DS 760
Behavior Mining

Rick W. Lentz

4 November, 2017

Drawing on the internet readings of this lesson, what lessons can be extracted that might apply to data science as it applies to private business?

This week, we were introduced to the concepts behavior search in the context of data mining. Behavior mining caused me to pause and visualize what the author was saying. My conclusion was that to infer behavior; one would need full-scope access to the same information the individual experiences.

I did some research to see how this subject-behavior data mining (contrasted with limited scope search) applies to private business. One huge market is in network communications. Many companies perform SSL traffic inspection. This means that any traffic 'secured' with HTTPS/TLS layer encryption is decrypted and inspected in the same manner as non-encrypted traffic. Simply put, this means that green lock in your browser is just a Maginot Line.

When viewing this depth of information, as the reading suggests, other details may emerge that raise subject-behavior mining questions. For example, a private company's compliance staff may have a mandate to ensure that trade secret information does not show up next to OkCupid's data dump on FreeNet. I'd imagine that even seemingly small bits of information related to these sensitive strategies may help a competitive adversary mosaic together a critical piece of a company's secret.

A broader search of behavior mining found many academic articles on the topic. I found reference to a tool that data scientists can use to mine a user's email to detect social clique, detect similar users, and flag anomalous user behavior.

Commercial SSL product reference:

https://www.cisco.com/c/en/us/products/security/ssl-appliances/index.html

Behavior tools reference:

https://academiccommons.columbia.edu/download/fedora_content/download/ac:125721/CONTENT/nsf-nij-emt.pdf

http://dx.doi.org/10.1080/08850607.2016.1148488