TAB Observer Commentary

Provided By

Jeff Schmidt, TAB Observer
Independent Consultant specializing in identity and authentication systems
JAS Communications LLC
jschmidt@jschmidt.org

Disclosures

I am presently engaged as a technical consultant to Fox Interactive / MySpace regarding identity and authentication issues. That said, the opinions contained within this document are my own and not that of any client. Moreover, my views on this topic pre-date my engagement with Fox Interactive / MySpace and are well documented in numerous presentations, publications, and testimony.

Commentary

The following commentary is offered on all identity/authentication related submissions including credentialing, age verification, identity provider, and parental consent approaches, specifically:

Aristotle
AssertID
Chatsafe
Checkmyage.com
Choicepoint
eGuardian
Gemalto
GenMobi
IDology
Microsoft Cardspace
NetIDme
Portcard
Privo
RedStar hs
RelayID
VerificAge

Identification and Authentication

A discussion of age verification or parental consent systems necessitates discussion of identification and authentication. Many of the online security and identity fraud/theft problems we face today are caused by the failure to fully appreciate the complexities and subtleties of identification and authentication systems. Identification is the process of matching identifying information such as a name, account number, etc, with a particular individual. Authentication is the process of proving the relationship. Authentication comes in many shapes and sizes ranging from very weak techniques like passwords to very strong techniques like DNA matching.

Age verification is the act of attaching an age or date of birth attribute to an identifier. In other words, we attach an age (“12”) to an identifier (“Sally”). Once we’ve made that association, if we successfully identify and authenticate “Sally” in the future, we’ll also be able to look up her age. Similarly, parental consent systems attempt to match the identities of children with the identities of their parents. Given the fact that we’re dealing with the safety of children, we need the age and family relationship information to be highly resistant to forgery, and we need authentication strong enough to make it sufficiently difficult for motivated child predators to impersonate children and parents.

Age verification, parental consent and similar systems raise two separate problems I call the **Initial Subscription Problem** and the **Subsequent Visit Problem**. The first time (initial subscription) we see a person identifying herself as “Sally,” how do we determine her age and/or the identity of her parents? Then, on subsequent visits, how do we reliably identify and authenticate that the person claiming to be “Sally” is the same one we subscribed initially?

Reliable Sources of Information (The Initial Subscription Problem)

In the U.S., there is only one unquestionably reliable source of age information: the birth certificate. Birth certificates are not public records. All other records, public and private, derive age information from a birth certificate. Minors present unique challenges because there exist no public records that substitute for the accuracy of birth certificate information; there simply are no public records that provide useful identity and authentication information about minors.

Moreover, the birth certificate is the only universal record that authoritatively ties parents to their minor children. Any parental consent or “adult vouching” approach, absent a birth certificate, is only as reliable as the individuals making the assertions. In fact, using only public records, it is impossible even to prove the existence of a child let alone her age or any family relationships that may be claimed.

Initial subscriptions performed in schools or by trusted third parties such as police officers are more reliable than self-reporting and public records approaches; however, these techniques present numerous additional practical, legal and security challenges.

It is also important to note that since successful age verification or parental consent may prevent the child from accessing resources she desires, not only child predators, but the very children we want to protect will be trying hard to defeat these verification systems. Recent data confirms this unfortunate reality.

Identification and Authentication of Children (The Subsequent Visit Problem)

After the child has been subscribed, each and every time she uses the online site she must be reliably authenticated, allowing the site to look up the information about her parents or her age that was determined in the subscription process. A system that attempts to use age verification or parental consent must have the ability to reliably re-identify and re-authenticate children on an ongoing basis at Internet scale; this important detail is often overlooked. As security is only as good as the weakest link, even a strong initial subscription is negated by weak authentication on subsequent visits.

The only conceivable authentication mechanism appropriate for this task at Internet scale is username/password. In other words, assuming that we could create an account for a child and somehow reliably add the age attribute and/or obtain reliable parental consent (i.e., solve the initial subscription problem), we would still need that child to use a username and password to subsequently authenticate her use of the “verified” credential (the subsequent visit problem).

We know from vast experience with Internet credentialing systems that password authentication fails - and fails often. We know that a black market of “verified” credentials will surface. We know children will share or lose their “verified” credentials. We know child predators will become skilled in guessing and phishing for children’s passwords. We know enterprising children will sell their “verified” credentials. In the frightening case where a child predator is also a parent of a young child, we know that predators will use their children’s “verified” credentials.

Adult Age Verification vs. Child Age Verification

Some vendors claim that online age verification is already being performed when purchasing age restricted goods and services such as alcohol, tobacco, pornography, and online gambling. These applications require the assertion of adulthood, which is a very different objective than asserting childhood.

First, there is a difference in motivation. Adults want to prove they are old enough to engage in the activity, so they cooperate with an adult age verification system. Adults are not motivated to defeat an adult age verification system. However, a child age verification system will be attacked by both adults and children – kids pretending to be adults, kids pretending to be parents, predators pretending to be kids, etc, leading to substantially higher error rates.

Secondly, it is a logical fallacy to equate the failure to prove adulthood as proof of childhood. While rather esoteric, this is an important scientific distinction and it is critical not to confuse the two.

Here is an example: An individual wishing to enter an online gambling site must prove she is 18 years of age or older. Identification and initial subscription may be performed through public records which provide a basis to assert the identity and age of adults. This application of age verification technology can be reasonably effective, depending on the implementation and requirements of the specific application.

However, creating a “kid safe zone” requires the inverse: assertion and proof of childhood. Assume a “kid safe zone” wishing to admit only children under the age of 16. Let’s say Sally is 14. Sally wishes to enter the safe zone and must prove one of two assertions: either that she is really 14 years old, or that she is not some age over 16.

Exploring the first possibility, let’s try to prove that Sally is actually 14. Since there are no public records to this effect, the only reliable and authoritative source of this information is Sally’s birth certificate. We are left with the difficult Initial Subscription problem previously discussed.

Exploring the second possibility, let’s try to prove that Sally is not some age over 16. This is a classic example of the difficult logical problem of “proving a negative.” We would first have to prove that Sally is not a fictitious identity by matching the person at the keyboard to their real identity. The only way to do this is to find a positive match for the information Sally voluntarily provides with some authoritative source (such as a public record) and then authenticating the individual against that identity to the required strength. Since Sally is 14 and has no public records, we’re stuck.

At this point, we fall into another trap: a youth under 18 has no public records. A fictitious identity also has no public records. There is no way to tell the difference. The result is that any predator wishing to impersonate a child can do so simply by fabricating a fictitious identity. This has been proven repeatedly by numerous researchers and child advocates.

Looking at this from the other side, let’s assume that child predator Mallory is an adult and wishes to impersonate a child to enter the safe zone. In order to be correctly denied access to the safe zone, Mallory would have to voluntarily provide accurate information asserting his adult age and allowing his real identity to be matched to public records. *In other words, Mallory would have to willingly cooperate with the process that would eventually block him from the desired resource.*

As you can see, asserting childhood is a very different objective than asserting adulthood and the two must not be confused. While the risks of a child impersonating an adult can be controlled, it is far too easy for an adult to impersonate a child for this to be an effective safety mechanism.

Confusion Reduces Safety

Any system that attempts to determine a child's age and/or family relationships at Internet scale will be easily and frequently circumvented by predators and will result in error rates so high that the system will be counterproductive and confusing to parents and children alike. Should parents tell their kids that "verified" individuals they meet online are more trustworthy than "unverified" individuals? Are areas that admit only "verified" individuals safer? Do such approaches encourage parents and children to let their guard down? Experience clearly demonstrates that motivated child predators will become "verified," creating dangerous wolves in sheep's clothing. The uncertainty and confusion surrounding credentials of dubious reliability will actually make children less safe.

New Risks and Unintended Consequences

Any centralized credentialing system will, by definition, create a massive database of sensitive information about our children. This valuable database will almost certainly be in the hands of a private sector, for-profit vendor. With ever larger data breaches in the news almost daily and concerns about identity theft front-of-mind, this is an unsettling prospect to say the least. Not only do we threaten our children's safety and privacy, but we also expose them to a lifetime of identity-related frauds. Most concerning, a centralized identity system also creates a target list of young children that would be very valuable if it got into the hands of child predators.

Ineffective Security Measures

Age verification systems are predicated on the false belief that creating partitions between "adults" and "children" online will make kids safer. We have demonstrated that age verification systems will fail at such high rates that the partitions will be meaningless and dangerously counterproductive. Moreover, overwhelming research and real-world analogies clearly indicate that such partitions, even if effective, will not help keep kids safe.

Parental consent systems have the objective of empowering parents to control their children's access to online sites. However, numerous methods already exist to achieve this objective including local software filters, software, and hardware policy enforcement mechanisms. Several vendors have for years made excellent filtering software available for free. Microsoft's latest operating system includes such functionality by default. Policy and filtering approaches are far more effective, reliable, and have far less dangerous failure modes than a massive child credentialing system and as such are preferable.

Summary and Recommendations

Age verification and parental consent systems represent a bad risk / reward tradeoff. These approaches fail to make our children any safer and introduce dangerous new risks that could follow our children for many years after their 18th birthdays.

Therefore, I strongly recommend against the implementation of any child credentialing, age verification, or parental consent system as they are ineffective, confusing, and counterproductive.