An approach to dynamically integrate heterogenous AI components in a multimodal user authentication system use case

Talk prepared for tinyML Asia 2021, scheduled 2021-11-05
An approach to **dynamically integrate** heterogenous AI components in a multimodal user authentication system use case

- "An approach to" : a concrete approach
- "Dynamically Integrate" : dynamically configurable integration
- "Heterogenous AI components" : AI components utilizing different underlying types of technologies
- "in a multimodal user authentication system use case" : applied to the specific application domain of Multimodal User Authentication
AnchorZ Inc.

"Security should be both easy and robust, for everyone, at all time"

--- motivation and guiding principle of DZ Security
Application Domain

Continuous User Authentication
dzsecurity @tinyml-asia2021

• **DZ Security**(*) : AnchorZ's personal authentication solution
  
  • *Continuous, Background, Multimodal* Personal Authentication
  
  • Optimized for user experience while not compromising security

• "**Continuous**" : throughout a session, (cf. login-time only authentication)

• "**Background**" : authentication mostly does not require active user interaction

• "**Multimodal**" : multiple sensory sources and authentication methods with various modalities are utilized and integrated together dynamically to achieve the personal authentication task

• "**Personal Authentication**" : authentication of human-users of computing systems (i.e. PC, Smartphone, smart ticket gate, etc.)

(*) : multiple international patents granted/pending
Overview

Basic System Structure

dzsecurity @tinyml-asia2021

[Key Observations]

- **Cyber-physical system**:  
  - Inherit system uncertainties  
  - Nonexistence of perfect solution
- **Multiple Input**:  
  - Inputs are of low information quality and density; thus  
  - Necessity for information distillation and extraction → AI/ML comes to rescue!
- **Various Input Types**:  
  - Many different type of algorithms  
  - Also vary from device to device
- **Single output**:  
  - Necessity for information integration  
  - Large design space
- **Large and Complicated Input Space**:  
  - Impossible to perfectly classify all system inputs; thus  
  - Difficult to evaluate system performance
Our Approach

Step 1: Decompose the System

dzsecurity @tinyml-asia2021

• **Sensor Interface**: Abstraction over device sensors, with well-defined interface for various classes of sensors (e.g. camera, fingerprint sensors)

• **Elemental Information Processing Units**: Information distillation and extraction from device-supplied sensory information, usually utilize ML-based algorithms

• **Elemental Module Interface**: Abstraction over algorithm-dependent outputs of various EIPUs, with well-defined interface for various modalities of information sources (e.g. face recognition result, fingerprint matching result, location frequencies)
  - Each EIPU will report its processing result, as well as meta-data including:
    - Authentication performance characterization
    - Quality indication of underlying sensor data

• **Integrated Authentication Algorithm**: The algorithm that (1) schedule data acquisition and processing and (2) fuse different data sources to give the final output
  - The commander and the core of the system
  - Decides the security and usability performance of the whole system
Our Approach

Step 1: Decompose the System

dzsecurity @tinyml-asia2021

Separation of Concerns

- **Technical Concern** Separation
  - much clearer **design goals** and **performance measurement** for each components
  - clear **boundaries** for development work breakdown
  - well-defined boundaries provides **observability** into system insides

- **Business Concern** Separation
  - allowing multiple party to collaborate and co-benefit
  - provide users much boarder choices cross criteria like cost / performance / security level

Green: DZ Security Core Technology

Orange: Pluggable and dynamically configurable
Our Approach

Step 2 : Build the Foundation
dzsecurity @tinyml-asia2021

- **dzPPL & dzSpec**: are two fundamental building blocks we built for DZ Security

- **dzPPL**: DSL for authoring and evaluating Integrated Authentication Algorithms (IAA)
  - "PPL" = Probabilistic Programming Language
  - IAA written as stochastic programs with stochastic inputs from EIPUs
  - Algorithm behavior be precisely evaluated using stochastic methods

- **dzSpec**: collection of specs defining APIs and evaluation metrics
  - defined for each major sensor data class / authentication modalities
  - provides a dynamic linking layer between the IAA and device/configuration-specific collections of available sensor sources / EIPUs

Green: DZ Security Core Technology

Orange: Pluggable and dynamically configurable
Our Approach

Step 3 : Focus on the Core

dzsecurity @tinyml-asia2021

- **ARUAR** : our current-generation framework for the Integrated Authentication Algorithm (IAA)
  
  - "ARUAR" = Accumulated Registered User Absence Risk
  
  - an adaptive framework built upon dzPPL for the implementation of IAA

- Design Goals :
  
  - provide support for **flexibly configurable** combinations of Elemental Information Processing Units (EIPU) without the need to rewrite IAA
  
  - ensure necessary level of security, while
  
  - maximizing user experience
  
  - establish **clear logical link** between final authentication outcome with EIPU results
Our Approach

Step 3: Focus on the Core

dzsecurity @tinyml-asia2021

- ARUAR Design Goals:
  - provide support for **flexibly configurable** combinations of Elemental Information Processing Units (EIPU) without the need to rewrite IAA
  - ensure necessary level of security, while maximizing user experience
  - establish **clear logical link** between final authentication outcome with EIPU results

- ARUAR Design Principles:
  - **Dynamic Fusion**: combination and weight contribution to the final result of EIPU (Elemental Information Processing Unit) is not predetermined but dynamically derived from EIPU supplied meta-data regarding methodology-intrinsic-characteristics and sensory data quality
  - **Risk-Management Driven**: final decisions are directly derived from the calculated risk of absence of the legit user
  - **Separation of "Smartness" and "Correctness"**: make clear separation of the part of algorithm that values "smartness" and the part of the algorithm that ensures the "correctness" (i.e. security in this case) of the overall algorithm
Our Approach

Step 3 : Focus on the Core
dzsecurity @tinyml-asia2021

- Design Goals : (1) **flexibly configurable** (2) **ensure security levels** (3) **max UX** (4) **clear logical links**

- Design Principles : (1) **Dynamic Fusion** (1) **Risk-Management Driven** (3) **Separation of "Smartness" and "Correctness"**

- ARUAR Anatomy and Basic Operation :

  - **Elemental Authentication Modules (EAMs)** : when invoked, from info provided by EIPUs, produce internal representation of authentication result of specific modalities

  - **Situation Inference Modules (SIMs)** : from info provided by EIPUs, infer the instantaneous situational risk factors, and adjust accordingly the level of scrutiny applied when fusing EAM results in calculating **User Absence Risk**

  - **External Invocation Scheduler (ES)** : given past and present (1) situational information (2) EAM execution history, and (3) required security level, dynamically schedule the invocation of EAMs

  - **Model Keeper (MK)** : according to interpretation policy derived by SIMs, fuse elemental authentication results from EAMs to derive the instantaneous User Absence Risk, and decides the final authentication outcome in accordance with the security level stipulated by the application
Our Approach

Step 3: Focus on the Core

dzsecurity @tinyml-asia2021

- Design Goals: (1) **flexibly configurable** (2) **ensure security levels** (3) **max UX** (4) **clear logical links**
- Design Principles: (1) **Dynamic Fusion** (1) **Risk-Management Driven** (3) **Separation of "Smartness" and "Correctness"**
- Materialization of the ARUAR Design Goals:
  - **Flexibly Configurable**: a library of EAMs and SIMs are prepared, each would work with certain combination of available EIPUs, and available EAMs and SIMs are dynamically derived from EIPUs available on the system configuration
  - **Ensure Security Levels & Clear Logical Links**: EAM results interpreted with SIM-derived policies gives traceable and tunable risk assessment result, and directly from which the outcome is decided. Therefore adequately implemented EAMs + SIMs will ensure adequately assessed user absence risk, and the final outcome always corresponds to the risk profile provided by the containing application, which ultimately ensuring the necessary security level
  - **Maximize User Experience**: each EAM, with meta-data provided by EIPUs, provides the External Scheduler information about the degree and nature of hinderance to user experiences in case of its invocation. a "smart" External Scheduler could then take these into account to maximize UX
Our Approach

Step 4 : Putting it All Together
dzsecurity @tinyml-asia2021

• Using the ARUAR framework, we have built our first experimental Integrated Authentication Algorithms that works with dynamically pluggable
  • Facial recognition modules
  • Location (from GPS / WiFi / BLE data) based risk-factor classifier modules
  • Fingerprint authentication modules
  • Voice authentication modules
  • Password / Pin authentication modules
  • 2FA OTP authentication modules
• And have preliminarily benchmarked its performance under a set of selected use cases
• Since those algorithms are built upon dzPPL, we could perform evaluation of the algorithms in terms of security and user experience performance robustly and with relative ease, against a wide range of EIPU configurations and usage scenario classes.
Our Approach

Step 4 : Putting it All Together

dzsecurity @tinyml-asia2021

- The currently available DZ Security products uses our previous generation of integrated authentication algorithms that is carefully crafted for each individual combination of EIPUs

- We are working on finalizing and thoroughly benchmarking our first ARUAR based algorithms and expect the first products with this new technology to be available in Q2 2022

- We are also working on a framework to allow secure and easy integration of 3rd party EIPUs, which is expected to be launched 2022Q2~2023Q1

- With this work as one of the cornerstones, we are also building a Strongly-Established-Identity-Centric Trustworthy Computing Platform using other exciting technology sets AnchorZ is developing, which is also expected to be launched by 2022Q3
AnchorZ Inc.

"Security should be both easy and robust, for everyone, at all time"

--- motivation and guiding principle of DZ Security
Questions?