



# Secure Identities

Vinton G. Cerf • Google

Security is a major focus of attention for operators and users of the Internet and its many applications. Among the thorny problems still inadequately addressed is identity authentication for purposes of associating a particular user with particular services and authorizations. What we seek is a way to identify users such that forging credentials is difficult for adversaries, while providing strong authentication of their chosen identifiers remains easy and convenient for users.

Note that, here, I distinguish “identifier” from “identity.” An identifier doesn’t necessarily need to reveal personal information (such as name, address, birth date, or phone number). Rather, it need refer only to a unique symbolic string that can be repeatedly and strongly validated without compromising its associated credentials or necessarily revealing a user’s personal identity. What’s needed, in effect, is a way to confirm that an online service has “seen” a user before and can reliably identify him or her as the same user (within the scope and strength of the identification and validation method used).

Any such scheme must be easy for users to employ and for online services to validate. The method must be sustainable in that its costs are affordable and don’t impose such a burden on users that they abandon it owing to inconvenience.

In the online environment, we commonly use identifiers to associate a user with a particular service and privileges, so commonly accepted methods should exist for achieving these goals that are applicable across a range of applications and services. We also want these methods to be readily accessible to service providers and users.

A recent development within the US government is its National Strategy for Trusted Identities in Cyberspace (NSTIC), which is intended to improve significantly the strength of identity

credentials while increasing protection of personally identifiable information. The US government is also applying this idea for its own purposes, as you can see in the Federal Identity, Credential, and Access Management (FICAM) roadmap (see [www.idmanagement.gov/documents/FICAM\\_Roadmap\\_Implementation\\_Guidance.pdf](http://www.idmanagement.gov/documents/FICAM_Roadmap_Implementation_Guidance.pdf)).

Among the desirable properties of an identity management system is that users be able to hold more than one identity and that some or even all of the associated identifiers need not be strongly bound to personally identifiable information. For some applications, knowing that a party is known under the authenticated identifier is more than enough.

Passwords have weaknesses that are by now very well documented. Conventional passwords are typically re-used until changed and might be used to authenticate more than one identifier (I use the term “authenticate” rather lightly here). The NSTIC proposition offers much stronger standards for authentication, including cryptographically generated passwords that, even if exposed, can’t be re-used (for some very long time, if ever). These are sometimes imprecisely called “one-time passwords.”

The NSTIC idea is grounded in several important principles. The private sector should be able to offer credentialing services that users can employ for multiple applications. The ecosystem supporting such credentialing should permit competitive offerings while assuring minimum levels of proof against forgery and strength of trust.

The system of strongly authenticable identifiers should also be interoperable so that users can select among several providers through which they can access a range of online applications. This system should also allow software

*cont. on p. 95*

cont. from p. 96

to act on a particular user's behalf, generating on-demand authentication even without user intervention – for example, by having the user enable the authenticating system for autonomous if local operation. An active USB device, for instance, might require that a user provide an activation PIN or password, after which it will continue to dispense strong authenticators on demand until disconnected from its USB socket.

What's important about the NSTIC proposition isn't that it's government operated but rather that it establishes security and compatibility standards so that private sector offerings are interoperable and of comparable strength.

The US National Institute of Standards and Technology's involvement

to foster the development of standards for strong identifier authentication is facilitative in nature. This isn't a National Identity program. The US government can, however, establish standards for its own use with government employees and might also require that contractors use comparably strong and compatible methods for strong identifier authentication that can also help validate personal identity, if necessary.

It appears possible to implement systems compatible with a strategy that would let a single device house and authenticate more than one identifier so as to avoid the need for multiple devices. This would let users employ distinct identifiers for different services, not unlike the notion of multiple credit cards to allow for consumer choice of credit and debit services.

As I read it, the program's intent and effect is to establish both a technical basis and sustainable ecosystem for competing and interoperable identifier authentication products and services that achieve minimum security levels. Such mechanisms can strongly enable the healthy evolution and expansion of online products and services. To the extent that the standards are adopted broadly beyond US borders, the effects are even more important for the security of online businesses and consumer Internet use on an international basis. □

Vinton G. Cerf is vice president and chief Internet evangelist at Google. Contact him at [vint@google.com](mailto:vint@google.com).

**cn** Selected CS articles and columns are also available for free at <http://ComputingNow.computer.org>.

## IT Professional

TECHNOLOGY SOLUTIONS FOR THE ENTERPRISE

# CALL FOR ARTICLES

IT Professional seeks original submissions on technology solutions for the enterprise. Topics include

- emerging technologies,
- cloud computing,
- Web 2.0 and services,
- cybersecurity,
- mobile computing,
- green IT,
- RFID,
- social software,
- data management and mining,
- systems integration,
- communication networks,
- data center operations,
- IT asset management, and
- health information technology.

We welcome articles accompanied by Web-based demos. For more information, see our author guidelines at [www.computer.org/itpro/author.htm](http://www.computer.org/itpro/author.htm).

**WWW.COMPUTER.ORG/ITPRO**



This article was featured in

# computing **now**

ACCESS | DISCOVER | ENGAGE

For access to more content from the IEEE Computer Society,  
see [computingnow.computer.org](http://computingnow.computer.org).



**IEEE**

IEEE  **computer society**

Top articles, podcasts, and more.



[computingnow.computer.org](http://computingnow.computer.org)