Biometrics Today

How to Achieve Good Security Using an Imperfect Technology

Miroslav Kis, Ph.D.
Senior Advisor
Strategy - Information Security
BMO Financial Group

BMO Financial Group

The Objective

- To present an overview of the current state of biometric technology and its theoretical and practical limitations.
- Show how risk – based approach can be used to design biometric systems.

The Scope

1. Theoretical analysis of speaker and fingerprint recognition systems is used to motivate the discussion.
2. Speaker and fingerprint recognition systems have been tested. Test results support the conclusions.

Presentation Overview

1. Biometrics: Expectations and Technology Fundamentals
2. Speaker and Fingerprint Recognition
   - Theory and Test results
3. Biometrics: Theoretical and Practical Limitations
4. Fundamentals of Information Security
5. Information Security Engineering
   - Risk Based Approach
6. Biometric device implementation – A case study

Biometrics: Expectations

'Bio-Signature' uniquely identifies you!

Advantages:

- Your entry pass is always with you.
- No need to remember several passwords.

Concerns:

- It might be hard to protect 'bio-signature'. What happens if somebody steals an electronic copy of your 'bio-signature'!?

Are the expectations realistic?

Biometric Systems: Key Elements

1. **Features:** What are the characteristics we look for?
2. **Pattern Matching:** Compare the templates.
3. **Decision:** Is this the person?

Biometric Systems: Modes of Operation

1. **Enrolment:** New person is introduced.
2. **Normal operation:** Verification or identification.
3. **Maintenance:** Users are removed or templates are changed.

Features

Physiological or behavioural characteristic that can be used for personal identification has to be [3]:

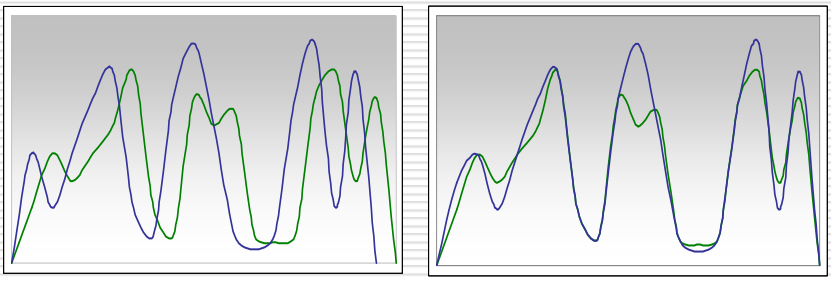
1. **Universal**: every person should have the characteristic;
2. **Unique**: no two persons should be the same in terms of the characteristic;
3. **Permanent**: the characteristic should be invariant with time;
4. **Collectable**: the characteristic can be measured quantitatively.

Speaker Recognition Features

1. The features are low-level speech signal representation parameters that convey complete information about the signal.
2. High-level characteristics like accent, intonation, etc. are encoded within the representation in a very complex and cryptic manner.
3. The features contain speaker-dependent components.
4. Uniqueness and permanence of the features is problematic.

Pattern Matching
Dynamic Time Warping

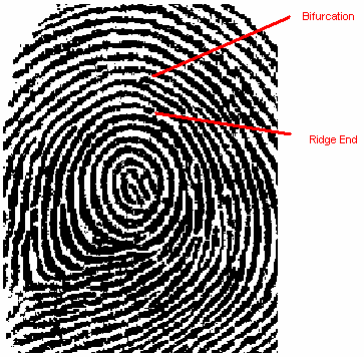
Scaling of patterns to achieve time alignment by using Dynamic Programming.



Alignment of two signals in time domain.

Fingerprint Recognition

1. Minutia based:
   - Minutia – features of a fingerprint (i.e. pores, ridges, etc.)
   - Features tested in practice for hundred years.
   - Minutia points are examined and stored as templates.
2. Template matching systems.



Sample Test Results

System	FAR	FRR	Remarks
Fingerprint	1.5 %	Up to 15%	An acceptable FRR can be achieved while keeping FAR low.
Voice	Up to 50 %	0 %	To achieve low FRR, FAR become prohibitively high.

Biometrics: Theoretical Limitations

Q1 Do the features that uniquely characterize people exist?

A1 Uniqueness and permanence of most of the features used in biometric systems have not been proven.

Q2 Is the human's ability to identify a person a limit that no automatic system can overcome?

A2 Automated systems might be able to identify people better than average person can do.

In practice, expert systems do not perform the task better than the experts who built them.

Biometrics: Theoretical Limitations

Q3 How important are the algorithms versus the knowledge of features and their relationships to achieve high identification accuracy?

A3 Knowledge of features and their relationships is fundamental for accurate biometric systems.

The algorithms play an important, still secondary, role in the process as no algorithm can compensate for the lack of the adequate features.

Biometrics: Practical Usability

The dream of perfect biometric systems that would recognize people with absolute accuracy is unrealistic.

For groups of a limited size, it is possible to find features that discriminate the members. Retraining of the system might be needed when a new person joins the group.

Combination of authentication mechanisms can provide better security.

Risk analysis should be used to determine where biometric systems can be used.

Information Security Fundamental Concepts

- Information reduces uncertainty about an event.
- Key elements:
  - Event (e.g. stock value increase),
  - Observer uncertain about the outcome.
- The observer can find out about the event directly or by learning from some data: written, stored electronically, communicated over the phone, fax etc.

Information Security Fundamental Concepts

- Two types of observers in information security:
  - Intended, *legitimate user*
  - Illegitimate user - *attacker*
- Information security protects information. What exactly does it mean?
  - Information has to be available to the legitimate user and its integrity has to be preserved
  - Prevent unauthorized users from obtaining the information - confidentiality.

Information Security Fundamental Concepts

- We have to understand who might learn about the event.

  Specifically:
  - Who might need or want the information and
  - Who might have means to get it

Information Security Engineering Key Steps

1. Resource Characterisation
2. Threat Analysis
3. Architecture definition
4. Vulnerability Analysis
5. Risk Analysis

Resource Characterisation

Key steps:

1. Identify all the data groups the systems will process.

2. For each group analyze:
   - Confidentiality -> Data shouldn't be seen!
   - Integrity -> Is the information changed?
   - Availability -> How quickly do we need it?

This is business' representative assessment!

Resource Characterisation Example

A high-level resource characterization of a trader's system would identify the following data groups:

- Reuter's stock price reports (I, A)
- Stock price trends analyses (C, I)
- Summary reports of completed trades (C, I)
- Trading system (C, I, A)
- Traders' personal information (C, I, A)

Note: the letters in brackets show which security attributes of the data group are important to protect (C – confidentiality, I – integrity, A – availability).

Threat Analysis Example
External Threats

- An attacker outside of the corporate network tries to gain the access to a trader's system and to impersonate him or her.

  This scenario would mean that the attacker breaks into the corporate network from outside, start remote session on a workstation and impersonates a trader by compromising the biometric device software.

- A person from another organizational unit or a non-employee gains a physical access to a trader's workstation.

  This scenario would mean that the attacker enters the trading floor and impersonates a trader by exploiting biometric device's vulnerabilities.

Threat Analysis Example
Internal Threats

- A trader gains remote access to another trader's system and impersonates him or her.

  This scenario would mean that the attacker starts remote session on another workstation and impersonates another trader by compromising the biometric device software.

- A trader impersonates another trader using the other trader's workstation.

  This scenario would mean that the attacker sits by another trader's workstation and impersonates him or her by compromising the biometric device software.

Threat Analysis Example
Internal Threats

- A system administrator gains remote access to a trader's system and impersonates him or her.

  This scenario would mean that the system administrator starts remote session on a trader's workstation and impersonates the trader by compromising the biometric device software.

- A system administrator impersonates a trader using the trader's workstation.

  This scenario would mean that the system administrator sits by trader's workstation and impersonates him or her by compromising the biometric device software.

Threat Analysis Example
External and Internal

- An attacker uses 'malware' application to monitor or change a trader's transactions.

  This scenario requires that an attacker has access and administrative privileges on the trader's workstation as well as an open communication channel to it.

- The biometric device misbehaves and attacks the trading applications.

  This scenario would mean that the biometric device software has malicious parts embedded into it.

Architecture Definition

- Architecture includes security components definition:
  - Technological solutions (e.g. Biometrics, VPN, Firewall)
  - Processes (e.g. Separation of duties)
  - People (e.g. logical and physical access to a system)
- The architecture has also to take into account:
  - Legal and regulatory requirements (e.g. Privacy)
  - Characteristics of existing infrastructure and components that will be used (e.g. CWAN, OS)
  - Time to market, financial, and risk constraints.

How to Select a Biometric Device?

ECOM (The Electronic Commerce Promotion Council of Japan) proposed the following six evaluation criteria:

1. Social acceptability
2. User acceptability
3. Threat countermeasure
4. Accuracy of authentication
5. Ease of use

How to Select a Biometric Device?

Template storage security.
Enrollment and verification times.
FAR vs. FRR.
Accuracy claims have been verified.
Resistance to impostors:

- Latent prints – Fingerprints
- Recordings – Voice

User-friendly system and administration tools.
Interoperable across platforms.
Vendor stability.

Biometric System:
Nonfunctional Requirements

- Training procedure for entering a new user into the system cannot last longer than 30 minutes.
- Removing an existing user from the system should be done in an hour.
- The alternative procedure for accessing the system in case biometrics fails has to be available. It should not take more than 3 minutes to start the system after a failure.

Vulnerability Analysis

- No system is absolutely secure!
- Higher the security - higher the price: we want to be secure but competitive at the same time.
- Vulnerability analysis reveals points in the architecture that can be used to compromise the information (e.g. OS weaknesses, encryption algorithm).
- Level of technical sophistication needed to exploit the vulnerability should be determined (user vs. an expert).

Risk Assessment

- Takes into account all already analyzed the components
- Compares calculated risk with acceptable risk threshold and
- Answers the question what should be changed in the architecture to keep the risk within the limits.

Quantitative Risk Analysis

- Classical definition:

$$r = \sum_i c(x_i)\,p(x_i)$$

$c(x_i)$ – price to be paid if x_i occurs

$p(x_i)$ – probability of x_i

- How do we estimate probabilities?
  - Frequency of occurrences
  - Level of belief
- What is the price of the reputational risk?

Quantitative Risk Analysis
Game Theoretic Approach

Company		B		
	Strategy	*Invest 5*	*Invest 2*	*Don't Invest*
A	*Invest 5*	**(-5, -5)**	**(-5, -8)**	**(-5, -10)**
	Invest 2	**(-8, -5)**	**(-3, -3)**	**(-2, -10)**
	Don't Invest	**(-10,-5)**	**(-10, -2)**	**(-10,-10)**

- Cooperate with others!
- Winner's curse – don't overspend in order to be the best!
- Who constitutes your group?
- Industry average is the best strategy in 'n players' game!

Quantitative Risk Analysis
Game Theoretic Approach

- What is 'rational' behaviour?

Risk averse	*Risk seeking*
Select between:	Select between:
1. $ 10 - sure gain	1. -$ 10 - sure loss
2. $ 100 p = 10%	2. -$ 100 p = 10%
$ 0 p = 90%	$ 0 p = 90%

- Do we make informed decisions?

Qualitative Risk Analysis: Scenario Based Assessment

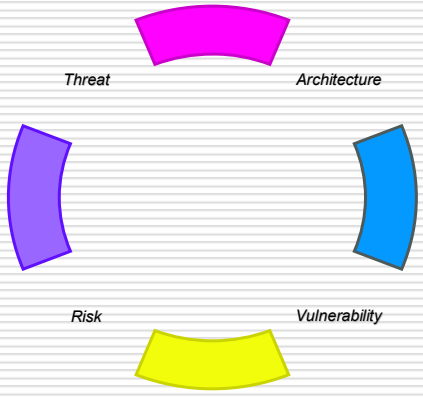
Questions answered by business and technical experts:

1. What can go wrong? *Identifies the event scenarios.*
2. How bad could it be? *Identifies the impacts.*
3. How could it happen? *Identifies the threats and vulnerabilities.*
4. What does this mean? *Identifies the business risks.*

Risks are estimated as High, Medium, Low.

Product Development - IS Risk Assessment Cycle

- The cycle is repeated synchronously with product development iterations as many times as necessary to optimize return on investment.



The Solution - Eliminate Some Risks

- **Malware**: User doesn't have administrative rights on their workstations.
- **Misbehaving Biometric Device:** The system will not be connected to the central directory. Security code review of the biometric application.
- **High Value Transactions:** Additional authentication is needed for transactions over a certain limit.
- **Trader's Personal Information:** Store the biometric information on a smart card.

The Solution – Mitigating Controls

- **Trader's Attack:** Trader uses only his or her workstation. All workstations are visible to all staff.
- **Administrator's Attack:** All the administrative actions are logged. Logs are reviewed.
- **Non-employee Attack:** Physical access to trading area enforced by a security guard.
- **Attacks Originating from Network :** Limited network access to the trading applications.
- **Trojan Horse Attack:** Limiting access from the trading application to external addresses.

Key Conclusions

1. The dream of perfect biometric systems that would recognize people with absolute accuracy is not realistic.
2. The key to the improvement of the existing biometric systems is better utilization of domain specific knowledge.
3. Disappointment with 'imperfect' biometric systems shouldn't prevent us from using it.
4. Risk analysis can tell us where we can use them.

Questions and Answers

Thank you!

You can also contact me later:

miroslav.kis@bmo.com
phone: (416) 513 - 5283