File 20111121.0930: Notes from AFRL Semantic Rules Whitepaper Discussion, 0900 today:

Kevin Newman, Carl Weir, Martin Hofmann, Joe Loughry, and Bill Ratliff were on the call. This group responded to the AFRL RFI as well. Focus is on a semantic software application that Kevin Newman has been working on. When they looked at recent changes to the BAA, they noticed emphasis on malicious users and thought they could do something with it.

Ways of defending against malicious users: making it tough and resilient to attack, passively auditing and watching for attacks, or trapping detected attacks quickly and trying to render them harmless.

This customer (AFRL) is highly concerned with three things: guard agnosticism, metrics for improvement, and the risk of malicious insiders. Keep those points in mind when writing for them, and mention them when presenting to AFRL.

CLOAK has a large number of counters inside it that collect statistics. Data not used currently, but we hoped in future to use it to prioritise workflow to particular analysts that have been shown to have a talent for particular types of documents. Conversely to shift particular troublesome types of documents away from analysts who have a low score of effectiveness on those types of documents. Note that this workflow functionality is not implemented yet; it is a maybe future capability.

I thought the Export Agent in the DUET proposal might be the right place to take in this sort of metadata emitted by CLOAK, Purifile, or IC Clear for analysis and decision making.

Other potential applications of the AFRL Semantic Rules Whitepaper ideas: electronic health care records quality, fraud detection in financial records or regulation, assessing and maintaining quality of electronic forensic evidence (under chain-of-evidence rules) in law enforcement. Look for clues at the statistical process monitoring techniques used in chemical plants. They often cannot directly measure the variables they really need to know—such as the instantaneous rate of a chemical reaction, or the concentration a particular reactant—but they can monitor indirect indicators of the reaction progress, such as temperatures and pressures in the reactor. Process operators pay attention not only to the instantaneous values of these indirect indicators, but also to trends; they keep the reaction under control by making sure first and second derivatives stay within certain bounds.

Application to electronic health care records: as more and more historical paper records are brought on-line, old information has the potential to conflict with new information, with mismatches disambiguated. This is completely separate from the whole other issue of privacy of electronic health care records and the question of how to grant access securely for epidemiological studies without damaging privacy rights. Sooner or later companies are going to figure out widely that ownership of large collections of random people's electronic medical records is intrinsically valuable.

The application to detection of fraud, waste, and abuse in financial regulation is equally current. Here, you have malicious insiders built right into the system (in the sense that actors will always try to exploit any opportunity for advantage). A system that can spot malicious insiders trying to find covert channels past a guard can also spot insider trading, defalcation, and attempts to evade risk management protocols.

References