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

Prof. Christos Xenakis
Department of Digital Systems
University of Piraeus
ReCRED Project – Consortium

www.recred.eu

Project funded by EU under H2020
Call Identifier: H2020-DS2-2014-1
ReCRED’s goal is 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**

1. Password overload
   - User
   - Username, Password 1 → Service 1
   - Username, Password 2 → Service 2

2. Identity Fragmentation
   - User
   - Facebook, LinkedIn, Q+

3. Lack of real-world binding
   - User A
   - Passport
   - User B
   - Passport
   - Account

4. Lack of support for Attribute based access control
   - Attribute Verification request
   - Verified Attribute
   - Access
   - Service
   - Attribute Verifier

Infocom Security, Athens, April 6th - 7th 2016
ReCRED’s approach – employed technologies

User to device & device to service
ReCRED’s approach – employed technologies

- **FIDO** (Fast IDentity Online)
  - Standardized protocols for **password-less** authentication

![Diagram of FIDO's approach](image)
ReCRED’s approach – employed technologies

• **OpenID Connect** (Single Sing On)
  • Online services authenticate their users by employing **Google, Microsoft, PayPal**, accounts

• **OAuth 2.0** (Open standard for Authorization)
  • Issues and uses **access tokens** to be used for **authorization**
ReCRED’s approach – employed technologies

- **Mobile Connect** (Provided by mobile operators) – GSMA
  - **Universal log-in** solution by matching the user to their mobile phone/subscription
ReCRED’s approach – employed technologies

- **Trusted Execution Environment (TEE)**
  - A **secure area** of the main processor of a smart phone that provides **secure storage** and **cryptographic functions**
ReCRED’s approach – employed technologies

ID Consolidator Credential Management Module

- Identity consolidation
- Real-to-online identity mapping
ReCRED’s approach – employed technologies

Attribute-based access control

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

Issue cryptographic or anonymous credentials

idemix - pseudonymity for e-transactions

U-Prove
ReCRED’s Innovation

• **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** & **secure storage** of **TEE**

• **Privacy** of **online identities** using **anonymous credentials**
  • **Unlinkability** & **untraceability**
  • **Attribute-based access control**
ReCRED’s Innovation

• 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** and **physical authentication** and **authorization**
  
  • Using **off-the-self mobile devices**

• It is **attainable** and **feasible** to implement in the existing products
ReCRED’s pilots

**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

---

Infocom Security, Athens, April 6th - 7th 2016
ReCRED project is partially an outcome of Research & Development in the Field of Security and Privacy.
Before R&D!
A few words about us ...

• University of Piraeus, Greece
• School of Information and Communication Technologies
• Department of Digital Systems
• System Security Laboratory founded in 2008
• Research, Development & Education
  • systems security, network security
  • computer security, forensics
  • risk analysis & management
• MSc course on “Digital Systems Security” since 2009
What we do for education

• **Undergraduate studies** ....
  • Security Policies and Security Management
  • Information Systems Security
  • Network Security
  • Cryptography
  • Mobile, wireless network security
  • Privacy enhancing technologies
  • Bachelor Thesis
What we do for education

• Postgraduate studies in Digital Systems Security

• 1st semester
  • Security Management
  • Applied Cryptography
  • Information Systems Security
  • Network Security
  • Security Assessment and Vulnerability Exploitation
What we do for education

• **Postgraduate studies in** Digital Systems Security

• 2\textsuperscript{nd} semester

  • Privacy Enhancing Technologies
  • Mobile Internet Security
  • Digital Forensics and Web Security
  • Advanced Security Technologies
  • Legal Aspects of Security
What we do for education

• Postgraduate studies in **Digital Systems Security**

• 3rd semester
  • Master Thesis

• ISO 27001
• Certified Information Security Manager (CISM)
• .....
Next, my colleagues are going to present ...

- **ROPInjector**: Using Return Oriented Programming for Polymorphism and Antivirus Evasion

- **(U)SimMonitor**: A New Malware that Compromises the Security of Cellular Technology and Allows Security Evaluation

- Perform effective **command injection** attacks like Mr. Robot
Σας ευχαριστώ!

Χρήστος Ξενάκης

Εργαστήριο Ασφάλειας Συστημάτων
Τμήμα Ψηφιακών Συστημάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
UNIVERSITY OF PIRAEUS

http://ssl.ds.unipi.gr/
http://cgi.di.uoa.gr/~xenakis/
email: xenakis@unipi.gr