Standards Today

A Journal of News, Ideas and Analysis

A publication of CONSORTIUM INFO.ORG
GesmerUpdegrove LLP

June–July 2009 Vol. VIII, No. 4

EDITORIAL:

Technology's Reach and Security's Grasp

Andrew Updegrove

Modern society harbors many bad habits. One is its penchant for enthusiastically embracing the benefits of new technologies before considering their less desirable side effects. Whether we look at the development of automobiles (first) and safety features (much later), or industrialization (first) and environmental protection (much, much later), the story is always much the same: we reach for the candy before we grasp the reality of the cavities. Only after the problems become too great to ignore do we investigate the unintended consequences, realize how difficult and expensive they are to address, and grudgingly start to rein in our appetites and exercise a bit of prudent self-discipline.

Perhaps we should not be surprised, then, that the U.S. government is only now becoming alarmed over the vulnerability to which we have become exposed as a result of our whole-hearted embrace of the Internet. With the operations of government, defense, finance, commerce, power distribution, communications, transportation, and just about everything else now dependent on the healthy operation of the Internet, that alarm is well-justified. And with the creation and storage now of virtually all data in digital, rather than physical form, exposure of our financial as well as our most intimate personal and health information is only a hack away as well.

With the creation and storage today of virtually all data in digital, rather than physical form, exposure of our financial as well as our most intimate personal and health information is only a hack away

In some ways, finding ourselves at such a pass is not so surprising, largely because in the past we have been able to create security barriers when and as needed, and allocate the costs of security failures in a workable manner that has been acceptable to those directly involved. Think of the evolution of the credit card industry, for example, in which the individual card owner whose card is stolen is effectively immune from financial liability for the card's misuse. Instead, the commercial entities that benefit from the existence of the cards accept that risk and absorb it into their cost structures. From an economic point of view, this is a

rational response, and so it might seem that that the Internet simply replicates old risks in new settings that can still be adequately managed in a traditional way.

But no. As recent retail security breaches have shown, far too much information can be exposed via a single successful assault to rely upon reallocation of risk to manage the impact. The same is true in many other domains. Whether it be managing a national air traffic control system, processing billions of financial transactions a day, or operating a unified national "Smart Grid," the stakes are simply too high to rely on damage control. Instead, we must prevent the breaches entirely, by building the firewalls higher and stronger. We have no choice but to learn how to repel the rapidly increasing horde of cyberbarbarians gathering outside our digital gates.

Somewhat paradoxically, one key to the security solution can be found in standards. Paradoxically, in that we think of security in the given case as being based upon doing things uniquely rather than all in the same way. But in fact, security has always been based on standardized approaches (think of standard locks with unique keys, and single algorithms that generate and then interpret multitudes of scrambled messages). So also it is that the only feasible manner in which security can be achieved in a networked world is through the use of standardized approaches and tools – in this case, a multitude of them, both technical and procedural. The former makes security possible in the first instance, while the latter allows it to be maintained reliably as the network is upgraded on a constant basis.

We need to grasp that a digital 9/11 event is already within the reach of too many – and act to protect ourselves against the consequences

Happily, there are many formal standards development organizations and consortia actively engaged in supporting existing security standards, and developing new ones. They range from protocols, to federated identity tools, to biometric identification standards, to holistic suites of standards, auditing requirements and certification programs created to maintain end-to-end security within complex commercial environments, such as the payment card industry. But much more work remains to be done to implement reliable security across many crucial domains.

The advent of the Obama administration offers a unique opportunity to close the gap between technology's reach and our grasp of the risk that must be managed. Today, there is a confluence of opportunity made possible by the technological sophistication of the Obama team, the launch of simultaneous initiatives to rapidly implement new technologies to address significant national objectives, and the funding needed to tackle these enormous jobs. In each case, whether it be making the transition to Web-based open government, deploying electronic health records for all citizens, or putting in place a new interactive power grid, implementing effective security protections will be crucial to success. Otherwise, the new benefits we gain may be outweighed by the new risks that we will assume.

In other words: there is no choice for the Obama administration – and Congress - but to make achieving a new level of data security a national imperative. We are

already farther down the road of risk than we should be. If we fail to act, the consequences may not be gradual and reversible, as with pollution, but sudden and disastrous, perhaps as the result of the acts of a rogue state taking down the financial markets, or an international terrorist organization bent on crashing the air traffic control system at rush hour.

Is that an alarmist statement? Hardly. We have already seen the personal information of millions of individual citizens exposed through single data breaches, presumably by rings of foreign criminals, as well as government Web sites taken down by persons (or nations) still unknown. Before it is too late, we need to grasp that a digital 9/11 event is already within the reach of too many – and act to protect ourselves against the consequences.