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

A Federated Architecture for Attribute-based and Behavioral Authentication as a High-Assurance Service

Dr. Michael Sirivianos
Cyprus University of Technology

Keynote, Tyrrhenian Workshop 2017: Towards a smart and secure future Internet
Palermo, 19 September 2017

Co-funded by the Horizon H2020 Framework Program of the European Union under grant agreement no 653417.
Our perception of safety and security is not commensurate with the level of threat. Humans tend to underestimate threats they are not familiar with.

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.

"This summer, hackers destroyed my entire digital life in the span of an hour," says Wired senior writer Mat Honan. ☘ ETHAN HILL
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 installing the backdoor through a keystroke logger or fake antivirus.
If secure, then it is not user-friendly

- A secure password should be resistant to offline dictionary attacks.
- It should not contain full words.
- It should not be reused across accounts.

If secure, then it is not user-friendly.

**Online Passwords: The Complete Rules**

Your password must:

- 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)

For example, create a phrase like "I hope Juventus will win the Champions League in 2017". Then, take the initials of each word and all numbers and symbols to create your password. This would result in: IhJwwtCLi2017.

You can make it even more secure by adding a random symbol every one to four words, for example:

Ih#Jw#wt#CL#i2017#

A secure password (hard to be guessed via offline dictionary attack) should be 15 random characters long.
Something you know -> something you have and you are

**HACK BRIEF: PASSWORD MANAGER LASTPASS GOT BREACHED HARD**

*Andy Greenberg, Security 06.15.15 05:01 PM*

**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

Cyberdefense Day, Cyprus, June 2017
• To promote the user’s personal mobile device to the role of a unified authentication and authorization proxy towards the digital world.
Integration between strong device-centric authentication methods and federated login solutions

Separation of concerns for Identification, Authentication, Authorization and Behavioral Authentication
- Incremental deployability
- Wide adoption and compliance with NIST assurance levels

A novel centralized component that enables:
- Identity management
- Account recovery in case of device loss
Many significant benefits, including, but not limited to:

- **Enhanced UX**
  - A user can be authenticated once and reuse the issued credential at multiple Service Providers

- **Cost reduction** to the end-user (reduction in authenticators)

- **Data minimization** and **focus on mission**
  - Service Providers do not need to collect and store personal information

- **Pseudonymous** attribute assertions
  - Service Providers can request a minimized set of attributes
- **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**
• Identity Assurance Levels (IAL)
  – Addresses how end-users can register and prove their identities to an identity management system

• Authenticator Assurance Levels (AAL)
  – Addresses how end-users can securely authenticate and access a Service Provider

• Federation Assurance Levels (FAL)
  – Provides requirements and assertions to convey the results of authentication processes and relevant identity information to a Service Provider
  – Privacy-enhancing techniques for identity management
  – Methods for strong multi-factor authentication while the end-user remains anonymous
• “Something you know” -> “Something you have”

• Solves the password overload problem and introduces high assurance authenticators

• The mobile device of the user is required for:
  – Mobile Connect
  – Behavioral Authentication
  – Privacy-preserving Attribute-Based Access Control (P-ABAC)
Why DCA needs Federation?

• DCA needs federation for **Identity Management**

• DCA requires a **trusted registry** for reliable **Failure Recovery**
  – Lack of device failure/loss recovery mechanisms → passwords are still in use

  – To offer failover authentication with Mobile Connect and BAAs
• The **main problem** for adoption of various password-replacement schemes

• ID Federation (OpenID Connect) and Consolidation ease recovery
  – Together they support multiple backup factor mechanisms

• Users have to remember only one backup password
  – No need to use it frequently
  – TypTop: Personalized Typo-tolerant Password Checking
• The Identity Consolidator is the **main reference** to a user’s identity attributes

• Main Components:
  - Physical and Online Identity Acquisition
  - Identity Integration
  - Credential Management
  - Identity Management (Profile and Consent Management)
  - Authentication Management
  - Account Management
Why ID Consolidator (IDC)?

• It solves the Identity Fragmentation problem
  – Real to Online identity binding
  – Enables proof of joint attribute ownership
  – Keeps track of all IdPs and BAAs of a user
  – Acts as a consolidated OIDC Identity Provider

• Facilitates the verification of ID attributes
  – by combining multiple soft proofs of identities
  – via statistical correlations (Identity Integration Module)

• Allows for effective Profile and Consent management
• Acts as trusted authority able to issue P-ABAC credentials

• Can also acts as a Mobile Connect proxy Identity Provider
OpenID Connect + FIDO UAF

• Password-less OpenID Connect experience

• Integration of the FIDO UAF server to the OpenID Connect Provider

• Replacement of username/password authentication with biometrics (e.g., fingerprint) or pins
OpenID Connect + FIDO UAF

FIDO UAF Authentication

Biometrics, PIN, ...

Challenge/Response

Identity Provider

Identity Consolidator

Service Providers
Federated identities with OpenID Connect/OAUTH 2.0

Identity Provider → Single Sign On → Identity Consolidator

Identity Provider ← Single Sign On ← Service Providers

Identity Provider

Single Sign On

Service Providers
Extending OpenID Connect to support attribute write on the ID Provider

• Update, delete, transfer of identity attribute between different Identity Providers

• The Service Provider can write attributes to the ID Provider instead of only reading
Extending the OpenID Connect Protocol

OpenID Connect + P-ABAC (Idemix/U-Prove)

• Integration of Cryptographic credentials stacks within the OpenID Connect Provider

• The OpenID Connect Provider acts as an Idemix/U-Prove issuer and verifier
Attribute combination suggestion based on requested resource

- The Service Provider suggests possible attribute combinations to the OpenID Connect Provider

- Offers more flexibility and increased privacy if desired by the user
What is and why do we use Mobile Connect?

- Mobile-based secure universal authentication, authorization, and attribute sharing solution
- Matches the user to his mobile phone
- Provided by a global network of Mobile Network Operators (MNOs)
- Mobile Connect is required to achieve IAL3
Behavioral Authentication Authority (BAA)

• 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 he has normally done in the past
• Abstraction for behavioural authentication modalities
• Provides a common API based on two designs
  – Transparent (Mobility, Weblog) → Pull-base
  – Non-transparent (Gait, Keystroke) → Push-based
– BAA as a Service (Stand-alone IdP)
– Alert ID Consolidator on suspicious behaviour
• Latch for the online world
  – Real world
    → Door latched → No entrance, even with right key
  – Online world
    → Account latched → No login, even with right password (or other credentials)

• ALM keeps account “status”
  – User define policies (e.g., latch on at night)
  – Allows for latching based on BAA alerts
• User authentication to a Service Provider

• Multi-factor Authentication

• IDC as Profile Management Tool
User authentication to an SP (OIDC / FIDO)

1. SP Access Request
2. Authentication Redirect / Required User Attributes
3. FIDO Authentication Request (Fingerprint, pin, etc.) / Attributes Authorization Request
4. Successful FIDO Authentication / Authorization Granted
5. Authentication Result / User Attributes
6. Access Granted
Multi-factor Authentication

1. Redirect for OIDC/FIDO Authentication
2. Redirect for OIDC/FIDO Authentication
3. FIDO Authentication Request / Attributes Authorization Request
4. Successful FIDO Authentication / Authorization Granted
5. Authentication Result / User Attributes
6. Request for the available BAAs for the given username
7. BAA endpoint
8. Redirect for OIDC/FIDO Authentication
9. Authentication & Authorization request
10. Authentication & Authorization
11. Success
12. Access Granted

User

Identity Provider

Service Provider

ID Consolidator

BAA
IDC as a Profile Management Tool

1. Attribute transfer request
2. Redirect to the source IdP
3. Authentication request
4. Authentication
5. Redirect to the destination IdP
6. Authentication & Authorization request for attribute write
7. Authentication & Authorization with the source IdP
8. Write attribute

User

Source Identity Provider

Destination Identity Provider

ID Consolidator
• **Demo 1** - Physical Identity Acquisition using NFC Technology

• **Demo 2** - Transfer of identity attributes between different Identity Providers
Service Provider (SP) entrusts user authentication to the Identity Provider (IdP)

IdP provides two authentication factors
  - FIDO and behavioral authentication

Storyboard
  - User behavior is the expected one
  - User behavior is NOT the expected one

SP can tailor the service based on the authentication result
BAA continuous Authentication and Account Locking

- SP entrusts user authentication to IdP
- IdP: FIDO + check for account locking status
- Keystroke-based BAA

**Storyboard**
- User authenticates to IdP → IdP check for account lock status
- An adversary takes possession of the user smartphone
- BAA detects change in behavior and triggers account locking
- The attacker tries and fails to authenticate to the IdP → User account is locked
Demo 5

Fail-over Authentication with Mobile Connect and BAA

• The user has lost his device and purchased a new one
  – Tries to regain full access to the IDC by proving his identity
    → Using Mobile Connect and BAA

• Storyboard
  – User authenticates to IDC with master password
    → He is granted access in “tentative mode”
  – User proves his identity
    → Mobile connect (he has acquired a new SIM card with his phone number)
    → BAA (he has registered the new device to the BAA, also in “tentative mode”)
What is P-ABAC?

- Privacy-preserving Attribute-based Access Control

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

Issue cryptographic anonymous credentials
How P-ABAC works?

User

Service Provider

User Service Provider

TIWDC 2017, Palermo, September 2017
How P-ABAC works?

1. What is your name?
2. What is your password?

User:
1. John Doe
2. 12345678

Service Provider:
1. What is your name?
2. What is your password?
How P-ABAC works?

1. John Doe
2. 12345678
3. 6/7/1980
4. john.doe@uniroma2.it
5. Id Nr: AB12345CD
6. ...

User

1. What is your name?
2. What is your password?
3. Are you over 18?
4. Are you a student?
5. Are you EU citizen?
6. ...

Service Provider

User Service Provider

TIWDC 2017, Palermo, September 2017
How P-ABAC works?

User

- John Doe
- 12345678
- 1. 6/7/1980
- 2. john.doe@uniroma2.it
- 3. Id Nr: AB12345CD
- 4. ...

Service Provider

- What is your name?
- What is your password?
- 1. Are you over 18?
- 2. Are you a student?
- 3. Are you EU citizen?
- 4. ...
How P-ABAC works?

1. Are you over 18?
2. Are you a student?
3. Are you EU citizen?
4. ...

User

Identity Provider

Service Provider

1. 6/7/1980
2. john.doe@uniroma2.it
3. Id Nr: AB12345CD
4. ...

1. Over 18
2. Student @ Uniroma2
3. EU passport
4. ...

CERTIFIED
IRMA-like Architecture

1. User
2. Identity Provider
3. ReCRED Application
4. Crypto Server
5. FIWARE
6. U-prove
7. Idemix

TIWDC 2017, Palermo, September 2017
• Credential Management Module
  – P-ABAC Credential Definition
  – P-ABAC Credential Management
  – P-ABAC Credential Issuing
  – P-ABAC Credential Backup & Restore

• ReCRED Wallet Mobile App module
  – P-ABAC Credential Management
  – P-ABAC Credential Backup & Restore
• ABAC Policy Tools
  – Policy analysis/reasoning mechanisms
  – Policy suggestions for administrators
  – Policy management interface

• Consent Policy Management
  – Specific on P-ABAC credentials
  – Allows the user to define policies for the disclosure of her attributes

• Risk Assessment
  – Assess the risk of privacy leaks
• P-ABAC integration with FIWARE
  – Unifies the interfaces of different underlying P-ABAC engines
• P-ABAC integration with OpenID Connect
  – Allows online services to use P-ABAC seamlessly
• P-ABAC integration with FIDO
  – Allows FIDO-enabled services to use P-ABAC
P-ABAC Integration in ReCRED

Behavioal Authentication Authorities (BAA)
- Federated Login
- FIDO UAF Server
- Behavioral Profile Extraction
- Behavioral Profiles Repository
- Behavioral Verification results, Federated login

Service Provider (SP)
- Web Application / Resources
- Access Control Policy Reasoning Tool
- Machine Learning Data Mining
- Federated login

User Device (UD)
- FIDO UAF Client
- FIDO UAF Authenticators
- Cryptographic Credentials Stack
- Idemix / U-Prove
- Cryptographic Credentials Storage
- Behavioral Profile Capture

Identity Consolidator (IDC)
- Authentication Management
  - OpenID Connect
  - Federated Login
  - FIDO UAF Server
- Fingerprint Verification
- Identity & Consent Management
- Credential Management
- Idemix / U-Prove
- Identity Repository
- Federated login

Identity Provider (IdP)
- OpenID Connect
- Federated Login
- FIDO UAF Server
- Cryptographic Credentials Stack
- Idemix / U-Prove
- Identity Repository
- Identity Repository
- FIDO UAF, Federated login

Extracted Behavioral profiles, FIDO UAF, Federated login

Behavioral Verification results, Federated login

TIWDC 2017, Palermo, September 2017

H2020 – Grant Agreement no. 653417
IDC as P-ABAC Credentials Issuing IdP

1. Request for online account linking and attributes acquisition
2. Authentication redirect to IdP
3. Authentication & Authorization request
4. Authentication & Authorization
5. User attributes
6. Request for idemix credential issuance from the acquired attributes
7. Issued idemix credentials
P-ABAC with OpenID Connect
• **Demo 6** - Credential Management

• **Demo 7** – P-ABAC through OpenID Connect

• **Demo 8** – Consent Management & Policy Reasoning Tool
## Identity Assurance Levels (IAL)

<table>
<thead>
<tr>
<th>Identity Assurance Level</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>IAL1</td>
<td>Identity attributes are self-asserted or should be treated as self-asserted</td>
</tr>
<tr>
<td>IAL2</td>
<td>Remote or in-person identity proofing</td>
</tr>
<tr>
<td>IAL3</td>
<td>In-person identity proofing</td>
</tr>
<tr>
<td>Identity Assurance Level</td>
<td>Supported with</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------------------------------------------------</td>
</tr>
<tr>
<td>IAL1</td>
<td>Online registration</td>
</tr>
<tr>
<td>IAL2</td>
<td>Physical and Online identity acquisition</td>
</tr>
<tr>
<td>IAL3</td>
<td>Mobile Network Operators and Mobile Connect</td>
</tr>
</tbody>
</table>
## Authentication Assurance Levels (AAL)

<table>
<thead>
<tr>
<th>Authenticator Assurance Level</th>
<th>Provides</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAL1</td>
<td>Some assurance that the user controls an authenticator registered to the Service Provider</td>
<td>Single-factor authentication</td>
</tr>
<tr>
<td>AAL2</td>
<td>High confidence that the user controls authenticator(s) register to the Service Provider</td>
<td>Two-factor authentication</td>
</tr>
<tr>
<td>AAL3</td>
<td>Very high confidence that the user controls authenticator(s) register to the Service Provider</td>
<td>Hard cryptographic authenticator + two-factor authentication</td>
</tr>
</tbody>
</table>
## How AALs are supported in ReCRED

<table>
<thead>
<tr>
<th>Authenticator Assurance Level</th>
<th>Supported with</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAL1</td>
<td>Backup Password + Behavioral Authentication</td>
</tr>
<tr>
<td>AAL2</td>
<td>Secure SIM (Mobile Connect) + Human to SIM authentication</td>
</tr>
<tr>
<td></td>
<td>Backup password + FIDO</td>
</tr>
<tr>
<td></td>
<td>FIDO</td>
</tr>
<tr>
<td>AAL3</td>
<td>Secure SIM + FIDO + Backup Password</td>
</tr>
<tr>
<td></td>
<td>Secure SIM + FIDO</td>
</tr>
<tr>
<td>Federation Assurance Level</td>
<td>Requirements</td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td><strong>FAL1</strong></td>
<td>The Identity Provider must sign the assertion using approved cryptography</td>
</tr>
<tr>
<td><strong>FAL2</strong></td>
<td>The assertion must be encrypted using approved cryptography such that the Service Provider is the only party that can decrypt it</td>
</tr>
<tr>
<td><strong>FAL3</strong></td>
<td>The assertion must be signed using approved cryptography and encrypted to the Service Provider using approved cryptography</td>
</tr>
<tr>
<td>Federation Assurance Level</td>
<td>Supported with</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------------------------------------------</td>
</tr>
<tr>
<td>FAL1</td>
<td>OpenID Connect</td>
</tr>
<tr>
<td>FAL2</td>
<td>OpenID Connect + ID Token encrypted with the public key of the Service Provider</td>
</tr>
<tr>
<td>FAL3</td>
<td>OpenID Connect + P-ABAC</td>
</tr>
</tbody>
</table>
Comparison with the State-of-the-art
• 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
- **Open source product** that offers **management of multiple online identities**
- 2 ways of authentication
  - Acts as an **Identity Provider**
  - **Delegates authentication** to other Identity Providers
- **Multi-factor authentication** (FIDO U2F)
- Provides **RBAC** and **ABAC**
• **Physical Identity Acquisition** and Verification

• **Password-less Authentication** (FIDO UAF)

• **Privacy-preserving** Identity Consolidator
  – Increased privacy if the user desires so

• **Locks online accounts** by performing **behavioral authentication**

• Support for **privacy-preserving ABAC** (Idemix, U-Prove, CP-ABE)
• Enhanced Physical identity acquisition and verification

• Online Identity Acquisition

• Integration with FIDO

• Behavioral continuous authentication

• Integration with **Federated ID systems** (e.g., OIDC) thus, it supports identity attributes storage or exchange
Paypal’s FIDO + OpenID integration

- User authentication with FIDO UAF
- Extended OpenID Connect in order to
  - Maintain an authentication token for persistent sign-in
  - No need for re-authentication
- Purchases from multiple apps with one authentication
- Integrated with Lenovo, Samsung devices as of 2017
- No source code released, just a 4-page documentation
• We kill the password with **DCA**

• DCA requires Federation, Identity Consolidation and Behavioral Authentication for efficient **failure recovery** and **identity management**

• Since we have **DCA, Federation, and IDC** we can support device-centric **Privacy-preserving ABAC**
From Real-world Identities to Privacy-preserving and Attribute-based CREDentials for Device-centric Access Control

Several slides and videos prepared by Konstantinos Papadamou (CUT), Alberto Caponi and Claudio Pisa (CNIT), Claudio Soriente (TID), George Gugulea (CertSign), Steven Gevers (Verizon), and Vasilis Sarris (Exus) at TIWDC 2017, Palermo, September 2017.