater than 7 [@]; all versions of Android [@], and Apple's two operating systems: OSX and IOS[@]. This means that the "cloud" storage appears as local storage on the local machine, and NetLogo models do not need to be changed to access such data (other than changing a file name).

The advantages listed above are also the method's disadvantages. The publicly accessible nature of such data could violate regional privacy laws. For instance storing personally identifiable data of a sensitive nature without sufficient safe-guards now violates the European GDPR [@]. The multiplicity of the storage means the creator of the data has largely lost control over the destruction of the data. Indeed if such data is of a personally identifiable nature, then, given GDPR requirements it is a legal requirement of the researcher to store the data in particular geographical areas (ibid.). The are stories of data n

The NetLogo Extension

Illustration

Discussion and conclusions

In conjunction with Infrastructure as a Service (IaaS), then it is becoming increasingly common to see NetLogo models.

We have developed a plugin that uses the Gnu PGP software to allow various types of encryption on the data only. We could develop a plugin that obfuscates the code, but we believe that this not only violates the code of openness that surround the NetLogo community, but also possibly violates the GNU Public License version 2 under which NetLogo is distributed. Taking somebody's open code and concealing it legally violates the license, as this is precisely the reason the license was created in the first place [@]. It also violates the principle of open science as people should be able to inspect models to see the reasoning that underlies them. This is increasingly important where such models are used for policy decisions [@]

This code has been tested on Linux, Windows 7, Windows 10, and OSX so far the code could be ported in entirety into NetLogo. There are java libraries available that mirror the functionality of PGP [@]. However this has the limitation of precluding the rapid release cycle of encryption software once vulnerabilities have been discovered.

Acknowledgements

Bibliography