Identity Assurance and Risk Aggregation

The Department of Defense of the US Government often gets things right, and one of the most recent cases of this was in their introduction of the term “Identity Assurance”. Now to be clear, they introduced the term to replace “Identity Management” because, internally, they thought it was a bad public relations idea to somehow indicate that they are managing peoples' identities. That sounds more like creating new identities for people than managing the use of identification and authentication. But this term is somehow more compelling than “Identity Management”.

Identity assurance is intended to provide the DoD with ubiquitous and secure access to identifying information. This is an increasingly common thread in information protection where false or avoided identification and authentication process is involved in many successful attacks. At one recent conference, I heard two different speakers tell me that the introduction of higher assurance authentication reduced the (1) total number of successful attacks and (2) the number of password guessing attacks by 47 percent in one year. Of course, as metrics go, that is a pretty poor one. I think they are talking about detected attacks rather than total attacks, and I think they are talking about some subset of attacks rather than all attacks, but they don't actually know. To be sure, improved identification and authentication are process elements that are critical to attaining effective protection in most information environments.

At the same conference, I heard about the US government-wide push for ubiquitous use of identity assurance technology. In this case, essentially all government workers (employees and contractors) are being issued identification badges that provide biometric information, pictures, and other identity-related information. This project, over the period of something like three years, is supposed to create the standards, certify the products and processes, and roll out well over a million electronic identities. That is impressive, but even more impressive, especially for government, is that a year and a half into the program, they are on track to succeed. They have defined and gotten standards accepted for most aspects of the process, in a period of about a year some 280 or more products have been certified for use (which I believe is more than the total number of US government certified security products over the previous 30 years), and are in the process of registering about 750,000 individuals over the next 6-12 months. The average operating cost is estimated at about $3/month plus $70 in initial cost, both per individual registered. Again, the government is doing something amazing and, in many ways, something that is very impressive.

One of the things that brings me concern, however, is where they have decided to use rhetoric rather than rationality. I heard very propagandistic and irrational positions taken with regard to gaining acceptance of this new technology, and whenever I hear this, a little alarm goes off in my head that tells me all is not well. Several people said that gaining acceptance of the technology requires educating people on why this is the right thing, all saying “put it in the right terms”. It sounds innocent enough until you realize that they are presenting identical falsehoods to support positions to people who don't understand the issues well. Examples:

- Better identity assurance will eliminate the need for guards at our facilities.
- Young people aren't worried about privacy, so that won't be an issue in the future.
- The agencies this is proposed to don't “get it” like we do.
- Don't worry about trusting the identity, you control the authorization.

- Ceding local control over identity improves your security (you can trust us).
- The information is safer, it's all in one place.

The biggest security problem with large-scale identity repositories seems to me to be the aggregation of risk. This is something that few people seem to understand or analyze, and is commonly referred to as “putting all of your eggs in one basket”. Instead of having a host of systems distributed throughout the government or your enterprise, each of which has to be independently broken into, disabled, corrupted, or exploited to do harm, and each of which only grants a limited capacity for harm, identity controls are moving rapidly toward massive data stores trusted to increasingly high levels oracle-like functions with perfection.

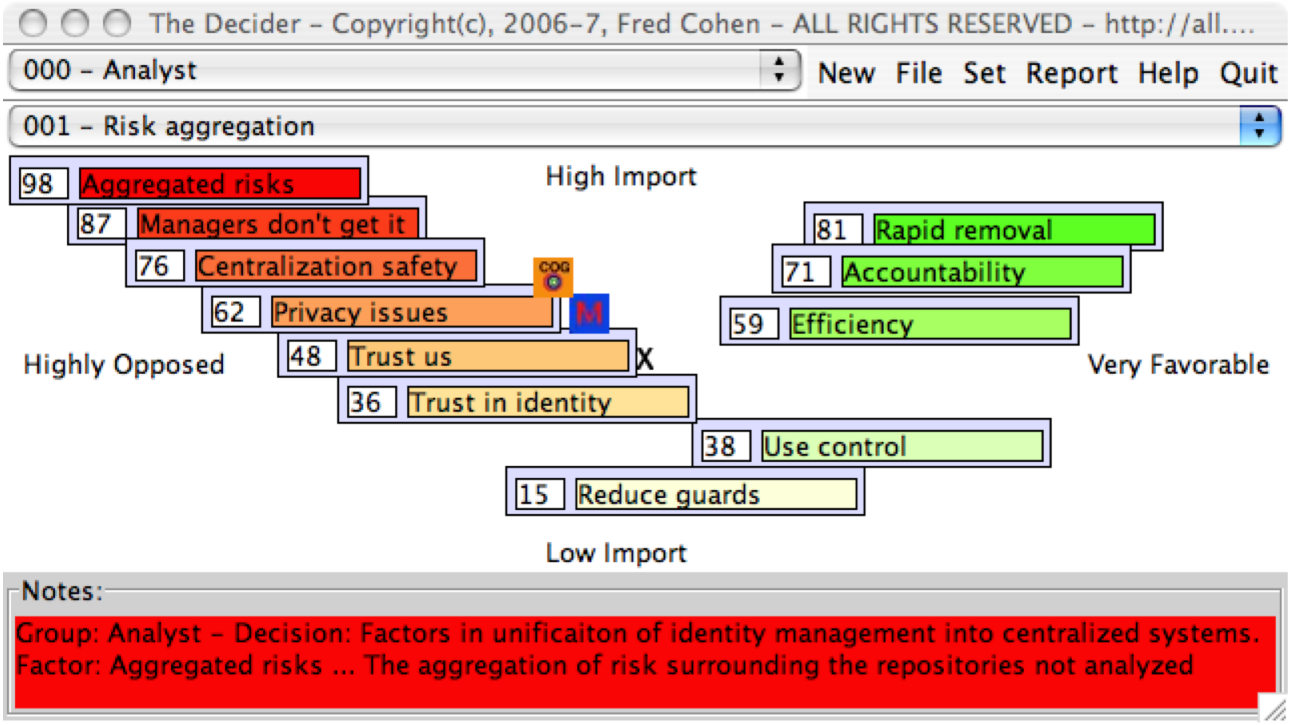

Figure 1: Issues in the decision to highly centralize identity assurance

Some factors involved in highly centralized identity assurance, including those address through public justifications are presented in Figure 1 along with our generic analysis. For specific situations, the placement of factors and factors chosen are certain to change, but clearly, the analysis indicates that excessive centralization drives away many advantages because of its aggregation of risks. Put more simply, don't put all of your eggs in one basket.

Anybody who has worked in information protection for a significant time knows well that any system can be defeated. Spend enough time, effort, and money, and you will, at some point, succeed. When we aggregate risks this highly by having one system that controls all access for a big enough target, we are making the target so important that enemies almost have to find ways to attack it. They will apply the resources necessary, and eventually succeed with high consequences. Anybody that does not assume that information protection will fail is making a big mistake, and as the stakes get higher, the implications of the mistake get larger.

