Authentication beyond Passwords

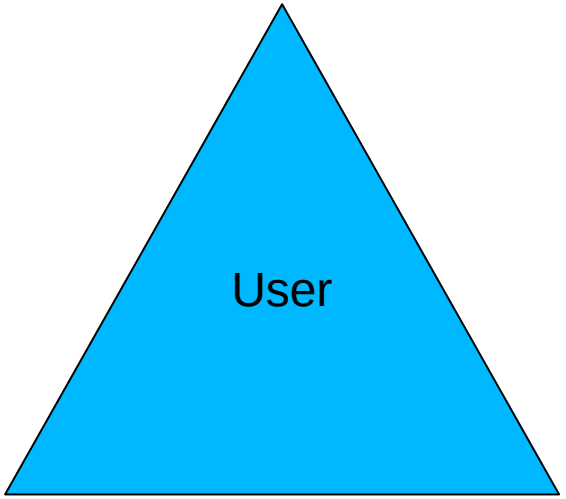
Prof. Ravi Sandhu
Executive Director and Endowed Chair

February 8, 2013

ravi.sandhu@utsa.edu
www.profsandhu.com

User Authentication

Something you know
e.g., passwords



Something you have
e.g., token, smartcard

Something you are
e.g., fingerprint

Single factor
Multi factor

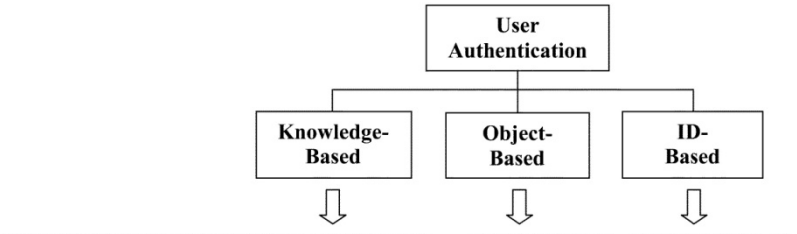
Primary
Secondary

Weak
Strong

Single sign on
Reduced sign on

Reset
Revocation

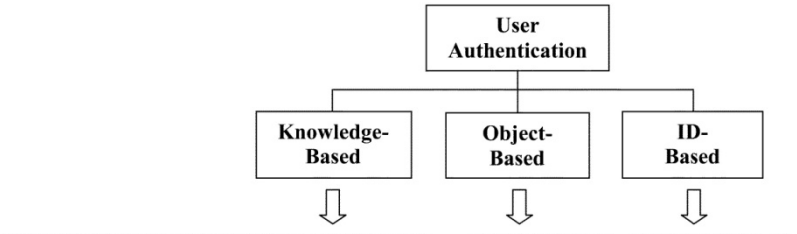
Gorman 2003



		Knowledge-Based	Object-Based	ID-Based
Commonly Referred to as:		Password, Secret	Token	Biometric
Support Authentication by:		Secrecy or obscurity	Possession	Uniqueness and personalization
Security Defense:		Closely kept	Closely held	Forge-resistant
Example	**Traditional:**	Combination lock	Metal key	Driver's license
	Digital:	Computer password	Key-less car entry	Fingerprint
Security Drawback:		Less secret with each use	Insecure if lost	Difficult to replace

"The focus of this paper is a comparison of human authenticators. Comparison factors are security, convenience, and cost. The latter two factors are relatively straightforward and are described only briefly in this paper; however, security as measured by vulnerability to applicable attacks is not so straightforward and thus constitutes the bulk of the paper."

Gorman 2003



		Knowledge-Based	Object-Based	ID-Based
Commonly Referred to as:		Password, Secret	Token	Biometric
Support Authentication by:		Secrecy or obscurity	Possession	Uniqueness and personalization
Security Defense:		Closely kept	Closely held	Forge-resistant
Example	Traditional:	Combination lock	Metal key	Driver's license
	Digital:	Computer password	Key-less car entry	Fingerprint
Security Drawback:		Less secret with each use	Insecure if lost	Difficult to replace

"The focus of this paper is a comparison of human authenticators. Comparison factors are security, convenience, and cost. The latter two factors are relatively straightforward and are described only briefly in this paper; however, security as measured by vulnerability to applicable attacks is not so straightforward and thus constitutes the bulk of the paper."

Must consider entire lifecycle

Nothing is straightforward in cyber security

Gorman 2003

RSA SecurID SID900

RSA SecurID SID700

RSA SecurID SD200

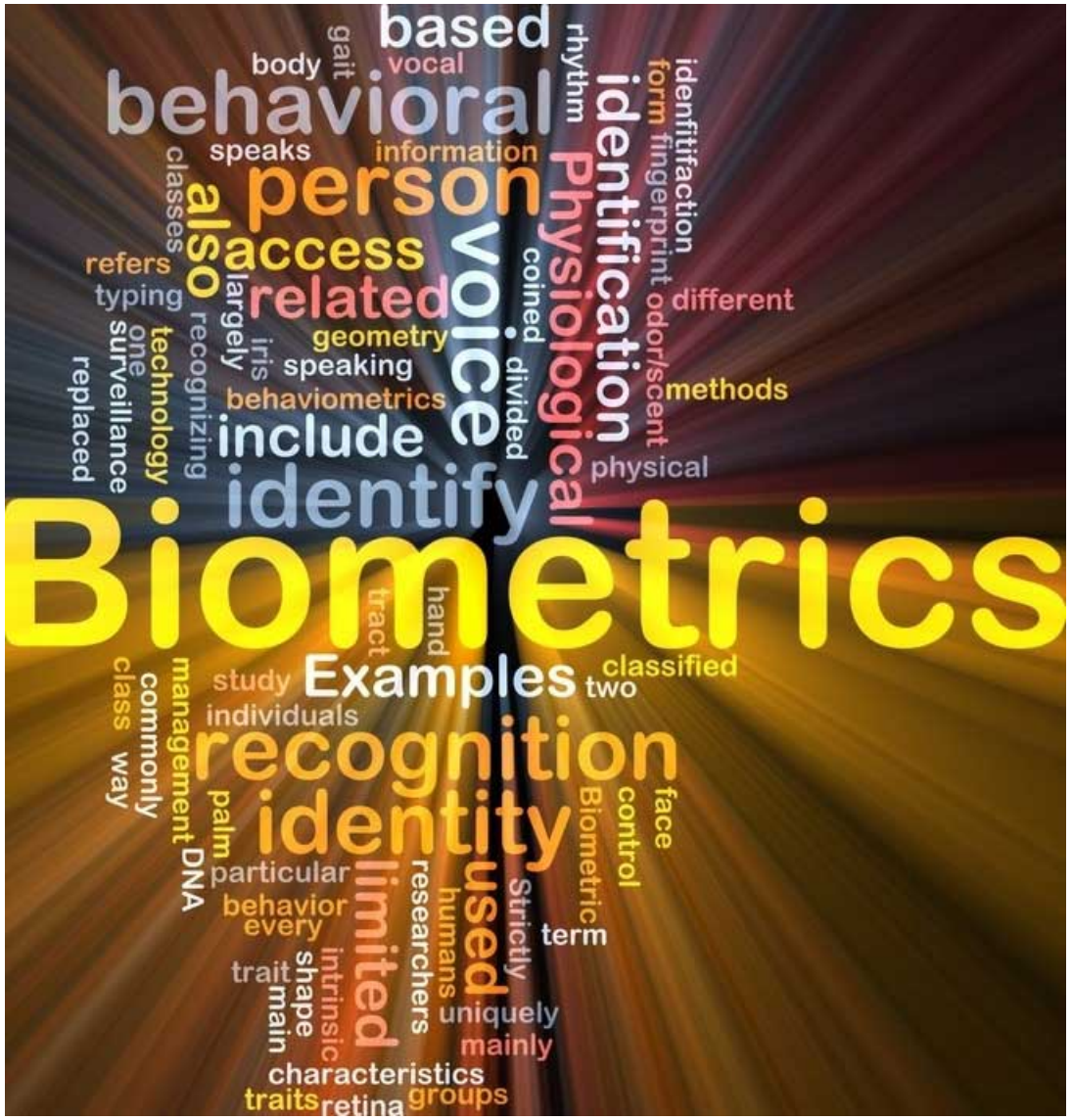
RSA SecurID SID800

RSA SecurID SD520

BlackBerry with
RSA SecurID software token

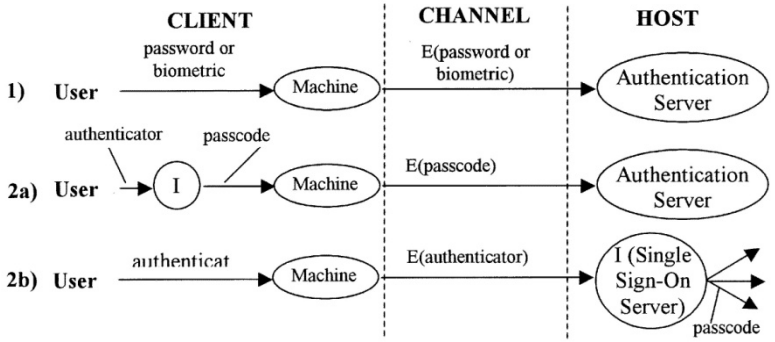
- Born in early 1990s
  - symmetric key based
- Biggest attacks to date:
  - lost master secrets
    - 1st half 2011, revealed June 2012
  - man-in-the-middle
    - July 2006

Gorman 2003



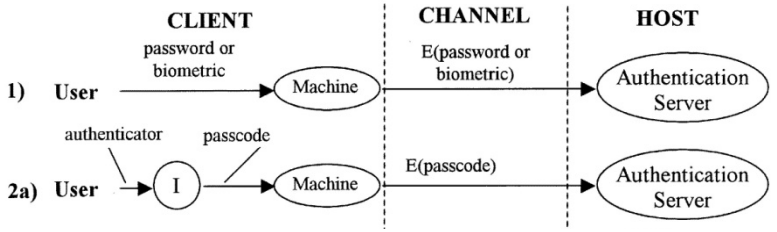
Verification
vs
Identification

Gorman 2003



We will discuss SSO separately

Gorman 2003



"Authenticators can be attacked at three locations: at the client, in the transmission channel, and at the host. Other papers cover protection of a password or passcode in the channel by protocols that encrypt the password [24]–[26]. We deal in this paper only with security issues at the client and host."

Gorman 2003

Attacks	Authenticators	Examples	Typical Defenses
Client Attack	Password	Guessing, exhaustive search	Large entropy; limited attempts
	Token	Exhaustive search	Large entropy; limited attempts; theft of object requires presence
	Biometric	False match	Large entropy; limited attempts
Host Attack	Password	Plaintext theft, dictionary/exhaustive search	Hashing; large entropy; protection (by administrator password or encryption) of password database
	Token	Passcode theft	1-time passcode per session
	Biometric	Template theft	Capture device authentication
Eaves-Dropping, Theft and Copying	Password	"Shoulder surfing"	User diligence to keep secret; administrator diligence to quickly revoke compromised passwords; multi-factor authentication
	Token	Theft, counterfeiting hardware	Multi-factor authentication; tamper resistant/evident hardware token
	Biometric	Copying (spoofing) biometric	Copy-detection at capture device and capture device authentication
Replay	Password	Replay stolen password response	Challenge-response protocol
	Token	Replay stolen passcode response	Challenge-response protocol; 1-time passcode per session
	Biometric	Replay stolen biometric template response	Copy-detection at capture device and capture device authentication via challenge-response protocol
Trojan Horse	Password, token, biometric	Installation of rogue client or capture device	Authentication of client or capture device; client or capture device within trusted security perimeter
Denial of Service	Password, token, biometric	Lockout by multiple failed authentications	Multi-factor with token

Gorman 2003

Security Issues	Authenticators	Examples	Typical Defenses
Non-repudiation	Password, token	Claim lost or stolen authenticator	Personal liability, two-factor with biometric (e.g., signature)
	Biometric	Claim copied biometric	Capture device authentication
Compromise Detection	Password, biometric	Stolen password or copied biometric	"Last login" displayed to user to detect anomaly
	Token	Lost or stolen token	User notes physical absence
Administrative and Policy – Registration/ Enrollment	Password	Initial password registration	Delivery to pre-established e-mail address
	Token	New token registration	Delivery to pre-established, physical address
	Biometric	Biometric enrollment	In-person with picture ID
Administrative and Policy – Reset and Recovery	Password	Forgotten password	Secondary authenticator (e.g., date of birth)
	Token	Lost token	Delivery to pre-established, physical address
	Biometric	Compromised biometric	Not much option but to revert to password

Status 2013

- Passwords dominate with one-time-password tokens a distant second

- Big unresolved threats:
  - Password reset
  - Social engineering
  - Keystroke loggers
  - Dictionary attacks at the server
  - Phishing
  - Man-in-the-middle
  - Man-in-the-browser
  - Man-in-the-PC

Futures Panel 2012

- Greatest problem:
  - "… theft of credentials, which comes in different flavors. It could mean that you get phished and hand your password to a phisher, or it could mean that you share passwords across different sites, and one of those sites gets compromised."
  - "… people"
  - "… from the user's perspective is "too many." "
  - "We need to look at better ways to actually know who's on the other end before we give them credentials for high-fidelity transactions."
  - "… insecure and cumbersome to use."
  - "I think we need to leave the current Internet with what it was intended for originally—the sharing of information. If we want to also have a network for high-fidelity transactions, we need to separate them."
  - " I think that having a single identity for all the different purposes that you need to conduct your life on the Internet is really an act in futility in terms of protecting all the things you need to protect."
  - "My opinion is you can have a single identity, but the identity has to allow for multiple levels of assurance …"

Futures Panel 2012

- What will happen next:
  - "I think user-visible changes will happen slowly. … Under the hood, I think there's a constant arms race going on."
  - "We're going to see one of the major players, and by that I mean a Google or Microsoft or Apple or Amazon, take some known technology and weave it seamlessly—including from a user interface perspective—into some widely used service that has a big user base, and that's going to turn the tide."
  - "We will still have to wait a little bit until there's enough of what I would call catastrophic events, where we just don't like the state of affairs anymore. Then enough forces in the market will come together."
  - "The current system is not sustainable, and I think that we have to move to something that's bet- ter. It's got to be something that we don't have today, because we already know the stuff today doesn't work."
  - "You're going to see an integration of event data that currently goes into your security event monitor, influencing authentication decisions. I think that you're going to start seeing these events also going into whether or not you're actually going to change the authorization corresponding to the initial authentication decision."