Evaluating Age Verification Systems

Jeff Schmidt
jschmidt@authis.com

Age Verification is actually two separate and distinct problems, the "Initial Subscription Problem" and the "Subsequent Visit Problem." For a detailed definition and discussion of these problems, please see my Gardian article.

As any Age Verification System must address these two problems, I propose the following taxonomy for quickly and consistently evaluating any approach. General techniques that may be used to address each question are listed in order of descending strength of security with answer "a" providing the highest level of certainty.[1]

The exact placement of techniques in these ordered lists is not critical and may be debatable. It is more important to recognize the general classes and flow from very strong to very suspect techniques when evaluating and comparing various approaches to age verification.

Note that this is strictly a security analysis; no consideration is given to scalability, practicality, or economic factors which are certainly critical in any real-world implementation. However, in general, we find that security strength is almost always inversely proportional to scalability and with exponentially increasing economic cost.

For purposes of this taxonomy, I assume that we are attempting to age verify a child under the age of 18 who does not possess a drivers license or any useful public records.

1. Initial Subscription – how is the existence of the child proven and age data ascertained?[2]

--- Class A: In-person by trusted 3rd parties using authoritative data ---

-- Expected failure rate: < 1% --[3]

a. In-person by a trustworthy 3rd party with authoritative data, namely birth certificate or medical records. Example: Child goes to a police station with his/her birth certificate and is enrolled by a police officer.

---

[1] While there are innumerable minor variations on each of these techniques, most have little impact on security. This is not an attempt to exhaustively list every conceivable option, but rather to categorize and rank the general approaches.

[2] "Bulk" approaches, such as a school or hospital releasing a list of children and ages are excepted. While the source of data may be authoritative, reliably matching bulk records to the appropriate child in order to complete the subscription is fraught with peril.

[3] While I couldn't find any solid numbers on this topic, it seems reasonable that these techniques would fail less than once in 100 chances.

b. In-person by a trustworthy 3rd party with reliable school data. Example: Child is enrolled in school by a DARE Officer; school provides name and approximate or actual age or child provides recent report card.

c. In-person by a trustworthy 3rd party medical professional who performs a biological determination of approximate age.

--- Class B: In person without authoritative data ---

-- Expected failure rate: < 20% --[4,5]

d. In person by a trustworthy 3rd party with no correlating documentation. Example: Child goes to a police station and self-reports age. Police officer enrolls after a "sanity check."

e. In-person by an unreliable[6] 3rd party with proxy data. Example: presenting a state drivers license when purchasing alcohol.[7]

f. In person by someone who has been proven to be a parent or guardian through inspection of authoritative documents such as birth or medical records proving the familial relationship.[8]

--- Class C: Not in person self-reported ---

-- Expected failure rate: > 20% --[9]

g. Not in person using a self-administered biological test such as a bone density scanner.

h. Not in person by someone claiming to be a parent who has been identified and authenticated to some degree (i.e. public records questions) but has not been authoritatively tied to the child in question.[10]

---

[4] Arizona Institutions of Higher Education Report on the Status of College Student Alcohol and other Drug Use in Arizona, 2006. There is a slew of other research that seems to indicate that fake ID usage in bars hovers between 20 – 25%. Since the other techniques in this class are stronger, I use the 20% number as an upper bound for the class.

[5] Literally hundreds of providers of high quality forged credentials were revealed with a quick Google search.

[6] The clerk at a supermarket or the bouncer at a bar is certainly less trustworthy than a police officer.

[7] I include this, the most common "age verification" scenario, as a reference point even though it is not a solution for those under 18.

[8] Not In Person but proven relationship to child seems feasible, but I can't think of a way to prove the existence of and a relationship with a child without in person inspection of authoritative documents, so that option does not appear in this taxonomy. If it were possible, it would appear next.

[9] This is hard to estimate, however, we know that these techniques are weaker than Class B techniques and therefore can, in general, be expected to fail more often.

[10] In fact, we don't even know if the child exists.

i. Not in person by multiple persons claiming familiarity with the child but have not been positively identified and authenticated.

j. Not in person by a single person claiming to be a parent who has not been positively identified and authenticated.

k. Not in person - possesses a valid credit card number.

l. Not in person - self provided.

2. Subsequent Visits – how to we authenticate the individual's use of the age verified credential during subsequent visits?

--- Class A: "Strong Authentication" as defined by the IETF ---

a. Multifactor authentication – any combination of biometric, token, and shared secret (password) authentication techniques.

-- Class B: "Weak Authentication" as defined by the IETF ---

b. Single factor biometric – fingerprint, retinal scan, etc.

c. Single factor token – RSA SecureID, smart card, perhaps a mobile phone.[11]

d. Single factor shared secret – password, credit file data, etc.

[11] The mobile phone must be cryptographically tied to the user in question to qualify as an authentication token.