Cyberspace 2025—Biometrics to Support Trusted Identities

Dr. Stephanie A. C. Schuckers, Clarkson University, April 15, 2014

In our society with the ubiquity of electronic mediums, there is a need to establish a trusted relationship between individuals and between individuals and organizations in order to support electronic commerce (including mobile transactions), worker and employer interactions, delivery of benefits from governments, movement of individuals across international borders, social connections, and delivery of quality healthcare. Creating and enabling trusted relationships makes it more difficult for those who seek to undermine and destroy that trust through cybercrime, terrorism, and identity theft[1]. There are many ways to establish a trusted relationship. These include: "What you have?" (birth certificates, drivers licenses, credit cards, passports, key); "What you know?" (passwords, PINs, mother's maiden name, address, email, phone number, Social Security Number); and "Who you are?" (personal traits, biometrics). Biometrics is defined as "automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics". Previously only used in limited cases, there has been a decade of dramatic expansion of biometrics for government and commercial applications as one component in the processes needed to establish identity as part of a trusted relationship[2]. ***Incorporation of biometrics not only promotes security but also reduces the burden on individuals by providing convenience, ease of use and reduction of the amount of private information that would need to be revealed repeatedly in order to (re)establish a trusted relationship.*** Depending upon the transaction, multiple levels of trust can be created by combinations of different forms of authentication. NSTIC and FIDO alliance are efforts emerging to create an identity ecosystem to support identity management in cyberspace. While there has been a positive trend in the past decade, there are two biometric research challenges which are critical to support trusted identities in cyberspace for 2025: (1) Security and privacy and (2) Usability.

Addressing Security and Privacy in Biometrics

As with other personal information such as demographic information, biometric data must be protected and remain confidential. Continuing to advance the state of the art will further the ability to use biometrics and reduce the need for the release of other personal information to confirm identity when other authentication methods such as passwords are lost or forgotten. This is critical to keeping personal information safe, while ensuring the free flow of data for the right people at the right time. Some examples of privacy enhancements in biometric addressing weaknesses, such as biometrics "are not secret" and "cannot be changed", include:

- *Template protection:* biometric matching is performed in the encrypted domain
- *Cancelable biometrics*: a transformation of biometric features such a template can be cancelled
- *Liveness detection*: the protection from an attack where an artificial biometric is used

Privacy and security are often spoken in terms of tradeoffs, i.e., giving up privacy in order to achieve security. The research goal in this area is to change the paradigm to achieve both privacy and security.

Enhancing Usability of Biometrics Through Continuous Authentication

Active (continuous) authentication can be used to continuously validate that it is the same, authorized user who is accessing the "system" and can be used as a seamless way to establish identity without specific action by the user. Active authentication can be achieved via behavioral biometrics such as mouse and keystroke usage patterns, gestures, accelerometer patterns, heart beats, etc. As devices interact more closely with the user (e.g., "smart" watch with heart beat sensor), this information can be used to confirm identity to support transactions.

In summary, research, close collaboration between industry, government and academia, and investment in education will continue to make the United States the world leader. In biometrics, this investment can reap benefits by improving our trust in cyberspace, by protecting our national security, and by stimulating technological developments that will drive the economy in the future.

[1] "Making Online Transactions Safer, Faster, and More Private," *National Strategy for Trusted Identities in Cyberspace.*

[2] "The National Biometrics Challenge 2011," 2011.