Association for
Computing Machinery

Advancing Computing as a Science & Profession

USACM

Issue Brief

Significant Concerns with REAL ID

Background

Passed by Congress in 2005, the Real ID Act would establish new physical security standards for drivers licenses, new document requirements for confirming identities, and - most troubling to computing professionals - would require states to digitalize and store identity documents in databases that would be linked to each other. The premise of the act was that it would help fight terrorism - a worthy goal and one that computing professionals support. But this worthy goal was undermined by poor policy decisions and inadequate rules, making REAL ID a real threat to the security and privacy of American citizens.

Reasons for Concern

The claim that the REAL ID card would be the “gold standard” for identity puts too much trust in the cards. Motivated criminals will find ways to make illegal copies, and bribe or threaten officials to alter records or issue falsified cards. Worse, these cards could actually create more criminal activity if potential lawbreakers determine that security professionals trust the system’s infallibility in identifying people. Further, knowing someone’s identity does not mean knowing his or her plans or intentions, making it unclear how REAL IDs would significantly combat terrorism.

Inadequate Standards

There is no accountability for those administering REAL ID, nor are there sanctions for compromising the databases and documents that support it. Without specific minimum standards, cash-strapped states may divert resources away from strong privacy and security controls in order to try and maintain current levels of customer service.

Identity Theft

Theft of driver's licenses is not the predominant form of identity theft today, Social Security numbers and credit card numbers are. Presenting the REAL ID as a “gold standard” identification document makes it a tempting target for a different form of identity theft: one where people will assume someone else's identity and conduct criminal acts as that individual. An identity stolen through a forged, stolen, altered or fraudulently obtained REAL ID would be much harder to recover.

Insider Threats

The most likely way a REAL ID would be compromised is through an insider accessing data without authorization. REAL ID regulations are silent on this point. Insider threats are a problem under the existing driver's license system, but the REAL ID Act makes the problem far worse. It vastly increases the amount of personal information stored, and therefore potentially exposed, on state databases. Each involved agency working on REAL ID needs strong access controls for the information they protect.

Conclusion and Recommendations

At a minimum, REAL ID should require stronger and more detailed privacy, security, access and accuracy provisions. Even with those provisions, existing technology and approaches cannot solve the policy problems raised by REAL ID. States, Congress and the Administration need to work together to address these fundamental flaws by overhauling the Real ID Act.

- Delay implementation of the REAL ID until all underlying databases and the federated query service have been fully tested and are operational.
- Minimize the data stored on the machine-readable zone (MRZ).
- Specify privacy, security and accuracy standards for the licenses, the databases, and the federated query service.
- Base the privacy standards on Fair Information Practices.
- Require security consistent with standards such as the Common Criteria Evaluation and Validation Scheme (CCEVS).
- Include strong access control procedures for REAL ID documents and data.
- Require data breach notification procedures for any agency controlling REAL ID data or documents.
- Limit the scope of the usage of REAL ID to only the uses specified by law.

You can read more about these recommendations and our objections to REAL ID at:
http://usacm.acm.org/usacm/PDF/USACM_REAL_ID_Comments_FINAL.pdf