**Authentication, 9/20/2018**

* Authentication is an ancient security requirement:
	+ Judge 12:5-6
	+ [**shib**-*uh*-lith, ‐leth]

1. a peculiarity of pronunciation, behavior, mode of dress, etc., that distinguishes a particular class or set of persons.

 <http://www.dictionary.com/browse/shibboleth>

* Authentication is closely closely-related to identification and authorization, although they are distinct concepts:
	+ Identification—Who are you?
		- Example: temple recommend. Identification, but no authentication.
	+ Authentication—Prove it.
		- Example: Testing center: show ID, give you access to take a test.
	+ Authorization—This is what you can do.
		- Example: possessing a key, no identification.
* Authentication usually happens in three ways:
	+ Something you know
	+ Something you have
	+ Something you are
* Passwords
	+ The most common example of something you know.
	+ Passwords are ancient:

“The use of secret words to authenticate humans has ancient origins. The concept dates at least as far back as the military of ancient Rome, which developed a careful procedure for circulating daily signa or “watchwords” to prevent infiltration as documented by the historian Polybius in 118 BCE [237]. It also appears in folklore, famously in the tale of Ali Baba and the forty thieves (first translated into English in 1785 [296]), with the protagonist using the phrase “open sesame” to unseal a magical cave. Ominously, Ali Baba’s greedy older brother Qasim forgets this password during the course of the story with disastrous consequences.”

—“ Guessing human-chosen secrets,” Joseph Bonneau, p. 19, <http://www.jbonneau.com/doc/jcb82-thesis.pdf>

* + Passwords are sort of an oxymormon: hard to guess, but easy to remember.

* Security recommendations by security experts (One of the top five recommendations of security experts (<https://www.usenix.org/system/files/conference/soups2015/soups15-paper-ion.pdf>):
	+ Use unique passwords.
		- According to a study of 29 million people, 38% reused their passwords: <https://arxiv.org/pdf/1706.01939.pdf>
	+ Use strong passwords.
		- Use passphrases, not passwords.
	+ Uses a password manager.
		- Use a password manager, like 1Password, LastPass, others.
	+ Use two-factor authentication.
* Something you have:
	+ One-time codes
	+ Access cards
* Something you are:
	+ Biometrics like fingerprint scans, iris scans
	+ iPhone 5S fingerprint hack
		- <https://blog.lookout.com/blog/2014/09/23/iphone-6-touchid-hack/>
		- <https://blog.lookout.com/blog/2013/09/23/why-i-hacked-apples-touchid-and-still-think-it-is-awesome/>
		- <https://www.youtube.com/watch?v=HM8b8d8kSNQ>
		- Face ID hack:
			* <https://www.youtube.com/watch?v=Y85pP35WPoY>
			* <https://www.wired.com/story/hackers-say-broke-face-id-security/>
			* [http://www.bkav.com/d/top-news/-/view\_content/content/103968/bkav%92s-new-mask-beats-face-id-in-twin-way-severity-level-raised-do-not-use-face-id-in-business-transactions](http://www.bkav.com/d/top-news/-/view_content/content/103968/bkav%EF%BF%BDs-new-mask-beats-face-id-in-twin-way-severity-level-raised-do-not-use-face-id-in-business-transactions)
* Someone who knows you:
	+ Facebook’s trusted contacts: <http://fieldguide.gizmodo.com/how-to-make-sure-you-never-get-locked-out-of-your-faceb-1787444461>
* Multi-factor authentication
* Why passwords persist: Deployability. Passwords have zero marginal cost, little start-up cost, and are easy for developers to implement.
	+ Joseph Bonneau, [Cormac Herley](https://www.microsoft.com/en-us/research/people/cormac/), Paul C. van Oorschot, Frank Stajano, <https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/QuestToReplacePasswords.pdf>