From Real-world Identities to Privacy-preserving and Attribute-based CREDentials for Device-centric Access Control

Killing the password and preserving privacy with device-centric, attribute-based and behavioral authentication

Dr. Michael Sirivianos
Electrical Engineering, Computer Engineering and Informatics

Cyprus University of Technology

Co-funded by the Horizon H2020 Framework Programme of the European Union under grant agreement no 653417.
Our perception of safety and security is not commensurate with the level of threat.

Complacency about authentication security

Flight security in the 60s
This summer, hackers destroyed my entire digital life in the span of an hour. My Apple, Twitter, and Gmail passwords were all robust—seven, 10, and 19 characters, respectively, all alphanumeric, some with symbols thrown in as well—but the three accounts were linked, so once the hackers had conned their way into one, they had them all. They really just wanted my Twitter handle: @mat. As a three-letter username, it’s considered prestigious. And to delay me from getting it back, they used my Apple account to wipe every one of my devices, my iPhone and iPad and MacBook, deleting all my messages and documents and every picture I’d ever taken of my 18-month-old daughter.
Our other common mistake is password reuse. During the past two years, more than 280 million “hashes” (i.e., encrypted but readily crackable passwords) have been dumped online for everyone to see. LinkedIn, Yahoo, Gawker, and eHarmony all had security breaches in which the usernames and passwords of millions of people were stolen and then dropped on the open web. A comparison of two dumps found that 49 percent of people had reused usernames and passwords between the hacked sites.

“Password reuse is what really kills you.” says Diana Smetters, a software engineer at Google who works on authentication systems. “There is a very efficient economy for exchanging that information.” Often the hackers who dump the lists on the web are, relatively speaking, the good guys. The bad guys are stealing the passwords and selling them quietly on the black market. Your login may have already been compromised, and you might not know it—until that account, or another that you use the same credentials for, is destroyed.

Hackers also get our passwords through trickery. The most well-known technique is phishing, which involves mimicking a familiar site and asking users to enter their login information. Steven Downey, CTO of Shipley Energy in
The hacker phished his way in: He sent her an email that linked to a bogus AOL page, which asked for her password. She entered it. After that he did nothing. At first, that is. The hacker just lurked, reading all her messages and getting to know her. He learned where she banked and that she had an accountant who handled her finances. He even learned her electronic mannerisms, the phrases and salutations she used. Only then did he pose as her and send an email to her accountant, ordering three separate wire transfers totaling roughly $120,000 to a bank in Australia. Her bank at home sent $89,000 before the scam was detected.

An even more sinister means of stealing passwords is to use malware: hidden programs that burrow into your computer and secretly send your data to other people. According to a Verizon report, malware attacks accounted for 69 percent of data breaches in 2011. They are epidemic on Windows and, increasingly, Android. Malware works most commonly by infecting a user's computer when they open a file or visit a website. The infection itself is generally benign at first. Then a few weeks or months later, it may activate itself and start sending information to a host of unknown computers and servers. The hacking then becomes the province of the software developers.
If secure, then it is not user-friendly

- A secure password should be hard to be guessed via offline dictionary attack.
- It should not contain dictionary words.
- It should not be related to personal information.

A secure password (hard to be guessed via offline dictionary attack)

You can make it even more secure by adding a random number and symbols to your password.

Create your password. So, that phrase would result in:

- Start with a letter, to your younger self
- Contain at least one character with a troubled backstory
- Include at least one non-standard character, like a talking fox or something
- Incorporate at least one character flaw
- Contain a number, of ill-considered diversions
- Have at least one capital (please note that São Paulo, Sydney, Zürich, Mumbai, Istanbul and Dubai are all largest cities but not capitals)

The Champions League in 2017. Then, take the initials of each word and symbols to

Adding a random number and symbols to your password would result in:

Insert the Champions League in the correct year.
HACK BRIEF: PASSWORD MANAGER LASTPASS GOT BREACHED HARD

EXPERTS RECOMMEND PASSWORD managers like LastPass as the easiest way to generate unique, strong security codes for every one of your online accounts—which sounds great, until that password manager itself is cracked, potentially offering attackers access to all the accounts it was designed to protect.

The Hack
On Monday password manager service LastPass admitted it...
• Funded by the EU under H2020
• Call Identifier: H2020-DS2-2014-1

ReCRED Consortium

Cyberdefense Day, Cyprus, June 2017

www.recred.eu
• To promote the user’s personal mobile device to the role of a unified authentication and authorization proxy towards the digital world.

Problems addressed by ReCRED
• User to Device & Device to Service.
• **FIDO** (Fast IDentity Online) – Standardized protocols for **password-less** authentication
• **OpenID Connect** (Single Sign On)
  – Online services authenticate their users by employing **Google**, **Microsoft**, **PayPal**, accounts
  – **Mobile Connect** (Mobile operators as ID providers)

• **OAuth 2.0** (Open standard for Authorization)
  – Issues and uses **access tokens** to be used for **authorization**
Federated identities with OpenID Connect/OAUTH 2.0

FIDO + OpenID Connect (2)
• **Trusted Execution Environment (TEE)**
  – A secure area of the main processor of a smart phone that provides secure storage and cryptographic functions

[Diagram showing trusted and non-trusted regions within a system.]
• ID Consolidation and Management
  – Profile Management
  – Credential Management
  – Real-to-online identity mapping
• Privacy-preserving Attribute-based Access Control

Account-less access through verified identity attributes (e.g., Age, Location, etc.)

Issue cryptographic anonymous credentials
Provides multi-factor device-to-service authentication based on the user’s behavioral biometrics

Extends the definition of biometric with mobility and traffic patterns

Acts as an ID provider verifying that the user continues to behave as she has normally done in the past
• **Standardized** and **secure** authentication using **FIDO**

• **Multifactor** & **easy to use** **password-less** authentication
  – Biometrics and behavioral authentication

• **Single Sign On (SSO)** with **federated identities**

• **Enhanced** **security & privacy** by employing the **crypto functions** and **secure storage** of **TEE**

• **Privacy** of **online identities** using **anonymous credentials**
  – **Unlinkability** & **untraceability**
  – **Attribute-based Access Control**
• It anchors all access control needs to mobile devices that users habitually use and carry.

• It is aligned with current technological trends and capabilities.

• It offers a unifying access control framework
  – On-line authentication and authorization
  – Using off-the-self mobile devices

• It is attainable and feasible to implement in the existing products.
Business Cases

Support to financial services

Campus Wi-Fi and Campus-restricted Web Services

Age Verification

Student Authentication and Offers
Security and privacy assessment

- Compliance with **EU Directives and Regulation**
  - 95/46/EC
  - 2002/58/EC
  - 2006/24/EC
  - GDPR/2016/EC

- Assessment of data privacy and security of ReCRED architecture

- Described process of
  - Code Review
  - Penetration Testing
• **First integrated system**
• Started recruiting students from university and library
• Students can access Web Services
  – Device-centric Authentication
  – Password-less experience
  – Fine-grained control of identity attributes to be revealed (ABAC)
• **FIDO + OpenID Connect Integration**
**Pilot 1:** Device-centric campus WiFi and web services access control

**Pilot 2:** Student authentication and offers

**Pilot 3:** Attribute-based age verification online gateway

**Pilot 4:** Financial services – microloan origination
• Multi-Modal Continuous Authentication System

• Captured attributes
  – Typing patterns
  – Browsing habits
  – Location
  – Face recognition
  – Walking habits
  – Speech recognition
  – Touch dynamics

• Calculates trust score according to captured attributes
• Behavioral profiles are stored on BAA
  – Innovative architectural component

• Behavioral attributes are either captured by the user’s device or directly by the BAA

• Account-wide lockdown and device-wide lockdown
Thank you

Dr. Michael Sirivianos
Electrical Engineering, Computer Engineering and Informatics

Cyprus University of Technology
• Definition of the ReCRED architecture
The problems with the password paradigm
Reference Architecture