

# BehavioSec

## 생체 행위기반 인증 솔루션

2015. 7. 16

- I. 보안 시장의 이슈
- II. 회사 소개
- III. 솔루션 소개
- IV. 기타 - 동영상 데모

# 1. 보안 시장의 이슈

해킹 등으로 유출된 개인정보를 활용한 보이싱 피싱, 스미싱 등에 의해서 불법 송금 등의 이슈가 발생하고 있고 금융규제 및 환경이 변화함에 따라서 보다 강력하고 진보된 사용자에게 특화된 행동기반의 보안 및 인증 솔루션이 필요하게 되었습니다.

## » 강력한 인증솔루션의 필요성



DoD IT Asset Type	DARPA Reference System	Non-DoD IT Asset Type	Hacked on	Credentials lost
NIPRnet	Windows DMSS	American Honda Motor Co.	27-Dec-10	4.9m
Laptop Encryption	Guardian Edge	Bank of America	25-May-11	1.2m
DARPA VPN	Nortel	Carnegie Mellon University	8-Oct-07	19k
PDA	Blackberry/iPhone	Citigroup	27-Jul-10	30m
SIPRnet	Windows DSN	Clarkson University	10-Sep-08	245
JWICS	Windows DJN	Countrywide Financial Corp.	2-Aug-08	17m
Source Selection	TFIMS, I2O BAA Tool	Fidelity Investments	24-Sep-07	8.7m
Contract Management	GSA Advantage, SPS	Heartland Payment Systems	20-Jan-09	130m
Contract Invoicing	Wide Area Workflow	IBM	15-May-07	2k
Payroll	MyPay	Johns Hopkins Hospital	22-Oct-10	152k
Benefits	Benefeds.com	SAIC	7-May-08	630k
HR	hr.dla.mil	Sony	27-Apr-11	12m
Training	DAU	Stanford University	6-Jun-08	82k
Collaboration	Defense Connect Online	TD Ameritrade Holding Corp.	14-Sep-07	6.5m
Financial System, Local	Momentum	Texas A&M University	9-Nov-08	13k
Financial System, Agency	DFAS	TJMax Stores	17-Jan-07	100m
Credit Union	PCFUCU, NCU, etc.	U.S. Depart. of Veteran Affairs	14-May-07	103m
		U.S. Marine Corp - PSU research	26-Jul-07	208k
		Visa, MasterCard, and American Express	27-Dec-10	4.9m

Source: www.privacyrights.org/Data-breach

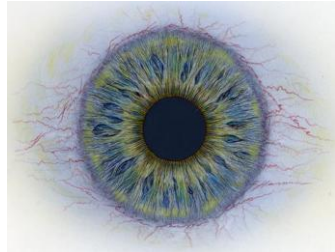
- 2014.03.12 ○ 카카오톡해킹, 스마트폰해킹, 스마트폰위치추적
- 2014.04.15 ○ 진화하는 악성코드...금융거래 추가 인증 우회 우려
- 2014.05.08 ○ 공인인증서 유출 관련 악성코드 주의
- 2014.06.18 ○ 스마트폰 해킹, 백신도 소용없다” [위키투리]
- 2014.09.04 ○ 공인인증서 1400건 해킹돼...특정 사이트 접속하자마자 공인인증서 유출
- 2014.09.28 ○ 급부상하는 핀테크의 세계①] IT, 금융으로 진격하다 [머니투데이]

- 개인정보보호법 강화, 전자금융거래법 강화
- 비밀번호, 보안카드 해킹에 의한 불법 송금 책임 문제
- 내부자 해킹에 의한 불법 내부정보 유출 문제

## 1. 보안 시장의 이슈

생체인증은 지문, 홍채, 정맥 등 신체의 특징을 이용한 인식과 사인, 목소리, 행동 등 행위를 이용한 행위 인증이 있으며, 행위 인증이 모방하기가 더 힘들어 보안수준이 더 높다고 할 수 있습니다.

### » 생체 인증 개요



## 2. 회사소개

### 2.1 제조사 : BehavioSec AB

BehavioSec은 스웨덴의 행동기반 인증 솔루션의 선두 주자로서 미국 국방성을 비롯하여 덴마크의 Danske Bank, 영국 Lloyds, 미국 Citi Bank 등 다양한 금융기관에서 이용중이며 6 digit Pin Key 만으로도 94%의 비정상 사용자를 식별할 수 있는 기술을 보유하고 있습니다.



#### BehavioSec AB



BehavioSec

스웨덴, BehavioSec AB” (비헤비오섹)

- 생체 행동기반 인증의 선두 주자
- 미국 국방성 DARPA (Defense Advanced Research Project Agency) 의 재정지원을 통한 기술 개발
- 미국 국방성 차세대 인증 시스템 후보
- 덴마크 Danske Bank : 2만 명 실 고객을 대상으로 Pilot 프로젝트를 수행 후 프로젝트 구축
- 영국 Lloyds, 미국 Citi Bank : Pilot 프로젝트를 수행
- 북유럽 120만 일반 모바일 사용자 Pilot 프로젝트 :
  - 6 digit PIN Key 만으로 94%의 비정상 사용자 식별
- 다수의 모바일 폰 파일럿
- 한국 Thetis FS(테티스에프에스), 국내 솔루션 및 서비스 공급계약  
→ BehavioSec Korea. (한국지사)

## 2. 회사소개

### 2.2 총판사 : 주식회사 앤서

최고의 기술력과 신뢰를 바탕으로 고객사의 중요 자산 및 정보를 안전하게 보호하여 본연의 비즈니스에 전념할 수 있도록 빅데이터 엔진을 기반으로 이상 금융거래탐지시스템, 통합보안모니터링시스템, 내부정보유출탐지시스템 등 솔루션'을 제공하는 금융보안 전문업체로서 고객과 더불어 Compliance & Security Community를 추구합니다.

#### » 주식회사 앤서



### VISION

- 빅데이터 엔진 개발 및 빅데이터 플랫폼 구축
- 빅데이터 엔진을 활용한 이상금융거래탐지시스템 등 시나리오 분석 시스템 구축
- 정보보호 전문 컨설팅 및 모의해킹 진단 수행

- 회사명

주식회사 앤서

- 대표자

박 준 형

- 전화번호

070-7768-4817

- 회사설립연도

2010년 5월 4일

- 사업분야

- 통합로그관리시스템 구축 및 개발
- 이상금융거래탐지시스템 구축 및 개발
- 빅데이터 플랫폼 구축 및 개발
- 통합보안관제시스템 구축
- 내부정보유출 감시 모니터링 구축
- 2차 인증 솔루션 컨설팅 및 구축

- 주소

서울특별시 강남구 테헤란로2길 21 (역삼동, 천궁빌딩2층)

- 해당부문 종사기간

2010년 5월 ~ 2015년 5월 현재 (만 5년)

### 3. 솔루션 소개

#### 3.1 제품의 구성



#### Two distinct solutions

##### Desktop

- 안티 바이러스 솔루션과 흡사한 형태
- 백그라운드에서 동작
  - 사용자는 인지할 수 없음
- 마우스와 키보드 모두 모니터링
- 비정상적인 행동 탐지 시 조치 가능
- 미국 국방성 DARPA 적용

##### Web & Mobile

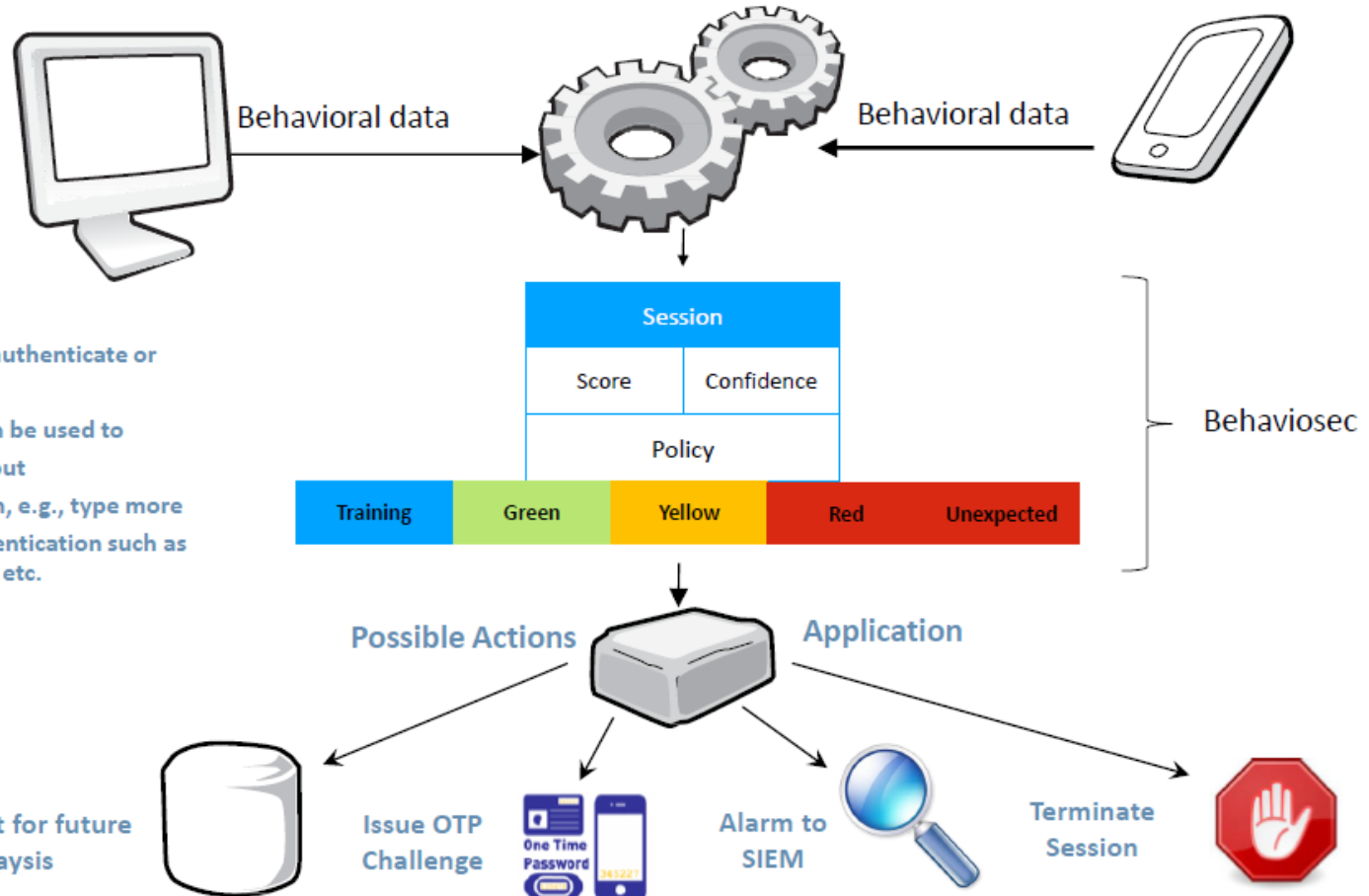
- 클라이언트 인스톨 과정이 없음
- 앱이나 웹 폼(forms)에 작은 코드 추가
- Stand-alone, server 인증
- 사용자의 학습에 의한 인증 체계
- RISK 스코어링을 통한 지수화 지원
- FDS 탐지를 위한 연동



### 3. 솔루션 소개

#### 3.1 제품의 구성

##### » 구성 개념도



- The score can be used to help authenticate or verify an end-user
- Failure to reach a threshold can be used to
  - Reject the user, i.e., logout
  - Ask for more information, e.g., type more
  - Request secondary authentication such as password question, OTP, etc.



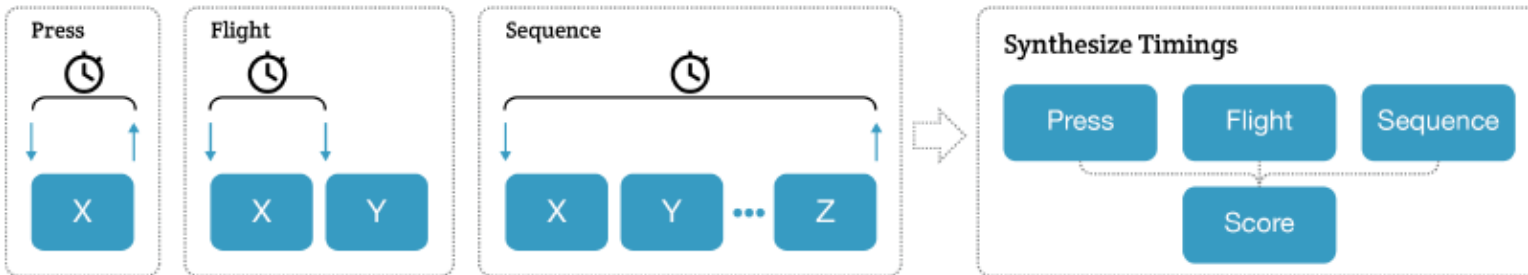
### 3. 솔루션 소개

#### 3.2 제품 종류 및 사용 방안

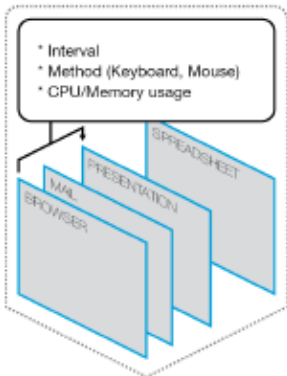
단순한 패스워드 입력이 아닌 패스워드를 입력하는 사용자의 행동 패턴, 예를 들어, 속도, 리듬, 위치, 압력, 가속도, 시퀀스 등 차이를 기반으로 사용자의 행위를 추적하면서 높은 정확도로 실제 사용자 진위 여부를 확인 해 줍니다.

#### » Desktop

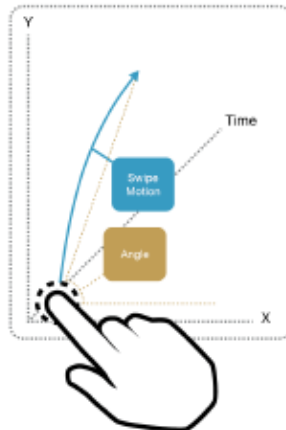
##### Keyboard Capture Intervals



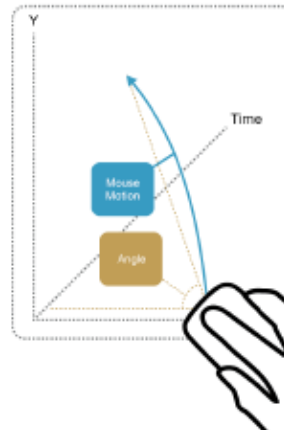
##### Application Switching



##### Touch Motion



##### Mouse Motion



*modality is the way or mode in which something exists or is done.*

### 3. 솔루션 소개

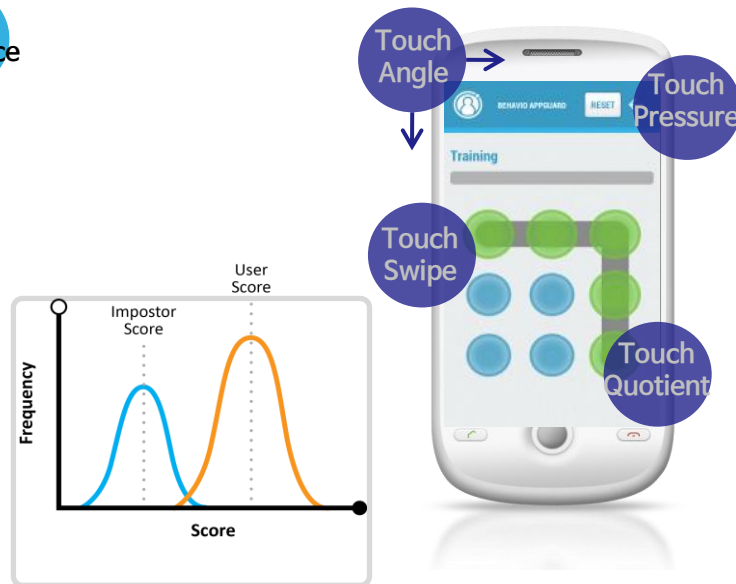
#### 3.2 제품 종류 및 사용 방안

» Mobile

#### IOS 인증



#### android 인증



#### ▶ 제품의 종류

컴퓨터 정보 및 e-Commerce, 모바일 디바이스 보호를 위한 사용자 인증 솔루션 (인터넷/모바일 상시 인증 시스템)

- BehavioWeb : PC 용
- BehavioMobile : 모바일 용
  - Apple IOS : 비밀번호 입력 패턴
  - google Android : 비밀번호 or 핀 입력 패턴

#### ▶ 활용 방안

- 비대면 금융거래를 위한 인터넷뱅킹, 스마트뱅킹 인증
  - FDS에서 의심거래로 판단된 거래의 본인 확인의 2차 인증 솔루션으로 활용
- CD/ATM 기기의 송금, 출금 등 비밀번호 인증 등

모바일 디바이스 사용자, 인터넷 상거래 사용자, 인터넷 금융 거래 사용자, 통신망 공급자, 인터넷 포탈 공급자 및 사용자, 기업 내 고객정보 관리자, 기업 내 중요정보 관리자, 국가정보기관 및 군 정보기관, 중요 연구소

**1회성 또는 테스트 성 인증이 아니라 사용자의 진위 여부를 지속적으로 확인하는 항시 2팩트 인증 시스템 (비밀번호 + 비밀번호 입력 패턴)**

### 3. 솔루션 소개

#### 3.2 제품 종류 및 사용 방안

##### » Mobile

App Fields

Backend Score

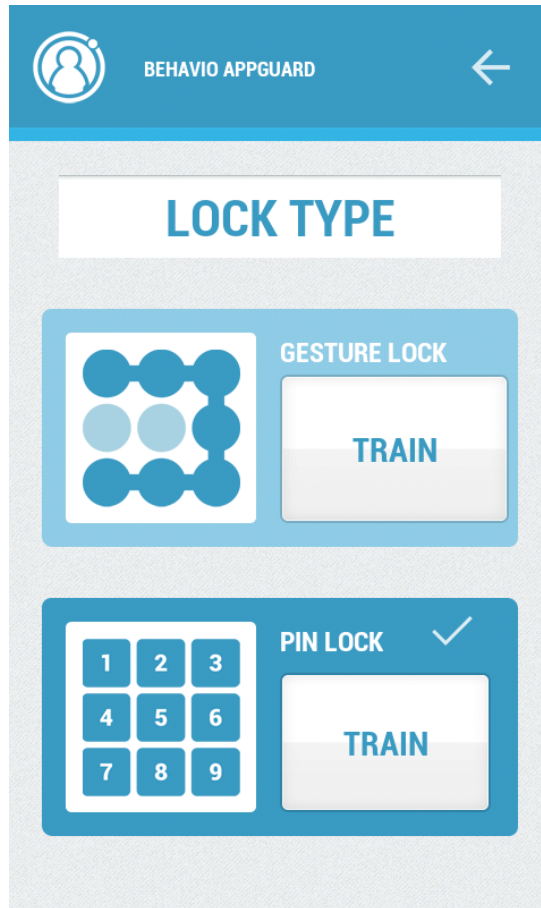


- SDK for App developers to get Biometric data from iPhone or Android.
- Rich behaviour monitoring if platform allows (Android).
- Keystroke timings from native keyboard.
- **Integrated** to BehavioWeb for back-end risk based authentication.

### 3. 솔루션 소개

#### 3.2 제품 종류 및 사용 방안

» Mobile



- Extended authentication methods for BYOD.
- Secure mobile devices.
- A Biometric lock without extra hardware.
- Looks at how the user types or swipes a PIN code.
- Allows or denies access to phone or specific applications

### 3. 솔루션 소개

#### 3.2 제품 종류 및 사용 방안



Gesture Demo

### 3. 솔루션 소개

#### 3.2 제품 종류 및 사용 방안

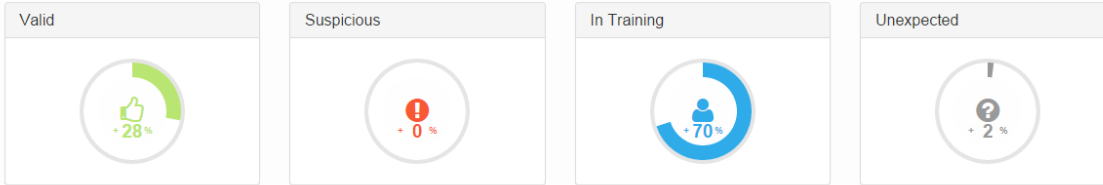
» Password Demo

### 3. 솔루션 소개

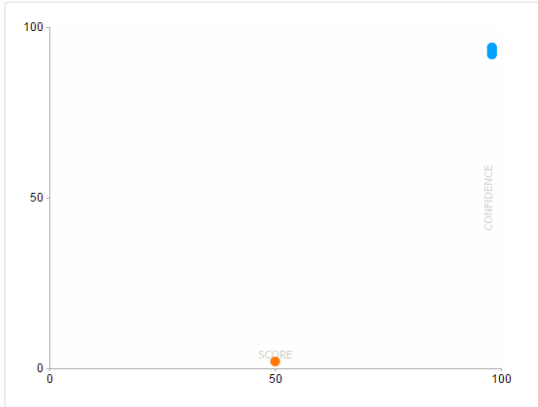
#### 3.2 제품 종류 및 사용 방안

##### » Dashboard

###### Overview



###### Latest Sessions



###### Filter

Date: 2015-04-14 10:40 tc

Tags:

User ID	Session ID	Score	Conf	Start date	End date	Options
✓ j park	75160367	100.00	94.67	2015-07-13 10:40:05	2015-07-13 10:40:09	📊 🔍
? magnustest	3tsl-DK08IPo6HXpVUqL0c6J.behav loweb	50.00	0.00	2015-07-09 19:04:59	2015-07-09 19:05:12	📊 🔍
✓ j park	24610231	98.79	93.24	2015-07-07 14:15:02	2015-07-07 14:15:12	📊 🔍
✓ j park	24605833	100.00	93.23	2015-07-07 14:14:18	2015-07-07 14:14:21	📊 🔍
🕒 j park	24604648	100.00	94.26	2015-07-07 14:14:06	2015-07-07 14:14:09	📊 🔍
🕒 j park	24603031	100.00	92.90	2015-07-07 14:13:50	2015-07-07 14:13:53	📊 🔍
🕒 j park	24600038	100.00	94.08	2015-07-07 14:13:20	2015-07-07 14:13:23	📊 🔍
🕒 j park	24588174	100.00	93.23	2015-07-07 14:11:21	2015-07-07 14:11:25	📊 🔍
🕒 j park	24586866	100.00	93.83	2015-07-07 14:11:08	2015-07-07 14:11:11	📊 🔍
🕒 j park	24581788	99.99	92.44	2015-07-07 14:10:17	2015-07-07 14:10:21	📊 🔍



### 3. 솔루션 소개

#### 3.3 솔루션의 핵심기술(1/2)

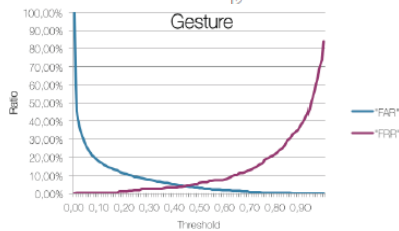
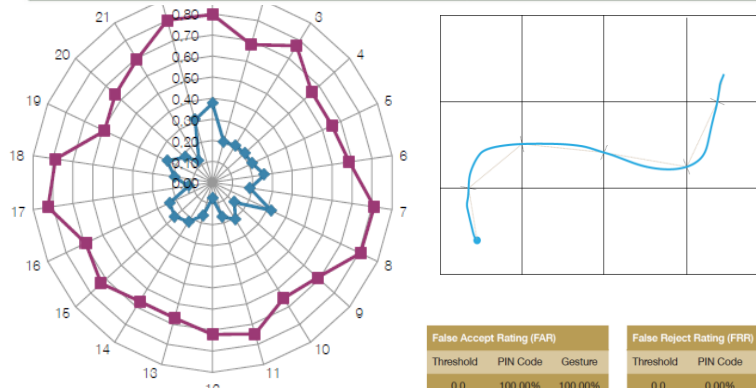
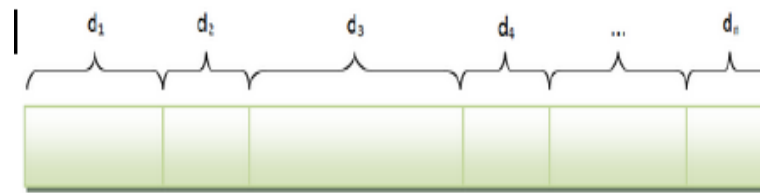
BehavioSec은 단순히 비밀번호나 PIN 패턴을 입력하는 속도뿐만 아니라 사용자의 행동패턴을 분석하는 것이 아니라 속도, 리듬, 위치, 압력, 가속도, 시퀀스 등 다양한 정보를 바탕으로 사용자의 행동패턴을 습득 & 축적 후 이를 통계 분석하여 사용자의 진위 여부를 정확하게 판단합니다.

#### » 핵심 기술

##### Bayes' Theorem

$$\frac{\prod_{i=1}^n E_i}{\prod_{i=1}^n E_i + \prod_{i=1}^n (1 - E_i)} \quad (n = 1, 2, 3, \dots)$$

Where  $n$  is the amount of tests



False Accept Rating (FAR)			False Reject Rating (FRR)		
Threshold	PIN Code	Gesture	Threshold	PIN Code	Gesture
0.0	100.00%	100.00%	0.0	0.00%	0.00%
0.1	27.80%	17.59%	0.1	0.00%	0.00%
0.2	19.20%	11.1%	0.2	0.40%	0.82%
0.3	12.60%	7.53%	0.3	1.60%	2.46%
0.4	10.20%	5.02%	0.4	2.40%	3.08%
0.5	7.30%	3.06%	0.5	4.00%	5.55%
0.6	4.60%	1.81%	0.6	6.80%	7.40%
0.7	2.50%	0.08%	0.7	9.60%	12.75%
0.8	1.00%	0.03%	0.8	14.80%	21.39%
0.9	0.20%	0.00%	0.9	30.00%	37.65%
1.0	0.00%	0.00%	1.0	96.80%	83.74%

#### 🕒 행동패턴의 분석

사용자의 행동 패턴, 예를 들어, 속도, 리듬, 위치, 압력, 가속도, 시퀀스 등 차이를 기반으로 사용자의 행위를 추적하면서 높은 정확도로 실제 사용자 진위 여부를 확인 해 줍니다.

사용자가 어떻게 타자를 치고 스크린을 밀고 확대하는지 등을 기억하며, 스크린 터치 시 자주 가해지는 압력의 세기와 특정 문자들을 입력할 때 그 사이에 생기는 간격을 계산하고, 평소 사용자가 기기를 드는 각도, 마우스를 놓은 위치도 기록합니다.

사용자의 행동패턴을 액션 별로 인지 트레이닝을 통해 습득 & 축적 후 이를 통계 분석을 통해 사용자 진위 여부를 정확히 판단합니다.

#### 🕒 FRR / FRA / EER

- 오탐/미탐/EER에 대한 최적화 계산방식

#### 🕒 부정 사용자의 식별률

- Danske Bank 사용자 : 2만 명 기준 99.8%
- 인터넷 쇼핑 신용카드 사용자 : 97.52~99.87 %
- 단순 6자리 비밀번호 사용자 : 94%

### 3. 솔루션 소개

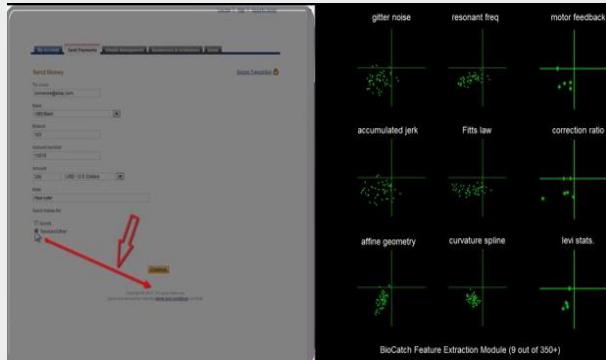
#### 3.3 솔루션의 핵심기술(2/2)

BehavioSec은 단순히 비밀번호나 PIN 패턴을 입력하는 속도만으로 사용자의 행동패턴을 분석하는 것이 아니라 속도, 리듬, 위치, 압력, 가속도, 시퀀스 등 다양한 정보를 바탕으로 사용자의 행동패턴을 습득 & 추적 후 이를 통계 분석하여 사용자의 진위 여부를 정확하게 판단합니다.

#### » 행동패턴 분석과 식별 과정

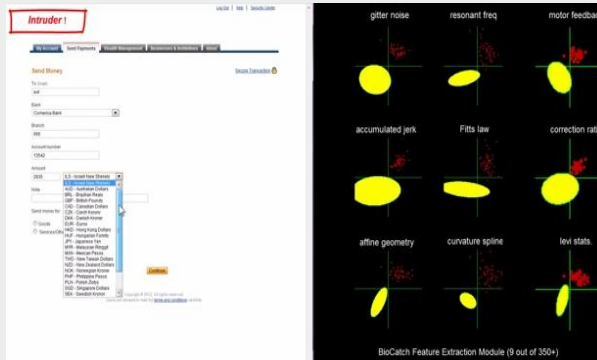
#### 1. 행동패턴 분석 및 학습

행동 패턴(마우스속도, 리듬, 위치, 압력, 가속도, 시퀀스 등)의 사용자 고유의 행동패턴을 학습



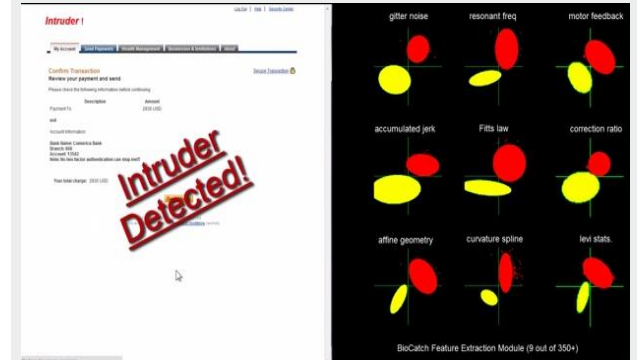
#### 2. 행동패턴 상시 모니터링 가동

사용자의 행동패턴이 불일치 여부 상시 모니터링 가동



#### 3. 불법 사용자 식별 및 차단

사용자의 행동패턴 불일치시 거래 중단 및 경고 발생





## 5. 구축 사례

### 5.1 덴마크 Danske Bank

Using only the login form we can properly verify if it is the correct user/an imposter in 97.4% of the cases. See figure 4.



#### Equal error rate of login

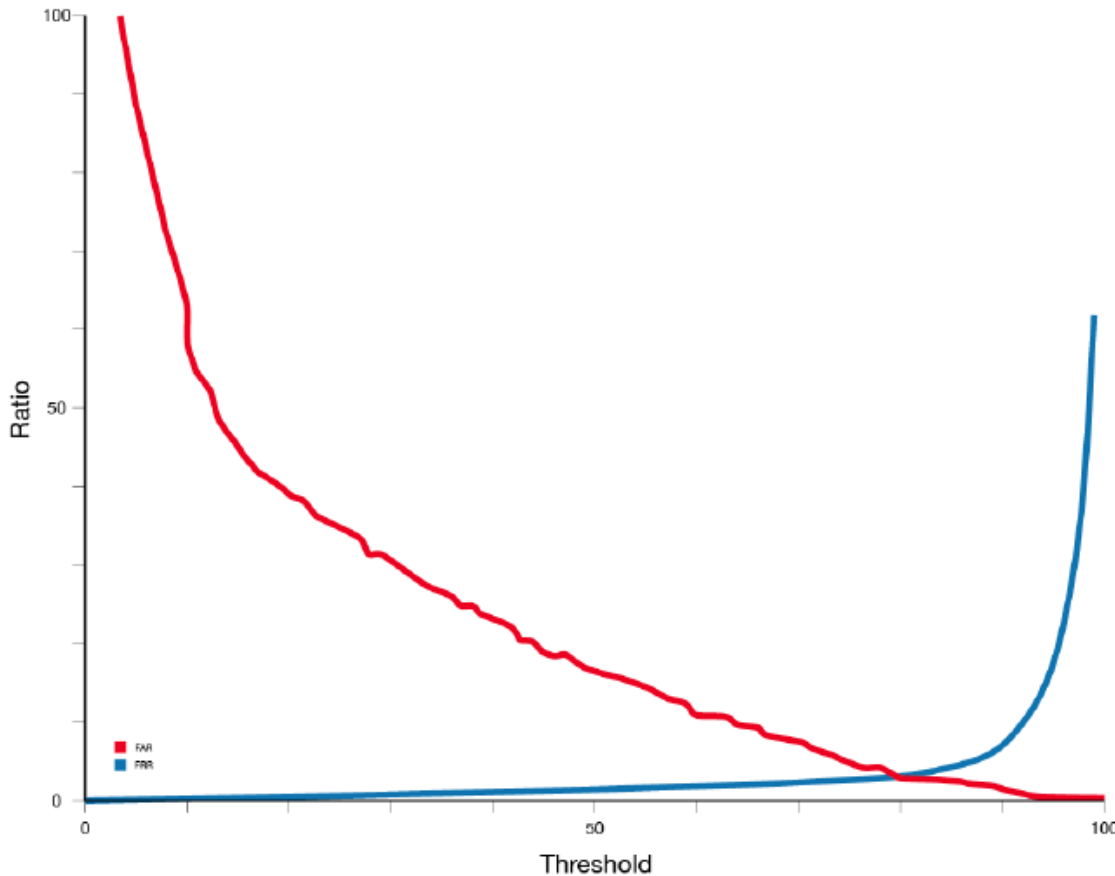


Figure 4: Equal error rate of login (combining Username/Password fields): 2.6% at threshold 79.9.

The timing data was gathered from 4 different input forms, as can be seen below, with their corresponding input fields:

- Login form
  - o Username (6-10 characters, static)
  - o Password (4-8 characters, static, anonymous)
- Verification form
  - o One-Time Password  
-6 characters, free text, anonymous
- Fund Transfer form
  - o 3-5 free text fields (various lengths)
- Signature form
  - o Password (same as login form)

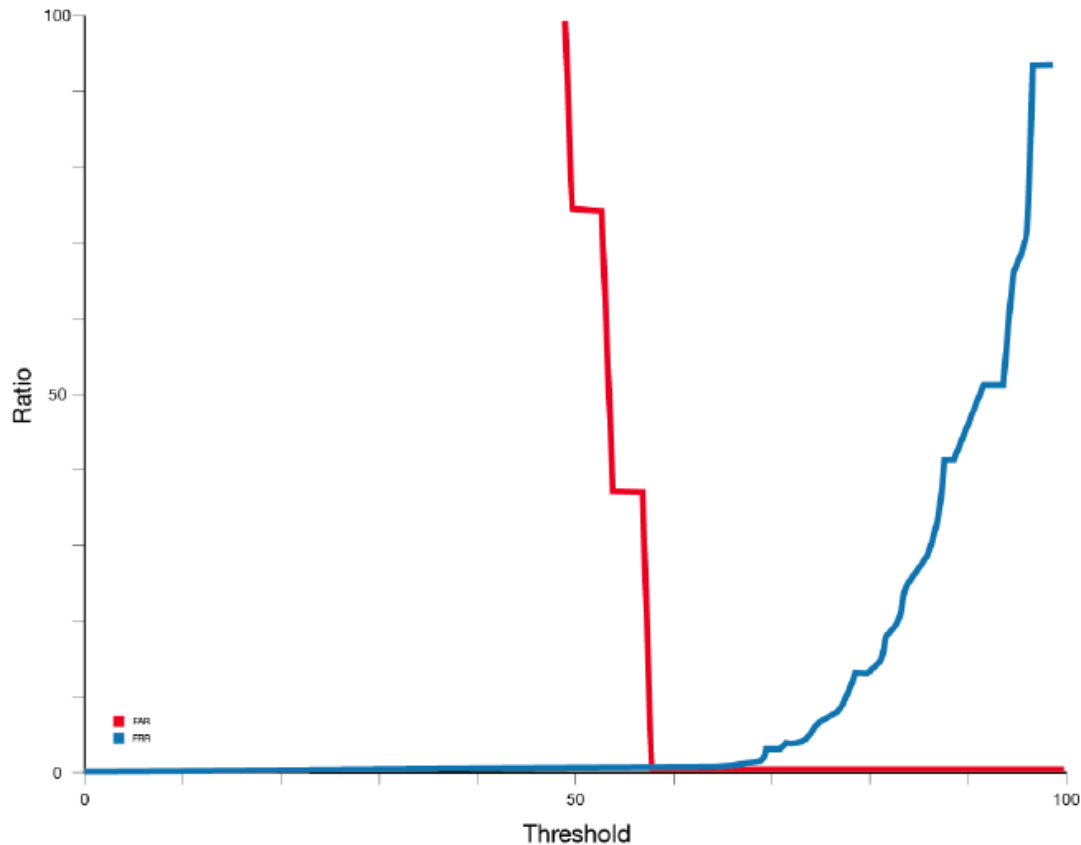
## 5. 구축 사례

### 5.1 덴마크 Danske Bank

Over a whole session, by combining the results from each individual transaction, we can see that the accuracy is increased significantly with an accuracy of 99.7%, see figure 5. To be able to test this we defined a session as the following combined transactions:



#### Equal error rate of a whole session



- Login (Username/Password)
- One-Time Password
- Fund transfer
- Signing of transfer (Password)

Figure 5: Equal error rate of a whole session: 0.3% at threshold 57.9.

감사합니다.  
Q&A