Securing Cyberspace by Ensuring Authenticity through Adaptive Multi Factor Authentication

ASEAN IVO Forum 2017

Presented by: Didi Rosiyadi

Prepared by: Rifki Sadikin[1], Didi Rosiyadi[1], Esa Prakasa[1], Hermawan Nugroho[2]

[1]Research Center for Informatics,
Indonesian Institute of Sciences, Indonesia
[2]Faculty of Engineering, Computing and Science
Swinburne Techonolgy University, Sarawak, Malaysia

24 Oktober 2017

Outline

- Background
- Objectives
- Members, Methodology and Roadmap
- Budget
- Facility and Equipment

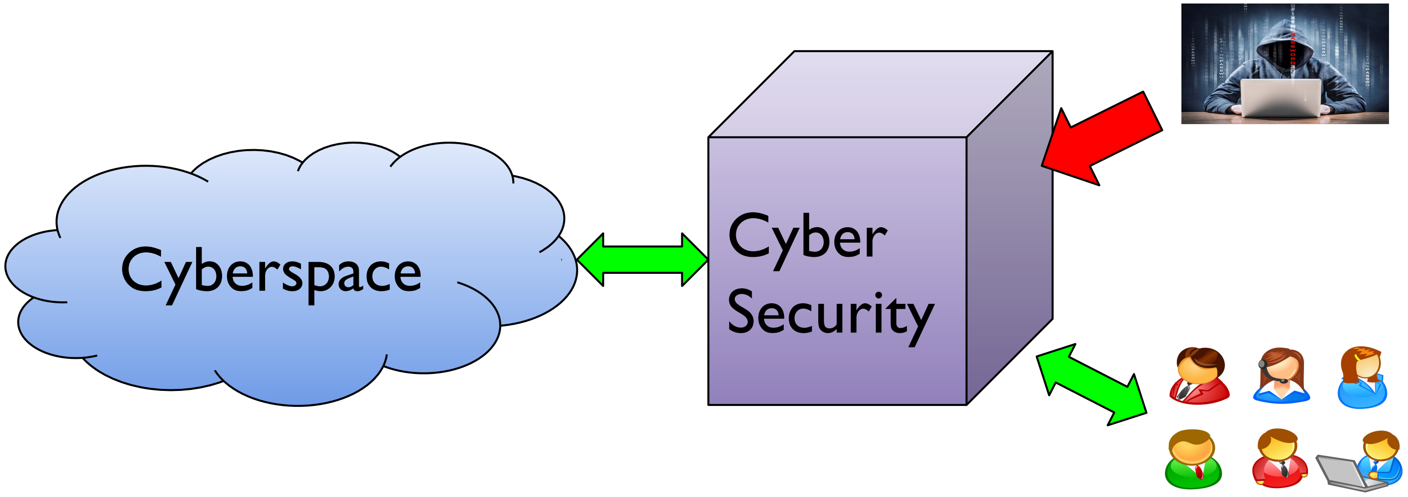
Outline

LIPI

- Background
- Objectives
- Members, Methodology and Roadmap
- Budget
- Facility and Equipment

Cyberspace and Security

- Cybersecurity: measure for protecting cyberspace from cyber crime such as disruption or unauthorized access, use, disclose, modification or destruction.



Cyberspace

Cyber Security

Banking Industry

- Cyber technology foster banking industry services.
- Security services: integrity, confidentiality, and availability

- Internet Banking
- ATM’s
- Tele banking
- E-Money
- E-Cheque

Security Services

Integrity

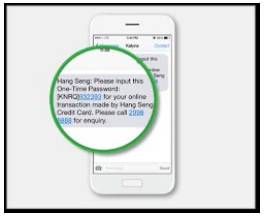
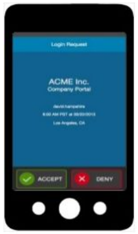
Confidentiality

Availability

Security Threats

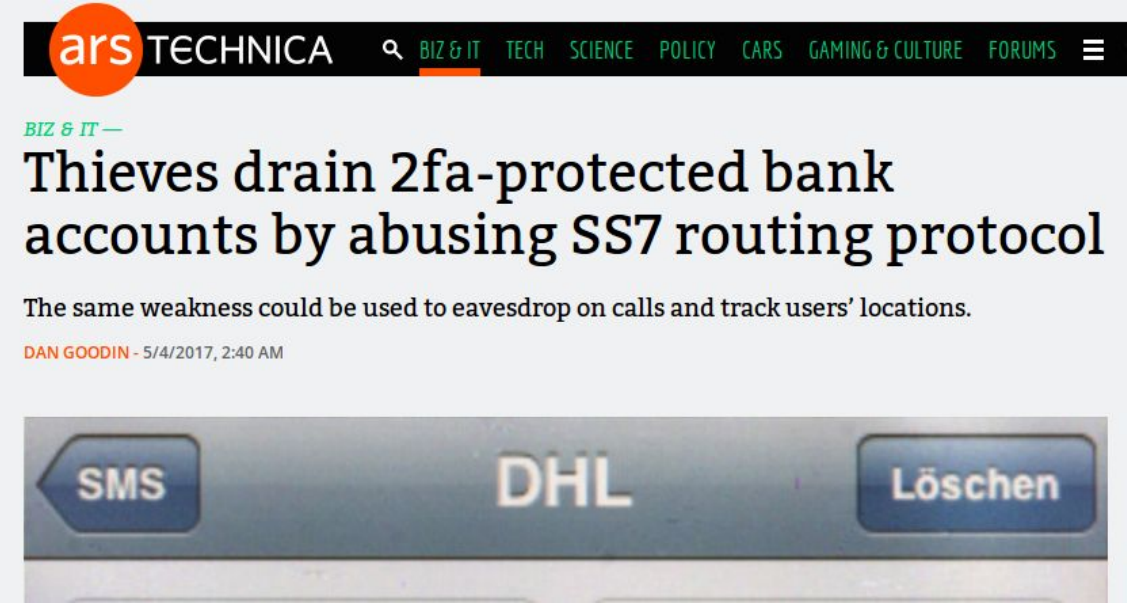
- 63 % of reported breached involve the use of compromised credentials (Verizon DBIR 2016)
- Threats:
  - Malicious software, vulnerability in new vectors: mobile phones, phishing by exploiting poor implementation or social engineering
- Recent issue in Malaysia - **leak of 46 million mobile users' data** (Reuters.com November 2017)
- Authentication provides assurance on entity identification to protect cyberspace from threats. However *username+password* is not enough.
- Common practice: two-factor authentication

2 Authentication Factors

Knowledge Based Question-Answer	Twitter Facebook YouTube Tumblr Snapchat Instagram Pinterest Skype
One Time Password delivered from SMS	Hang Seng: Please input this One-Time Password: [KNRQ]932393 for your online transaction made by Hang Seng Credit Card. Please call 2998 8888 for enquiry.
Hard token	
Push to accept	Login Request ACME Inc. Company Portal

Limitedness of 2F Authentication: Case OTP with SMS

- Hackers can intercept SMS messages and do man-in-the middle attack



BIZ & IT —

Thieves drain 2fa-protected bank accounts by abusing SS7 routing protocol

The same weakness could be used to eavesdrop on calls and track users' locations.

DAN GOODIN - 5/4/2017, 2:40 AM

Adaptive Multifactor Authentication

Adaptive

- Device recognition
- Geo Location
- Phone number protection
- Behavioral biometrics
- Identity Governence

Multifactor

- SMS OTP
- Email OTP
- Talk OTP
- Biometric
- Push to Accept

Goal:

- Raise confidence in authenticating identities
- Provide good user experience

Outline

- Background
- **Objectives**
- Members, Methodology and Roadmap
- Budget
- Facility and Equipment

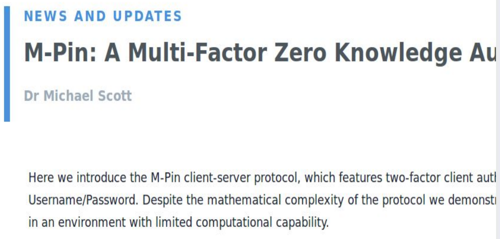
Research Objectives

LIPI

- To develop a new multi factor authentication method to provide authentication service in cyberspace.
- To develop an algorithm based on image processing techniques for creating an unique biometric key using facial expression.
- To implement the authentication scheme efficiently in smart devices environment
- To evaluate user experiment in conducting multi factor authenticationscheme.

Develop New Multifactor Authentication based on Strong Cryptographic Primitives

- Challanges in biometric-based authentication: probabilistic in nature.
- Storing biometric information raise security risk (how if server is compromised).
- Exploiting/Developing privacy preserving protocol from current crypto primitives such as *lattice-based/pairing-based cryptography* could lead more secure multifactor authentication.
- Research questions:
  - How to improve "Multi-Factor Zero Knowledge Authentication Protocol" with biometrics (which is naturally probabilistic)?
  - Previous study:

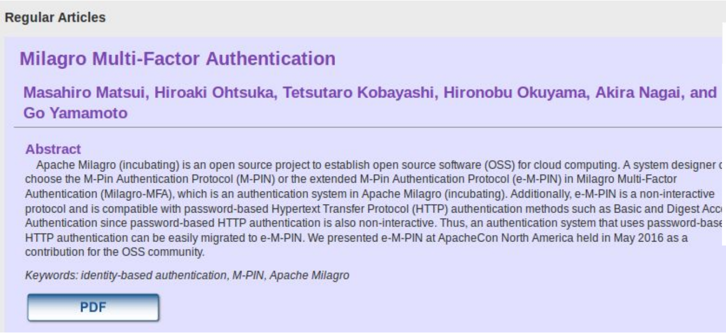


NEWS AND UPDATES

M-Pin: A Multi-Factor Zero Knowledge Au

Dr Michael Scott

Here we introduce the M-Pin client-server protocol, which features two-factor client auth
Username/Password. Despite the mathematical complexity of the protocol we demonstr
in an environment with limited computational capability.



Regular Articles

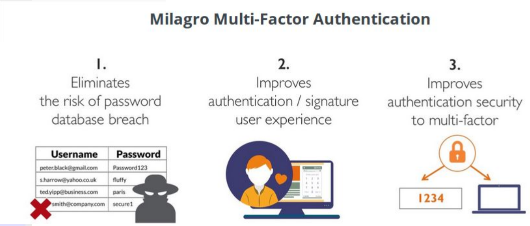
Milagro Multi-Factor Authentication

Masahiro Matsui, Hiroaki Ohtsuka, Tetsutaro Kobayashi, Hironobu Okuyama, Akira Nagai, and Go Yamamoto

Abstract

Apache Milagro (incubating) is an open source project to establish open source software (OSS) for cloud computing. A system designer c
choose the M-Pin Authentication Protocol (M-PIN) or the extended M-Pin Authentication Protocol (e-M-PIN) in Milagro Multi-Factor Authentication (Milagro-MFA), which is an authentication system in Apache Milagro (incubating). Additionally, e-M-PIN is a non-interactive protocol and is compatible with password-based Hypertext Transfer Protocol (HTTP) authentication methods such as Basic and Digest Acc
Authentication since password-based HTTP authentication is also non-interactive. Thus, an authentication system that uses password-base
HTTP authentication can be easily migrated to e-M-PIN. We presented e-M-PIN at ApacheCon North America held in May 2016 as a contribution for the OSS community.

Keywords: identity-based authentication, M-PIN, Apache Milagro



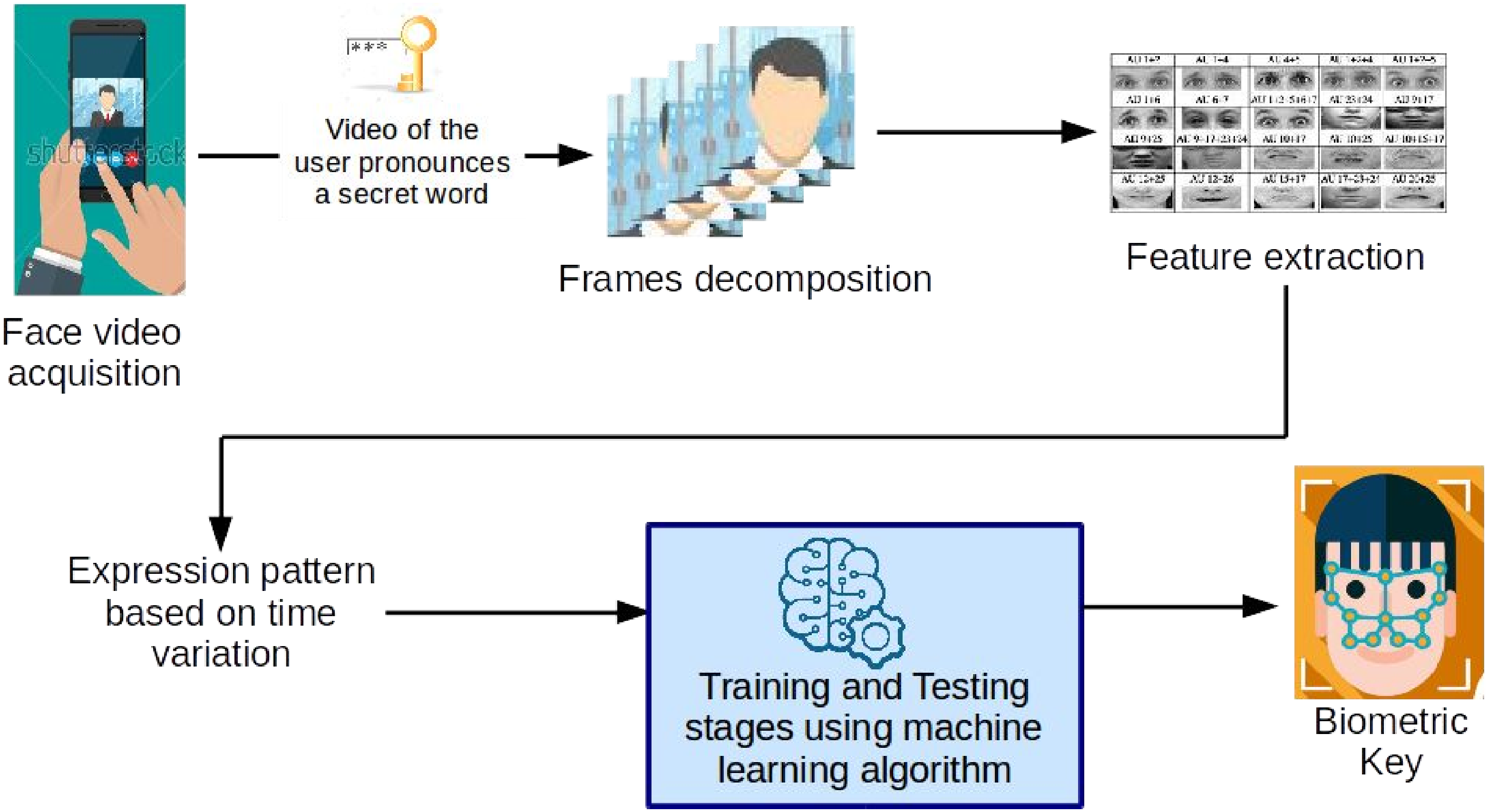
Milagro Multi-Factor Authentication

1. Eliminates the risk of password database breach

2. Improves authentication / signature user experience

3. Improves authentication security to multi-factor

Biometric-Key Using Facial Expression



Face video acquisition

Video of the user pronounces a secret word

Frames decomposition

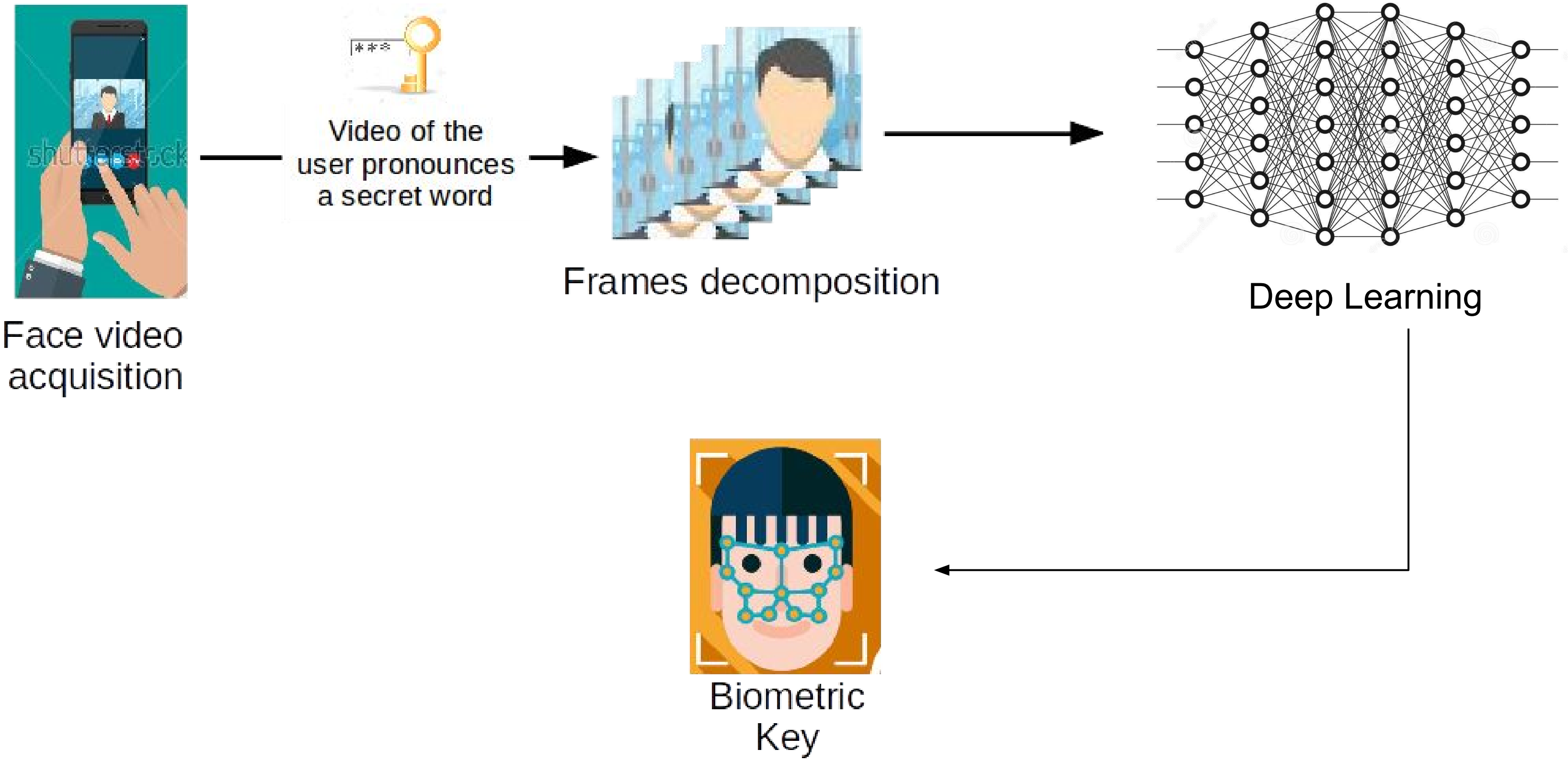
Feature extraction

Expression pattern based on time variation

Training and Testing stages using machine learning algorithm

Biometric Key

Biometric-Key Using Facial Expression



Face video acquisition

Video of the user pronounces a secret word

Frames decomposition

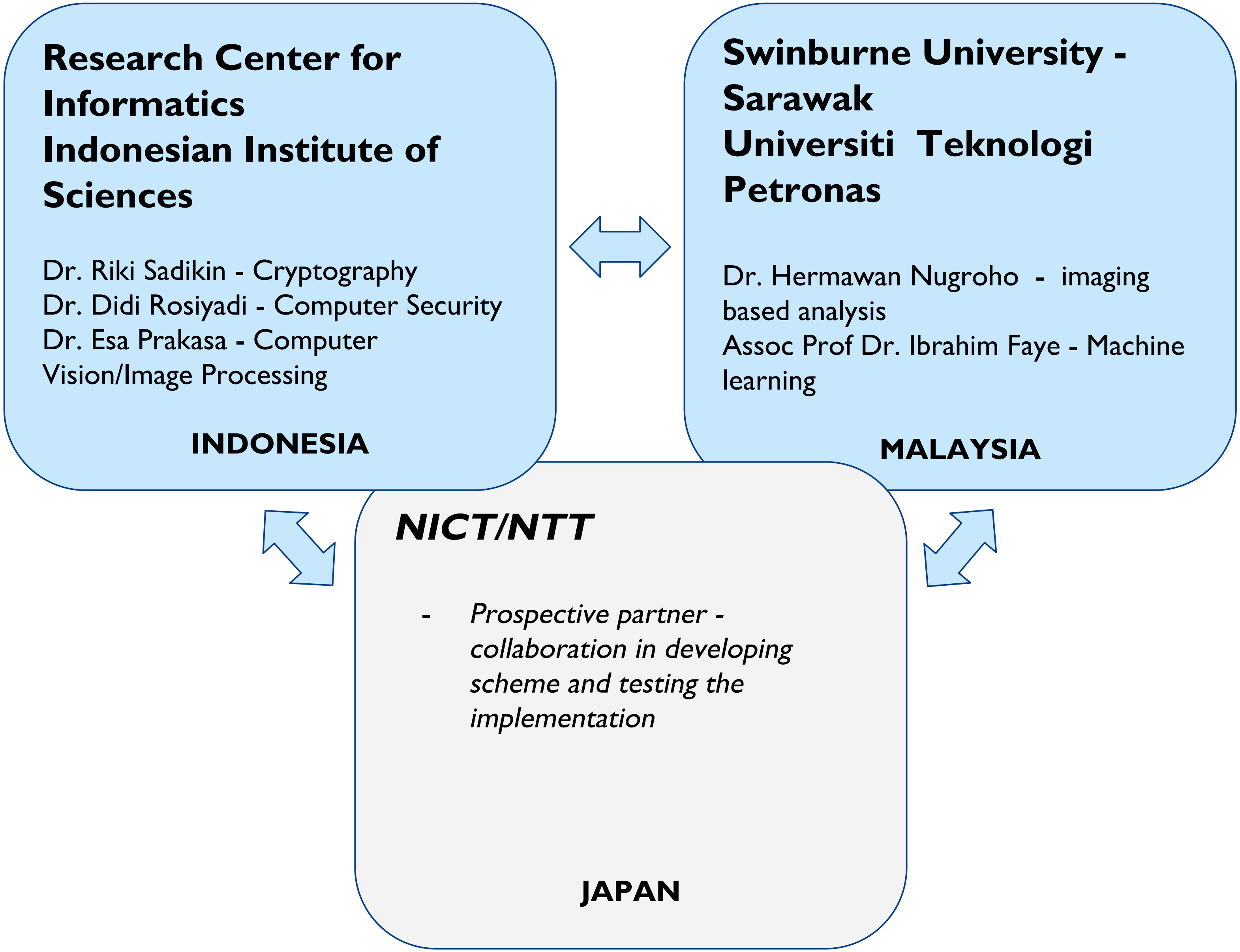
Deep Learning

Biometric Key

Outline

- Background
- Objectives
- Members, Methodology and Roadmap
- Budget
- Facility and Equipment

Research Members



Research Center for Informatics Indonesian Institute of Sciences

Dr. Riki Sadikin - Cryptography
Dr. Didi Rosiyadi - Computer Security
Dr. Esa Prakasa - Computer Vision/Image Processing

INDONESIA

Swinburne University - Sarawak Universiti Teknologi Petronas

Dr. Hermawan Nugroho - imaging based analysis
Assoc Prof Dr. Ibrahim Faye - Machine learning

MALAYSIA

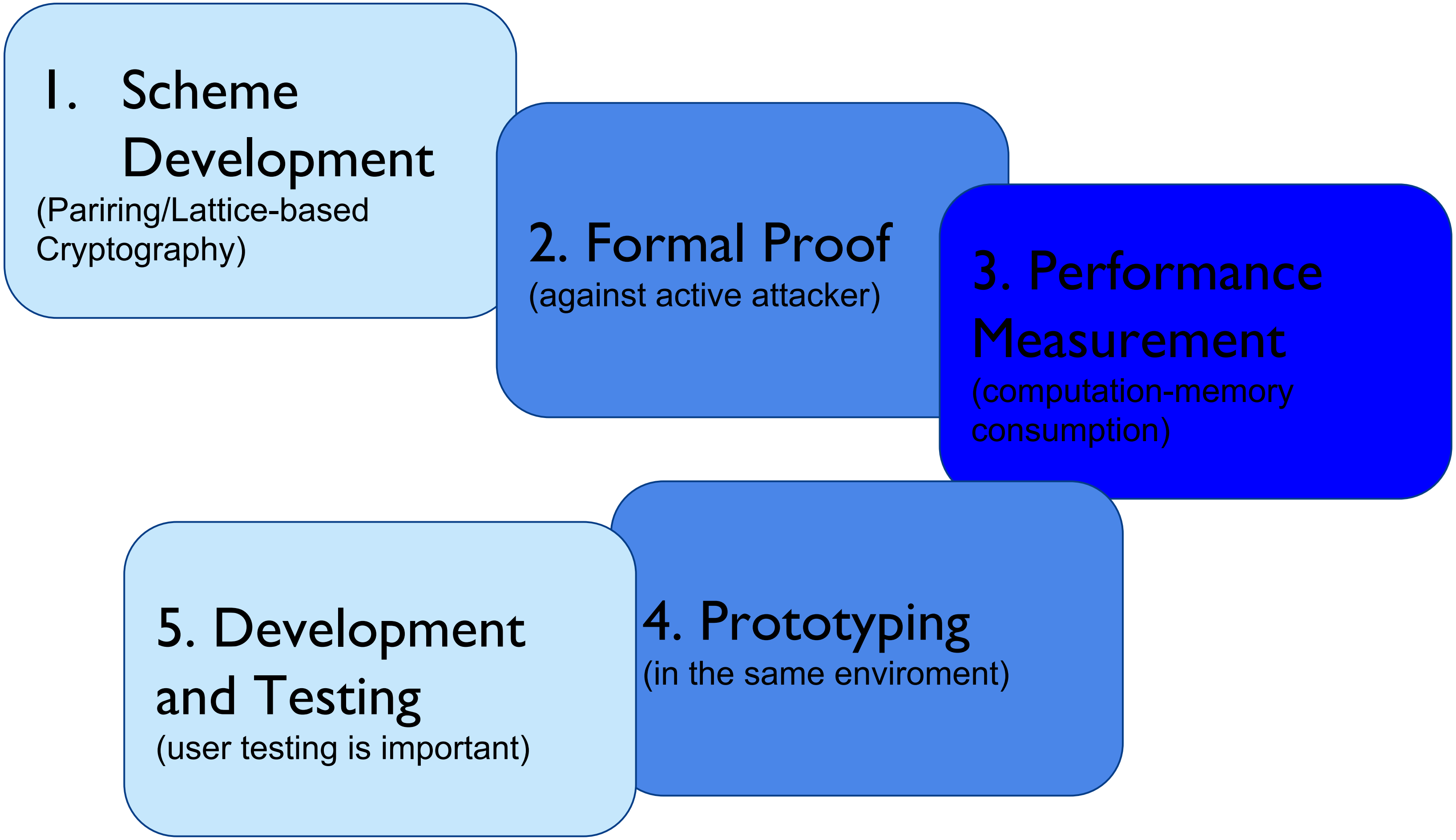
NICT/NTT

- *Prospective partner - collaboration in developing scheme and testing the implementation*

JAPAN

Methodology

For adaptive multi-authentication scheme we use provable cryptology, here are the steps:



1. Scheme Development
(Pariring/Lattice-based Cryptography)

2. Formal Proof
(against active attacker)

3. Performance Measurement
(computation-memory consumption)

4. Prototyping
(in the same enviroment)

5. Development and Testing
(user testing is important)

Methodology

For biometric based authentication the research are divided into two main stages, **training** and **testing** stages. In training stage, face videos are collected from various face databases. Several database that provided freely provided are listed as follows:

- MMI Facial Expression Database (http://mmifacedb.eu/)
- Facial Expression Dataset (http://www.affectiva.com/facial-expression-dataset/)
- Biwi 3D Audiovisual Corpus of Affective Communication - B3D(AC)^2 (http://www.vision.ee.ethz.ch/datasets/b3dac2.en.html)

Road Map

LIPI

Year	2018	2019	2020
Activities	Designing and Developing adaptive multi auth scheme Designing and Developing biometric key by face expression	Unit-module testing. Integrating between adaptive multi auth scheme and face expression Integration testing	User acceptance testing System improvement based on user testing result
Output	- scientific papers 4 proceedings: - requirement dan design report	- scientific papers 2 journal - prototype impelemtation system	- 1 patent - 1 copyright - system implementatioin

Outline

- Background
- Objectives
- Members, Methodology and Roadmap
- Budget
- Facility and Equipment

Budget Year 1

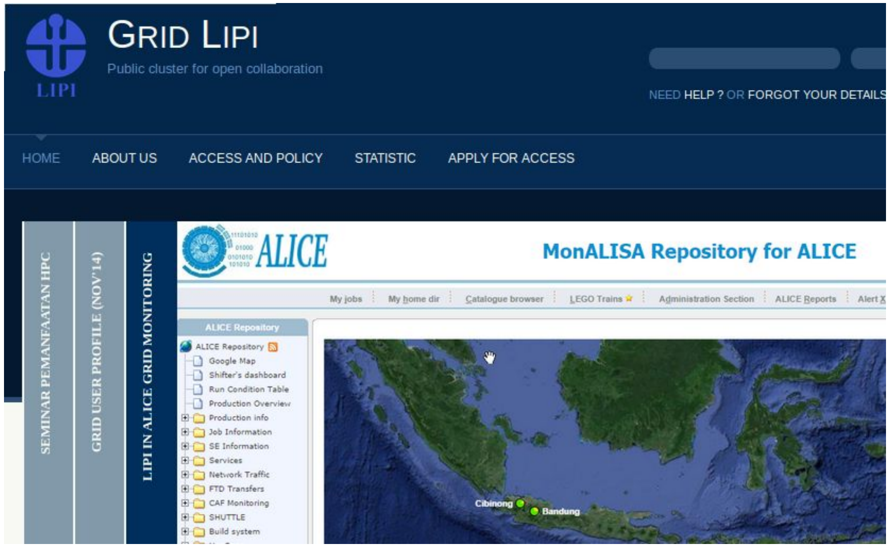
		Vol	Cost	Total cost
Equipment				
	Equipment for testing encryption scheme	1	550	550
	Data for Recruiting face expression video	350	25	8,750
	Equipment for develop mobile application for collecting face video	1	1,500	1,500
Travel				
	Attend a major international conf in Europe (i.e ECCV)	2	2,300	4,600
	Attend a major international conf in regional countries (Japan/China/Korea)	2	1,800	3,600
Joint workshop				
	Workshop in Indonesia	1	7,000	7,000
	Workshop in Malaysia	2	7,000	14,000
		TOTAL		40,000

Outline

LIPI

- Background
- Objectives
- Members, Methodology and Roadmap
- Budget
- Facility and Equipment

Facilities, Equipment and Other Resources



GRID LIPI

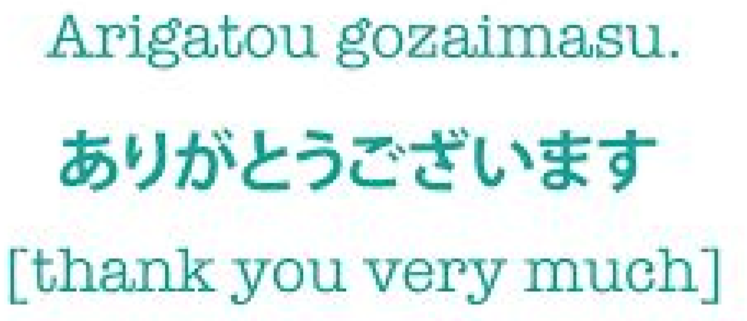
Public cluster for open collaboration

NEED HELP ? OR FORGOT YOUR DETAILS

Research Center of Informatics, Indonesian Institute of Sciences has a cloud infrastructure to develop and test the proposed system.

UTP and Swinburne Sarawak have small deep learning machines to develop the proposed system.

Thankyou - terima kasih



Arigatou gozaimasu.

ありがとうございます

[thank you very much]