17. Scenario IV: Ubiquitous Identity Theft

Ari Schwatz

This scenario offers a view of the world that most observers today would consider a worst case. Identity theft, characterized by law enforcement as the fastest growing crime in the United States, (GAO, 2000) has grown exponentially. Identity theft grew beyond epidemic proportions as confirmed by the Federal Trade Commission. (FTC, 2005) Due to continued weaknesses in identity frameworks, increased demands for information upon using and purchasing content and increased weaknesses in security, it is quite common for individuals to feel comfortable assuming the identity of others simply to protect themselves. For example, the medical database begun under Bush has no meaningful privacy protection. (Pear, 2007) Obtaining care at a pharmacy or minor emergency center that might result in future refusal to insure or personal embarrassment requires a credit card and id in a false name.

Assertions of identity are still utilized for social protocol and historical necessity. Yet the assumptions about individual identity to information links on which so many systems have been built have been broken down. Continuing ad-hoc methods of authentication are attempted, but subverted as soon as they are widely implemented.

The State of Identity

Interacting with the government in a world of ubiquitous identity theft is confusing and frustrating endeavor. Some agencies still have complex authentication, verification and authorization schemes in place that just do not work and burden the process. Other agencies have given up completely, preferring instead to rely on face-to-face transactions. Most service agencies have learned to live with high rates of fraud and exposure of citizen information to snooping.

New laws have been put in place to harshly punish the worst fraud offenders. While the deterrent does not seem to work for small time theft, it has been somewhat effective for large-scale long-term repeat offenders where prosecutors can build up a case. This has relieved enough pressure on the judicial system to make most believe that this is all that can be expected from

law alone at this point. Most of the culprits of widespread fraud are beyond the reach of American law, in Nigeria or Eastern Europe. The credit card processing companies have no interest in investing to reduce such fraud, because the investments may cost as much as the fraud. In addition, the cost of much fraud can still be pushed to the consumer through the use of PIN systems as with the United Kingdom.

One example of the repeated failures in authentication systems is the online Personal Earnings Benefit Estimate Statement online at the US Social Security Administration (SSA). Originally, beneficiaries could get an online statement describing working history and long term benefits by filling out a detailed form providing explicit personal information such as mothers maiden name, date of birth and address as listed on their last paycheck. Soon after going online, it was recognized that this information was far too easy for anyone to get. The SSA tightened security by sending a confirmation email message with a password. Soon after this measure went into effect, it became an increasingly easy and common practice for identity thieves to hijack email accounts. Then SSA switched to telephone "call backs" where they would ask "out-of-wallet questions" such as employment history, salary information and more. This process had the down side of being expensive (to pay for call centers) and cumbersome (true beneficiaries often could not answer the out of wallet questions correctly), but it did work for a few years. Eventually, however, even this measure has failed. Insiders in call centers of this kind began to regularly misuse and share the transaction information and it is quite simple and common to set up a phone in another person's name for a short period of time.

RealID was an expensive debacle that increased the flow of citizen information and ease of information theft. Driver's license authorities continue to be valuable sources of false identities, only those now work uniformly across state lines. The rate of identity fraud, and the economic necessity of credentialing illegal immigrants doomed the project from the start.

Other government offices have simply stopped providing services that require authentication. For example, individuals can no longer reserve a campground space in a national park in advance. Secondary markets and the ease of identity fraud caused the cost of popular campsites to skyrocket, and organized crime had become involved. Campsites had to return to first come, first serve.

Obviously many government agencies do not have the ability to reduce services in this way. For example, while most benefit offices have abandoned hope of providing benefits electronically over distances, they still need to provide basic services that require authentication. Beneficiaries are now expected to come into the office where large amounts of biometric data (via photographs and DNA samples) are taken about each visitor. The biometric information does not help in authenticating individuals. Identity thieves were able to duplicate and falsely populate biometric databases long