STRATEGIC **INSIGHTS**

Putting a Familiar Face on Key Verification
(Published in *Government CIO*, 2014)

By Anne Dunne

STRATEGIC RESULTS

Putting a Familiar Face on Key Verification

As consumers, retailers and banks make more use of customer accounts and data thieves grow more sophisticated at hacking into them, it is increasingly important to develop methods of communication security that are not only reliable but also user-friendly.

The more we make communication secure, the more we are likely to come into conflict with the desire to make communication easy and transparent to users. Consumers are finally being warned against using familiar words or numbers they easily remember as their passwords. Microsoft Corporation, for example, tells them that a strong password:

- Is at least eight characters long
- Does not contain their user name, real name or company name
- Does not contain a complete word
- Is significantly different from previous passwords
- Is made up of upper-case letter(s), lower-case letter(s), number(s), and keyboard symbols(s)
- Isn't the same as a password the consumer uses elsewhere

And even these rules aren't strong enough for truly secure communication. For that purpose, people are sent further up the ever-more-shaky ladder of communication security into the realm of cryptography, in the form of key verification public key/asymmetric cryptography.

For example, Pretty Good Privacy (PGP) or GnuPG (GPG) programs are used to provide cryptographic privacy and authentication for data communication via secure emails. These forms of public-key/asymmetric cryptography employ key fingerprints to confirm the identity of the sender or recipient. Communication security is ensured because a message encrypted at one end of a transmission can only be decrypted by an authorized user at the other end.

Keys used in secure email and websites are commonly encrypted and decrypted in a form readily comprehensible to computers—hexadecimal strings. That is, key fingerprints typically appear in a language designed to be recognizable to computers, using the letters "a" through "f" and the numerals "0" through "9."

To a computer, this is native language. To most people, it is gobbledegook. So in web browsers, key verification is made transparent (invisible) to the user by creating a chain of trust that validates the key of the remote site. This became a problem, however, when third-party Certificate Authorities (CAs) became known to have issued keys arbitrarily.

New systems such as Domain Name System Security Extensions (DNSSEC) and the Electronic Frontier Foundation's SSL Observatory have been developed and deployed. The centralization of these systems is a weakness, however, and they do not fundamentally address the problem of placing blind trust in some outside authority.

Finally, public key/asymmetric cryptography still requires use of obscure passwords and is anything but user-friendly. When Edward Snowden decided to share secrets of the National Security Agency (NSA) with journalist Glenn Greenwald, he tried to get the reporter to use GPG when corresponding with Snowden. He sent Greenwald a remarkably helpful and detailed instructional video on "GPG for Journalists." Greenwald didn't bother to use it.

Instead of forcing people to navigate this inhuman maze, why not make use of something humans naturally do well?

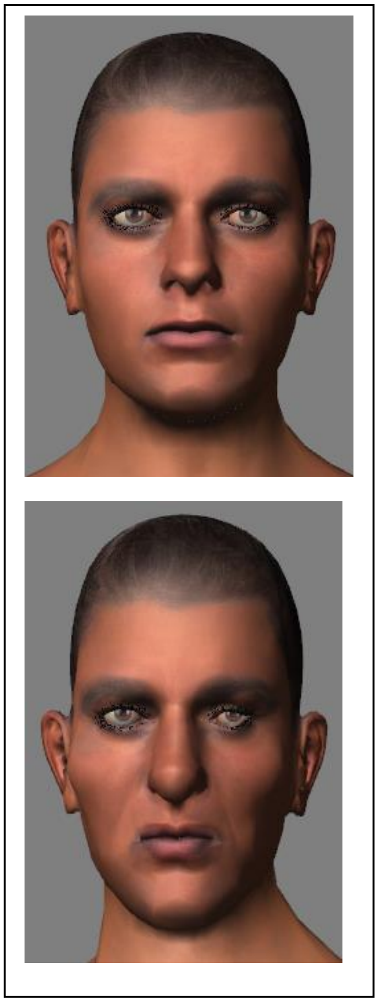
Under contract with the Defense Advanced Projects Agency (DARPA), we explored this very possibility.

One human trait that is either innate or develops rapidly from very early infancy onward is *face recognition*. Much of the research into face recognition has been gathered by computer vision researchers whose goal has been to create automated face-recognition systems that can equal, and eventually surpass, human performance. In the process of trying to get computers to recognize faces, however, these researchers also confirmed that humans are already very good at it. People can reliably recognize faces even in very low-resolution images.

So we inverted the concept of how to use face recognition. Instead of teaching it to computers, we explored ways humans could use this natural trait to communicate better when they do it via computer.

The vision was to take advantage of the brain's natural cognition in order to optimize encryption, and the challenge was to enhance both the usability and security of encryption by improving the method of comparing key fingerprints. The resulting software algorithms enable public key fingerprints to be depicted as unique graphical representations. These algorithms take advantage of the natural trait of face recognition in a way that improves security of email messages through creating effective key visualization methods that are quick, accurate and extremely difficult to defeat.

Putting a Familiar Face on Key Verification



When the key fingerprint is represented as a memorable face or other graphic depiction, it can be quickly and easily compared to a known key visualization. For example, if the key fingerprint is depicted as a face, the tedious task of remote identification becomes as simple as asking the user, “Do you remember this face?” Our test subjects quickly and reliably recognized the difference between the two shown here, although many people would have difficulty distinguishing between these hexadecimal strings:

> 43:51:43:a1:b5:fc:8b:b7:0a:3a:a9:b1:0f:66:73:a8
> 43:51:43:a1:b5:fc:8b:b7:0a:3a:a9:b1:0f:68:73:a8

Even if someone steals your laptop loaded with all your passwords and passphrases, you would remember your mother’s face.

Cryptographic key visualization can be used to aid any encryption technology including public key infrastructure (PKI) or web of trust. The method is unique and nearly impossible to forge.

The visualizations are designed to require relatively un-intensive computations. Besides faces, they include:

- Color patterns
- Graph points
- Elliptical curves
- Maze-like patterns
- 3-D objects

Using this technology could enhance messaging security by improving usability of public key/asymmetric cryptography. It makes the process of comparing key fingerprints faster, more reliable and intuitive to the user.

References:

Microsoft Corporation, 2014, Tips for creating a strong password, http://windows.microsoft.com/en-us/windows-vista/tips-for-creating-a-strong-password, accessed 10 October 2014.

Sinha, P., Balas, B, Ostrovsky, Y., and Russell, R., 2006, Face recognition by humans. *Proceedings of the IEEE,* 94, 1948–1962.

Putting a Familiar Face on Key Verification

Peterson, A., 2014, “Edward Snowden sent Glenn Greenwald this video guide about encryption for journalists. Greenwald ignored it.” *The Washington Post*, May 14, 2014.

STRA
TEGI
CRES
ULTS

Shared Ambition, True Partnership

STRATEGIC RESULTS works shoulder to shoulder with civilian government and military clients to help them deliver on their service missions, whether ensuring citizen safety and well-being or making discoveries in health, energy, and science.

For more information, email anne@strategicresults.com

For more information about Strategic results, visit www.strategicresults.com