Universitatea Ştefan cel Mare Suceava

Facultatea de Inginerie Electrică şi Ştiinţa Calculatoarelor

**Seminarul ştiinţific cu participare naţională**
***Sisteme Distribuite***
**Ediţia a XII-a, Suceava, 17 decembrie 2014**

# SECURING INTERNET-BANKING APPLICATIONS BY USING BIOMETRICS

## *Securizarea aplicațiilor de tip internet-banking folosind tehnologii biometrice*

**Eng. Cătălin Lupu, PhD Stud,** *"Ştefan cel Mare" University of Suceava, ROMANIA*
**Valeriu Lupu, prof.dr.,** *"Ştefan cel Mare" University of Suceava, ROMANIA*


**Investeşte în oameni !**

FONDUL SOCIAL EUROPEAN
Proiect cofinanțat din Fondul Social EUROPEAN prin Programul Operațional Sectorial Dezvoltarea Resurselor Umane 2007 – 2013
Această lucrare a beneficiat de suport financiar prin proiectul

**Performanță sustenabilă în cercetarea doctorală şi post doctorală – PERFORM**

**Contract nr POSDRU 159/1.5/S/138963**
Axa prioritară 1 - Educația şi formarea profesională în sprijinul creşterii economice şi dezvoltării societății bazate pe cunoaştere
Domeniul major de intervenție 1.5 - „Programe doctorale şi postdoctorale în sprijinul cercetării”

# 1. Introducere

- Cele mai multe bănci din România și din lume furnizează servicii de internet banking clinților
- Sunt mai multe tipuri de autentificare în acest tip de aplicații, dintre care cele mai importante sunt: prin utilizator și parolă, cu utilizarea sau nu a unui certificat privat; prin utilizator și o parolă generată dinamic, de către un dispozitiv de tip “digipass” (OTP – one time password – o parolă formată de obicei din 6 cifre, generate după un anumit algoritm) sau primită printr-un mesaj scris (SMS) pe un număr de telefon înregistrat în baza de date a băncii
- Datorită creșterii numărului de utilizatori și a tranzacțiilor realizate prin această metodă, este nevoie de o creștere a securității în procesul de autentificare sau de semnare a operațiunilor

- Parolele și token-urile pot fi furate, pierdute sau uitate
- Și din acest motiv, este mai simplu să utilizăm ceva ce nu poate fi pierdut sau uitat (deşi poate fi falsificat, dar există metode foarte puternice de determinare a realității caracteristicilor), cum ar fi o amprentă digitală sau imaginea unui iris
- Acestea pot înlocui cu mult succes clasicele parole
- S-au realizat mai multe studii referitoare la utilizarea caracteristicilor biometrice în domeniul bancar, nu doar pentru aplicații de internet banking, dar şi pentru accesul angajaților la conturi, în cadrul ATM-urilor, POS-urilor, etc.
- Un studiu foarte bine documentat este cel scris de Hosseini S. Mohammadi, intitulat "*Review Banking on Biometric in the World's Banks and Introducing a Biometric Model for Iran's Banking System" ("Analiză a utilizării biometriei în băncile din lume şi introducerea unui model biometric pentru sistemul bancar din Iran"*), Journal of Basic and Applied Scientific Research, 2(9) p. 9152-9160, 2012

- Principalele concluzii ale acestui studiu sunt:
  - din cele 121 de bănci incluse în acest studiu, cele din Asia dețin o proporție de 52% în ceea ce priveşte utilizarea biometriei în diverse scopuri;
  - amprenta digitală este cea mai utilizată caracteristică, având un procent de utilizare de 48%;
  - operațiile la bancomatele băncilor (ATM) reprezintă 45%, urmate de controlul accesului în clădiri (24%) şi la aplicațiile internet destinate angajaților (22%), iar pentru internet-banking proporția este de doar 10%.
- În continuare se vor prezenta:
  - principalele metode de autentificare în cadrul aplicațiilor de internet banking;
  - o scurtă introducere referitoare la cele mai utilizate caracteristici biometrice, potrivite pentru a fi utilizate în acest tip de servicii (amprenta şi irisul);
  - specificațiile unei aplicații în Java, care este în curs de dezvoltare, în vederea simulării accesului la o pagină securizată de internet banking prin folosirea amprentei digitale

# 2. Internet banking

- Termenul are ca sinonime “online banking”, “virtual banking” sau “e-banking”
- Conceptul de internet-banking reprezintă o pagină web furnizată printr-un canal securizat (https), în care utilizatorul se poate autentifica, în vederea realizării de operațiuni sau de gestionare a conturilor proprii
- Este o metodă mai veche de management a conturilor, începuturile fiind în anii ‘80, când a fost introdus “sistemul bancar la distanță, folosind mediul electronic”

- Principalele modalități de autentificare sunt:
  - User  şi parolă, una dintre cele mai comune şi mai nesigure metode;
  - Utilizator şi parolă, împreună cu un certificat digital privat, furnizat de bancă; această metodă este mai sigură decât precedenta
  - User-name static şi parolă o parolă generată dinamic, denumită OTP (one-time password), generată de un dispozitiv de tip “digipass”, prezentat în figura de mai jos:

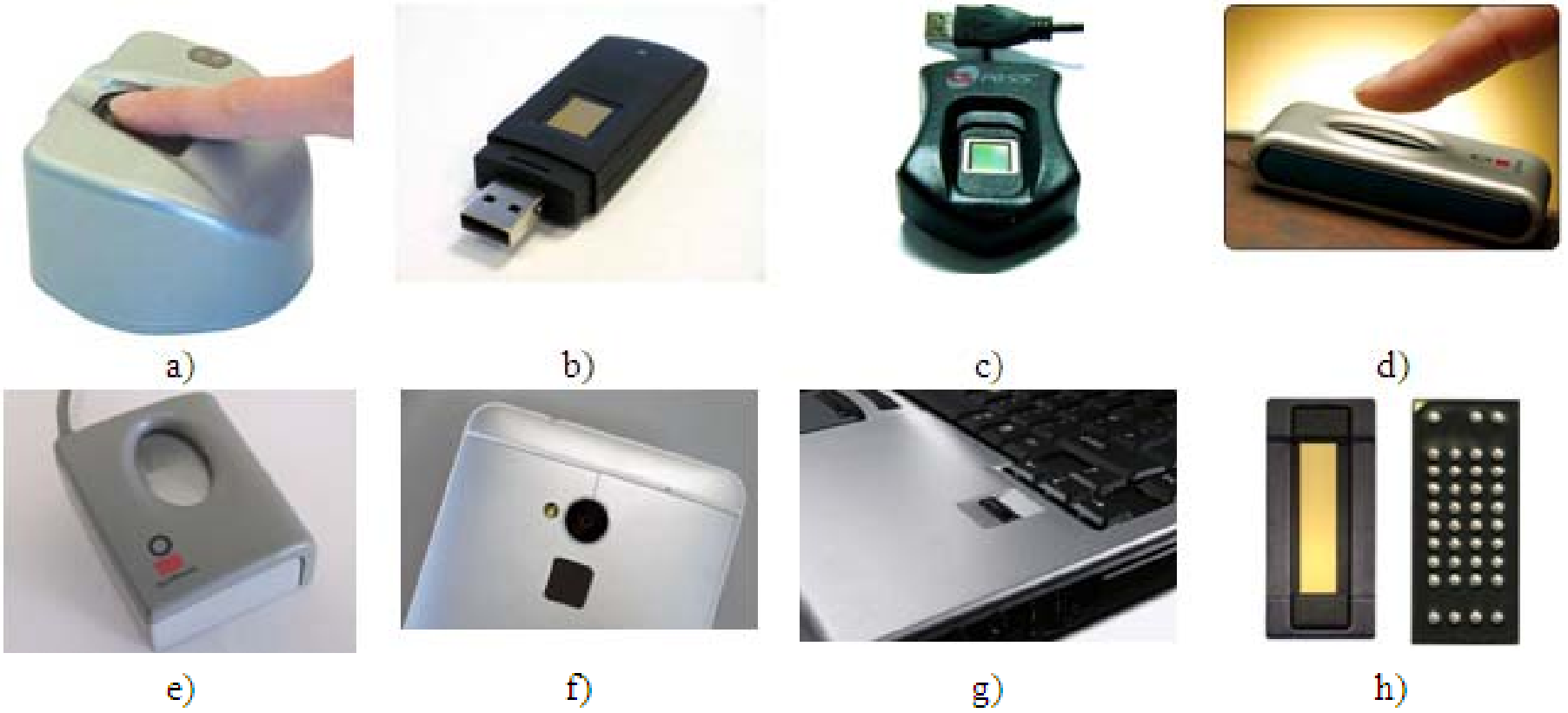
# 3. Caracteristici biometrice

- Biometria, termen derivat din cuvintele greceşti bios (viață) şi metrikos (măsură), reprezintă un complex de metode automatizate destinate identificării unei persoane folosind unele caracteristici biometrice (geometria palmelor, amprenta digitală, irisul, retina, geometria feței, presiunea sanguină, etc.) sau comportamentale (timbrul vocal, configurația ADN, dinamica scrisului, scanarea semnături, dinamica acționării tastelor, etc.) ale acesteia, ştiut fiind faptul că unele dintre acestea pot identifica în mod unic o persoană. Dată fiind această unicitate, informațiile biometrice pot fi folosite pentru proiectarea şi implementarea unor tehnologii, echipamente şi sisteme destinate diseminării identității cu performanțe mult superioare celor existente.

# 3.1. Amprenta digitală

- Una dintre cele mai cunoscute caracteristici biometrice este reprezentată de amprenta digitală, savantul britanic Sir Francis Galton fiind primul care a propus utilizarea amprentei degetelor în scopul identificării,  în secolul al XIX-lea. Acesta a elaborat un studiu detaliat asupra amprentelor degetelor în care a prezentat şi un sistem de clasificare bazat pe amprentele tuturor celor zece degete ale mâinilor, sistem ce stă şi astăzi la baza schemelor de identificare aflate în uz; amprentarea a fost introdusă ca metodă de identificare a persoanei în poliția britanică începând cu anul 1890 de către Sir Richard Edward Henry.

- În figura de mai jos sunt prezente mai multe dispozitive pentru preluarea amprentei digitale:




Sensors and scanners for acquiring fingerprints: (a) Lumidigm, Inc. - Venus Series Biometric Fingerprint Sensor, (b) Kingston USB Fingerprint flash drive, (c) CS PASS, (d,e) digitalPersona, U.are.U, (f) HTC One with fingerprint sensor below the camera , (g) UPEK - TCS5 TouchStrip Fingerprint Sensor , (h) AuthenTec - AES1711

# 3.2. Irisul

- În anul 1987, doi oftalmologi, Leonard Flom şi Aron Safir, au descoperit că irisul uman posedă caracteristici care permit folosirea imaginii sale pentru identificarea persoanelor. Ei au arătat, prin metode statistice, pe un eşantion cuprinzător de persoane, că irisul fiecărui ochi este specific fiecărei persoane, fiind diferit chiar şi la gemenii univitelini.
- Concomitent, au fost dezvoltați algoritmi matematici care folosesc ca bază de comparație aproape 250 de caracteristici independente ale irisului. Folosind acest model matematic, probabilitatea ca două persoane să aibă acelaşi iris este mai mică de $10^{-72}$.
- Sistemul este puțin invaziv, bazându-se în special pe tehnici fotografice. Imaginea irisului este preluată corect, chiar dacă persoana respectivă poartă ochelari sau lentile de contact. Substituirea persoanei este posibilă, dar foarte dificilă, fiind necesare lentile de contact care să imite toate caracteristicile folosite de sistemul de identificare.

- O proprietate importantă a ochiului real este faptul că diametrul pupilei prezintă mici oscilații („hippus”) o dată sau de două ori pe secundă, chiar şi la o iluminare uniformă. O fotografie a unui iris sau a lentilelor de contact imprimate cu imaginea unui iris nu vor suferi astfel de variații în timp.
- O absență a oscilațiilor de tip „hippus” sau a altor mici variații în structura irisului în timp ar putea constitui o dovadă a faptului că o fotografie sau un simulacru al ochiului a fost prezentat, în locul unui iris real, şi va indica o intenție de fraudă. Această facilitate de a face o diferență între un iris real şi o fotografie sau un simulacru reprezintă un atu important în ceea ce priveşte securitatea, fiind posibilă prin mijloacele rapide pentru definirea şi trasarea frontierei pupilei.

În figurile de mai jos se prezintă o utilizare a irisului pentru accesul la sistemul de operare Windows, precum şi camera folosită pentru preluarea imaginii irisului.

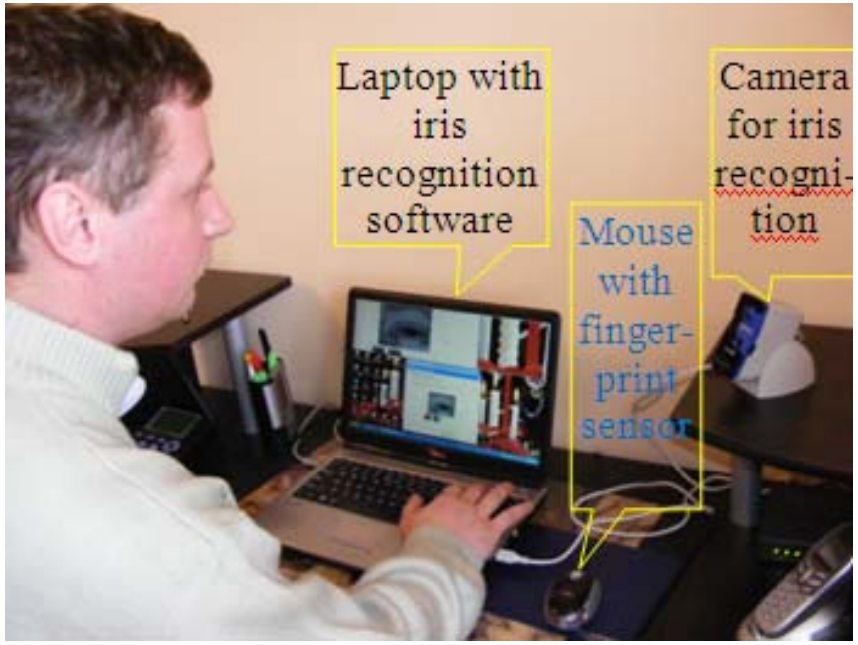

1. Irisul folosit pentru “login”


2. Camera Panasonic BM-ET100US

# 4. Utilizarea biometriei pentru accesul la aplicații internet-banking

- Caracteristicile biometrice pot fi folosite pentru creşterea securității în procesele de autentificare la aplicații de internet banking
- Pot fi folosite în mai multe scopuri:
  1. Un scanner de amprentă poate fi montat pe un dispozitiv digipass, pentru a nu mai fi necesară introducerea unui PIN pentru deschiderea acestuia. Conceptul, această posibilitate este prezentată în figura de mai jos:

2. Acelaşi scanner poate fi conectat la un calculator pentru a se realiza autentificarea în aplicațiile de tip internet-banking pe baza acestuia. De asemenea, în cazul dispozitivelor de tip smart-phone, se poate folosi ecranul de tip capacitiv al acestora pentru preluarea amprentelor. În cazul irisului este puțin mai complicat, deoarece imaginea acestuia se preia în infra-roşu, pentru o mai bună determinare a caracteristicilor, mai ales la irişii de culoare foarte închisă, în care imaginea preluată în lumină naturală nu ar furniza suficiente informații necesare atingerii scopului propus.
3. Se poate realiza de asemenea un sistem multimodal, compus din iris şi amprentă, după cum este prezentat în figura de mai jos:



# 5. Aplicație JAVA pentru managementul accesului la servicii de internet-banking

- Pe parcursul cercetărilor în domeniu, autorii au dezvoltat şi continuă îmbunătățirea unui software în Java, pentru managementul accesului la servicii de internet-banking.
- Aplicația dezvoltată este capabilă să:
  1. Preia imaginea de la un dispozitiv de citire a amprentei;
  2. Execute operația de înregistrare (enrollment) în sistem a utilizatorului şi stocarea datelor într-o bază de date;
  3. Realizeze identificarea sau verificarea persoanei pe baza comparării unei amprente furnizate de un utilizator cu una stocată anterior în baza de date. Sistemul poate permite sau nu autentificarea în sistem. După validarea amprentei, utilizatorul va fi redirecționat automat către pagina de internet-banking a băncii selectate.
- S-a ales mediul de dezvoltare Java deoarece poate fi integrat foarte uşor pe majoritatea dispozitivelor, de tip desktop, laptop, telefon mobil, etc.

# 6. Concluzii

- Acest subiect poate fi dezvoltat în continuare, existând numeroase domenii în care se poate utiliza biometria;
- Se poate îmbunătăți aplicația realizată, în aşa fel încât să poată funcționa cu iris şi amprentă, sau doar cu una dintre acestea. Este cazul persoanelor care nu posedă una dintre aceste caracteristici (de exemplu, care au amprente care nu pot fi preluate prin mijloace clasice - se întâmplă la aprox. 7% dintre persoane)
- Utilizarea biometriei este foarte utilă în creşterea securității referitoare la identificarea şi semnarea electronică a operațiunilor din cadrul serviciilor de internet banking.


# MULȚUMIRI

Această lucrare a beneficiat de suport financiar prin proiectul "Performanță sustenabilă în cercetarea doctorală şi post doctorală - PERFORM", Contract nr. POSDRU/159/1.5/S/138963", proiect cofinanțat din Fondul Social European prin Programul Operațional Sectorial Dezvoltarea Resurselor Umane 2007-2013.

Vă mulțumesc pentru atenție !!!

seminarul ştiinţific

# SISTEME DISTRIBUITE





Google

Go

CENTRUL DE CERCETARE STIINTA CALCULATOARELOR


## Seminarul ştiinţific cu participare naţională

## Sisteme Distribuite

### Ediția a XII-a, Suceava, 17 decembrie 2014

**Tematica seminarului:**
- Calcul paralel si distribuit
- Inteligenta artificiala distribuita
- Sisteme industriale distribuite
- Baze de date distribuite
- Recunoasterea formelor si procesarea imaginilor
- Sisteme informatice educationale
- Tehnologii web
- Tehnologii informationale

Seminarul se adreseaza in primul rand tinerilor cercetatori si cercetatorilor in curs de devenire: doctoranzi si masteranzi.

Pot fi trimise spre publicare articole de specialitate, lucrari de cercetare, studii de caz cu caracter stiintific, demonstratii practice ale unor produse inovatoare, care se încadreaza in tematica seminarului sau in domenii inrudite.

Lucrarile vor fi redactate si prezentate în limba romana sau într-o limba oficiala a Uniunii Europene. Rezumatul si cuvintele cheie vor fi redactate in limba engleza. Se accepta maxim doua lucrari de autor. Instructiunile de redactare sunt aceleasi cu cele descrise in documentul "Preparation of Papers for IEEE TRANSACTIONS and JOURNALS (May 2007)" (o copie poate fi descarcata si de la adresa TRANS-JOUR.doc).

**Date importante:**
Trimiterea lucrarilor: 2 decembrie (ora 16:00)
Comunicarea de acceptare: 8 decembrie

Trimiterea lucrarilor

**Galerie imagini:**



seminarul ştiinţific

# SISTEME DISTRIBUITE



EDITIA 2014
- Apel participare
- Organizatori
- Cuprins
EDITIA 2013
EDITIA 2012
EDITIA 2011
EDITIA 2010
EDITIA 2009
EDITIA 2008



CENTRUL DE CERCETARE STIINTA CALCULATOARELOR

**Universitatea "Stefan cel Mare" Suceava**
**Centrul de Cercetare in Stiinta Calculatoarelor**
organizeaza

Seminarul stiintific cu participare nationala
**Sisteme Distribuite**
Editia a XII-a, Suceava, 12 decembrie 2014

**Program Committee**

Sabin BURAGA– A.I. Cuza University of Iasi, Romania
Christophe CHAILLOU – Laboratoire d'Informatique de Lille, France
Mitica CRAUS – Technical University of Iasi, Romania
Adina Magda FLOREA – "Politehnica" University Bucuresti
Vasile Gheorghita GAITAN – Stefan cel Mare University of Suceava, Romania
Ileana HAMBURG – IAT Gelsenkirchen
Stefan HOLBAN – Universitatea Politehnica Timisoara
Adrian GRAUR – Stefan cel Mare University of Suceava, Romania
Laurent GRISONI – Universite des Sciences et Technologies de Lille, France
Daniel KAYSER – Universite Paris-Nord, France
Vasile MANTA - Universitatea Tehnica Gh. Asachi, Iasi
Vladimir MESYURA – Vinnitsya State University, Ukraine
Nadejda Ruxandra MEZINCESCU – Academia Romana
Dan Laurentiu MILICI – Stefan cel Mare University of Suceava, Romania
Cornelia NOVAC – Universitatea Galati
Stefan-Gheorghe PENTIUC – Stefan cel Mare University of Suceava, Romania
Ioan SALOMIE – Universitatea Tehnica Cluj Napoca
Bernard TOURSEL – Laboratoire d'Informatique de Lille, France
Cristina Elena TURCU – Stefan cel Mare University of Suceava, Romania
Alexandru VALACHI – Technical University of Iasi, Romania
Radu VATAVU – Stefan cel Mare University of Suceava, Romania
Mihai Horia ZAHARIA - Technical University Iasi, Romania

**Organizing Committee**

Stefan-Gheorghe PENTIUC
Radu VATAVU
Vasile Gheorghita GAITAN
Cristina Elena TURCU
Doru Eugen TILIUTE
Dan Laurentiu MILICI
Remus Catalin PRODAN
Mirela DANUBIANU
Nicolae MORARIU
Marius Cristian CERLINCA
Tudor Ioan CERLINCA
Adina Luminita BARILA
Andy Cristian TANASE
Alexandru LARIONESCU
Ovidiu SCHIPOR
George VLAD
Gabriela FREITAG

seminarul ştiinţific

# SISTEME DISTRIBUITE



EDITIA 2014
- Apel participare
- Organizatori
- Cuprins

EDITIA 2013
EDITIA 2012
EDITIA 2011
EDITIA 2010
EDITIA 2009
EDITIA 2008



CENTRUL DE CERCETARE STIINTA CALCULATOARELOR

**Chairmen:**
Vasile Gheorghita GAITAN
Cristina Elena TURCU
Stefan-Gheorghe PENTIUC

**Lucian Andries, Vasile Gheorghita GAITAN**
Overview of a Microcontroller with a hardware Scheduler

**Adina BARILA**
Implementation of quantum algorithms. A study case

**Ioan UNGUREAN, Nicoleta Cristina GAITAN**
A solution to integrate de Internet of Things concept in a SCADA application

**Nicoleta Cristina GAITAN**
An overview regarding the improvement of the nMPRA architecture

**Adrian POPOVICI, Ioan UNGUREAN**
An Architecture for the Industrial Internet of Things

**Ionel ZAGAN, Vasile Gheorghita GAITAN**
CPU architecture description based on fine-grained multithreading and hardware scheduler engine

**Catalin LUPU, Valeriu LUPU**
Securing internet-banking applications by using biometrics

**Catalin LUPU, Valeriu LUPU**
Overview on the beginnings of personal recognition based on human iris

**Stefan-Gheorghe PENTIUC**
Geographical Localization Techniques in Android

**Ionut-Alexandru ZAITI**
Human-Mobile Device Interaction Based on Natural Gestures