Mandatory Electronic Employment Verifications Systems: Technological Implications

Background

The Department of Homeland Security (DHS) has been testing a system for employers to electronically check an employee's work eligibility. This system, recently renamed "E-verify" attempts to match an employee's personal information (such as name and Social Security number) against databases at the Social Security Administration and DHS to verify whether he or she is eligible to work. Congress has developed several different legislative proposals that would greatly expand the system by mandating that employers verify all new hires and existing employees. The Administration has also announced it will expand the system to cover all Federal agencies regardless of Congressional action.

Reasons for Concern

Computing professionals have often witnessed large-scale federal information technology projects start with good intentions but fail under the weight of design flaws and overambitious goals. These experiences show that it is extraordinarily difficult to meet objectives and deliver these projects on time and on budget. The state-of-practice for building such large systems and satisfying security, reliability, survivability and guaranteed real-time performance is not dependable. The proposed national verification system seeks to create a Federal IT system on a scale and complexity never seen before, so there is a large possibility of major cost overruns and significant shortcomings. Because the envisioned employment verification system would control the access of all native and foreign-born citizens to employment in the United States, it would have to be very carefully designed and tested if it is to be adequately secure, reliable, accurate and respectful of privacy. ACM's U.S. Public Policy Committee (USACM) sees issues related to privacy and security, accuracy, scalability and access that must be addressed and resolved before this massive new identity verification system could sensibly be adopted.

Privacy and Security

Privacy problems are becoming increasingly complex as ubiquitous dependence on computerized databases increases. Information used in these systems includes all the primary personal identifiers in the U.S., and thus leaks, theft, destruction or alteration of this data have severe consequences, including identity theft and impersonation. Protections must be put in place that follow established Fair Information Practices. It is important that policymakers understand that the existing infrastructure is riddled with security and reliability vulnerabilities, and is not sufficiently trustworthy. The total system cannot be adequately protected by purely technological approaches, because many of the privacy problems arise from the large number of people who will require, or who will improperly obtain, access to the system. This system will be no more

secure than the security of any point of access – even the dial-up connection from an outdated, unprotected terminal. Carefully designed operational procedures will be essential to limit system access to just the amount necessary for the intended purpose of the system.

Accuracy

Data quality, both in the entry of names for checking purposes and the original underlying data, for large-scale databases of public records is a difficult problem. Because this system will use multiple databases for verification of records, the problem is further compounded. The Social Security database is known to have a high number of errors in name matches, as well as some duplicate numbers. The Social Security Administration's (SSA) Office of the Inspector General recently estimated that the SSA's 'Numident' file -- the data against which Basic Pilot checks worker information -- has an error rate of 4.1 percent. A SSA official, testifying before Congress[1], indicated that if Basic Pilot were to become mandatory and the databases were not improved, SSA database errors alone could result in 2.5 million people a year being misidentified as not authorized for employment. This figure does not take into account errors in the DHS database. Strong safeguards have to be built into the system that allow for individuals to check the accuracy of the stored information and and to provide redress for employers or employees that may be affected.

Scalability

About 23,000 employers are using the voluntary system[2]. This represents .39% of employers in the United States[3]. Scaling the system up would require at least a thousand-fold increase in users, queries, transactions, and communications volume. As a general rule, each time a system grows even ten times larger, serious new technical issues arise that were not previously significant. Furthermore, the error rate can be expected to increase, rather than decrease.

Access

A great many businesses do not currently have reliable Internet access to be able to use the proposed web-based verification system. Requiring employers to use such a system will be a burden for many, an impossibility for some, and will impose a huge cost in IT and create new security issues for many small and medium-sized employers.

Conclusion

Data security, system integrity, and individual privacy must be anticipated from the beginning and throughout the design, implementation, and operation of an electronic verification system. Congress should establish clear policies and required outcomes for this system. More careful thought is needed on total-system approaches to address identity authentication, authorization, and data protection, along with incentives to ensure that these advances result in practical systems.

---

[1] June 7, 2007 testimony of Steve Schaeffer, Assistant Inspector General for the Office of Audit, Social Security Administration before the Social Security Subcommittee of the House Ways and Means Committee.
[2] U.S. Citizenship and Immigration Services September 25, 2007 Fact Sheet on E-verify, http://www.uscis.gov/files/pressrelease/EVerifyFS25Sep07.pdf
[3] June 7, 2007 Government Accountability Office testimony before the Social Security Subcommittee of the House Ways and Means Committee cited 5.9 million employers in the U.S. as of 2004; the latest data was available. http://waysandmeans.house.gov/hearings.asp?formmode=view&id=6095