The long history, and short future, of the password

May 4 2017, by Brian Lennon

An artist's depiction of the 'shibboleth incident.' Detail from art by H. de Blois. Credit: The Bible and Its Story Taught by One Thousand Picture Lessons, vol. 3, edited by Charles F. Horne and Julius A. Bewer, 1908

In Western history, the concept of the password can be traced as far back as the so-called "shibboleth incident" in the 12th chapter of the biblical Book of Judges. In the chaos of battle between the tribes of Gilead and Ephraim, Gileadite soldiers used the word "shibboleth" to detect their enemies, knowing that the Ephraimites pronounced it slightly differently in their dialect. The stakes were life and death, we're told, in a confrontation between Gileadites and a possible Ephraimite fugitive:

"Then said they unto him, 'Say now Shibboleth'; and he said 'Sibboleth'; for he could not frame to pronounce it right; then they laid hold on him, and slew him at the fords of the Jordan."

The literary history of the password also includes the classic tale "Ali Baba and the Forty Thieves," invented in the 18th century by the French Orientalist Antoine Galland. Used in the tale to open a magically sealed cave, the invocation "Open, Sesame!" enjoys broad currency as a catchphrase today, not only in other literary, cinematic and television adaptations of the tale itself, but in many other contexts as well.

Password security was introduced to computing in the Compatible Time-Sharing System and Unics (Unix) systems developed at the Massachusetts Institute of Technology and Bell Laboratories in the 1960s. Today we use passwords to restrict access to our personal computers and computing devices, and to access remote computing services of all kinds. But a password is not a physical barrier or obstacle,

like a lock on a gate. Rather, it is a unit of text: that is to say, written language. As an important part of the linguistic history of computers, password security links my research in the history of writing to my interest in the early history of computing. But it is an episode in that history that may now be coming to an end.

In the earliest civilizations, writing was used to record financial and other administrative transactions, ensuring that records could be consulted in the case of disputes over debt, land ownership or taxation. Soon, there was another use for writing: what we now call mail. Writing made it possible to communicate without being physically present, because a written message could stand in the writer's place.

When I use a password, it also stands in my place. The password represents me within a virtual or nonphysical system, regardless of whether I am physically present, entering a passcode on a smartphone or a PIN code at an ATM, or physically absent, connecting remotely to my bank with a web browser. Anyone else who knows my password can also use it this way.

This characteristic of password security, which has its roots in writing's (necessary and useful) dissociation from the writer's physical presence, is also the root of its problems. Poorly chosen and repeatedly used passwords are easy to guess, either through computational techniques (such as the "dictionary attack," which might test all known words and word combinations in a particular language) or so-called social engineering (that is, tricking someone into disclosing a password).

Once it has been guessed, there isn't much to prevent a password from being used for unauthorized purposes, at least until the theft is discovered. But even the strongest password, a sequence of alphanumeric and punctuation characters utterly devoid of linguistic meaning and long enough to defeat automated password guessing by

software running on the fastest processor hardware available to a professional criminal (these days, that means international organized crime), can be used anywhere and at any time once it has been separated from its assigned user.

It is for this reason that both security professionals and knowledgeable users have been calling for the abandonment of password security altogether.

Looking to introduce new methods of authentication, device manufacturers are moving toward biometrics, from the fingerprint sensors on any recent smartphone to Android 4.0's Face Unlock feature, iris or retina scanning and others. It seems unlikely that password security will last anywhere near another half-century.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation