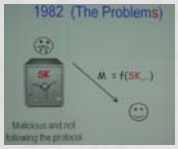
Cryptographic Protocols

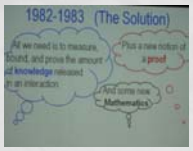
Cryptographic Protocols(I)

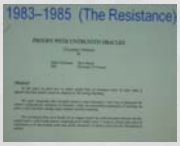
- 1976 : Birth of concepts of PKC
- 1978 : Birth of RSA
  - New applications compared to traditional concepts
    - ✓Digital Signature
    - ✓Bit Commitment
    - ✓Coin Flipping
    - ✓Mental Poker (Mental Go-stop)
    - ✓Fair Contract Signing
    - ✓Comparison of Richness
    - ✓etc.

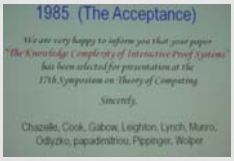
Cryptographic Protocols(II)

- 1978 - 1984
  - A variety of PKCs (RSA, ElGamal, ...)
  - Cryptographic protocols
- 1985 ~
  - ZKIP (Zero Knowledge Interactive Proof)









❑3

Cryptographic Protocols(III)

- Authentication Protocol using cryptographic primitives
  - Identification
  - Bio-identification
  - Authenticated Key Distribution
- Multiparty Protocol to practical application such as e-cash, e-voting, e-auction, e-game, etc.

❑4

Cryptographic Protocols(IV)

- 1987 NIZK(Non-interactive ZK)
  - Sharing common, short, random string
  - M. Blum, P. Feldman, S. Micali,"Non-interactive Zero-Knowledge and its Application," ACM STOC, pp.103-112, 1988
- Application of NIZK
  - Strong PKC against Chosen Ciphertext Attack
  - Digital signature against Chosen Plaintext Attack

❑5

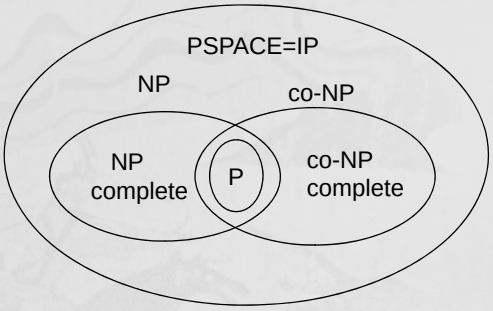
Interactive Proofs

❑6

Complexity Class(I)

Language L={0,1}*: infinite set of elements with various input size
Uniform Model : Turing Machine (computer algorithm)
Non-uniform Model : Circuit model (VLSI)
P : Deterministic poly, NP : Non deterministic Poly

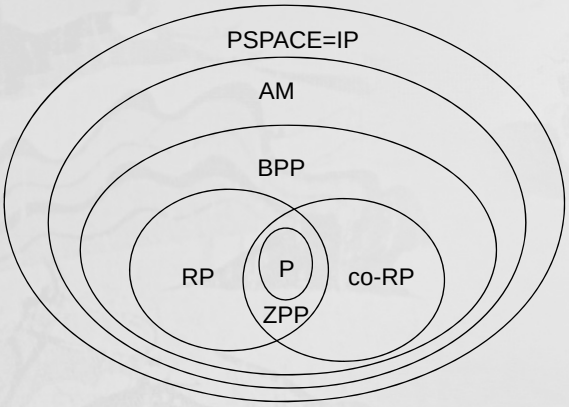
P /= NP !!



❑7

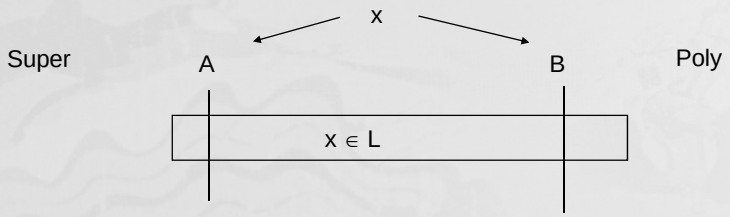
Complexity Class(II)

Allows random coin -> error



❑8

Computation & Proof(I)

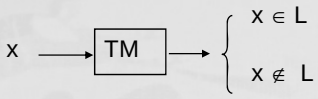


For B
- no help : P, BPP
- 1-way proof : NP
- interactive proof : IP
- \+
- zero knowledge = ZKIP

❑9

Computation & Proof(II)

$L \in P$

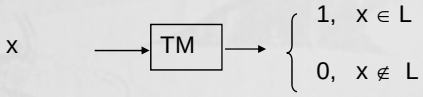


Prob. of error =0

$L \in BPP$

Poly-time

Random tape

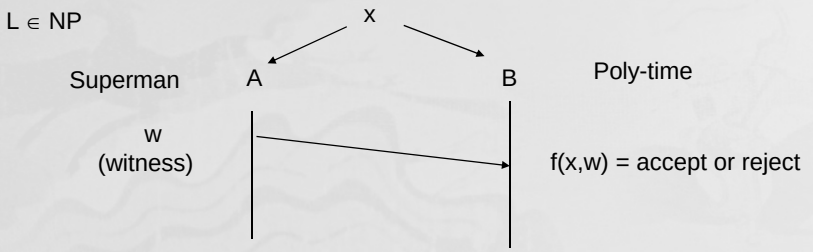


Completeness $x \in L$ $Prob(TM(x)=1) \geq 2/3$

Soundness $x \notin L$ $Prob(TM(x)=0) \geq 2/3$

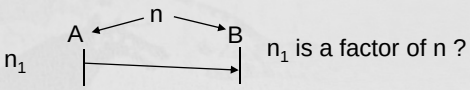
❑10

Computation & Proof (III)

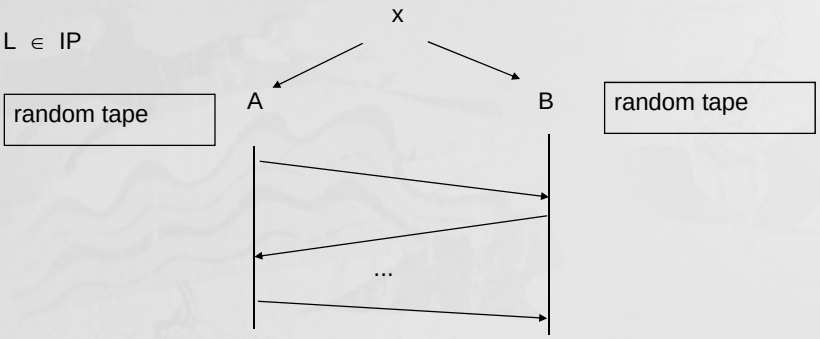


Completeness : if $x \in L$, $f(x, \exists w)$ = accept
Soundness : if $x \notin L$, $f(x, \forall w)$ = reject

(Ex.) L = { n | n = composite}, $n = n_1 n_2$



Computation & Proof (IV)



Completeness if $x \in L$, prob[B accepts x] $\geq 1 - \varepsilon$
Soundness if $x \notin L$, prob[B rejects x for $\forall$A] $\geq 1 - \varepsilon$

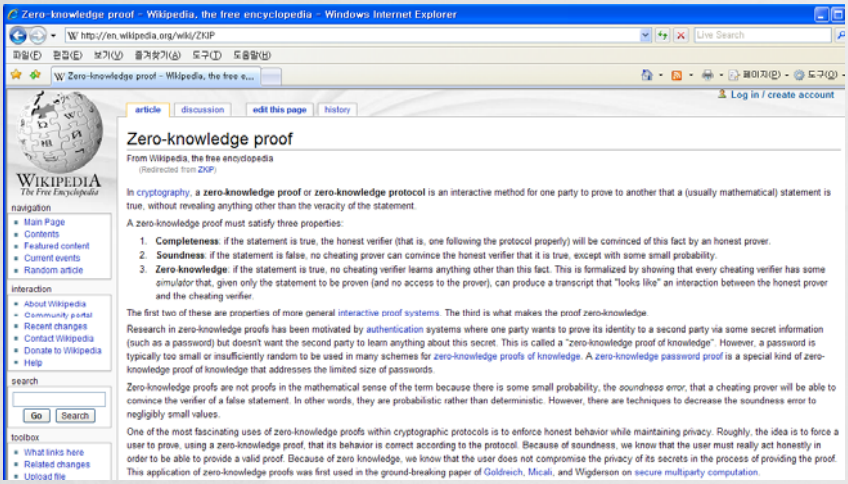
Interactive Proof System

- Protocol : a pair of algorithm (A,B)
- Interactive Proof System : Protocol (A,B) satisfying completeness and soundness
- If L ∈ IP (Interactive Poly-time), L has an IPS (Interactive Proof System).

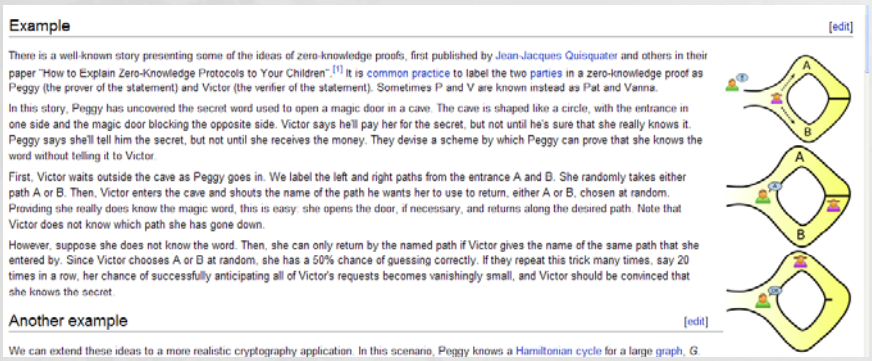
ZKIP(I)

- GMR(Goldwasser, Micali, Rackoff) ; Proposed at first in 1985
- ZKIP (Zero Knowledge Interactive Proof) : Between P and V,
  - Completeness : Only true P can prove V.
  - Soundness : False P' can't prove V.
  - 0-Knowledge : No knowledge transfer to V.

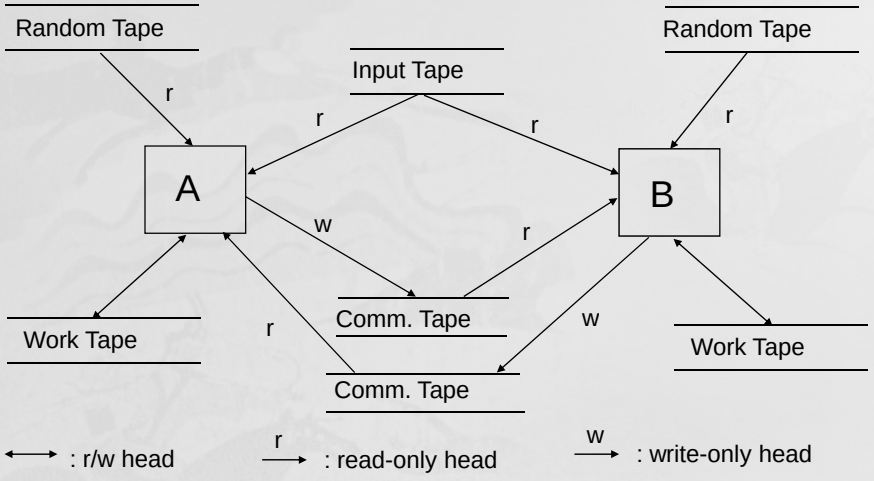
ZKIP(II)



Concept of ZKIP

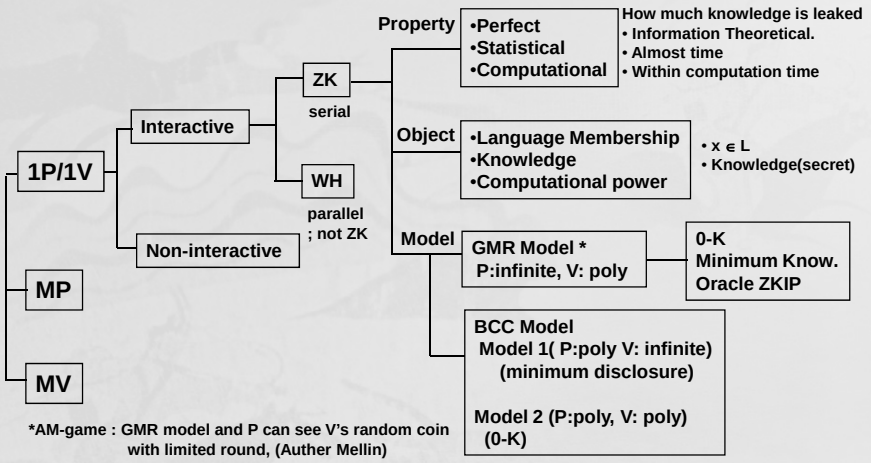


Turing Machine Model



❑17

Classification of ZKPS



❑18

Indistinguishability (I)

- Family of r.v., U ={U(x)} where *x* is from L, a particular set of $\{0,1\}^*$, all r.v. are taken from $\{0,1\}^*$, U and V are r.v.
- Verdict who can tell a bit from U or V is limited to
  - infinite time and space : perfect
  - infinite time and polysize space : statistical
  - polysize time and space : computational

Indistinguishability (II)

- L : Language
- {U(x)}, {V(x)} : family of random variable
- (Perfect) If for all $x \in L$, $U(x) = V(x)$ (where "= " means "equal as random variables") , {U(x)} and {V(x)} are perfectly indistinguishable for L.
- (Statistical) If $\Sigma_{\alpha \in \{0,1\}^*} |Pr[U(x)=\alpha] - Pr[V(x)= \alpha]| < \varepsilon (|x|)$, {U(x)} and {V(x)} are statistically indistinguishable for L.
- (Computational) For all circuit C (distinguisher) with polynomial size of |x| , if $|Pr[C(U(x))=1] - Pr[C(V(x))= 1]| < \varepsilon$, {U(x)} and {V(x)} are computational indistinguishable for L.

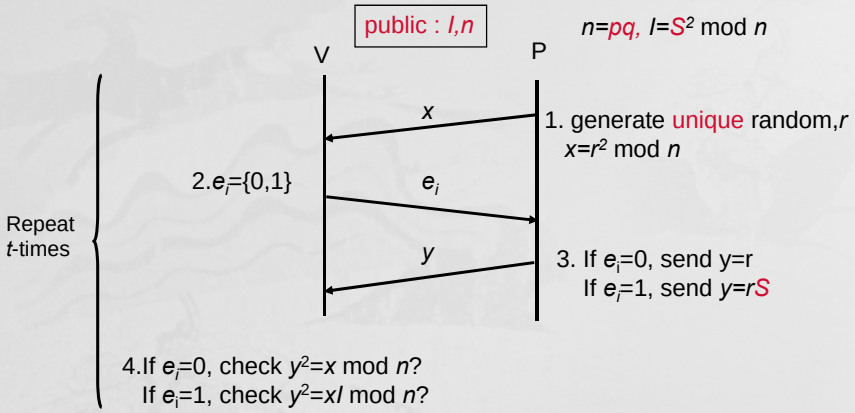
F-S Identification (I)

- (Preparation)
  (*TA*) Generate a universal n, used by everyone as long as none knows the factorization.
  (*P*)
  (1) private key: choose random value S, s.t. $\gcd(S,n)=1.(1 < S < n)$
  (2) public key : P computes $I=S^2 \bmod n$, and publishes (I,n) as public
- Goal
  P has to convince *V* that he knows his private key *S* and its corresponding public key (I,n) (*i.e., to prove that he knows a modular square root of* $I \bmod n$), without revealing *S*.

F-S Identification (II)

1. P chooses random value r $(1<r<n)$ and computes $x=r^2 \bmod n$. then sends x to V.
2. V requests from P one of the following request at random
   (a) r or (b) $rS \bmod n$
3. P sends the requested information to V.
4. V verifies that he received the right answer by checking whether
   (a) $r^2 = x \bmod n$ or (b) $(rS)^2 = xI \bmod n$
5. If verification fails, V concludes that P does not know S, and thus he is not the claimed party.
6. This protocol is repeated t (usually 20 or 30) times, and if in all of them the verification succeeds, V concludes that P is the claimed party.

F-S Identification (III)



* commitment-witness-challenge-response-verification and repeat

Security of F-S scheme

(1) Assuming that computing S is difficult, the breaking is equivalent to that of factoring n.

(2) Since P doesn't know (when he chooses r or rS mod n) which question V will ask, he can't choose the required answer in advance.

(3) P can succeed in guessing V's question with prob. 1/2 for each question. If the protocol is repeated t times, the prob. that V fails to catch P in all the times is only 2^{-t}, which is exponentially reducing with t. (t=20 or 30)

(4) Convinces V that P knows the square root of I, without revealing any information on S. However, V gets one bit of information : he learns that I is a quadratic residue

F-S scheme is ZKIP

- The F-S protocol convinces V that P knows the square root of I, without revealing any information on S. However, V gets one bit of information : he learns that I is a quadratic residue

In number theory, an integer q is called a **quadratic residue** modulo n if it is congruent to a perfect square (mod n); i.e., if there exists an integer x such that:

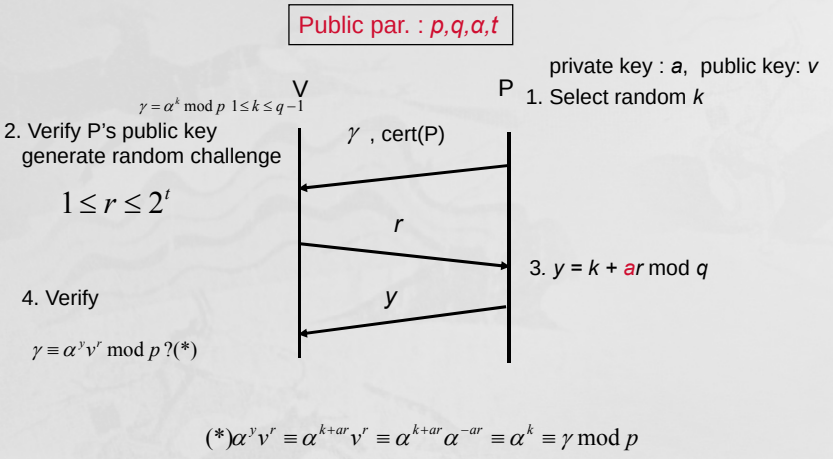
$$x^2 \equiv q \pmod{n}.$$

Otherwise, q is called a **quadratic nonresidue** (mod n).

Schnorr Identification (I)

- Based on DLP under Trusted Authority (TA)
- TA decides public parameters
  - p : large prime (1024 bit)
  - q : large prime divisor of p-1 (160 bit)
  - $\alpha \in Z_p^*$ has order q
  - t : security parameter s.t. $q > 2^t$
  - Public parameters : p, q, α, t
- Prover choose
  - private key : a ($1 \le a \le q$-1)
  - public key $v = \alpha^{-a} \bmod p$
- Honest Verifier (choose r at random by the scheme) ZKIP

Schnorr Identification (II)



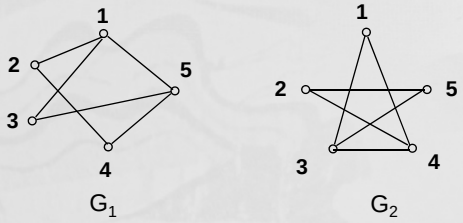
$$(*)\alpha^y v^r \equiv \alpha^{k+ar} v^r \equiv \alpha^{k+ar}\alpha^{-ar} \equiv \alpha^k \equiv \gamma \bmod p$$

Schnorr Identification (III)

- (TA)
  - p=88667, q=1031, t=10, α=70322 has order q in Z_p^*
- (P)
  - private key a = 755
  - public key $v = \alpha^{-a} \bmod p = 70322^{1031-755} \bmod 88667 = 13136$
- P: random k = 543,
  $\alpha^k \bmod p = 70322^{543} \bmod 88667 = 84109$, commit
- V: random challenge r =1000
- P: $y = k + ar \bmod q = 543 + 755 \text{x} 1000 \bmod 1031 = 851$
- V: on receiving y, verify that $84109 = 70322^{851}\ 13136^{1000} \bmod 88667$. If equals, accept

GI(Graph Isomorphism)

- (Def) G={V,E}=((1,...,n),({(i,j)})), n vertex
- ∃ a 1-1 and onto mapping ϕ keeping the incidence relation of Graph G_1 and G_2.

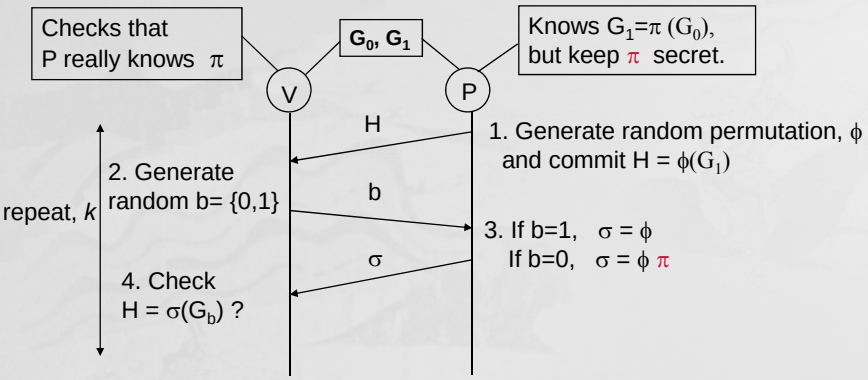


G_1 G_2

ϕ =(1, 2, 3, 4, 5, → 4, 2, 1, 5, 3) $G_2 = \phi(G_1)$

GI belongs to NP (Non deterministic Polynomial).

ZKIP using GI



Random Self-reducibility :
average = worst complexity
(*e.g*) GI,DL,QRA

Key Distribution Protocols

Characteristics of protocols

- *Computation in advance: pre- processing*
- *Mutually subscribed*
- *Unambiguous*
- *Complete*
- *Separate the process of achieving something* from a mechanism of achieving it

Classification of Protocols based on entities

- Arbitrated protocols
  - CA(Certificate Authority)
  - KDC(Key Distribution Center)
  - TTP(Trusted Third Party)
- Adjudicated protocols
  - Key-revocation
  - Key-escrow
  - Key-recovery
- Self-enforcing protocols
  - self-certified digital signature

Characteristics of security protocols

- Cryptosystems are always applied as cryptographic protocols.
- Using secure cryptosystem does not guarantee security of transactions.
- Inappropriate sequence or semantics of protocol messages may disclose information.
- Designing security protocols is a very difficult job.

Problem of Key Distribution

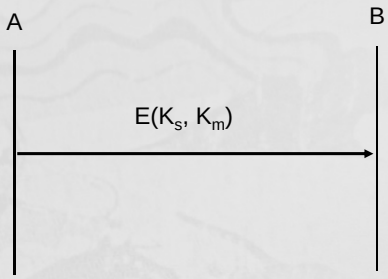
- Two different types of key
  - Long-term key
    - Set up initial key for each entity
    - Key Pre-distribution System
  - Session (short-term) key
    - After long-term key set up, share secret information among 2 or multi entities
    - Key Establishment System
- Key Distribution Center
  - Highly trustful entity, easy but maintenance cost overhead
  - Without online KDC, extremely hard to establish (agree)

Ways of Key Distribution

- Symmetric key exchange without KDC
- Symmetric key exchange with KDC
- Asymmetric key exchange without KDC
- Asymmetric key exchange with KDC

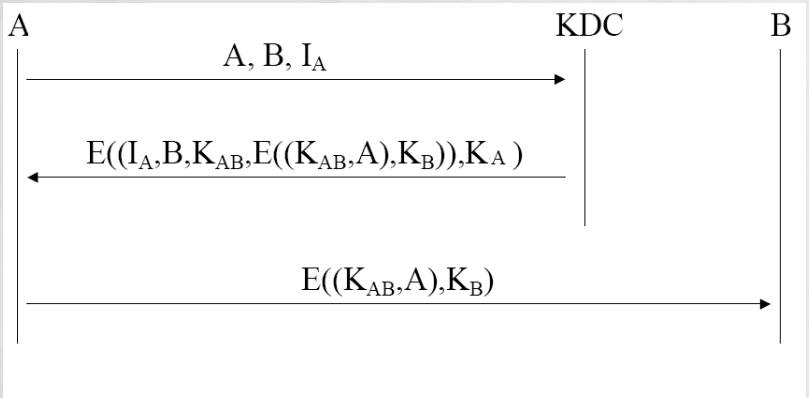
Symmetric key exchange without KDC

- Assume master key K_m shared by A and B
- Requires *n(n-1)/2* keys for *n* users

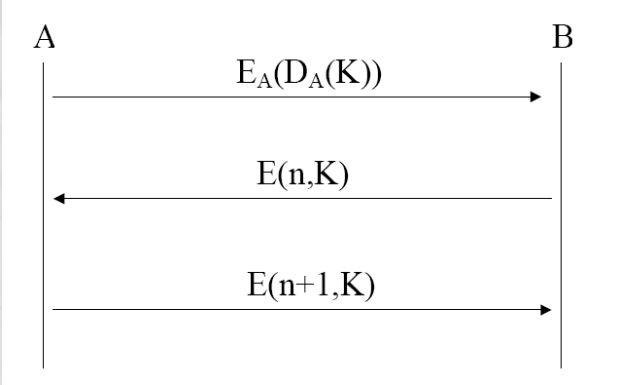


Symmetric key exchange with KDC

- Assume keys K_A and K_B that A and B share with KDC, respectively
- Shared key A and B is K_{AB}



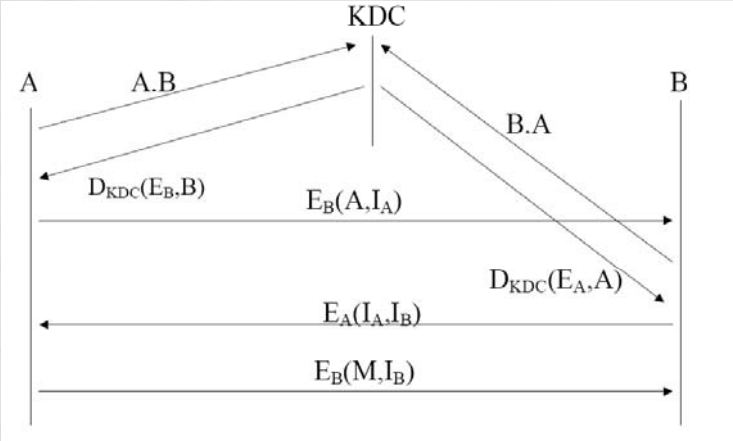
Asymmetric key exchange without KDC



n: nonce for mutual authentication

Asymmetric exchange w/KDC

- Assume A and B know the public key of KDC



Key Distribution Considerations

- What are the operational restrictions?
- What are the trust requirements?
- How are failures dealt with?
- How efficient is the protocol?
- How easy to implement is the protocol?

Key Establishment

- "*A process or protocol whereby a shared secret becomes available to two or more parties for subsequent cryptographic use*."
  - Key transport: one party creates and transfers it to the other(s)
  - Key agreement: a shared secret is derived by two or more parties as a function of information contributed by. No party can determine the resulting value.
- Use symmetric or asymmetric cryptosystem under PKI

Key Pre-distribution System

- Diffie-Hellman Key Pre-distribution (Key Agreement scheme)
  - Under DDH is hard, passive attacker can't compute a shared secret
  - Intruder-in-the middle attack
- Unconditionally Secure Key Pre-distribution
  - Secure against any attackers
  - Using off-band transfer, we can achieve unconditional-secure KPS → need n^2 complexity
  - Blom Key Pre-distribution System

Authenticated Key distribution

- (Implicit) key authentication: identity of party which may possibly share a key (No other party may gain access to a particular secret key)
- (Implicit) Key confirmation: evidence that a key is possessed by some party (He actually has possession of a particular secret key)
- Explicit key authentication: evidence an identified party can possess a key and any other party can't create this.
- Perfect forward secrecy: compromise of long-term keys does not compromise past session keys

Station-to-Station protocol (STS)

- Notation
  - E: symm. encryption
  - SA(m): A's signature on m
- Setup
  - System select and publish a prime p and generator g of GF(p)
  - Each user selects a public and private signature keys (e_A, n_A) and d_A.
- Protocol actions
  - A chooses a random secret x and sends g^x
  - B chooses a random secret y and sends $k=(g^x)^y$ and $E_k(S_B(g^y,g^x))$
  - A computes $k=(g^y)^x$, decrypt, verify and sends $E_k(S_A(g^x, g^y))$
  - B decrypts and verify A's signature
- Properties
  - Mutual key confirmation

❑45

MTI key agreement protocol

- Key generation
  - System select and publish a prime p and generator g of GF(p)
  - Alice /Bob selects a long-term private key a/b and publish a public key $A=g^a$ mod p , $B= g^b$ mod p
- Protocol actions
  - Alice chooses a random secret x and send g^x
  - Bob chooses a random secret y and send g^y
  - Alice computes $k=(g^y)^a B^x (=g^{ay+bx})$
  - Bob computes $k=(g^x)^b A^y (=g^{bx+ay})$
- Properties
  - Two-pass key agreement secure against passive attacks

❑46

Summary

- Key transport based on symmetric encryption
  - Shamir's no-key protocol: none
  - Kerberos: Use KDC
  - Needham-Schroeder: Use KDC
  - Otway-Rees: Use KDC
- Key transport based on asymmetric encryption
  - Needham-Schroeder : mutual entity authentication
  - X.509: mutual entity authentication
  - Beller-Yacobi: mutual entity authentication
- Key agreement based on asymmetric encryption
  - Diffie-Hellman: none
  - ElGamal: unilateral key authentication
  - MTI: mutual implicit key authentication
  - STS: mutual explicit key and entity authentication

Authentication Protocols

Authentication Protocols

- Verifying an identity
- People authentication
- Host authentication

Authentication vulnerabilities

- Eavesdropping
- Password database
- Replay
- Online/ offline guessing
- Session maybe hijacked after authentication!

Authenticating people

Computer verifying who you are

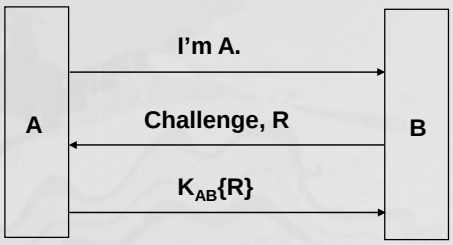
- what you know : password
- what you have : physical keys
- what you are : fingerprint *etc.*

Best : at least two of the above

Authentication protocols

- one-way
  - password
  - challenge/response
  - public-key
- two-way (mutual authentication)
  - trusted intermediary (Kerberos)
  - public-key

Shared secret(I)

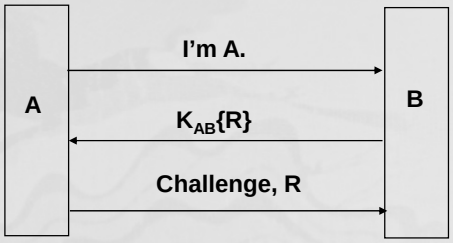


K_{AB} : Shared secret key between A and B.

Risks

- Not mutual authentication
- Off-line password guessing attack
- Some who reads B's database can later impersonate A.

Shared secret(II)

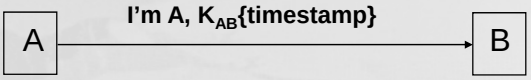


K_{AB} : Shared secret key between A and B.

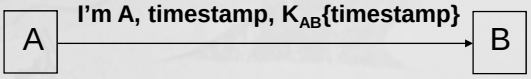
Risks

If R is recognizable quantity, password guessing attack is possible

Shared secret(III)

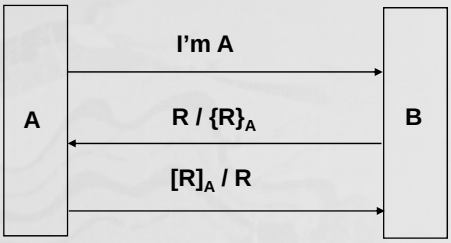


B authenticates A based on synchronized clocks and a shared secret



B authenticates A based on high resolution time and a shared secret

Public Key



B authenticates A based on her public key signature.
B authenticates A if she can decrypt a message encrypted with her public key
$[R]_A$: A signs R with private key.

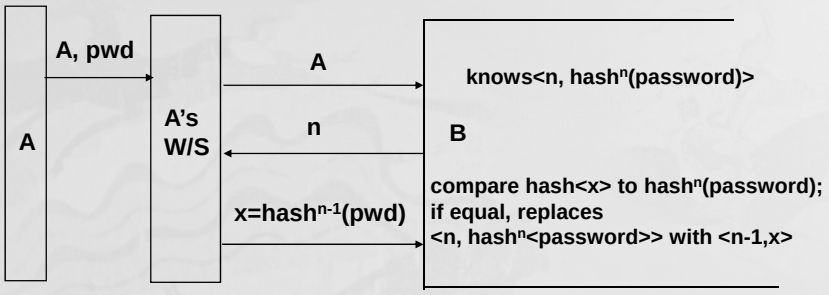
Risk : man-in-the middle attack

Lamport's hash(I)

- A remembers passwd
- B has DB for eash user
  - username
  - n, an integer which decrements each time B authenticates the user. (ex) n=1000
  - $hash^n$(passwd) i.e., hash(hash..hash(passwd)...))
- Risks
  - password access in system DB
  - eavesdropping communication line
  - revelation of password by careless user

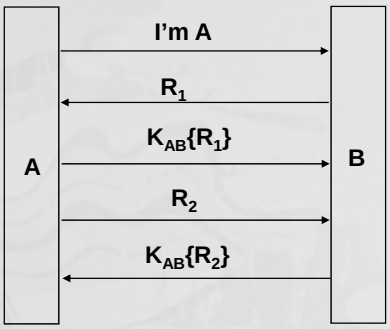
* L. Lamport, "Password Authentication with Insecure Channel",Comm. of the ACM, pp. 770-772, No.11, Vol.24, Nov., 1981

Lamport's hash(II)



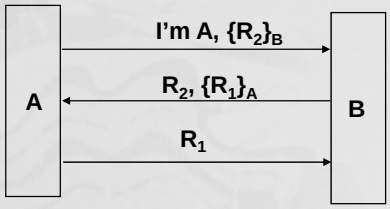
- Solving Encryption and integrity together :
  use password||salt instead of password only -> advance to S/KEY
- No mutual authentication

Mutual authentication(I)



- Mutual authentication based on shared secret, K_{AB}
- Risk of simplified 3-pass version (Protocol 9-9)
  - Man-in-the-middle attack (reflection attack)
  - password guessing

Mutual authentication(II)



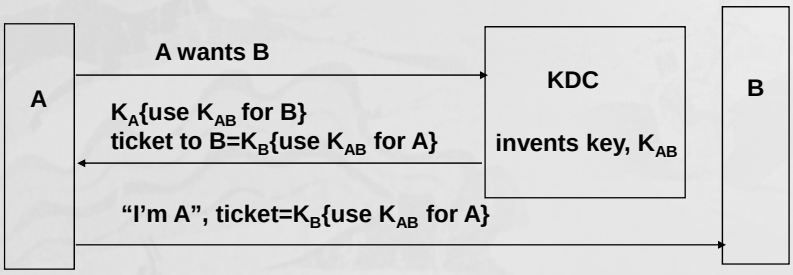
Mutual authentication with public keys
assuming that A and B know each other's public keys.

Mediated Authentication(I)

KDC operation (in principle)

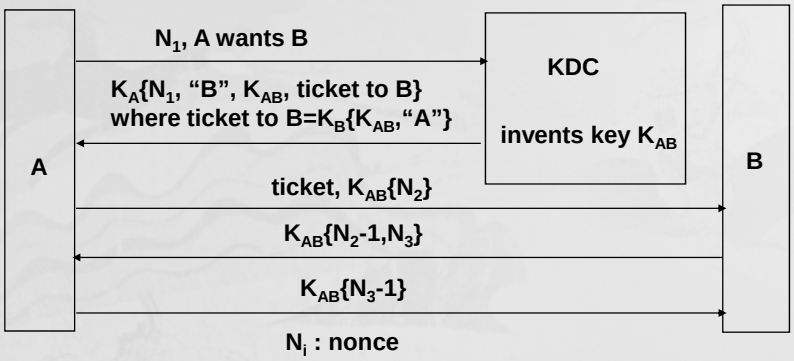
* anyone can impersonate A

Mediated Authentication(II)



KDC operation (in practice)

Needham-Schroeder



N_i : nonce

Properties

- Entity Authentication
- Key Confirmation
- Denning-Sacco attack

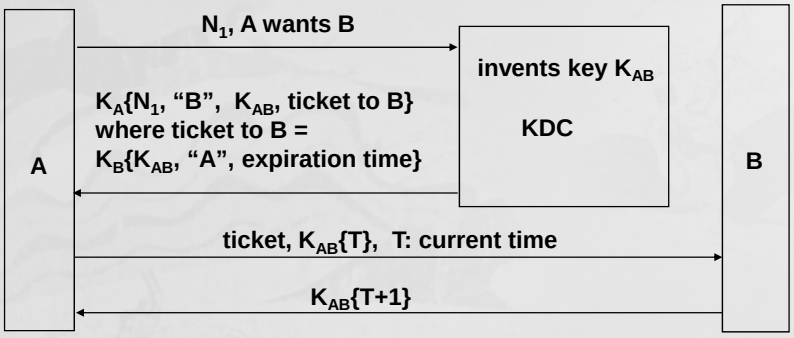
R.G.Needham and M.D. Schroeder, "Using encryption for authentication in large networks of computers", Comm. of the ACM, pp.993-999, Vol.21, No.12,Dec. 1978

Nonce

a number use only once

- timestamp
  - synchronized clocks
  - guessable
  - set clock back
- sequence number
  - guessable
  - requires state
- large random number

Kerberos



Performance Evaluation of Protocol

- Computational Complexity
  - # of cryptographic operations using a private key
  - # of cryptographic operations using a public key
  - # of bytes encrypted or decrypted using a secret key
  - # of bytes to be cryptographically hashed
- Communication Complexity
  - # of message transmitted

Identification by Bio-Metric information

❑67

Identity Questions ?

- Should this person be granted a visa ?
- Has this person already been issued a driver license ?
- Is this person authorized to access the information ?
- Is this person withdrawing money from the ATM machine really the account holder ?

❑68

How do I know who you are ?

- Current methods based on credentials (passwords and ID) are not adequate
  - The nineteen 9/11 hijackers had a total of 63 valid driver licenses
  - ~ 5 million identity thefts in US in 2004
  - 6.7 million victims of credit card fraud
  - People do not protect their credentials

❑69

Biometric Trails

❑70

Biometric Recognition

- Personal recognition based on "who you are" as opposed to/in conjunction with "what you know" (PIN) or "what you have" (ID card)

- Recognition of a person by his body, then linking that body to an externally established "identity", forms a very powerful tool for identity management.

Application

Goal: Automatic & reliable person identification in unattended mode, often remotely

Iris matching: Heathrow Airport

US-VISIT Program

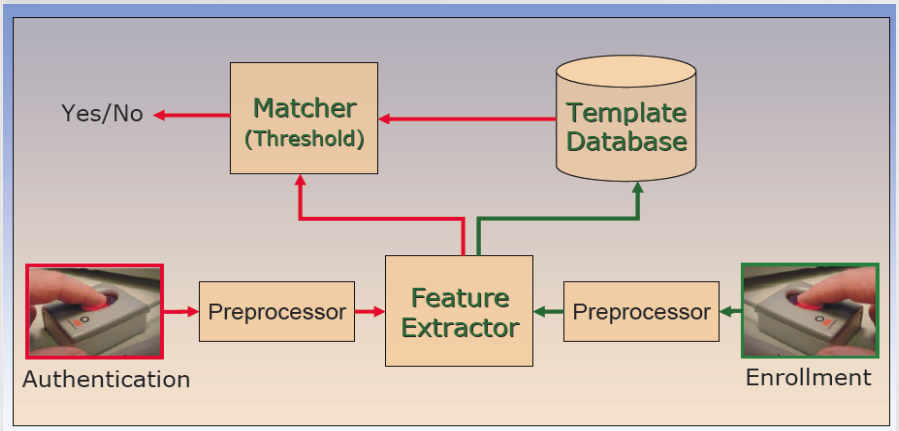
Cellular phone: Siemens

Grocery store payment: Indivos

Automobile: Audi A8

Disney World

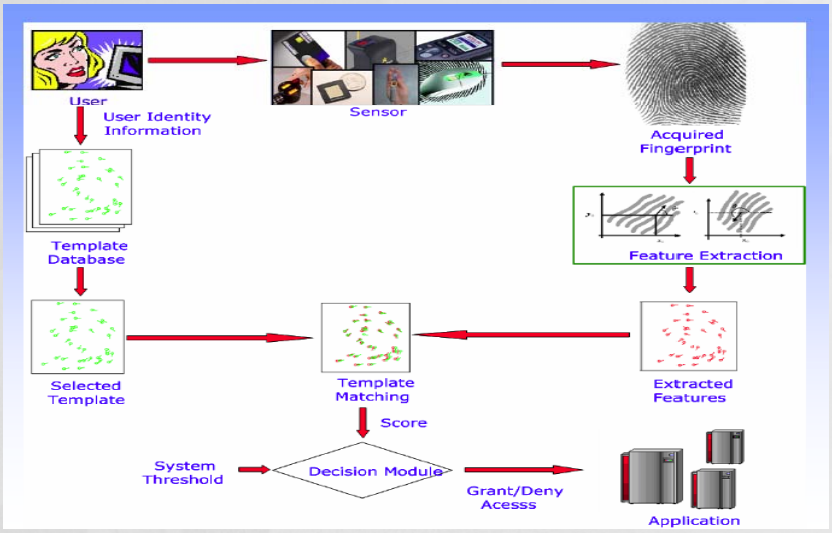
Biometric Recognition System



- False accept rate (FAR): Proportion of imposters accepted
- False reject rate (FRR): Proportion of genuine users rejected
- Failure to enroll rate (FTE): portion of population that cannot be enrolled
- Failure to acquire rate (FTA): portion of population that cannot be verified

❑73

Fingerprint System



❑74

Challenges

- Accuracy
- Cost
- Speed
- Ease of Use
- Failure to Enroll
- Robustness

} Return on investment

- Security
- Privacy

❑75

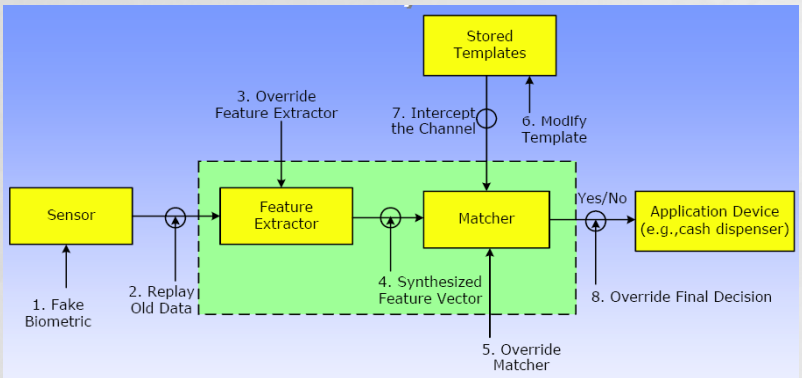
"State-of-the-art" Error Reports

	Test	Test Parameter	False Reject Rate	False Accept Rate
Fingerprint	FVC [2004]	20 years (average age)	2%	2%
	FpVTE [2003]	US govt. ops. Data	0.1%	1%
Face	FRVT [2002]	Varied lighting, outdoor/indoor	10%	1%
Voice	NIST [2004]	Text independent, multi-lingual	5-10%	2-5%

At NY airports, an average of ~ 200,000 passengers pass through daily. There would be 4,000 falsely rejected (and inconvenienced) passengers per day for fingerprints, 20,000 for face and 30,000 for voice. Similar numbers can be computed for false accepts

❑76

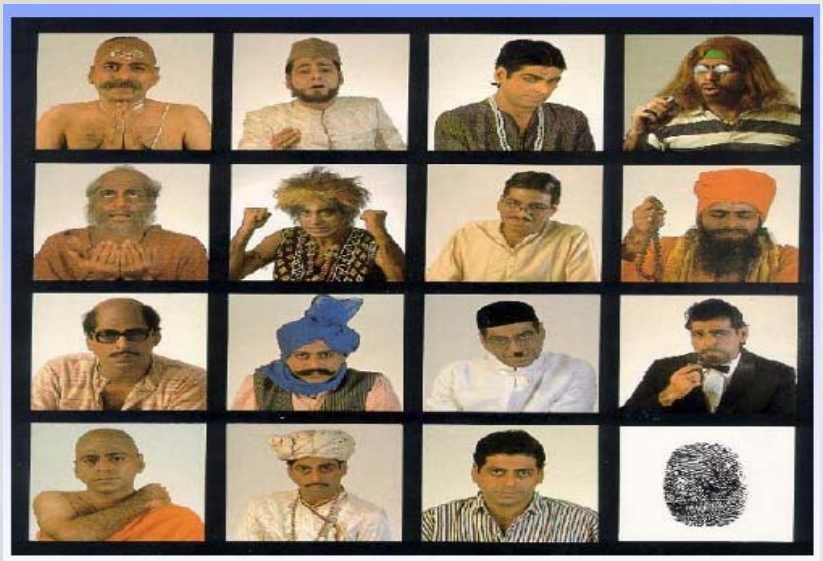
Biometric System Attack



Type 1: A fake biometric is presented at the sensor; Type 2: Illegally intercepted data is resubmitted (replay); Type 3: Feature detector is replaced by a Trojan horse program; Type 4: Legitimate features are replaced with synthetic features; Type 5: Matcher is replaced by a Trojan horse program; Type 6: Templates in the database are modified; Type 7: Template is intercepted & altered in the channel; Type 8: Matching result (e.g., accept/reject) is overridden

❑77

Comouflage

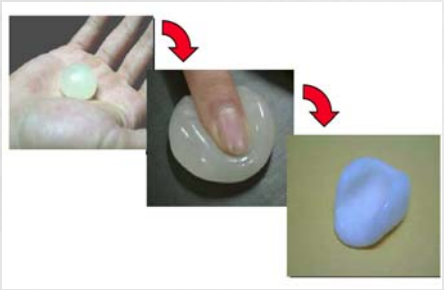


❑78

Fake Fingerprint by gelratine (I)

Step 1. Get Gelratine leaf, etc (< 10$)

Step 2. Make flexible mold from gem

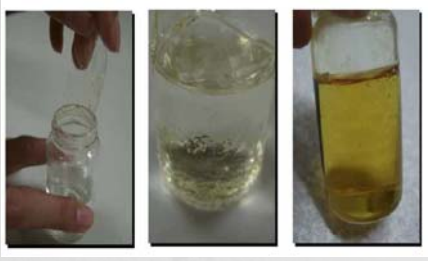


Extracted from A. Jail's presentation in SCIS2006, Japan

❑79

Fake Fingerprint by gelratine (II)

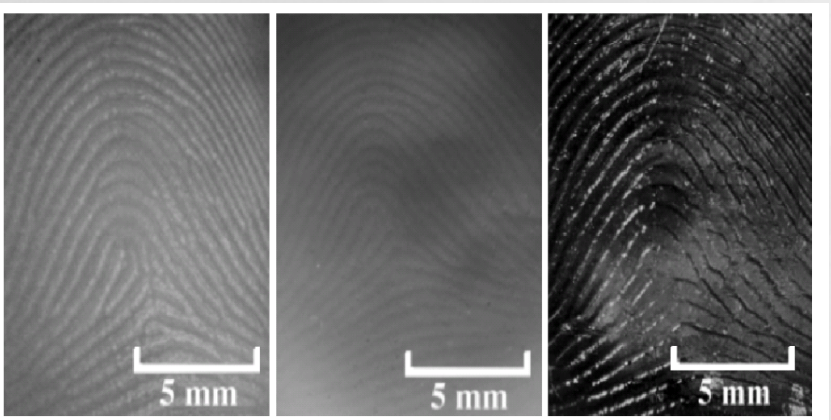
Step 3. Mix gelratine with water and boil



Step 4. Spill gelratine into mold

❑80

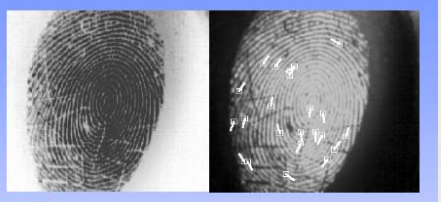
Fake Fingerprint



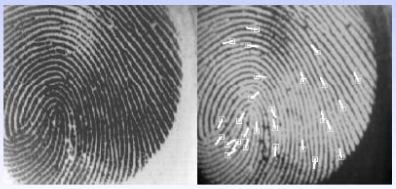
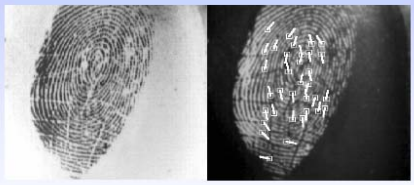
Real fingerprint Silicon fingerprint Gelratine fingerprint

❑81

Fake Fingerprint

Live finger

Gummy finger

Access was granted 75% of the time using gummy fingers

❑82

Other Attacks

- Insider attacks
- Integrity of the enrollment process
- Once initial access is granted, an imposter can spoof the system in the absence of real-time continuous authentication
- Exception handling may introduce a weak link
- By providing poor quality images at input
- Biometrics is made ineffective by attacking other components of the security system

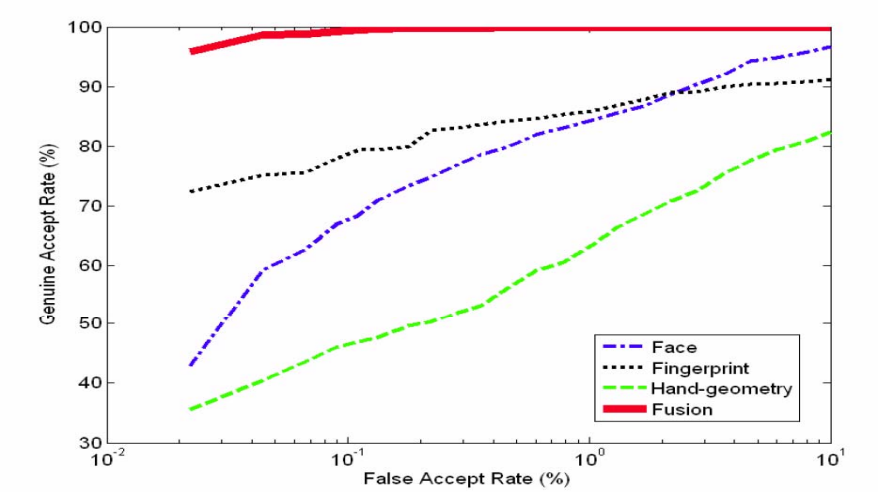
❑83

Multibiometrics

Provides resistance against spoof attacks; also improve matching accuracy and population coverage

❑84

Biometric System Performance



❑85

Securing wireless devices with multibiometric

AuthenticTec has sold 4 million fingerprint sensors world-wide to provide secure authentication for mobile commerce and mobile banking applications

❑86

Summary

- Biometrics are an essential component of any identity-based system, but they themselves are vulnerable
- Some of these attacks are simple to execute; solutions to these attacks have been identified, but there is still room for improvement
- Attacks on biometric systems can result in loss of privacy and monetary damage, so the users need to be convinced about the system protection
- New security issues with biometric systems may arise as their use becomes more widespread
- In spite of this, biometric systems are being deployed for securing international borders, controlling access and eliminating identity theft