IDENTITY AND AUTHENTICATION

Chad Spensky
Allhenticate
WHO AM I?
WHO AM I?

• Chad Spensky (Professional)
  • Ph.D. Student
  • Computer Security Researcher
  • Founder of Allthenticate
WHO AM I?

- Chad Spensky (Social)
- Beach Volleyball Player
- Country Music Enthusiast
- Fried Chicken Connoisseur
WHO AM I?

• Shortman (Online)
• Hacker
• CTF Player
• You?
THE PROBLEM

I should have access to some things, and not others
THE PROBLEM

My Bank Account

Your Bank Account
THE PROBLEM

My E-mail

Your E-mail
THE PROBLEM

Your House
AUTHENTICATION

Convincing a digital entity that I am me
AUTHENTICATION

Convincing a digital entity that I am me authorized
AUTHENTICATION

Only permitting authorized users to access a resource
AUTHENTICATION

- What you know
- What you have
- What you are
WHAT YOU KNOW

A Secret

Personal Details
WHAT YOU HAVE
WHAT YOU ARE
THE GOOD

- **Know**: Always with you

- **Have**: No mental burden

- **Are**: Just be yourself
THE BAD

• **Know**: You must remember it. always.

• **Have**: You must always have it.

• **Are**: What if you temporarily change? (e.g., cold or injury)
THE UGLY

• **Know**: You must be better than a computer.

• **Have**: What if it gets stolen?

• **Are**: You can never share or revoke who you are.
1990s
PASSWORDS

chad 1

**********

1990s

**********
PASSWORDS

chad1

chad86

1990s

*******
PASSWORDS

- **chad1**
- **chad86**
- **NotChad!**

1990s
PASSWORDS

- Attackers were blinding guessing or cracking offline credentials
- Stronger passwords are harder to guess/crack

1990s
PASSWORDS

More than 15 usernames
- cspensky@ucsb.edu
- cspensky@gmail.com
- cspensky@mit.edu
- chad@allthenticate.net
- cspensky@cs.ucsb.edu
- chad@cspensky.info
- cspensky@unc.edu
- cspensky@alumni.pitt.edu
- chad.spensky@ll.mit.edu
- cspensky@comcast.net
- cspensky@alumni.unc.edu

More than 150 saved passwords

3 dedicate apps

Today
PASSWORDS

- Attackers are phishing users to steal the credential outright
- Password strength is completely irrelevant
HARDWARE TOKENS

Second Factor

Hardware Credential

Portable Computer
HARDWARE TOKENS

- Attackers can still phish second factors
- Most hardware credentials can be outright stolen
BIOMETRICS

Fingerprint

Voice Recognition

FaceID
BIOMETRICS

• Easily accessible (e.g., pictures, recordings, or fingerprints)

• Once replicated, are gone forever
FINDING THE RIGHT FIT

Value of Asset

Security Requirements
FINDING THE RIGHT FIT

User Burden vs Security
FINDING THE RIGHT FIT

User Burden

Security
FINDING THE RIGHT FIT

Implementation Cost

Security
FINDING THE RIGHT FIT
THE PROBLEM

There are too many options
MORE IS NOT BETTER

More bugs

More user burden

More overhead
WE NEED FLEXIBILITY
WE NEED FLEXIBILITY
MORE SECURITY. LESS BURDEN.

chad@allthenticate.net

www.allthenticate.net