Proper User Authentication

Max McCarty

@maxRmccarty https://lockmedown.com

Authentication Overview

Password Storage

Password Strength

Brute-Force Safeguards

The Problem with Password Storage

The New York Times

RSA Faces Angry Users after Breach

- New York Times June 2011

THE WALL STREET JOURNAL.

LinkedIn 2012 Data Breach May Have Hit Over 100 Million

- WSJ May 2016

THE WALL STREET JOURNAL.

Anthem: Hacked Database Included 78.8 Million People

- WSJ Feb 2015

WIRED

65 million hacked Tumblr passwords are up for sale

- Wired May 2016

Forbes

40 Million Target Customers Affected By Data Breach

- Forbes Dec 2013

The New York Times

LivingSocial Hack Exposes Data for 50 Million Customers

-New York Times April 2013

Los Angeles Times

Hackers appear to leak information on over 30 million Ashley Madison users

-LA Times Aug 2015

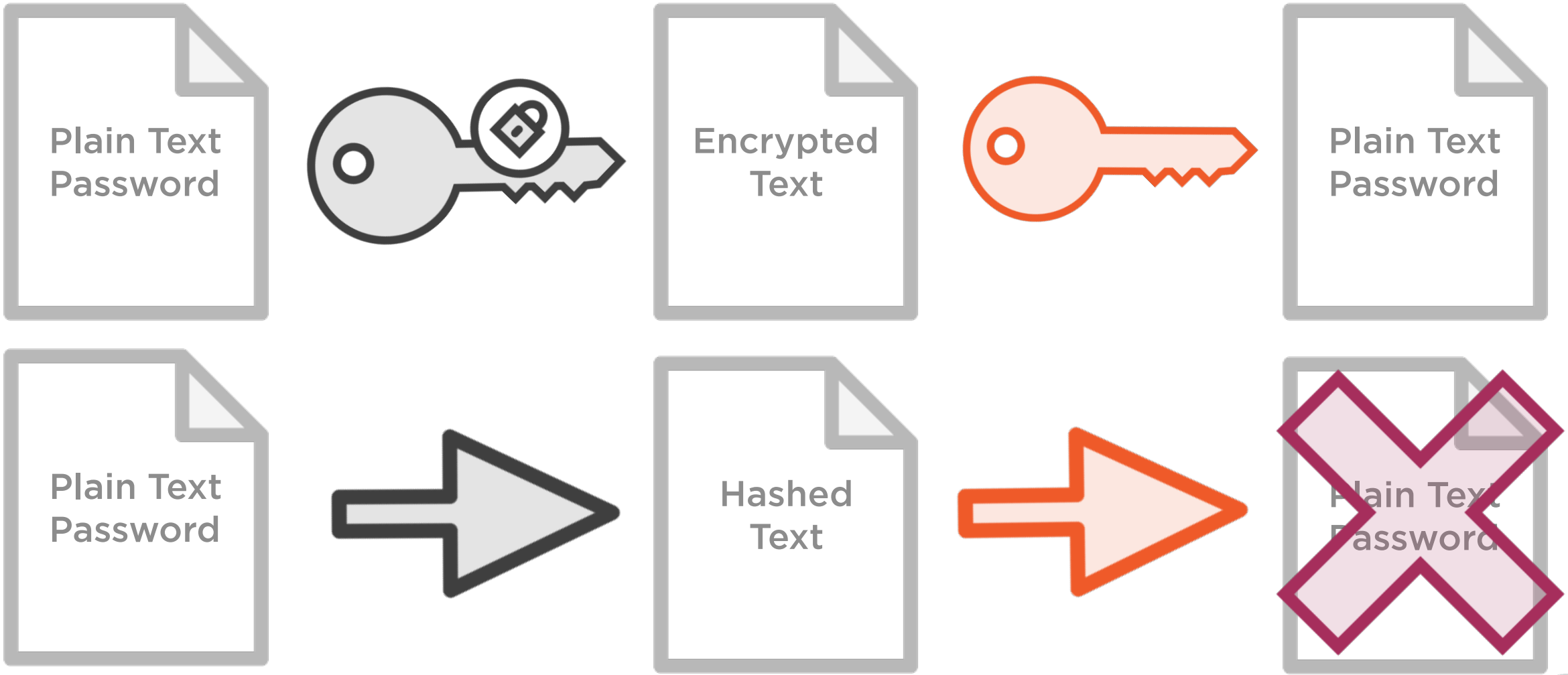
BBC

Hackers steal T-Mobile data on 15 million US customers

- BBC Oct 2015

So how should passwords be stored?

Cryptographic Hash vs Encryption



What Cryptographic Hash Function?

MD5 *SHA-1* *SHA-2* *SHA-3*

Brute-Force Password Cracking

Function	Tries/Sec
NTLM	350,000,000,000
MD5	180,000,000,000
SHA-1	63,000,000,000
SHA-512Crypt	364,000

-Jeremi Gosney Stricture Consulting Company

Hash + Time = Key Derivation

bcrypt

Durability

Bcrypt

- Password hashing function
- Implements salt with high entropy
- Based on the block cipher *Blowfish*
- Accumulative hashing rounds

Password Strength (The Missing Ingredient)

Most Popular Passwords 2015

Rank	Password	Changed 2014
1	123456	Unchanged
2	password	Unchanged
3	12345678	Up 1
4	qwerty	Up 1
5	12345	Down 2

- Splashdot Annual Report

Pro-tip

Mongoose Schema declarations are isomorphic.

Consider validation tools that will ensure consistency with your validation rules.

Brute-force Safeguards

Security vs. Convenience

Pro-tip

An ounce of prevention is worth a pound of cure. Don’t wait for your security needs to bubble up over time.

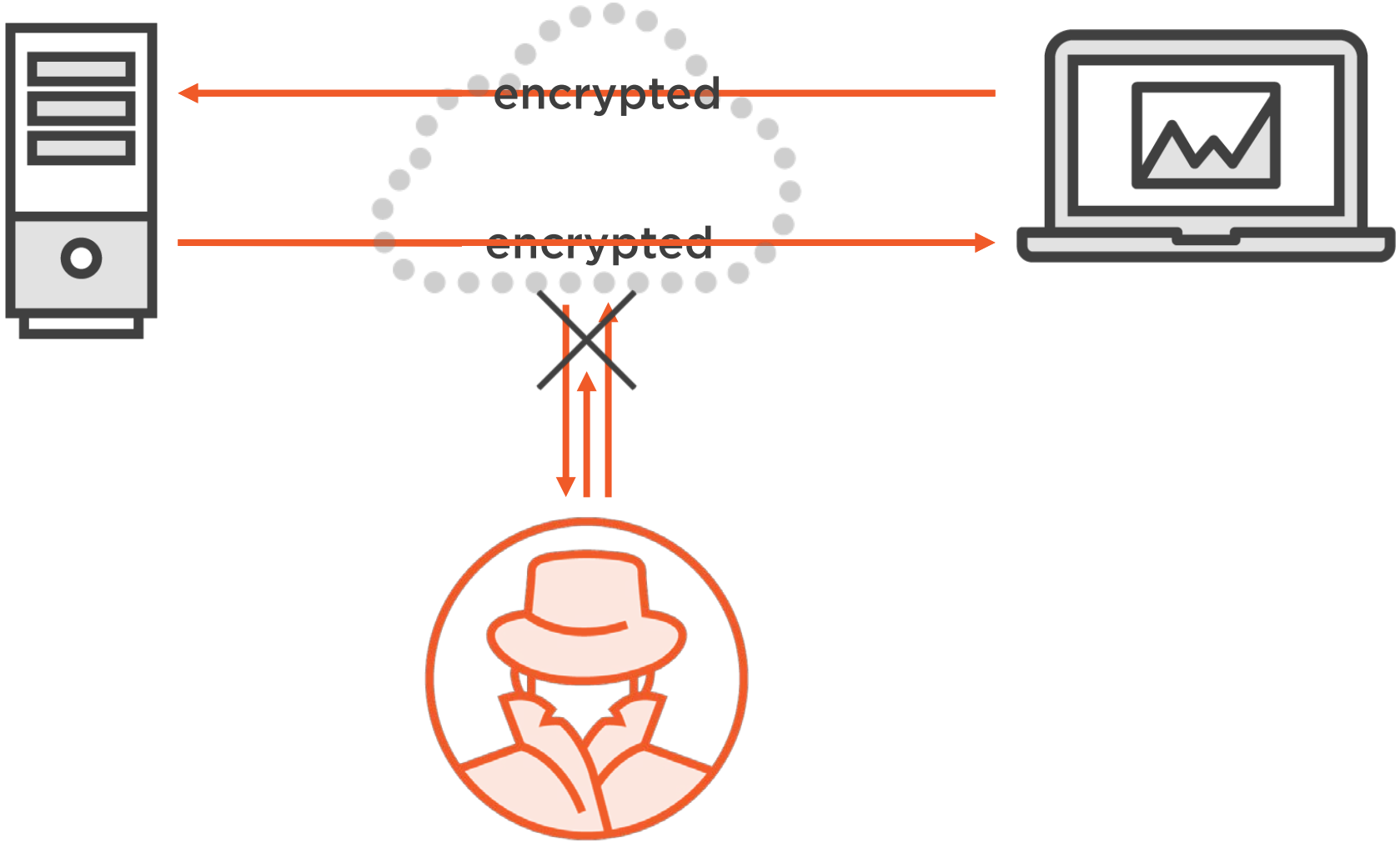
Transportation Layer Security

Transport Layer Security

The successor protocol to secure socket layer (SSL). Originally developed by Netscape, and advanced by the Internet Engineering Task Force (IETF) to TLS 1.0. Providing secure communications of a computer network.


TLS
HTTP
=
HTTPS

Man-in-the-Middle Attacks



Authentication: Golden Rule

The entire authentication from serving of login forms to the submission of user credentials, must occur over HTTPS

Summary

Password Storage

Password Strength Requirements

Brute Force Safeguards