MICHIGAN STATE UNIVERSITY

Personal Authentication in Cyberspace

Arun Ross

Associate Professor

Michigan State University

rossarun@cse.msu.edu

http://www.cse.msu.edu/~rossarun/i-probe

The i-PRoBe Lab at MSU

- Director: i-PRoBE Lab
- Co-authored: Two books on Biometrics
- Research Advisor: 6 PhD Students, 4 Post-doctoral Fellows
- Collaboration: Several biometric research groups
- CITeR: NSF Center for Identification Technology Research
- VP of Education: IEEE Biometrics Council
- Vice-Chair: IAPR TC-4 (Biometrics)

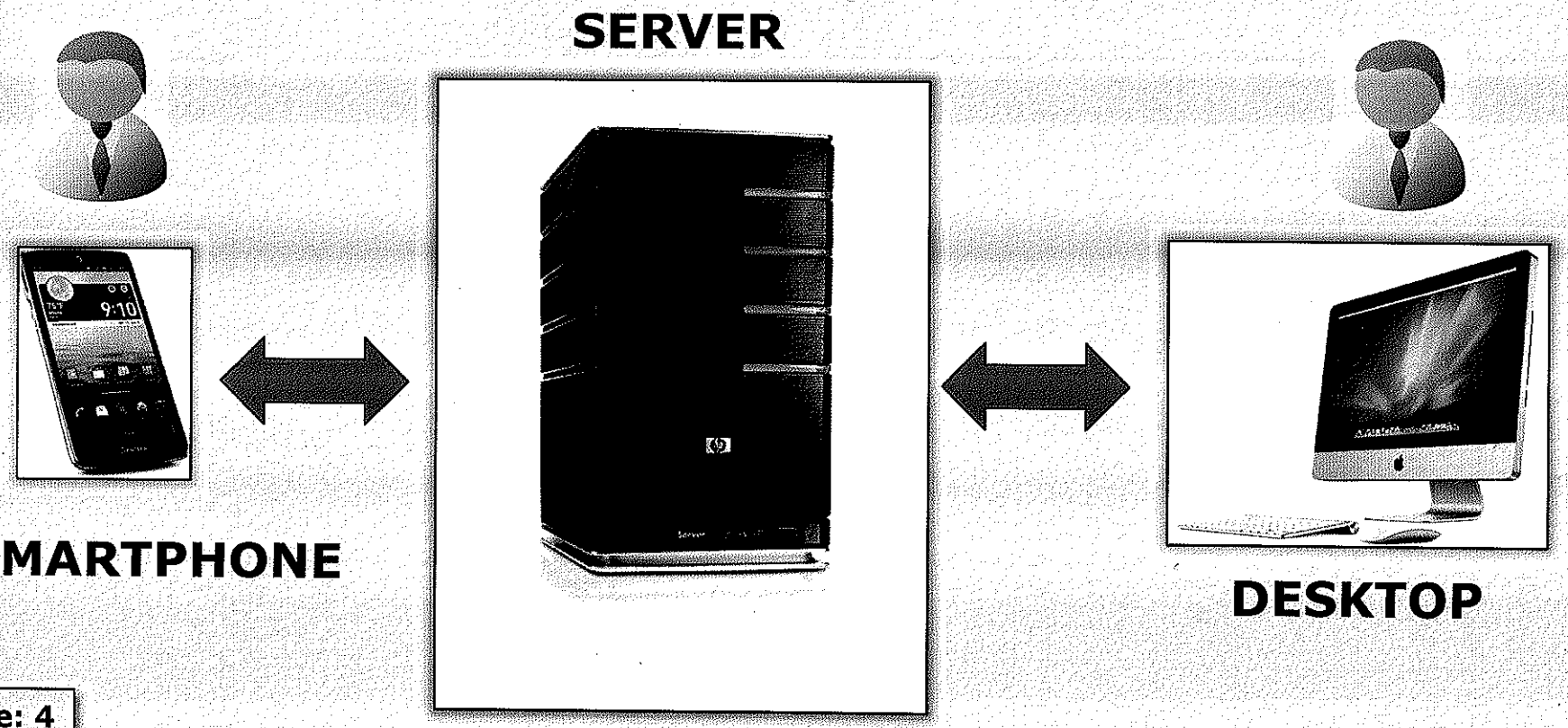
Internet and the Web

- Increasing number of Internet and Web users
- The Web is no longer an impassive entity presenting static information
- Rather, it is a dynamic engine ingesting and disseminating a variety of multimedia, financial, health and textual data pertaining to individuals, corporations, organizations and governments
- The preponderance of data accessible via the Internet, poses several security and privacy concerns

© Arun Ross

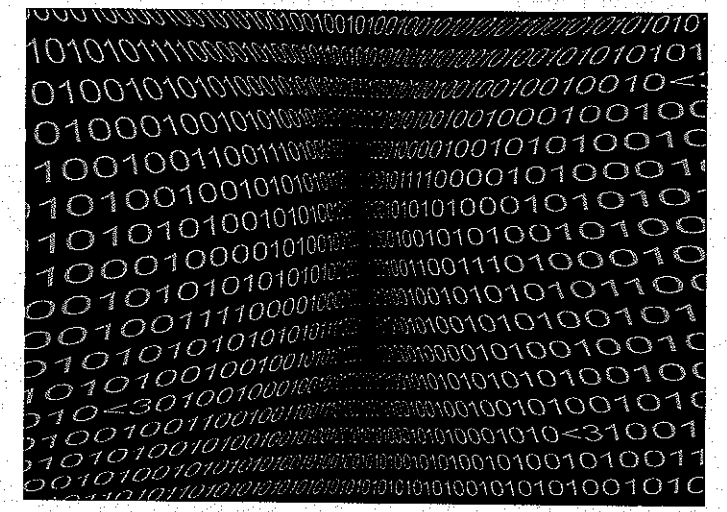
Complex Network: Man and Machine

- Computers, Laptops, Servers, Smartphones, TVs
- People



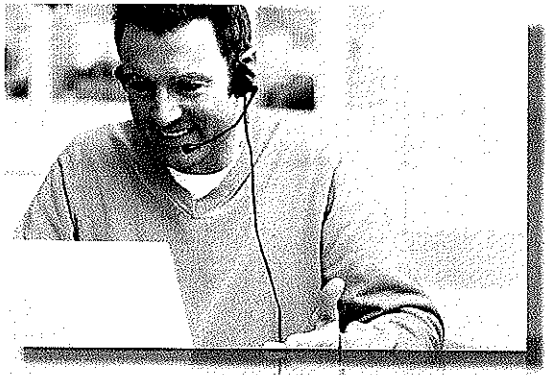
CyberSpace

- A large number of social, financial, business transactions are being conducted over the Internet
- But Cyberspace is not just about data – it is also about individuals



Establishing Identity

Face-to-face interactions



Remote interactions

Human-machine interactions

- "The ease and confidence with which individuals can assert their identity improves economic efficiency and social cohesion".

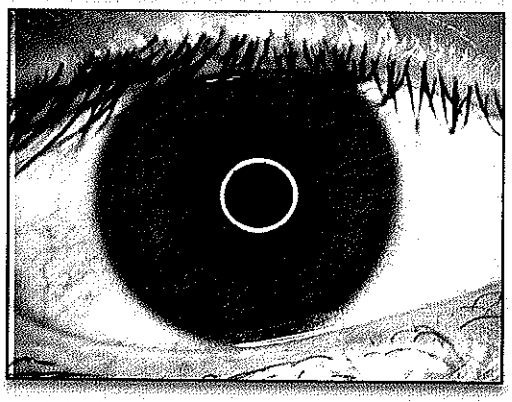
(Sir James Crosby, Former Deputy Chairman of UK's FSA)

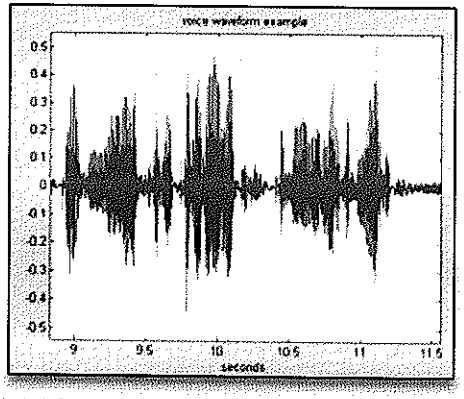
Authenticating Individuals

- A number of Internet-based applications require user authentication
- Necessary to verify the "identity" of the user prior to granting access
  - To user's account
  - To protected data
- Password-based authentication has limitations
  - Guessed, Shared, Divulged, Stolen
  - Forgotten, Reset,

Biometrics

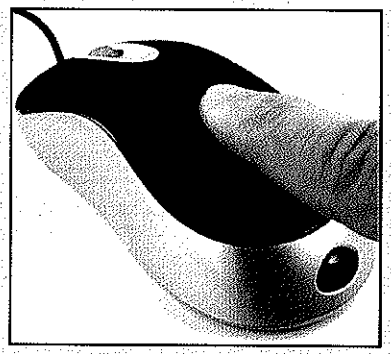
- Biometrics is the science of recognizing people based on physical and behavioral traits
- Examples include face, fingerprints, iris and voice

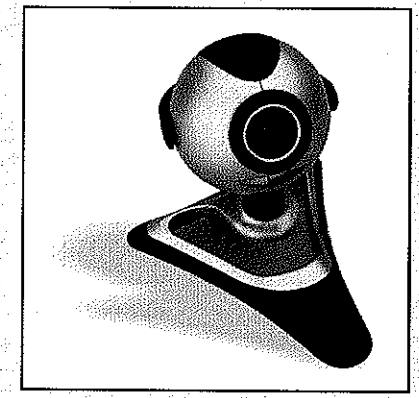




Biometric Sensors

- Biometric traits can be acquired using compact sensors





Why Biometrics?

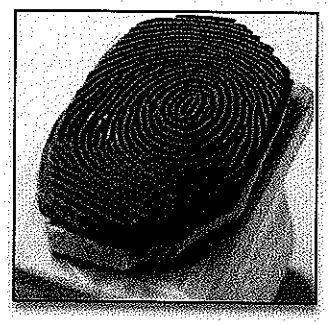
- Convenience: No need to carry credentials (pw, ID)
- Audit trail: Who accessed this bank account?
- Fraud detection: Is this person the rightful owner of the credit card?
- De-duplication: One person, one identity

Multi-factor Authentication

- Biometrics based on "something you are"
  - as opposed to "something you know" (password) or "something you have" (ID card)
- Facilitates non-repudiation
- Combining biometrics and passwords for secure access to protected data and information
- User is tightly connected to his/her digital identity
- Joint digital identity using biometrics

Privacy Enhancing Technology

- Preserving the privacy of a user's stored biometric data
  - Prevent cross-linking across applications
  - Prevent gleaning additional information from biometric data (e.g., medical ailment)
- Ensuring that the biometric trait being acquired is real and not an artificial object



Protecting Biometric Data

- Methods to impart security and privacy
  - Liveness detection
  - Data encryption
  - Biometric cryptosystems
  - "Cancellable" biometrics
  - Visual cryptography
  - Differential privacy

Summary

MICHIGAN STATE UNIVERSITY

- Personal authentication on the Internet is a critical factor
- Biometrics + passwords can be judiciously used
- Combining multiple biometrics can improve recognition accuracy
- Methods being developed to detect altered or spoofed biometric traits
- Methods being developed for protecting biometric data to improve system integrity and impart privacy