Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

www.nr.no

Different Ways to Authenticate Users with the Pros and Cons of each Method

FHI, Oslo 12/12-2006

Habtamu Abie, PhD

Senior Research Scientist

Norwegian Computing Centre

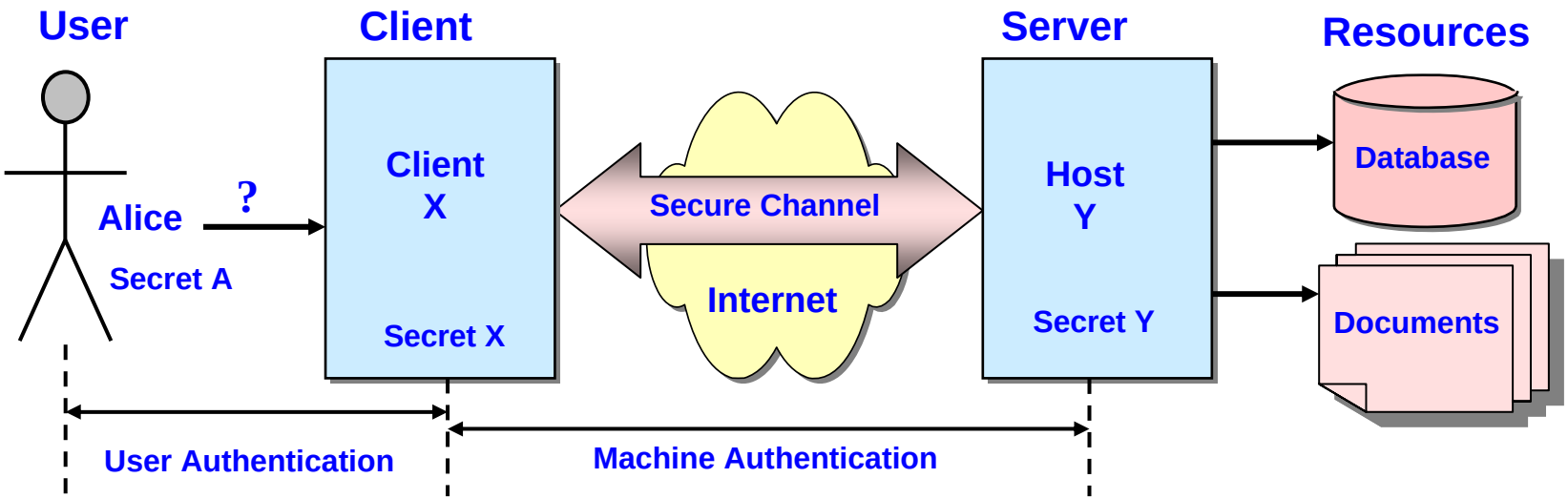
Outline

- Authentication: setting the scene
- Different ways to authenticate users
  - pros and cons of each method
- Technologies for user authentication
- Future trends
- Concluding remarks
- References

Authentication: setting the scene

- The authentication problem is simple to describe but hard to solve
  - two parties are communicating, and one or both wish to establish their identity to the other
- Authentication is the process of verifying
  - the digital identity of a process/computer
  - the physical identity of a person, i.e. user authentication
- Authentication, the *gatekeeper* for other security tasks
  - **confidentiality** – restricting data access to authorized persons
  - **integrity** – ensuring data modification by authorized persons
  - **non-repudiation** – conclusively tracing an action to an individual
  - **availability** – ensuring availability of data to authorised persons
- User authentication is a central component of any security infrastructure

Authentication: setting the scene…



- Alice performs user authentication to client A
  - by demonstrating knowledge of secret A (memorized password)
- Two machines Client X and Host Y perform machine authentication
  - by mutually demonstrating knowledge of their respective stored secrets (secret X and secret Y, respectively)

Different ways to authenticate users

- Users can be authenticated in many different ways, by using
  - **Something a user knows** – e.g. password
  - **Something a user has** – e.g. smart-card/token
  - **Something a user is** – e.g. biometrics
  - **Combinations of the above** (aka multifactor authentication) – e.g. PIN-enabled bank card
- Other methods
  - **Information about a user** – attribute authentication
  - **Where a user is** – location-based authentication (a special case of attribute authentication)

Passwords

- Passwords are simply ‘secrets’ that are provided by the user upon request
  - PINs - specific subset of passwords (comprised of numeric characters only)
- Using ‘something that is known’ to authenticate a user is a simple method
  - user lays claim to a particular identity, often represented by a username, and
  - supports this claim by demonstrating knowledge of some ‘secret’ information known only to that user and the system

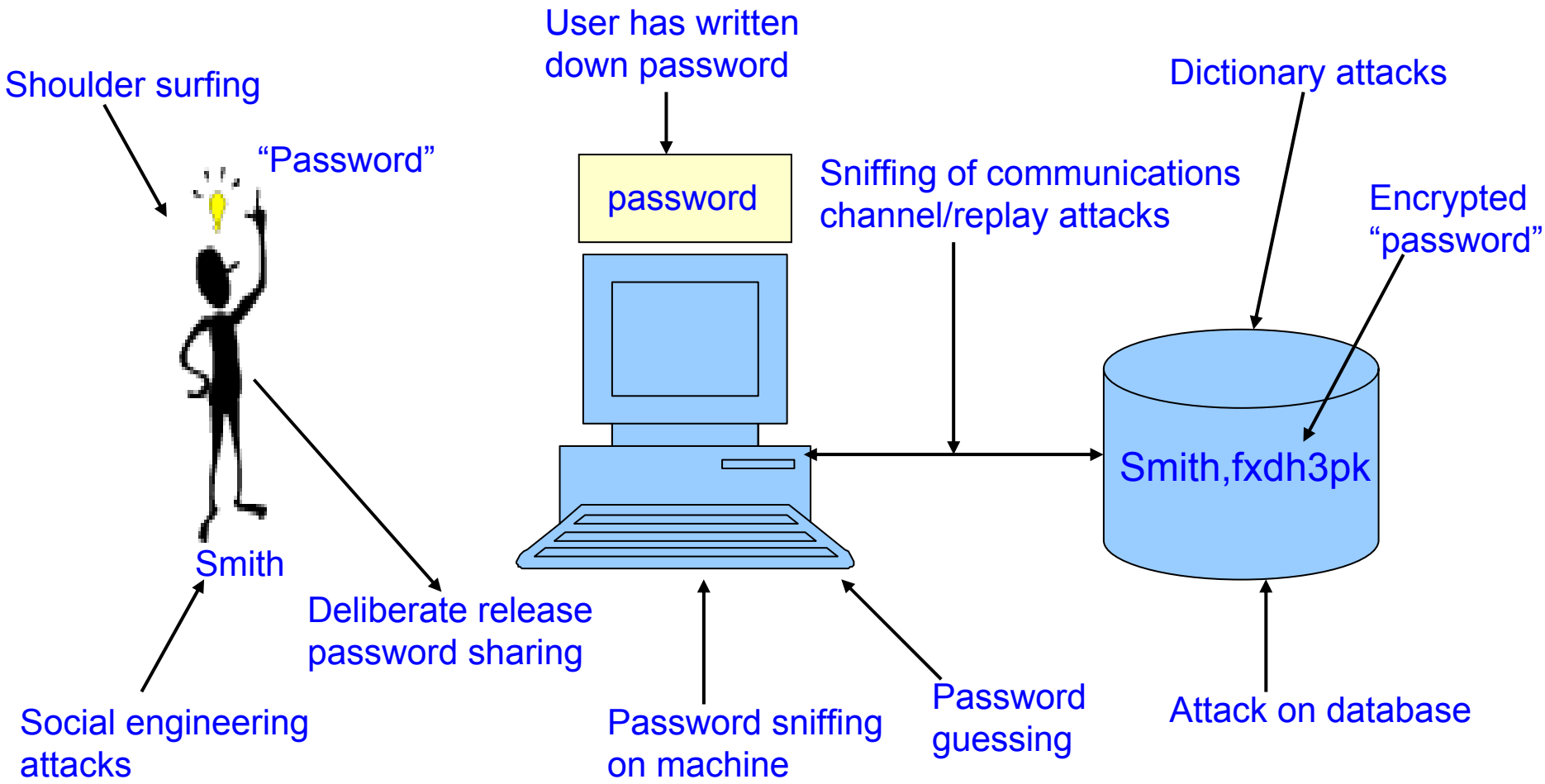
Passwords…

- Passwords
  - most predominant method of user authentication
  - demand a higher level of memorability from the user
- They suffer from two conflicting requirements
  - passwords must be sufficiently ‘random’ to prevent them being guessed by an attacker, and
  - must at the same time be not too difficult for the user to remember
- The security of a password-based authentication system relies on achieving the right balance between these two

Passwords…

- A user can use a password to authenticate **their** identity
  - a memorable password can often be guessed or searched for by an attacker
  - a long, random, changing password is difficult to remember
- Strong user authentication
  - combining password usage with stronger forms of authentication such as tokens and biometrics, although
  - users may face more inconvenience and frustration as a consequence
    - users may be required to carry tokens or provide their identification more than once

Passwords: Vulnerabilities



Source: QinetiQ

Passwords…

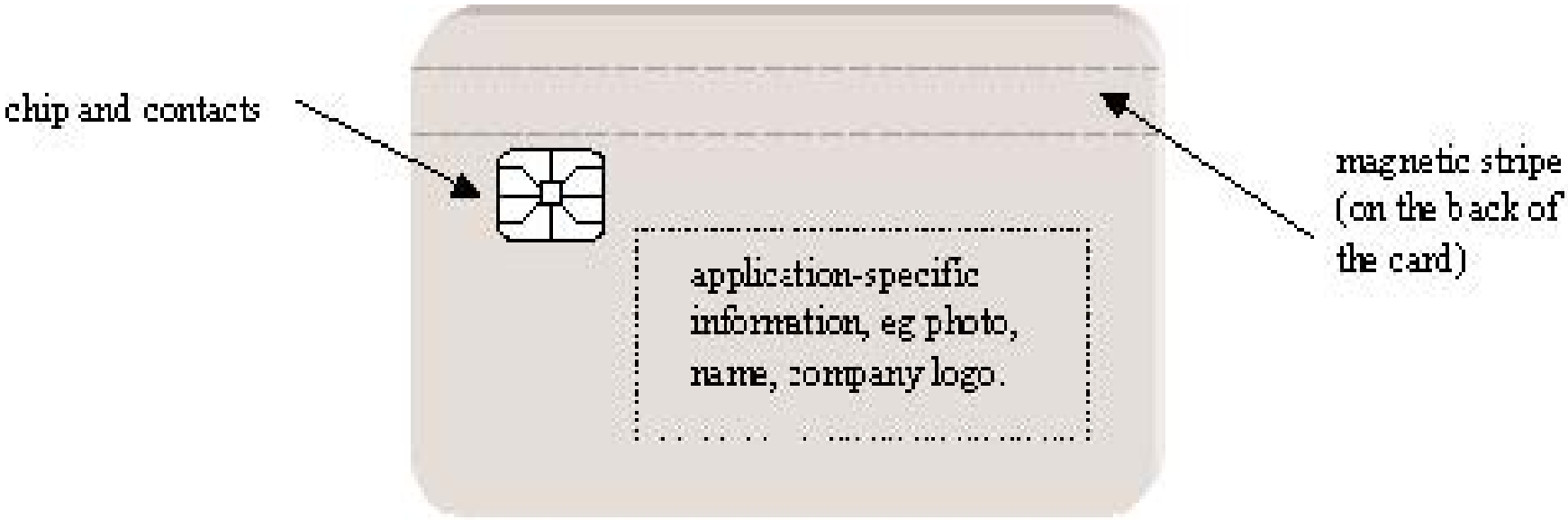
- Commonly used for logging on to computers, and most operating systems have password authentication built-in
  - therefore, the easiest option when choosing an authentication mechanism
- Convenient for most users and easily understood
  - because of their widespread usage
- Often cheaper to deploy
  - because they tend to require less investment in hardware
- Hidden costs involved in managing and maintaining them
  - users will always forget their passwords (whether or not they are complicated)
  - mechanism should be in place to deal with forgotten (or compromised) passwords
  - for large networks this may require the provision of a dedicated password helpdesk

Encrypted passwords

- Passwords can be encrypted for both storage and transmission on the network
  - prevents the problem of password sniffing present in plain-text storage and transmission

- However, for this to be effective
  - users are required to understand the correct procedures for management of the encryption protocol
  - for example, “plausible certificates are easy to forge, and blindly accepting dialogues to install certificates into a web-browser will completely invalidate any advantages”

Smart cards



- Credit card-sized hardware tokens: contact or contact-less
- Two basic varieties
  - memory cards (securely store data, cost-effective, popular method of providing two-factor authentication)
  - microprocessor (processing power, stronger two-factor authentication, multiple functions, etc.)

Smart cards: microprocessor card

- The microprocessor card supports public key technology
  - securely stores user's public key certificate and private key for use with PKI
- Restricts security-critical computations to the smart card
  - making identity interception difficult
  - preventing masquerading and data manipulation
- Limits the number of logon attempts
  - locks after a PIN is entered incorrectly a certain number of times
  - prevents a dictionary attack
- Multiple functions
  - reducing the number of devices that a user must carry
  - access control to buildings, student ID, micro-payments (bus fares, snack food, etc), patient data, etc
  - provision of portability of credentials (and other private information) between computers at work, at home, or on the road

Smart cards: authentication

- Smart cards
  - emerging user authentication technologies
  - store user identity and a PIN – two-factor authentication
  - stronger way to authenticate users
  - physically carried by users
- A user using smart card to authenticate their identity
  - inserts the smart card into a card reader
  - enters the required PIN to access the stored identity and to start the authentication process

Smart cards: authentication…

- Generally found to be acceptable to users
  - lightweight, portable, easy to use
  - most people are used to carrying cards with them
- More difficult to manage
  - users must be educated in their use
  - cards along with any assigned PINs must be issued and tracked
- Users may find them inconvenient
  - can be lost, stolen, or shared
  - must be kept close at hand
  - cause some problems for users who forget their PINs or make typographical errors
    - smart card becomes locked after a certain number of attempts
  - not very robust and can be easily broken

Attacks on smart cards

- Use doctored terminal/card reader
  - reuse and/or replay authentication to card
  - display $*x* transaction but debit $*y*
  - debit account multiple times
- Physical attacks
  - erase onboard EPROM with UV spot beam
  - use e-beam tester to read signals from the operational circuit, e.g. PIN recovery
  - attack the Random Number Generator

Other authentication tokens

- Two main types
  - challenge-response calculators
    - Encrypt a challenge from the server and return result to server
    - Server does the same and compares the result
    - Encryption usually seems to be DES
    - Encryption key is random (rather than a fixed password) which makes offline password guessing much harder
  - one-way authentication data generators
    - Non-challenge-response nature fits the “enter name and password” authentication model
- Other tokens
  - USB (Universal Serial Bus) token, functionally very similar to smart cards
  - PCMCIA card, TPM (Trusted Platform Module)
  - iButton, computer chip enclosed in a 16mm stainless steel can
  - Datakey (http://www.datakeyelectronics.com/)
  - RSA SecureID http://www.rsasecurity.com/node.asp?id=1157)
  - RFID (Radio Frequency Identification) (http://www.rfidinc.com/)

X509 certificate

- Digital certificates
  - software-based identifiers
  - use public key encryption to confirm a user's identity
  - serve as unique, "unforgeable" credentials
  - identify privileges for authorized access
  - enable digital signing and encryption to provide the privacy, data integrity, and non-repudiation services
- User is assigned a digital certificate in two parts
  - public key that can be made freely available
  - private key that must be kept secret by the user
- PKI
  - key management infrastructure must be in place

A PKI consists

- Certificate authority (CA)
  - issues and verifies digital certificate
  - signs the certificate to prove that the certificate belongs to the user who presents it
  - certificate of the signing CA must be trusted
- A registration authority (RA)
  - acts as the verifier for the certificate authority before a digital certificate is issued to a requestor
- One or more directories
  - where the certificates (with their public keys) are held
- A certificate management system
  - used to generate, distribute, store and verify certificates

Digital certificates with tokens/TPMs

- Digital Certificates with Tokens
  - offer greater security, convenience, and portability
  - placing the digital certificate on the token provides more protection
  - one or more identification certificates on the token, users can carry with them the appropriate credentials to access systems
- Digital Certificates with TPMs
  - TPMs are isolated chips
  - use digital signatures to verify that the operating system and other components of the software environment have not been compromised
  - combined with a digital certificate, they provide the strongest authentication

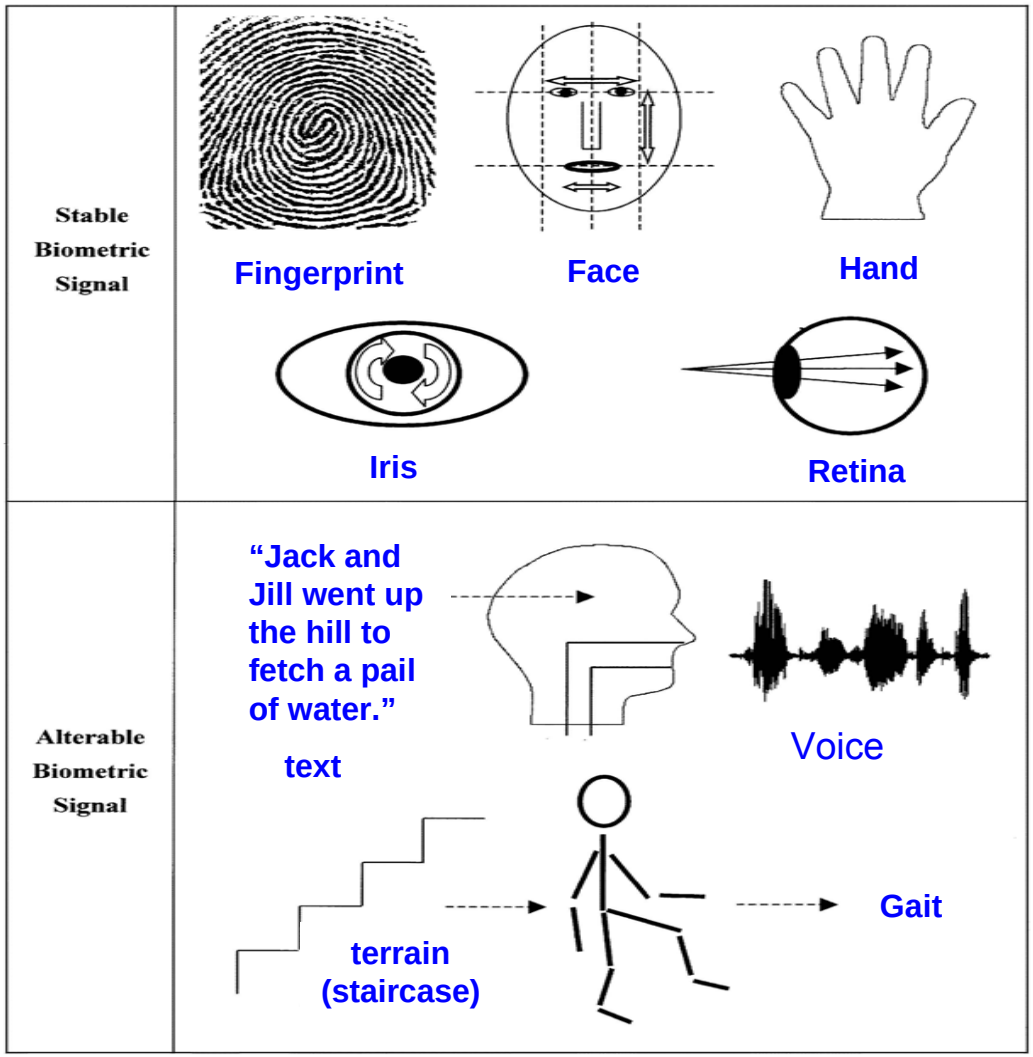
X509 certificate…

- Pros
  - certificates simplify authentication
    - system administrators don't need to maintain large databases of user accounts and logins
  - useful for single-sign-on
    - since servers are never given a copy of the password, compromising of any single server will affect only that server
- Cons
  - users must carry their certificate with them
  - users must keep the certificate secure
  - certificates (and their private keys) are messy to distribute
    - physically providing the certificate to the client might not be possible, e.g. at an internet Café.

X509 Certificate: cons…

- Certificates
  - tend to be vendor specific and may not be interoperable between vendors or products
  - complicated for users to install.
  - do not work well in cases where users share machines or use multiple machines
- Other significant difficulties
  - technical and administrative processes, involved in running a certificate authority securely
  - mechanisms for revocation (cancelling) of compromised certificates are not well established

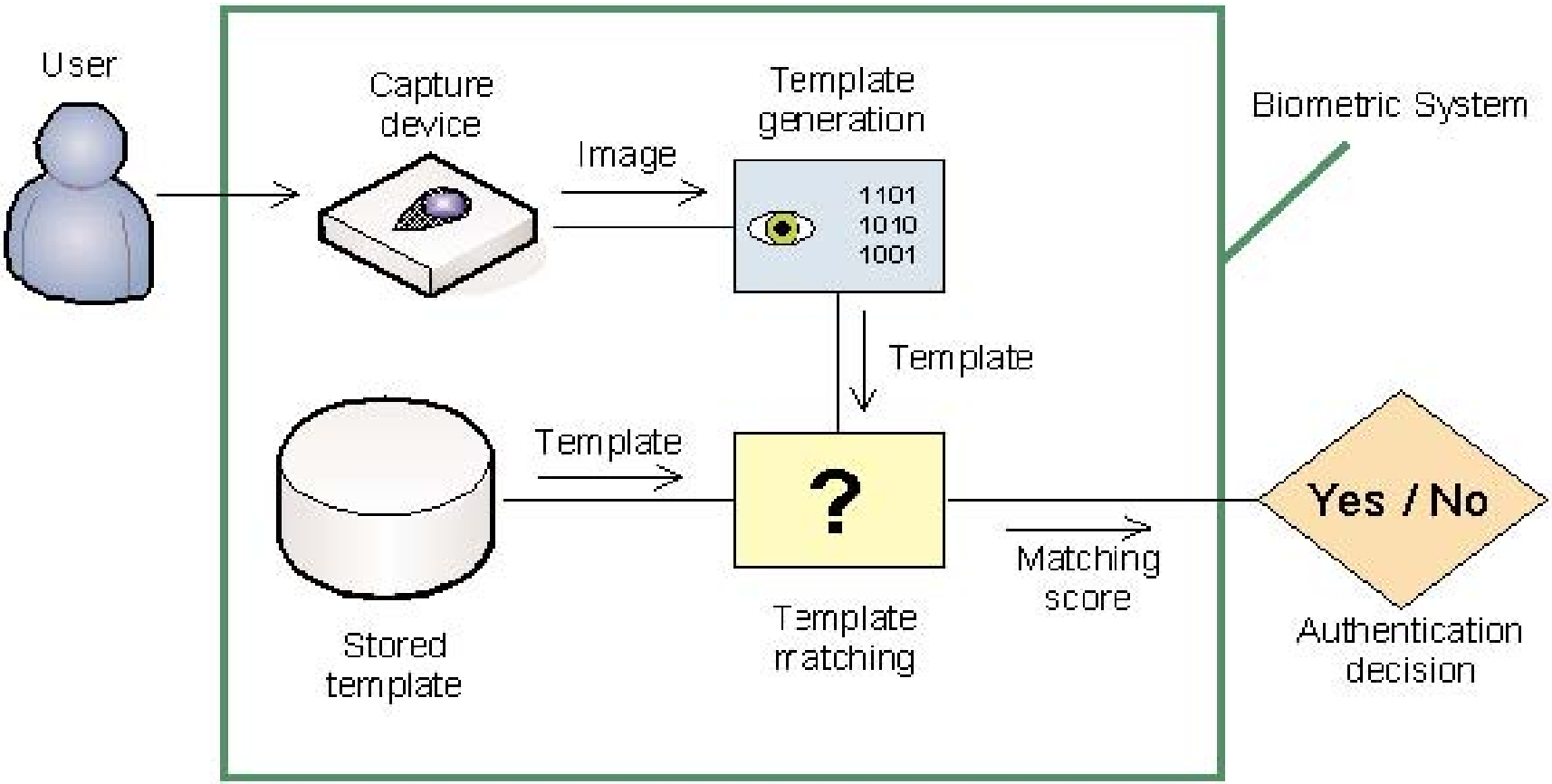
Biometrics



Source: L. GORMAN

- Biometrics user authentication is a method that identifies a user and/or verifies their identity based on the measurement of their unique physiological traits or behavioural characteristics
- Physiological biometrics are fingerprint, facial recognition, iris-scan, hand geometry, retina scan, etc.
- Behavioral biometrics are voice recognition, gaits, keystroke-scan, signature-scan, etc.

Biometrics authentication



Source: QinetiQ

Biometrics authentication…

- With biometrics, a stored pattern is compared with the actual measurements taken
  - but these patterns will hardly ever match precisely
  - hence, a new problem has to be faced, false positive and false negative
- Accepting the wrong user (false positive) is clearly a security problem
- Rejecting a legitimate user (false negative) creates embarrassment and a somewhat inefficient working environment [Gollmann]
- Thus, the security of biometrics relies on achieving the right balance between these two errors

Biometrics…

- Relieve user of the difficult task of choosing and remembering a good key
- Uniqueness of biometric attributes makes them an ideal candidate authenticating users
- User now unable to forget and share passwords
  - so password administration overheads are reduced while security as a whole is increased
- Thought to be much more difficult
  - to replicate a biometrics feature at the data acquisition stage than it is to replicate someone's user ID or password
  - as opposed to tokens a biometrics characteristic cannot be lost or stolen (except in exceptional cases)
- Behavioural biometrics
  - devices are less expensive and said to be less threatening to users

Biometrics…

- Major uses of biometrics today
  - at airports, passport/visa integration, for immigration purposes, in prisons
- Many users consider physiologically based biometrics authentication intrusive and obtrusive
- Fingerprints
  - small and inexpensive
  - associated with criminal identification
- Voice authentication
  - upset by background noise, illness, stress, intoxication
  - can be used over phone lines
  - more readily by users (non-intrusive)

Biometrics…

- Eye scans
  - high accuracy in identifying users
  - low data storage requirements
  - intrusive (scan blood vessels in retina/patterns in iris)
- Hand Scans
  - low data storage requirements
  - not unique to every one
- Facial scans
  - non-intrusive
  - users may feel violation of privacy as data may be captured, verified and used without their knowledge

Biometrics: general pros and cons

- Pros
  - everyone carries their ID on them
  - very hard to forge
  - easy to use
- Cons
  - you can't change your password (if compromised)
  - expensive
  - no real standards (half a dozen conflicting ones as well as vendor-specific formats)
  - user acceptance problems
    - users may feel treated like criminals if fingerprinted
    - may not like the idea of laser beams scanning their retinas

Technologies for user authentication

- Kerberos (http://web.mit.edu/kerberos/www/)
- Microsoft .NET passport (http://www.passport.net/)
- RADIUS (http://www.freeradius.org/)
- LDAP (Lightweight directory access protocol)
- Liberty Alliance Project (http://www.projectliberty.org)
- SESAME (https://www.cosic.esat.kuleuven.ac.be/sesame/)
- PKI-Based Technologies (http://www.pki-page.org/)
- ITU-T PMI (Privilege Management Infrastructure)
- SDSI/SPKI (http://www.syntelos.com/spki/)
- Shibboleth (http://shibboleth.internet2.edu/shib-intro.html)
- Athens (UK) (http://www.athens.ac.uk/)
- PAPI AuthServer (http://papi.rediris.es/dist/pod/AuthServer.html)

Future trends

- Graphical passwords are claimed to be more memorable to users
  - Déjà vu project at University of California at Berkeley – array of abstract images
  - HumanAut project at Carnegie Mellon University – pictures
  - Draw-a-Secret project at Bell Labs AT&T Labs – a line drawing within a grid pattern
- Enhancing tokens
  - combining smart cards with RFID (Radio Frequency Identification) http://www.smartcardalliance.org/
  - combing two-factor authentication (smart cards and biometrics) with NGSCB to enhance security [NGSCB]
- Multi-modal biometrics
  - combining different biometrics modalities to strengthen security (http://biometrics.org/)
  - fusing several types of biometrics (Anil Jain seeks to improve security by fusing several types of biometrics [Buderi])
  - use of DNA in identification [DNA]
- Robustness, platform flexibility, scalability, etc.
  - procedure for recovery from compromise from token clone, server compromise or key compromise (For biometric enthusiasts – how do you recover from compromise?)
  - withstand change of servers, client workstations, operating systems, etc.
  - how easy is it to handle scaleable responses to increased threats?
  - how easy is it to size for performance to handle peak demand?

Concluding remarks

- Depending on the information that you are securing and the number of users for whom access to that information is required
  - you need to consider the pros and cons of various authentication solutions until you find the one that best fits your needs - and
  - “one size won’t necessarily fit all”!
- A key problem with user name and password, the human factor
  - passwords are easy to guess or search if easy to remember
  - passwords are easily stolen if written down
  - users may share passwords
  - passwords can be forgotten if difficult to remember

Concluding remarks…

- Physical tokens
  - provide easy storage and transportation of credentials and other secrets
  - ensure uniqueness of that information
  - password or PIN may still be needed to access that information, i.e. human factor still exists
- Biometrics
  - proves physical presence of owner credentials, eliminating human factor
  - nonetheless vulnerable to attacks
  - thus, a combination of the above may be a better solution
- Important consideration when matching an authentication solution with a specific application
  - user environment (convenience/ease of use, robustness/reliability, portability)
  - application environment (security requirements, secure identity management, integrating with PKI, ease of management and administration)
  - business environment (acquisition, deployment, maintenance, and integration costs)

Bibliography

- **Authentication and smart cards**
  - D. Gollmann, Computer Security, John Wiley & Sons, 2000
  - R. Clarke, Authentication: A sufficiently Rich Model to Enable e-Business, 2001, http://www.anu.edu.au/people/Roger.Clarke/EC/AuthModel.html
  - QinetiQ: B. Pomeroy and K. Shorter, Authentication Technologies, 2004, www.QinetiQ.com/perspectives
  - Smart Card Alliance: http://www.smartcardalliance.org/
  - NGSCB (Next-Generation Secure Computing Base): http://www.microsoft.com/resources/ngscb/archive.mspx
- **Biometrics**
  - Biometric Consortium: http://www.biometrics.org/
  - Biometric Research, MSU: http://biometrics.cse.msu.edu/
  - Conference and Exhibition: http://www.biometrics.elsevier.com/
  - L. GORMAN, Comparing Passwords, Tokens, and Biometrics for User Authentication, IEEE, Vol. 91, No. 12, 2003
  - G. Hachez, F. Koeune, and J. Quisquater, Biometrics, Access Control, Smart Cards: A Not So Simple Combination
  - R. Buderi, Demo: Me, Myself, and Eye, Februray 2005, http://www.techologyreview.com
  - DNA: Use of DNA in Identification http://www.accessexcellence.org/RC/AB/BA/Use_of_DNA_Identification.html

The End

- Thanks for your attention!