THE STATE OF AUTHENTICATION

Chad Spensky

Allthenticate
OUTLINE

• Who am I?
• Authentication overview
• Current state of Authentication
• The future of authentication
MY JOURNEY

1998-2004
Internet Pirate
Console Modder

2004-2011
B.S. in CS & Math
M.S. in CS (Authentication)

2012-2015
Staff at MIT LL
Offensive Security

2015-Present
Ph.D. CS (Security)
Founder of Allthenticate
THE PROBLEM

Everyone should not have access to everything.
AUTHENTICATION

Only permitting authorized users to access a resource
AUTHENTICATION

Real World

Digital World
AUTHENTICATION

• What you know

• What you have

• What you are
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

Dedicated apps

Today

More than 150 saved passwords
HARDWARE TOKENS

- Second Factor
- Hardware Credential
- Smartphone
- Portable Computer
AUTHENTICATION IMPLEMENTATIONS
HOW **PASSWORDS** WORK

- **Keyboard Entry**
- **Encrypted Tunnel**
- **Secure Hash Function**
- **Hash saved**
HOW PASSWORDS FAIL

Keyboard Entry → Chad I

Encrypted Tunnel → Secure Hash Function

Chad I → ac18753fe31

Hash saved
A CRYPTO NERD'S IMAGINATION:

His laptop's encrypted. Let's build a million-dollar cluster to crack it.

No good! It's 4096-bit RSA!

Blast! Our evil plan is foiled!

WHAT WOULD ACTUALLY HAPPEN:

His laptop's encrypted. Drug him and hit him with this $5 wrench until he tells us the password.

Got it.
HOW 2FA WORKS

Chad I
1234

Secure Hash Function

Chad I
1234
ac18753fe31

1234
HOW 2FA FAILS

Chad1

Secure Hash Function
ac18753fe31
HOW 2FA WORKS
(BETTER SOLUTION)

Chad1

Secure Hash Function

Challenge

Response

ac18753fe31
New reverse proxy tool posted on Github can easily bypass 2FA and automate phishing attacks

The tool can bypass traditional 2FA, but doesn't work against the newer U2F standard

By William Gayde on January 16, 2019, 3:44 PM
HOW **TOKENS** WORK

Request → Token Required

Challenge → Response
HOW **TOKENS** FAIL

Request → Lock → Token Required

Challenge → Response
Yubico recalls FIPS Yubikey tokens after flaw found

17 JUN 2019

Google, Security threats, Vulnerability

HOW BIOMETRICS WORK

Request

Biometric Required

Do X?

Challenge

Signed Response

Yes
HOW BIOMETRICS WORK

Request → Biometric Required

Challenge → Signed Response

Yes
Malaysia car thieves steal finger

By Jonathan Kent
BBC News, Kuala Lumpur

Police in Malaysia are hunting for members of a violent gang who chopped off a car owner's finger to get round the vehicle's hi-tech security system.
SECURITY VS USABILITY VS COST
FINDING THE RIGHT FIT

Value of Asset

Security
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
WE NEED FLEXIBILITY
WE NEED FLEXIBILITY
MORE SECURITY. LESS BURDEN.

chad@allthenticate.net

www.allthenticate.net