Statement by
Pat McGregor
Chief Information Security Architect
Intel Corporation
Before the Commission on Online Child Protection
9 June 2000
Washington, D.C.

Mr. Chairman and members of the Commission, thank you for the opportunity to speak today before this hearing of the Commission on Online Child Protection. I am glad of the opportunity to offer you my insights into technologies for age verification and the processes that will be required to support them.

Introduction

The problem of age verification on the Internet is, intrinsically, no different from the problem authorizing any user based on a role or criterion they possess. Age verification is a special case only because of the sensitive issue of children's access to material that their parents or guardians might find objectionable. Otherwise, the processes and decisions which support accepting and validating credentials and granting appropriate access are the same faced by corporations, ISPs, and movie theatres. My 11-year-old son summarized the issue neatly the other day, when I asked him how he thought we could prove someone's age over the net. He said, "If we can't see them, how can we prove they aren't lying about how old they are?"

Authentication Methods

There are four major methods that could be reasonably used for identifying and authorizing access to material across the net. Those methods are, generally, ID and Password, Biometric, Digital Certificates, and Proxies. Let me discuss briefly each of these methods and their advantages and drawbacks.

ID & Password

IDs and passwords are acceptable for access to material that does not need to be protected with high assurance. They are, as most of us are aware, vulnerable to cracking, theft, and other attacks. In addition, humans don't use passwords effectively because of differences in ability to remember passwords, remember IDs, and the general unwillingness to use well-known security processes (such as frequent changes or one-time passwords) that make IDs and passwords more effective. On Internet scale, the logistical issues presented by 25 million children[1], each with an account on every site they might want to access, are too many to discuss in any depth. Even the prospect of a central credential storage and authentication service, similar to the Microsoft Passport, is subject to the problems with children remembering IDs and passwords and taking proper precautions to protect those credentials.

Biometrics

Biometric technologies offer some interesting advantages for identification and the creation of credentials that can be linked with a high degree of assurance to a given human being. However, even with adults whose facial characteristics are relatively stable from day to day, the problems of changing biometric characteristics from morning to evening make for problems with consistent authorization to assets. With children who can grow and change substantially from one month to the

[1] Grunwald Associates. *Children, Families, and the Internet 2000 survey*. June 2000. http://www.grunwald.com/survey/survey_content.html

next, the problems of capturing and distributing valid biometric signature files for a rapidly changing population seem too complex for implementation on a large scale.

Digital Certificate

Digital certificates have the advantage over biometrics in that they are not based on characteristics that can change rapidly. They can be issued in a cryptographically secure fashion so that they are less vulnerable to cracking than other forms of credentials. However, certificates in isolation, separate from a security or authorization process, offer little advantage over any of the other forms of authorization and credentialing.

Proxies

I include proxies in this list because they can be configured to prevent access from a specific client to a given range of hosts. Parents find the use of proxies, or screening software, of value in preventing access to material they find objectionable when their children are surfing the Internet from home or school. The problem, of course, is when access is attempted from a client not behind the proxy, or when the password for the proxy is compromised and the filtering settings are changed.

Management Issues

The management issues and security processes for all of the authentication methods are the big obstacles in making any system of age validation work. Even in a corporation the size of Intel, with 80,000+ employees to track, we find that keeping credentials and access control lists current takes a major expenditure of staff resources. Multiplying the problem to include every child under 13 in the United States as well as every web server that might host objectionable material seems far too vast to be appropriately managed. Let me discuss some of the larger issues.

Security Process

Credentials can only be used to make a security decision in context of an appropriate security process. For example, look at the process you go through when you check a driver's license for identification. When you check a person's driver's license, you're doing a biometric test (face vs. picture). That involves: taking a sample (of the face), reading in the template (picture), and doing a comparison. You do all three of those steps inside your own body -- presumably an environment you have some assurance has not been compromised. When we do this sort of credential checking over the net, we must rely on some other entity – a card reader, a biometric device, or a keyboard – which is not under our control. The computer that the user wants to access must rely on another entity to take the sample or take in the credentials. It can compare the presented credentials against the records in its access database, but the process is as weak as the element that takes the sample -- and in the case of a computer in someone's house or school or library, that element is weak and untrustworthy.

Another security process we must look at is the issuing of credentials. If we mandate that children's credentials will be issued at, say, their school, we are requiring a security process infrastructure which most schools are not prepared to administer. Difficulties include the logistics of keeping track of highly transient populations, the varying implementation of the process in different school districts, and the fact that most school districts are barely funded for one computer technician, much less an administrator who will manage the issuing and revocation of credentials. In addition, not all children attend public school, and provision would have to be made for credentials for children at private schools, children who are homeless, undocumented aliens, or who do not attend school for other reasons, or who are home-schooled.

In addition to the simple mechanics of issuing and revoking credentials, we must consider that there may be disagreement over what age it is appropriate to begin issuing credentials. A Grunwald Associates survey this week says that children online range between two and seventeen years of age.[2]

[2] Martin Stone. More Online Kids, More Online Moms. E-Commerce Times, June 8, 2000. http://www.ecommercetimes.com/news/articles2000/000608-nb1.shtml

Do we issue credentials at birth? At entry into Kindergarten? When their parents purchase a home computer? How do we reconcile differing jurisdictions with differing standards or mandates?

Lost credentials

Human beings lose things. Children, in particular, lose things frequently. To be useful for allowing children access to the Internet in a protected fashion *wherever the child is* – not just at home or in the school – their credentials must be stored on some transportable media, such as a smart card, a watch fob (*a la* the fast sale gas pumps), or other easily carried item. If you have children, you can probably count the number of times they have lost sweaters, lunch boxes, house keys, and library books. I don 't want to think about how quickly my son could lose a plastic smart card, or how many times we would have to replace it in the course of a year.

Stolen or Forged Credentials

As my son said, one of the problems in this whole system is the fact that some people are not honest. They will lie about their age, their permissions, and their intent in accessing some material. We do not now have a good security process for identifying stolen or forged credentials (think of the bouncer at a bar reading driver's licenses, or a catalogue clerk accepting a stolen credit card over the phone, or the use of stolen telephone calling cards). If we go to a system where all children have children's credentials – or one where all adults have adult credentials – we must also implement a security infrastructure to do real-time validation of the credentials themselves, necessitating a reporting system where stolen credentials can be reported, forged credentials listed for confiscation, and new ones re-issued quickly.

Revocation of Credentials

When a child reaches 13 (or 18, under some proposals), they would no longer need credentials to validate their age. Some entity must revoke their credentials, in effect declaring them to be "old enough" to access any information they please. The logistical problem for this revocation can be highly complex. Can the school the child is in when they reach an acceptable age revoke the certificate, or must the school or post office or other agency make the revocation? Will all credentials be of the same manufacture, allowing for easy interoperability of systems, so that the revoking body can notify the issuing body that the certificate has been revoked? Or will the certificates expire on the date of the child's birthday, since the birth date must be known to issue an appropriate certificate? What happens if a school board in Oregon decides that the issuing school must actively revoke a certificate, while a school board in Florida uses an auto-expiration scheme? What will happen to the child who changes school districts? And what happens if the parents wish, for example, to keep controls on access for a child who is 13 but whom they feel is not sufficiently mature to handle adult material?

Global Issues

Since the Internet is a global entity, we must touch on the issues involved in giving access to materials outside the United States. It is in this global context that I fear most of the proposals to limit children's access to adult material will break down.

What is acceptable material for 13- or 18-year-olds in a European or Asian country may not be considered appropriate by parents (or school boards, or county boards of commissioners) in the United States. In fact, what is considered appropriate by many parents in Idaho may not match expectations of parents in Florida. We cannot enforce child protection guidelines in countries outside the US; therefore, there will always be a way for children to find adult material. Nor can we reasonably expect to limit or filter content based on domain name; we seldom use the ".us" domain identifier in the US, and many web sites based in other countries do not use their country's domain identifier. My expectation is that if the US tries to regulate access to content on US sites, the adult material sites will simply change their service providers to those based outside the US.

The nature of the Internet is that information can almost always be reached by taking a different path to the source. I am reminded of the policy of my local grocery store to hide the covers of Cosmopolitan, Fitness, and other magazines that sometimes have "suggestive" pictures on the

front by using a metal face shield over the magazine rack. Interested children will go to a store without the blinder policy, or a library that carries the magazine, or to the home of a friend whose parents subscribe. Or, even, to the website for that magazine.

Roles and guidance

We cannot conclude any discussion of age verification and access by children to adult material without at least a brief discussion of the roles of various entities in the access decision process.

Familial values

It is at home where the real responsibility lies for age-appropriate access to the Internet and its resources. The adult responsible for a child should pay attention to their children's surfing habits, discuss what is and is not appropriate according to their family's value systems, and use the family discipline process to enforce that access. With all the problems cited above, the government (ours or any other) cannot take the place of this critical familial responsibility. It may be possible to provide a mechanism to assist in enforcing these family standards, but we have seen over and over again that "one size fits all" government standards are unworkable with the wide variety of family choices in the United States.

Schools

While it might be possible for schools, libraries, post offices, and other governmental entities to take on the role of credential issuer and manager, I am particularly concerned that schools, asked to take on yet another non-educational role, will simply be unable to resource the infrastructure required appropriately. We cannot ask teachers to add any more tasks into their days; they already have far too few minutes per day to actually teach. Public schools are marginally resourced for many of their functions today; a major influx of funding and staff would be required to handle this new responsibility.

Summary

There are many technologies for authentication and authorization on the market today, and more are being devised every year. The problem of age verification for children will require not only legislated standards for credentials, but also the implementation of an infrastructure that will support the use and management of these credentials. Before any steps to require age validation are taken by this commission, I strongly recommend that the implications and support requirements be evaluated in depth. Without the supporting infrastructure, any system to enforce age-appropriate access to online material will be unworkable, unenforceable, and an expenditure of resources that could more effectively be used elsewhere.

I leave you with one more thought from my personal management and child-raising philosophy. "Never give an order you can't enforce."

Thank you.