# **Advantages and Disadvantages of Java Serialization**

Daniel García

Department of Computer and Mathematical Sciences, Lewis University

CPSC-24500-004: Object-Oriented Programming

Dr. Sheikh Shamsuddin

November 16th, 2021

Java features a mechanism called serialization which allows programs to transform Java objects into a byte stream. We can then use that byte stream to store data locally (like to a file) or transport it across the internet (like using HTTP requests to send byte streams from one endpoint to another). According to CS Professors from the University of Wisconsin-Madison, some benefits of serialization include allowing the object state information to cross implementation boundaries through standardized byte representation. This can be accepted by many programs, languages, clients, etc. That is, unless a secure environment is in place. One of the downsides to this is that serialized data is raw in the sense that if anyone intercepts that data or the transport of the data, it can be for the most part read as plain text. This means that you have to make sure that you are using a secure (and encrypted) protocol like TLS.

## References

Evans, H. (n.d.). Why Object Serialization is Inappropriate for Providing Persistence in Java. Retrieved November 17, 2021, from https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.737.6349&rep=rep1&type=pdf.

Kohnfelder, L., Heymann, E., & Miller, B. P. (2019). *Introduction to Software Security*. 3.5 Serialization. Retrieved November 17, 2021, from https://research.cs.wisc.edu/mist/SoftwareSecurityCourse/Chapters/3\_5-Serialization.pdf.