Biometrically Enhanced Software-Defined Radios

Joseph P. Campbell, William M. Campbell,
Douglas A. Jones, *Scott M. Lewandowski,*
Douglas A. Reynolds, Clifford J. Weinstein
{jpc, wcampbell, daj, scl, dar, cjw}@ll.mit.edu

MIT Lincoln Laboratory
Lexington, MA

Software Defined Radio Forum Technical Conference
Orlando, FL

17-19 November 2003

This work was sponsored by the Defense Advanced Research Projects Agency under Air Force contract F19628-00-C-0002. Opinions, interpretations, conclusions, and recommendations are those of the authors and are not necessarily endorsed by the US Government.

Outline

- Introduction & Motivation
- User Authentication
- Architecture
- Conclusions & Implications for Cognitive Radio

Authenticating Radios & Users (1)

- Motivation: need to authenticate users to their radios and networks to…
  - Ensure access and actions are authorized
  - Realize the full potential of software-defined radio and cognitive radio
- Observations:
  - Devices can be reliably authenticated (e.g., cryptographically)
  - Reliably authenticating users is a challenge
- Our approach: exploit many forms of user authentication, including biometrics and user behavior profiles (local actions and network interactions)

Authenticating Radios & Users (2)

- User recognition can be combined with situational awareness to enhance the authentication process
  - Strength of the user authentication can be adapted based upon the situation/environment/mission awareness and risk of operation (e.g., benign versus sensitive operations)
  - Multiple authentication factors (e.g., voice communication, mouse movement, dialogue structure, etc.) can be used to provide continuous authentication (e.g., to mitigate the impact of lost or captured radios)
  - Biometric-based authentication can be combined with tokens/knowledge for emergency transfer of operations

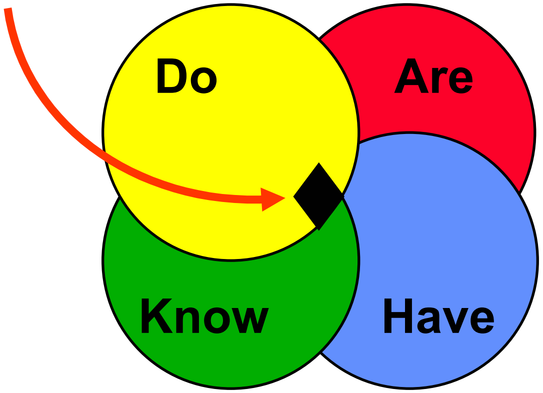
- Our approach enhances user convenience in addition to enhancing security
  - Automatic recall of user preferences
  - Biometric logins and screen unlocking
  - Application-specific predictive behaviors

Outline

- Introduction & Motivation
- User Authentication
- Architecture
- Conclusions & Implications for Cognitive Radio

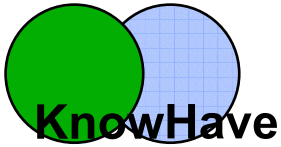
User Authentication

- Biometric: automatically recognizing a person using distinguishing traits
  - Voice, face, fingerprint, and iris are popular biometrics*
- Biometrics can be combined with other forms of authentication
- The four pillars:
  - Something you have - e.g., token
  - Something you know - e.g., password
  - Something you are - e.g., voice
  - Something you do - e.g., use patterns


Strongest authentication

*See Biometric Consortium www.biometrics.org for others

Why Not Use Just Knowledge and/or Tokens?



- Knowledge can be forgotten or compromised
- Tokens can be lost or stolen

- Ease of Use
  - How many good passwords can you remember?
    - Work, Home, Bank, …
- Cost Savings
  - 20-50% of corporate help desk calls are password related
  - 24*7 help desk support costs about $150/yr. per user
- Security
  - Common hacker tools can typically guess 30% or more of the passwords on a network
  - Some hackers claim 90% success
  - Guessing improves with side information
    - At DEA, 30% passwords = ? (hint: see monitor bezel)
    - Post-It Notes (hint: see under keyboard)

Why Not Use Just Biometrics?

Are

- Unlike knowledge- and token-based authenticators, biometrics cannot be transferred between users
  - Can lead to difficulties (e.g., difficulty transferring operation in cases of emergency)
- The four pillars can be used together to:
  - Overcome these difficulties
  - Provide convenience to users
  - Provide strong user authentication

Behavior-Based Authentication

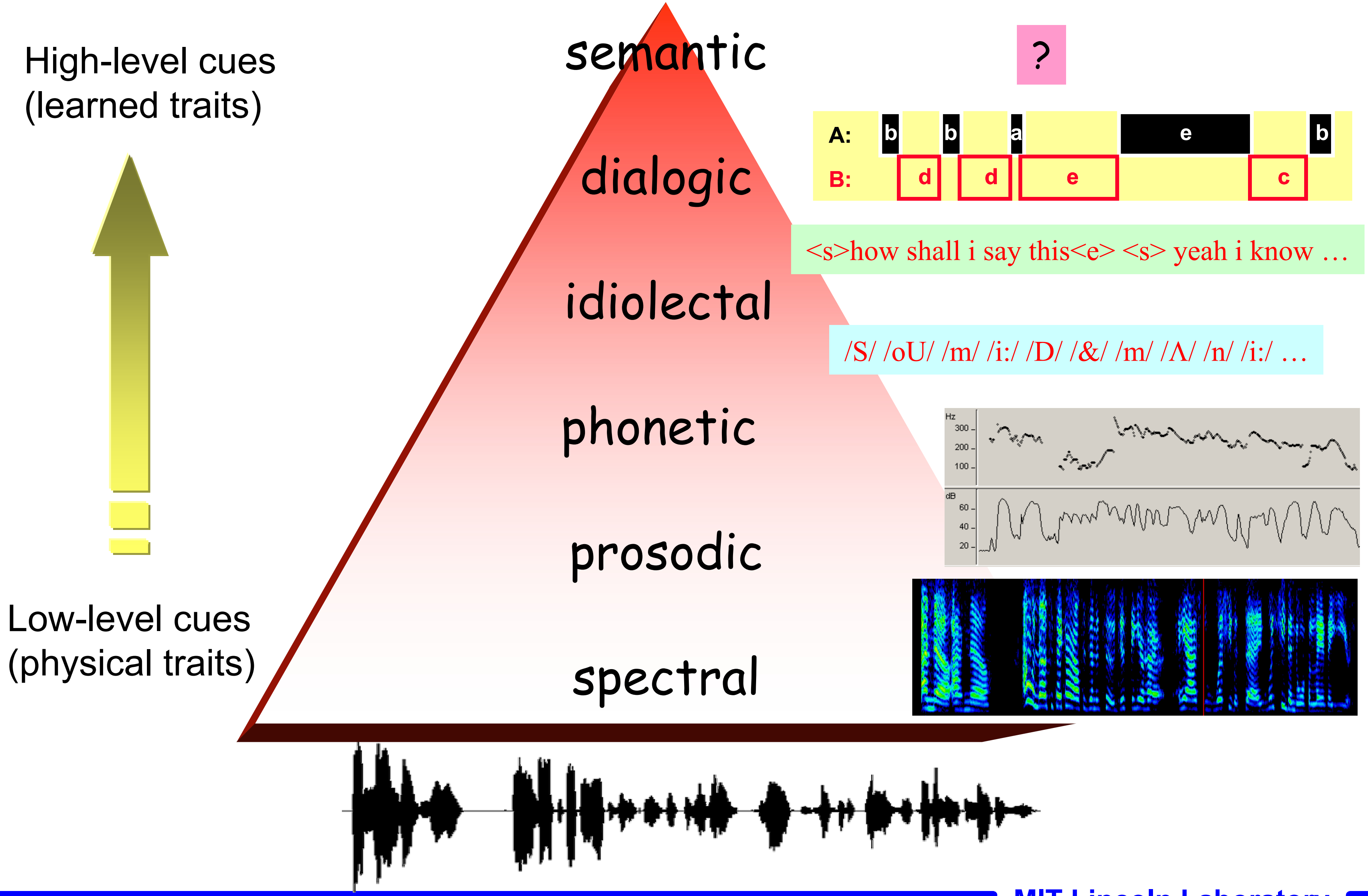
Do

- Goal: verify a user's identify using a behavior profile that consists of actions, interests, tendencies, preferences, and other patterns

- Benefit: accurate authentication without adverse mission impact
  - Authentication is inherent (no conscious user effort)
  - Low-cost in terms of resource utilization
  - High degree of user acceptance
  - Thorough user profiles are difficult to mimic
  - Continuous mode of authentication

- Examples
  - *How a user does something:* speed and pattern of typing, pen angle and intensity, use of menus vs keyboard shortcuts (user idiosyncrasies)
  - *What a user does:* pattern of application use, program features used, patterns of collaboration (user mission)
  - *What a user causes to happen:* sequences of system calls, patterns of resource access (low-level observables)

Speaker Recognition Using Many Levels of Information



High-level cues (learned traits)

Low-level cues (physical traits)

<s>how shall i say this<e> <s> yeah i know …

/S/ /oU/ /m/ /i:/ /D/ /&/ /m/ /Λ/ /n/ /i:/ …

D. A. Reynolds, et al., “The SuperSID Project: Exploiting High-level Information for High-accuracy Speaker Recognition,” *Proc. ICASSP,* 2003.

Continuous Authentication via Behavior & Voice

Trusted State

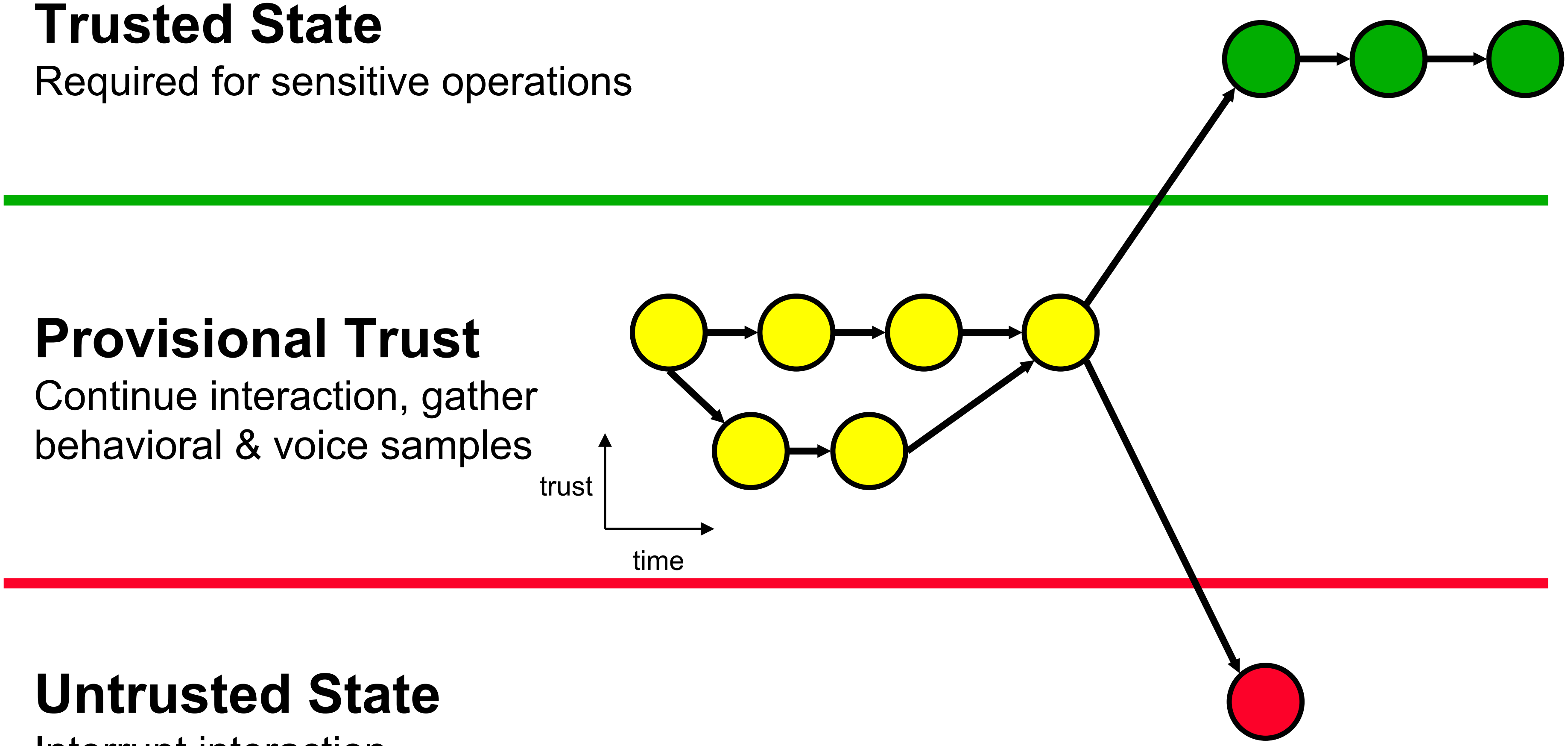
Required for sensitive operations

Provisional Trust

Continue interaction, gather behavioral & voice samples

Untrusted State

Interrupt interaction



T. J. Hazen, D. Jones, A. Park, L. Kukolich, D. Reynolds, “Integration of Speaker Recognition into Conversational Spoken Dialogue Systems,” *Eurospeech,* 2003.

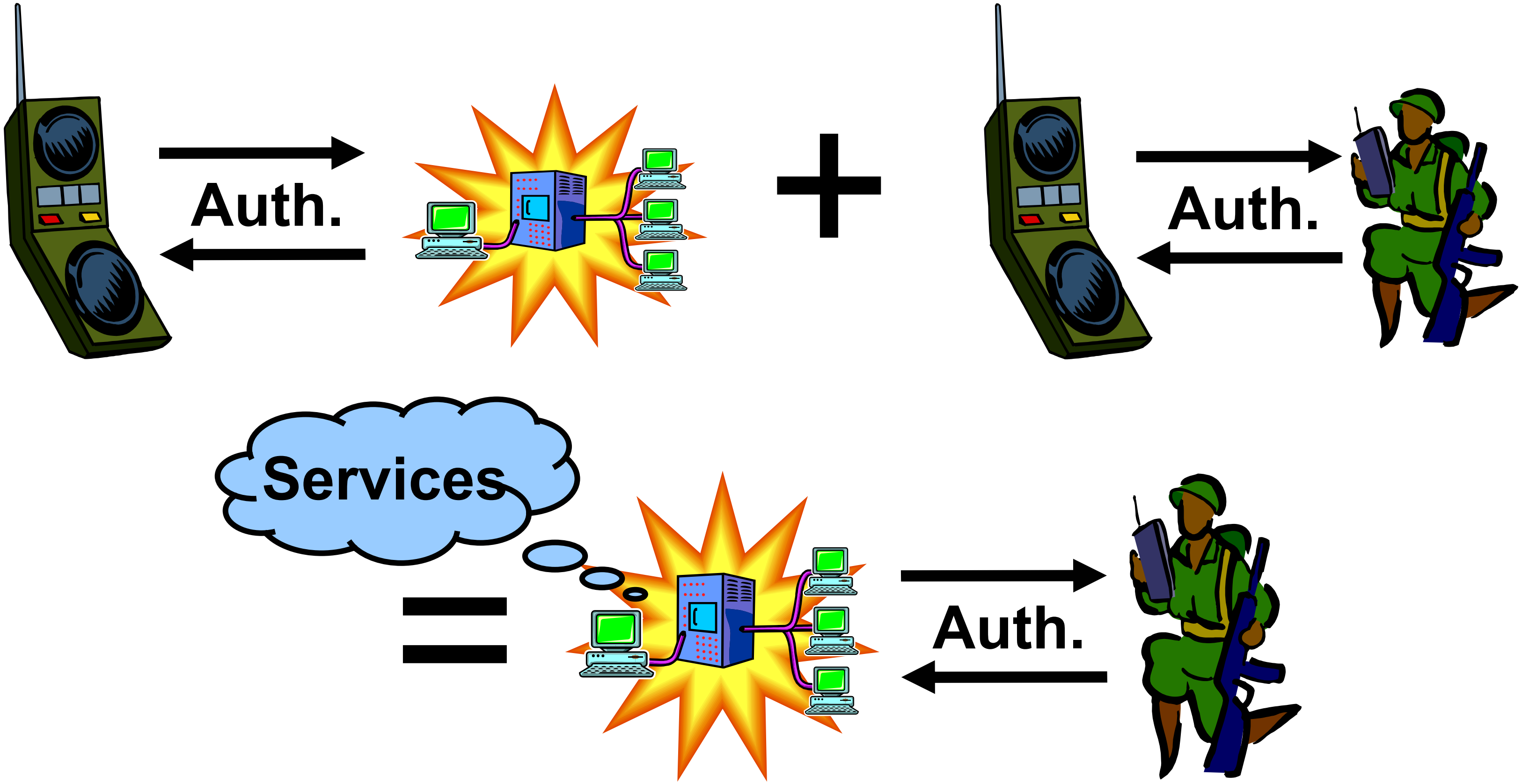
User Authentication Issues

- Remote/distributed/network enrollment and verification
  - Where are user models created and stored?
  - How are models maintained/updated?
  - How is enrollment conducted?
  - How are models bound to users?
  - Total verification time?
- New users
  - Are models transferred and how so?
  - Model integrity?
- Authentication
  - Policy?
  - Architecture?

Outline

- Introduction & Motivation
- User Authentication
- Architecture
- Conclusions & Implications for Cognitive Radio

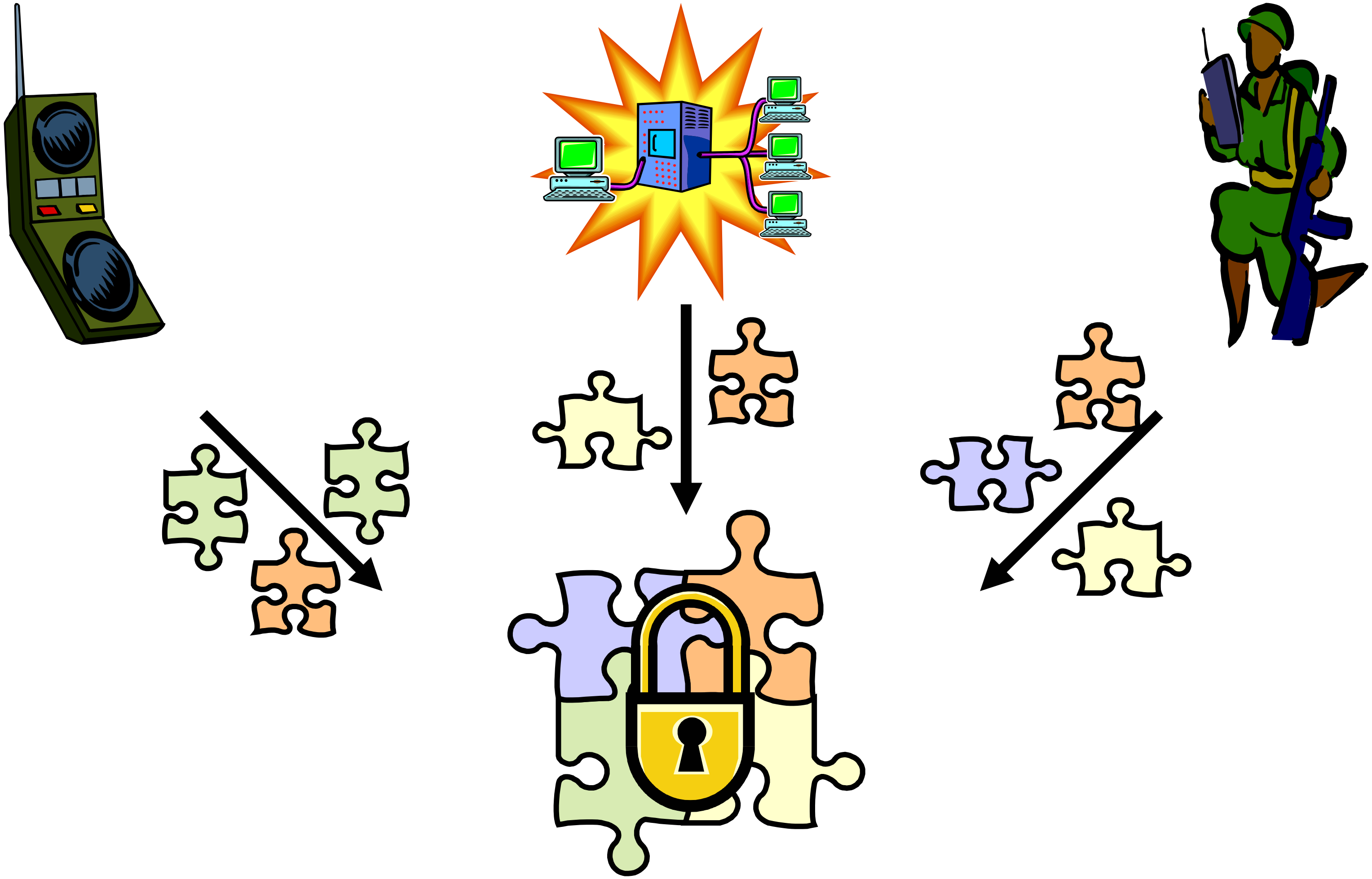
Authentication Requirements



Transitively authenticate users and services:

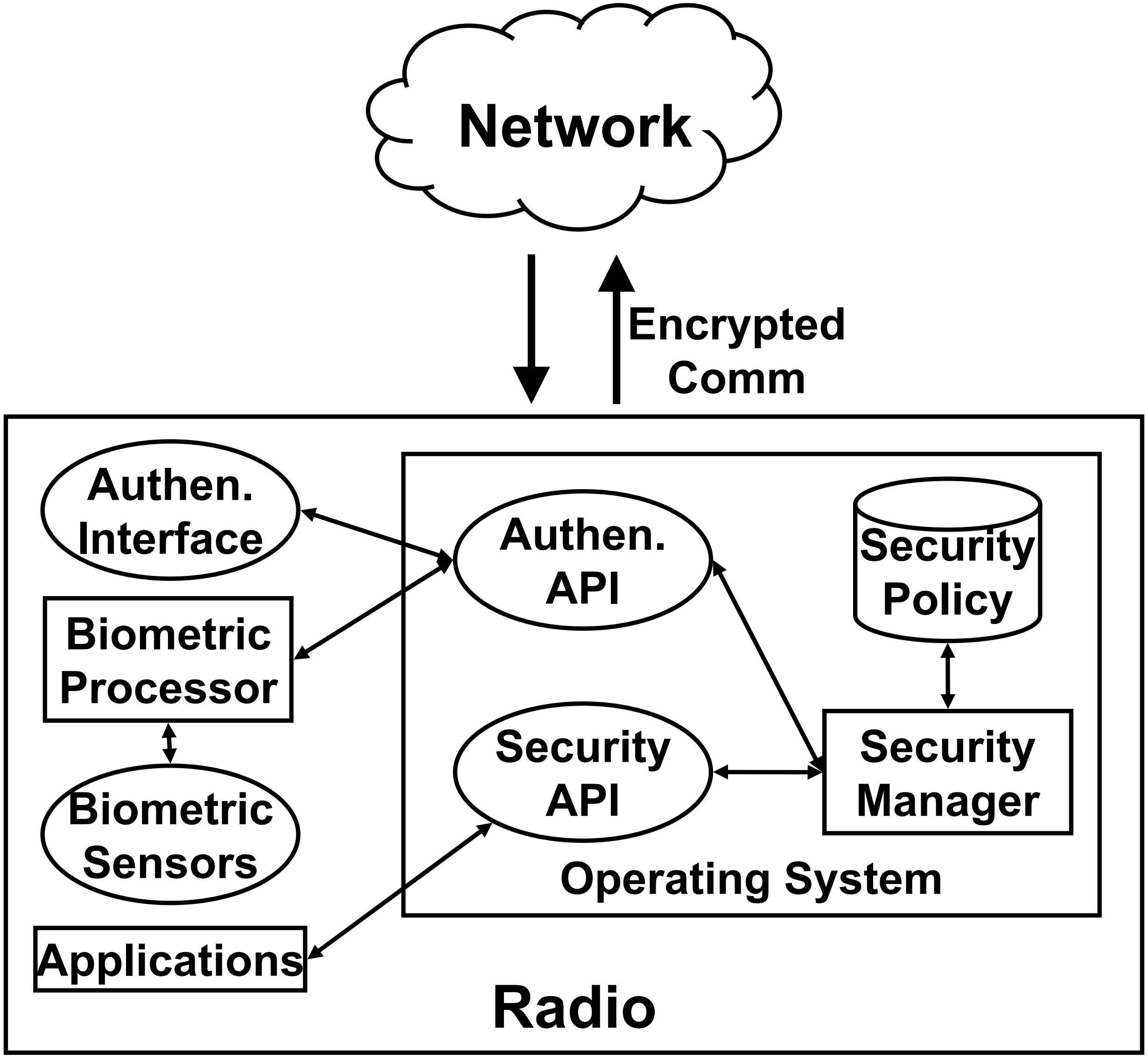
authenticate users and services using a two-step process

Who Is Responsible For Security?



Security functionality is distributed among radios, networks, and users

Notional Radio Security Architecture

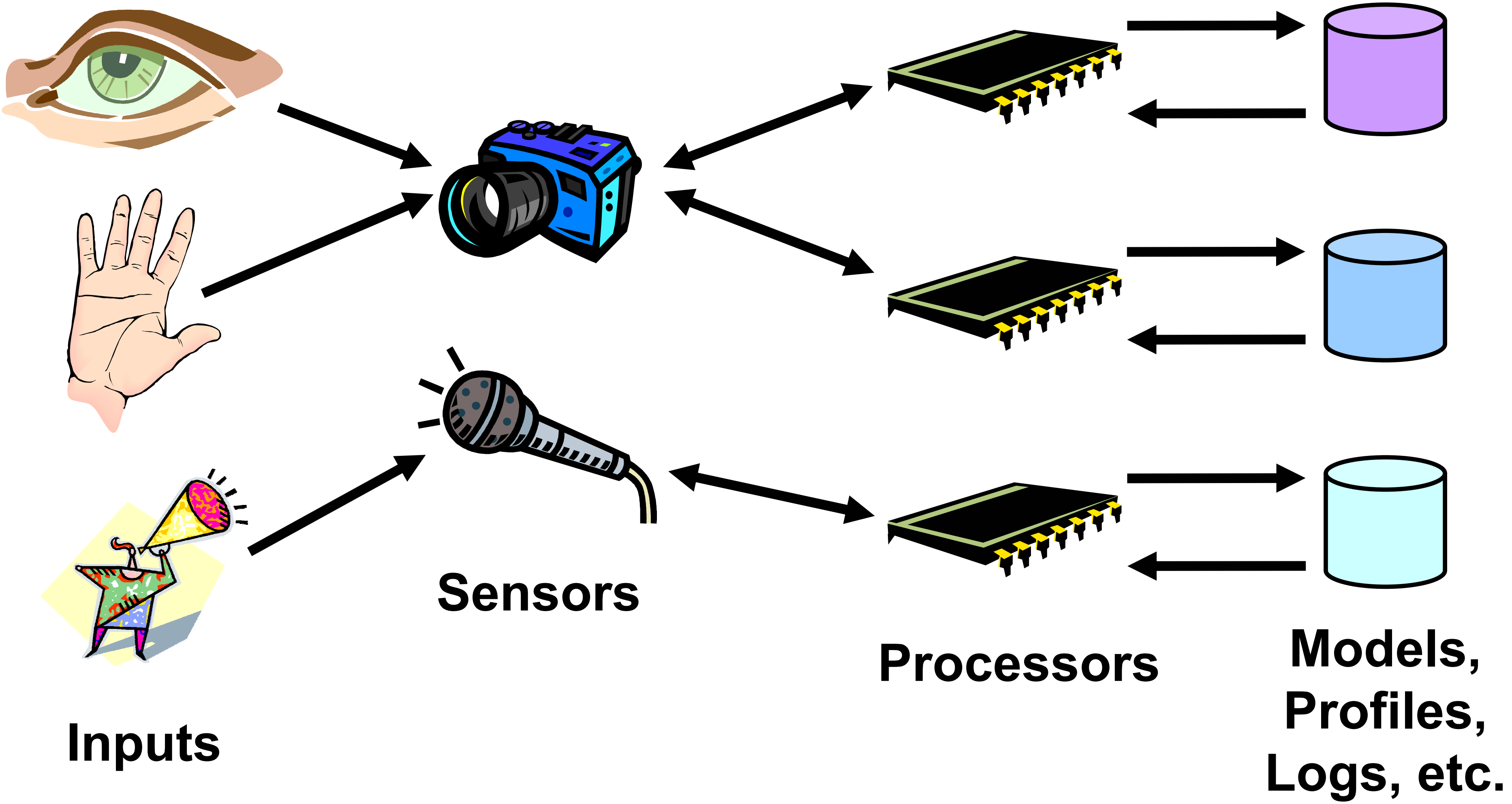


Secure Communication Interface Review

- Shared symmetric keys (closed, static environments)
  - Network and devices share a common key
  - Senders encrypt all data sent; if receivers can decrypt received data, it was from a trusted actor
  - Pros: simple, efficient
  - Cons: no per-client confidentiality, rekeying requires OOB comm.
- Public key approach (open, dynamic environments)
  - Network and devices have unique public/private key pairs
  - Senders encrypt data using receiver's public key; if receivers can decrypt data using their private key, it was from a trusted actor
  - All messages sent to the network: network routes messages
  - Pros: easy to add/remove clients, no trust required among clients
  - Cons: key management can be complex, inefficient (e.g., systems that support broadcast are costly)

Authenticates users and radios and provides confidentiality and integrity

Biometric Subsystems



Inputs

Sensors

Processors

Models, Profiles, Logs, etc.

Need high-performance, secure communication

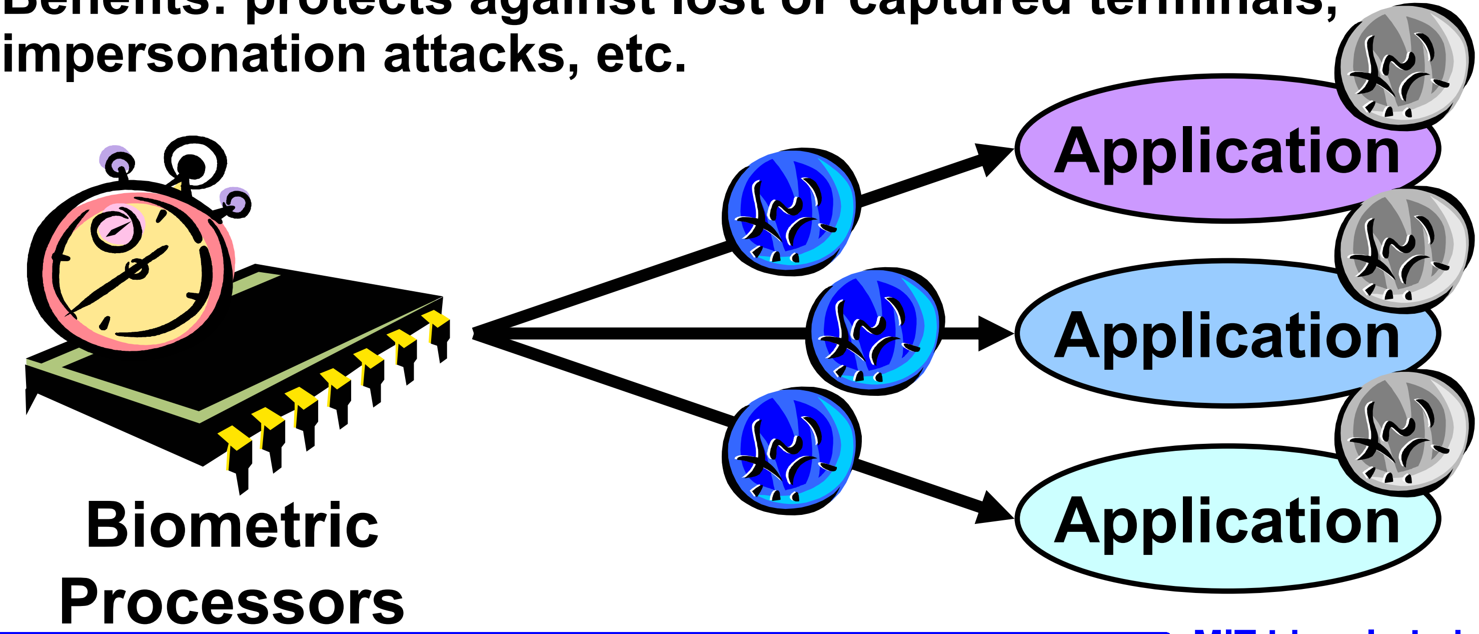
Output is a confidence measure for each biometric

Authentication API: Discrete vs Continuous Authentication

- Current approach: authenticate user once; assigned security token is used for the remainder of the session

- Our approach: authenticate user periodically and refresh all in-use security tokens (update grey tokens with blue ones)

- Benefits: protects against lost or captured terminals, impersonation attacks, etc.



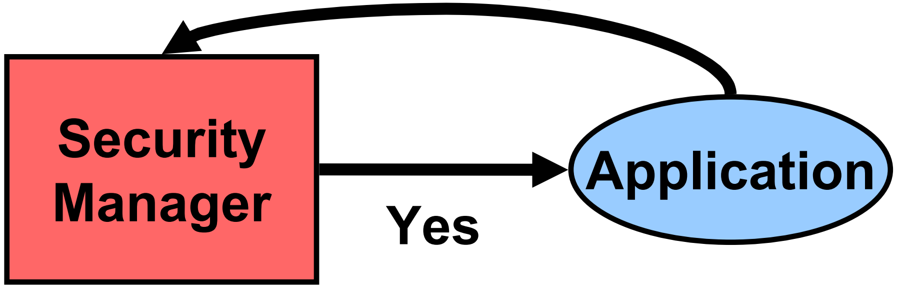
Authentication API: Binary vs Confidence-Based Authentication

- Current approach: authenticated users receive full privileges and unauthenticated users receive no privileges

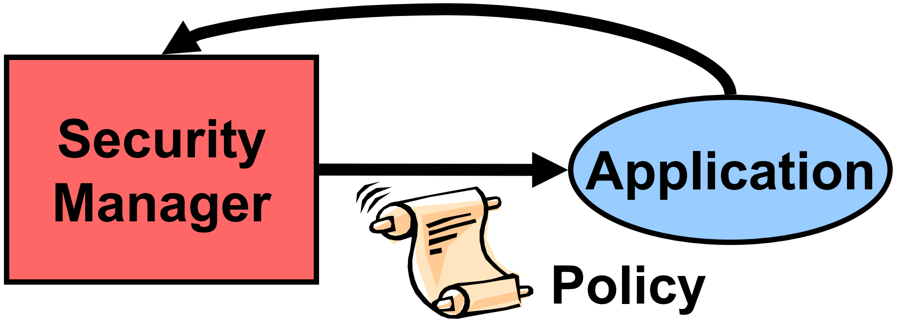
- Our approach: assign varying degrees of privilege based on the confidence in the authentication

- Benefits: access to applications and functionality can be mediated based on their sensitivity

Can This User Use Bob's Privileges?



Which of Bob's Privileges Can This User Use?



Security Manager: Enhancements to Current Systems

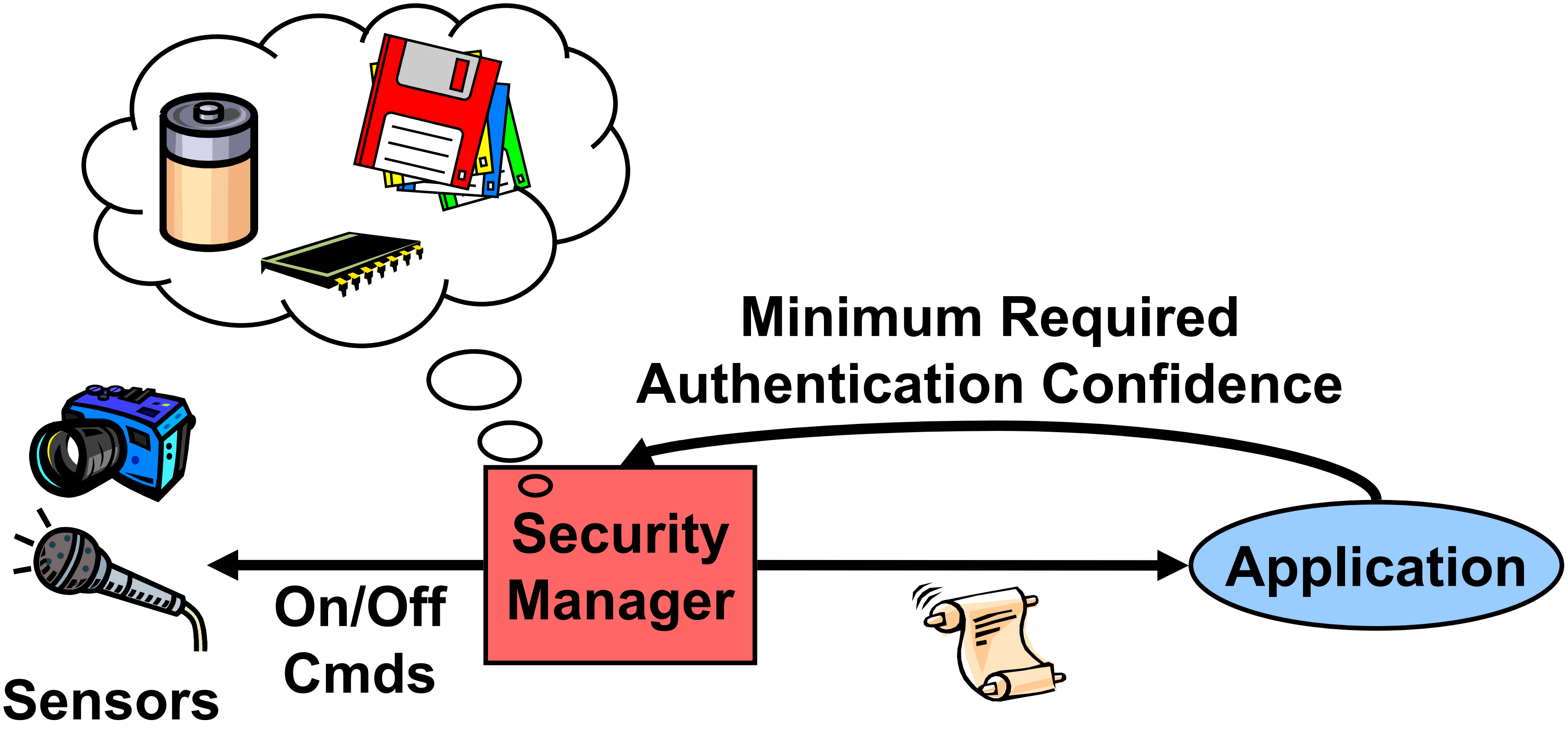
- Need to maintain confidence information
  - Current systems: *{object, principal, privileges}*
  - Our system: *{object, principal, confidence, privileges}*

- How to handle “insufficient privilege” failures?
  - Not a new problem – but now it is more likely to occur
  - Need to consider the impact on the user experience
  - One proposed approach:
    1. Attempt to “silently” acquire the necessary permissions
    2. Ask user to help acquire the necessary permissions
    3. Return insufficient privilege error to the application

- Implementation via replacement or software wrappers
  - Retain support for legacy applications

Security API

- Minimize resource utilization while ensuring the user can perform his mission by providing the *minimum* required level of authentication



Outline

- Introduction & Motivation
- User Authentication
- Architecture
- Conclusions & Implications for Cognitive Radio

Conclusions and Implications for Cognitive Radio

- We presented an integrated approach to user authentication and architecture to enhance trusted radio communication networks
- User authentication, via generalized biometrics, can be combined with other authenticators to provide continuous, flexible, and strong user authentication
- A biometrically enhanced authentication system approach can be extended to become part of a cognitive radio system which learns about users, situations, and surroundings and takes appropriate proactive or reactive actions
- Generalized biometric authentication is enhanced by machine learning, where a user’s distinctive behaviors and traits are learned and later recognized
- An advanced cognitive radio will also learn about and take action based upon user preferences, availability of network resources, and other elements of the situation and surroundings