u'smile

CORMORANT

Continuous risk-aware multi-modal authentication

Android Security Symposium, Vienna, Austria, 9th September 2015

Rainhard Findling, Muhammad Muaaz, Daniel Hintze
rainhard.findling@fh-hagenberg.at

Today we talk about...

- User friendly mobile security

Today we talk about...

- User friendly mobile security
- Multiple authentication mechanisms in Android framework

Today we talk about...

- User friendly mobile security
- Multiple authentication mechanisms in Android framework
- + continuous, cross-device, risk-aware

Why Security Matters on Mobile Devices

[businessnewsdaily.com]

Mobile devices

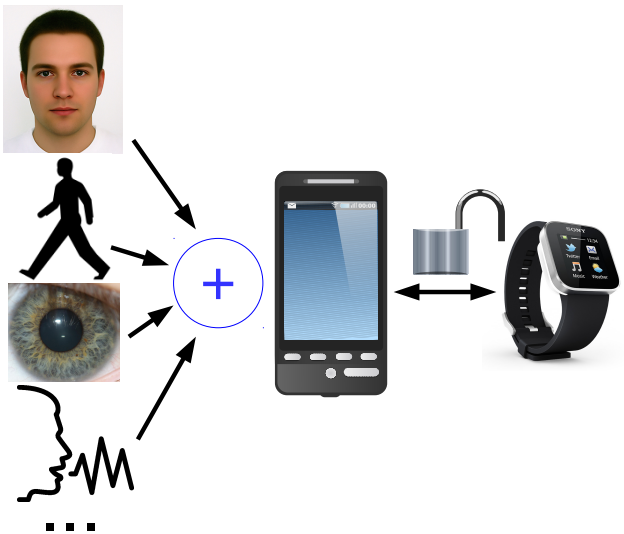
- Extensive access to private data/services, represents user in digital world (social media, payments, digital signatures)
- Easily accessed/lost/stolen

Security's usability: impact

- Disabled device locks
- Disabled encryption (e. g. file system)
- Data stored in cloud
- ...

Easier-to-use mobile security is of major importance

What Do We Contribute?



u'smile research

- Authentication (today's focus)
- HW/OS/application security
  - Embedded secure elements
  - Virtualization
  - Malware

Authentication and Usability

- Biometrics, sensors
- Unconventional approaches

CORMORANT

- ... the authentication framework

CORMORANT Authentication

CORMORANT allows an easy integration of implicit and explicit authentication and risk plug-ins.

- Conventional PIN/password
- Gait authentication (cell phone based accelerometer)
- Face authentication
- Voice authentication

Each authentication plug-in produces a binary or probability output [0,1].

Picture: Michael-Milfeit, https://500px.com/photo/100091973/wingspan-by-michael-milfeit?ctx_page=&from=related_photos&photo_id=7933118

Cost security trade-off

There is always a trade-off between **cost** and **security**

- A thicker front door offers better protection, but costs more.
- A 20-digit PIN is more secure than a 4-digit PIN, but also harder to remember and enter.
- 3-Factor-Authentication is more secure than 2-Factor-Authentication, but less convenient to use.

The level of security that is necessary depends on the actual risk.

Picture: Mike Baird, CC BY 2.0, https://www.flickr.com/photos/mikebaird/2354116406

Risk of unauthorized access

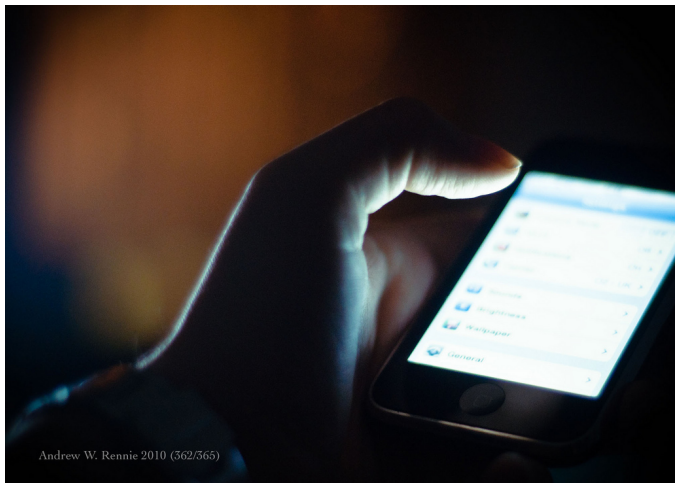
The risk of unauthorized access depends on

probability

- Time (e.g. daytime vs. nighttime)
- Location (e.g. home vs. public transport)
- Strangers nearby (some might be thieves)

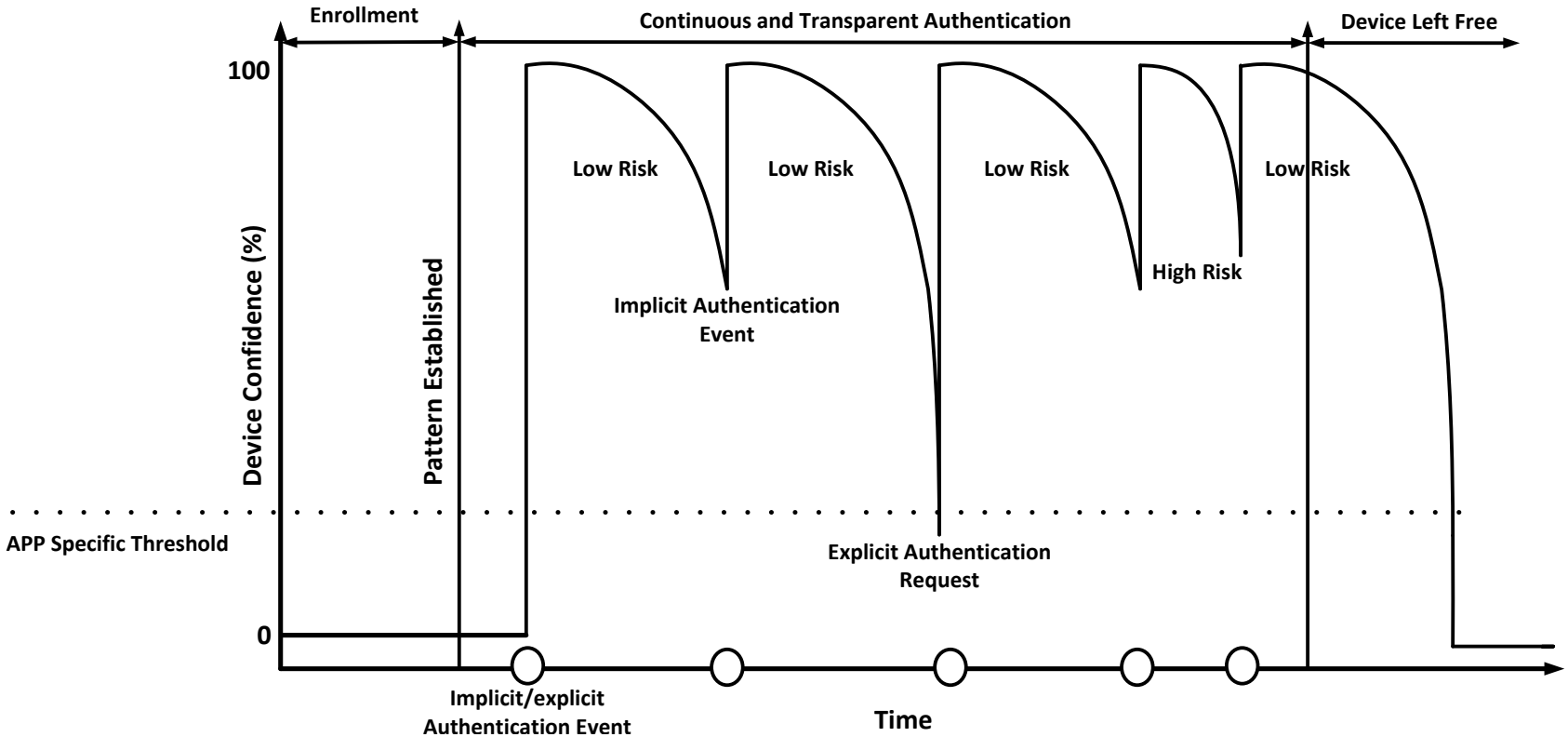
and **impact.**

- Accessible services, e.g. VPN, email
- Value of stored data (private vs. public)
- Transaction value (e.g. in money transfer)



Picture: Andy Rennie, CC BY-SA 2.0, https://www.flickr.com/photos/andrewrennie/5305466633

Risk aware device confidence



Users tend to own and use multiple devices

Picture: Jeremy Keith, CC BY 2.0, https://www.flickr.com/photos/adactio/6153558098

Basic Idea

Trusted devices within **close proximity** may share user authentication results as well as risk information among each other, thus significantly reducing the number of explicit authentication processes necessary.

"The whole is greater than the sum of its parts."

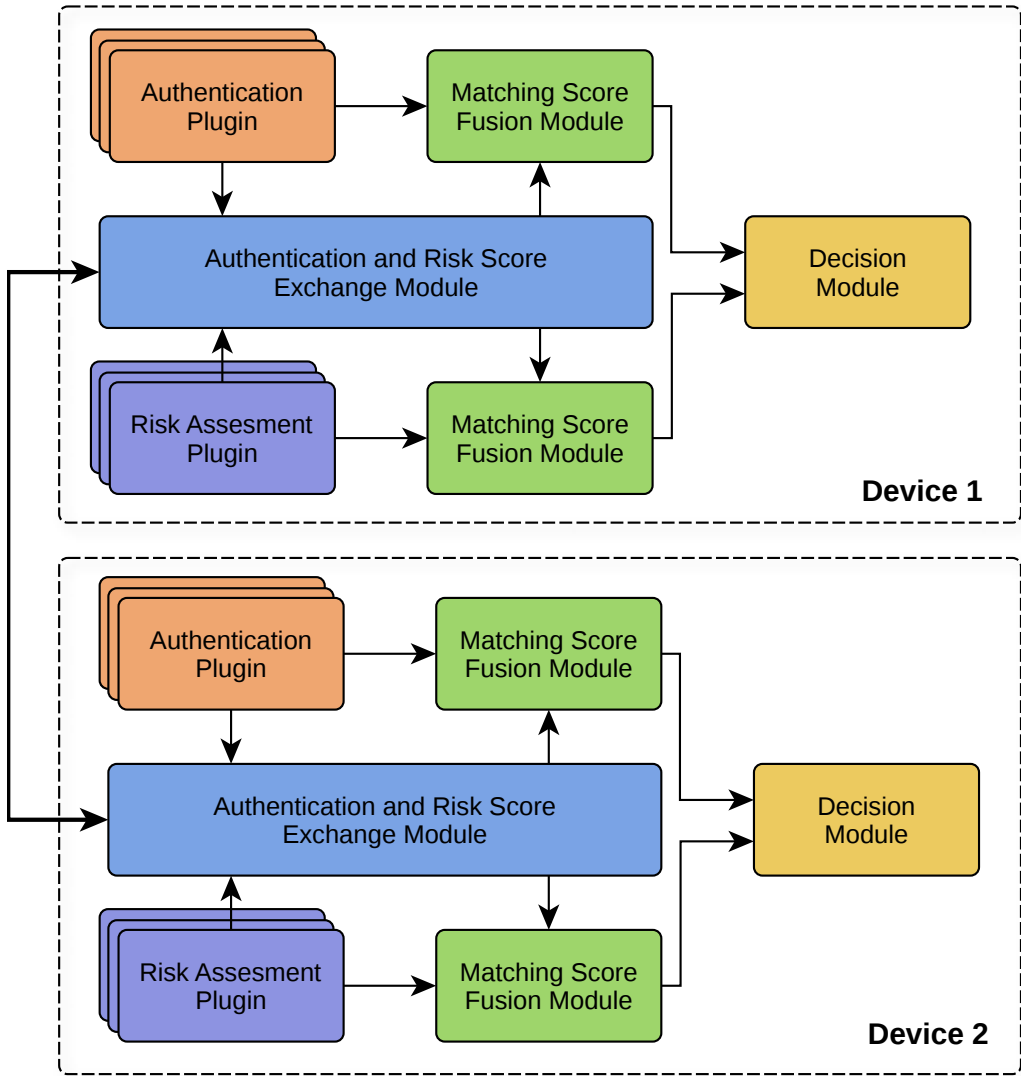
— Aristotle

Assumptions

- A user can only be in one place at a time.
- If successfully authenticated, device and user are co-located.
- A user has physical control over devices within arm's reach.

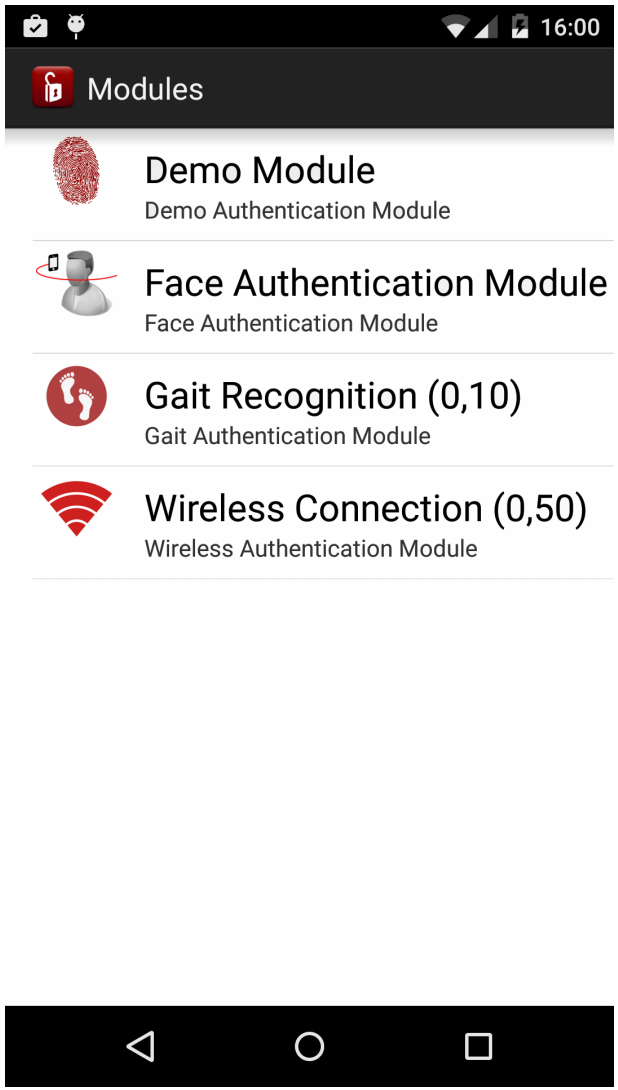
Picture: Unknown, CC0 1.0, https://pixabay.com/en/tablet-smartphone-laptop-hard-drive-626090/

CORMORANT Overview



Implementation

- Android open source implementation is currently work in progress.
- Easily extensible through arbitrary authentication and risk plugins.
- Provides fall-back authentication mechanisms, support for user studies and elaborated usage statistics (opt-in).
- We are inviting researchers to use and contribute to CORMORANT.



Android Implementation - Manifest

```
<?xml version="1.0" encoding="utf-8" ?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android">
 <uses-permission android:name="at.usmile.cormorant.REGISTER_AUTH_PLUGIN" />
 <application
  <service
     android:name=".DemoAuthenticationtPlugin"
     android:icon="@drawable/ic_launcher"
     android:label="@string/app_name"
     android:permission= "at.usmile.cormorant.permission.READ_PLUGIN_DATA" >
   <intent-filter>
    <action android:name="at.usmile.cormorant.Plugin" />
   </intent-filter>
   <meta-data android:name="protocolVersion" android:value="1" />
   <meta-data android:name="description" android:value="Demo Authentication Plugin" />
  </service>
 </application>
</manifest>
```

Android Implementation - Service

```
import at.usmile.cormorant.api.AuthenticationStatusData;

public class DemoExplicitAuthenticationtModule
    extends AbstractAuthenticationModule {

    @Override
    protected void onUpdateAuthenticationStatus(int reason) {
        publishUpdate(new AuthenticationStatusData()
            .status(Status.OPERATIONAL);
            .confidence(0.5));
    }
}
```

CORMORANT: Wrapping Up

[Michael Milfeit, 500px.com]

CORMORANT

- Android authentication framework
- Multi-modal, continuous, cross-device, risk-aware

Development

- Have: plugin system, confidence calculation
- Future: cross-device, authentication fusion, securing biometrics with template protection
- Active development, research in progress
- Researchers can easily join, develop plugins for new biometrics

Thank you for your attention!

u'smile

Questions?