Entity Authentication

Prof. Bart Preneel
COSIC – KU Leuven - Belgium
Firstname.Lastname(at)esat.kuleuven.be
http://homes.esat.kuleuven.be/~preneel
February 2014

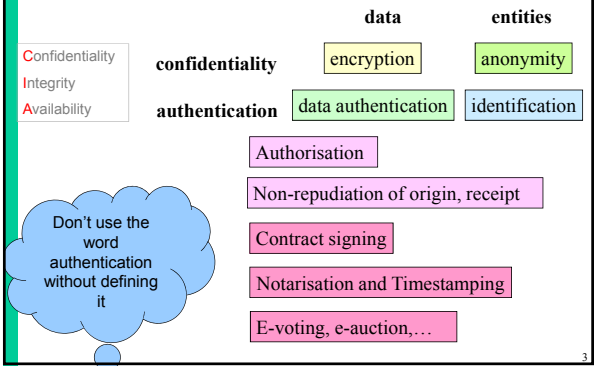
1

Goals

- Understand goals of entity authentication
- Understand strength and limitations of entity authentication protocols including passwords
- Understand subtle problems when entity authentication protocols are deployed in practice

2

Definitions (ctd)



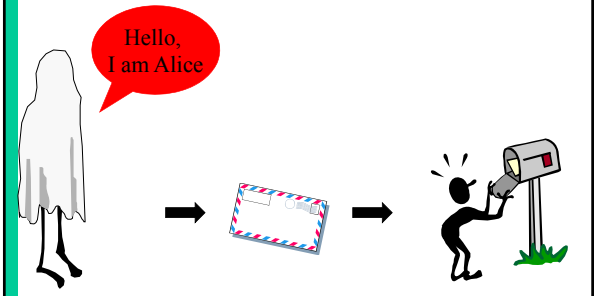
3

Identification

- the problem
- passwords
- challenge response with symmetric key and MAC (symmetric tokens)
- challenge response with public key (signatures, ZK)
- biometry

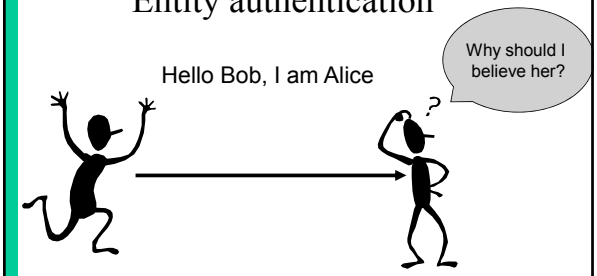
4

Entity authentication



5

Entity authentication



entity authentication: one is corroborated of the identity of another party, and of the fact that this party is **alive (active)** during the protocol

6

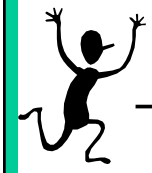
Entity authentication is based on one or more of the following elements:

- what someone knows
  - password, PIN
- what someone has
  - magstripe card, smart card
- what someone is (biometrics)
  - fingerprint, retina, hand shape,...
- how someone does something
  - manual signature, typing pattern
- where someone is
  - dialback, location based services (GSM, Galileo)

ert5^r$#89Oy

7

Entity authentication with passwords



Hello Bob, I am Alice.
My password P is
Xur%9pLr

Alice	Xur%9pLr

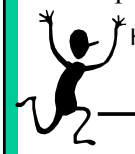
BUT

- Eve can guess the password
- Eve can listen to the channel and learn Alice's password
- Bob needs to know Alice's secret
- Bob needs to store Alice's secret in a secure way

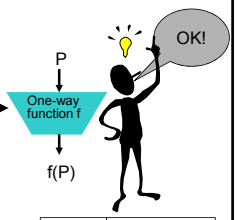
Possibility of replay: liveliness is missing

8

Improved identification with passwords



Hello Bob, I am Alice.
My password P is
Xur%9pLr



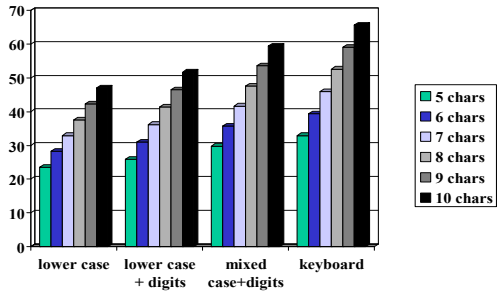
Alice	f(Xur%9pLr)

Bob stores f(P) rather than Alice's secret P

- it is difficult to deduce P from f(P)

9

Password entropy: effective key length

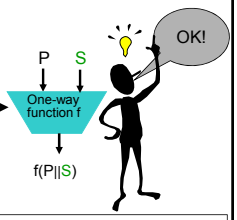


Problem: passwords from dictionaries

10

Improved+ identification with passwords

Hello Bob, I am Alice.
My password P is
Xur%9pLr



give every user at registration a random publicly known value S (salt)

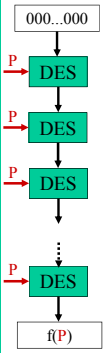
Alice	f(Xur%9pLr||987&*)|| 987&*)

Bob stores f(P,S) || S rather than Alice's secret P

it is harder to attack the passwords of all users simultaneously

11

Example: UNIX



- Function f() = DES applied 25 times to the all zero plaintext with as key the password P (8 7-bit characters)
- Salt: 12-bit modification to DES
- etc/passwd public
- PC: 20-40 million passwords/second
- But time-memory tradeoff…
  - Precomputation per salt $25 \cdot 2^{56}$
  - Storage per salt: 2 Terabyte
  - Find one key in time 25.2^{38}

12

Improving password security

- Apply the function f "x" times to the password (iteratively)
  - if x = 100 million, testing a password guess takes a few seconds
  - need to increase x with time (Moore's law)
  - Examples: PBKDF2 (Password-Based Key Derivation Function 2), scrypt, bcrypt
- Disadvantage: one cannot use the same hashed password file on a faster server and on an embedded device with an 8-bit microprocessor
  - need to use different values of x depending on the computational power of the machine

13

Problem: human memory is limited

- Solution: store key K on magstripe, USB key, hard disk
- Stops guessing attacks

But this does not solve the other problems related to passwords

And now you identify the card, not the user….

Possibility of replay: liveliness is missing

14

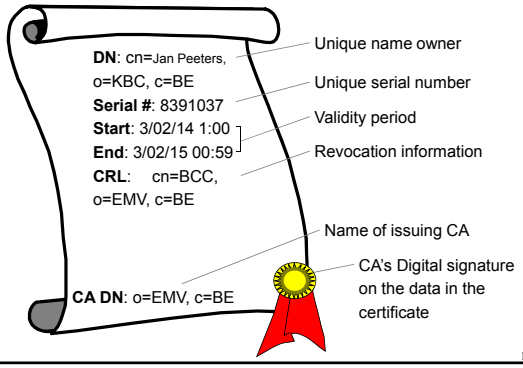
Improvement: Static Data Authentication

- Replace K by a signature of a third party CA (Certification Authority) on Alice's name: $SigSK_{CA}$ (Alice) = special certificate
- Advantage: can be verified using a public string PK_{CA}
- Advantage: can only be generated by CA
- Disadvantage: signature = 40..128 bytes
- Disadvantage: can still be copied/intercepted

Possibility of replay: liveliness is missing

15

"Certificate" for static data authentication



16

Entity authentication with symmetric token

or

Challenge response protocol

random number r

$MAC_K(r)$

- Eavesdropping no longer effective
- Bob still needs secret key K

Detects whether Alice is alive!

17

Entity authentication with symmetric token

With implicit challenge from clock

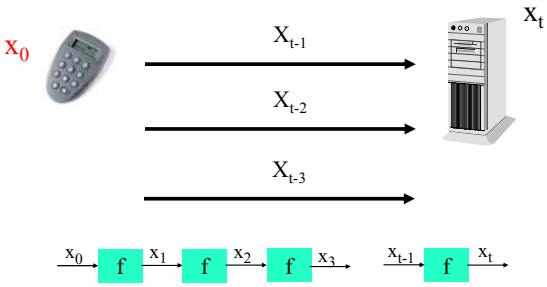
$MAC_K(time)$

- Eavesdropping no longer effective
- Bob still needs secret key K
- resynchronization mechanism needed

18

Lamport's one-time passwords

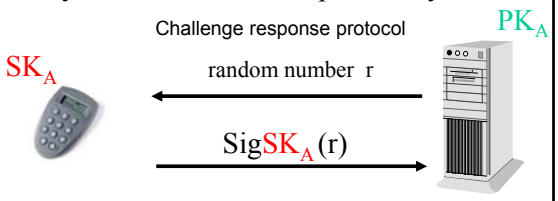
iterated one-way function



- Disadvantage: only works with one Bob

19

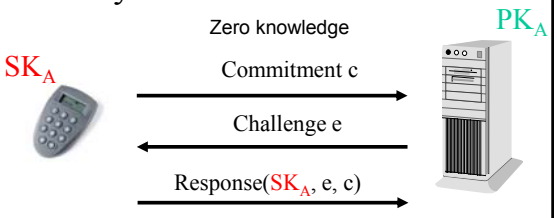
Entity authentication with public key token



- Eavesdropping no longer effective
- Bob no longer needs a secret – only PK_A

20

Entity authentication with ZK



- Mathematical proof that Bob only learns that he is talking to Alice (1 bit of information)
- Bob cannot use this information to convince a third party that he is/was talking to Alice

21

ZK definitions

- **complete:** if Alice knows the secret, she can carry outthe protocol successfully
- **sound:** Eve (who wants to impersonate Alice) can only convinceBob with a very small probability that she is Alice;
- **zero knowledge:** even a dishonest Bob does not learn anything except for 1 bit (he is talking to Alice); he could have produced himself all the other information he obtains during the protocol.

22

ZK: Fiat-Shamir (1986)

- central RSA modulus n
- per user:
  - identity I_A
  - secret key s_A $(0 < s_A < n)$
  - public key $y_A = s_A^2 \mod n$
- facts from number theory:
  - if one knows the factorization of n, it is easy to compute the square roots modulo n (if they exist);
  - if one can compute square roots modulo n, it is easy to factor n

23

ZK: Fiat-Shamir

All operations mod n

Complete: trivial
Sound: Eve's probability of success = ½
Eve gambles that Bob will choose e=0
then she chooses r, and computes $x=r^2$ and $z_0=r$
Eve gambles that Bob will choose e=1
then she chooses z_1, and computes $x=z_1^2/y_A$
If Eve knows both z_0 and z_1 then she knows $s_A=z_1/z_0$

24

ZK: Fiat-Shamir

- **zero knowledge:** Bob learns nothing about Alice's secret
- e=0: B sees r and r^2
- e=1: B sees r^2 (from $r^2 s_A^2 = r^2 . y_A$) and $r s_A$
  - $r . s_A$ is a Vernam encryption of s_A: statistically independent of s_A
- Hence B only sees 2 random squares mod n, which he could have produced himself (yet he is convinced that he has spoken to Alice!)
- in practice: more iterations (20...40) for better security ($1/2^{20}$ …$1/2^{40}$)

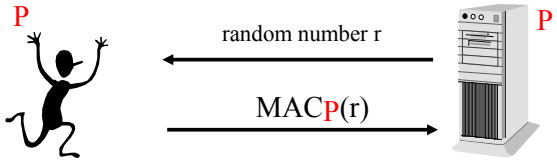
25

Overview Identification Protocols

	Guess	Eavesdrop channel (liveliness)	Impersonation by Bob	Secret info for Bob	Security
Password	-	-	-	-	**1**
Magstripe (SK)	+	-	-	-	**2**
Magstripe (PK)	+	-	-	+	**3**
Dynamic password	+	+	-	-	**4**
Smart card (SK)	+	+	-	-	**4**
Smart Card (PK)	+	+	+	+	**5**

Entity authentication with password

Challenge response protocol



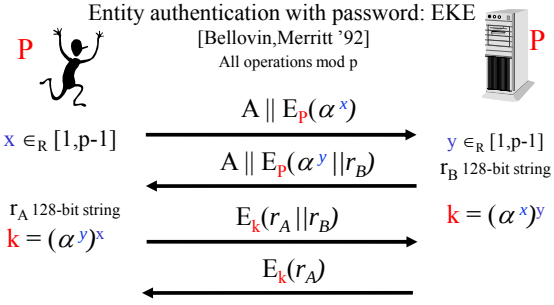
- Eavesdropping no longer effective
- Bob still needs secret key P
- Exhaustive search for P is easy based on a single transcript

27

Entity authentication with password: EKE

[Bellovin,Merritt '92]

All operations mod p



- Adds entity authentication to Diffie Hellman
- Attacker cannot perform off-line exhaustive search for the password P
- Attacker can still try on-line attacks; need to restrict number of uses of the account

- Literature: PAKE: Password Authenticated Key Establishment

28

Entity authentication in practice

- Phishing – mutual authentication
- Forward credentials - biometry
- Interrupt after initial authentication – authenticated key establishment
- Mafia fraud – distance bounding
- Protocol errors – check that local device authentication is linked to entity authentication protocol (example: EMV)

29

Mutual authentication

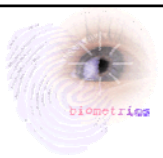
- Phishing is impersonating of the verifier (e.g. the bank)
- Most applications need entity authentication in two directions
- !! This is not complete the same as 2 parallel unilateral protocols for entity authentication

2 stage authentication

- Local: user to device
- Device to rest of the world

30

Biometry



- Based on our unique features
- Identification or verification
  - Is this Alice?
  - Check against watchlist
  - Has this person ever registered in the system?

31

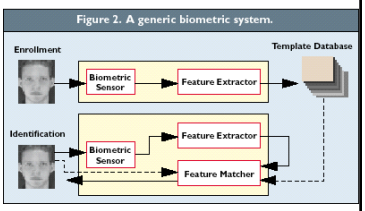
Some unique features

DNA
skin
…

32

Biometric procedures

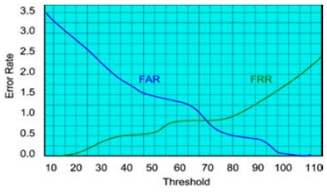
- Registration
- Template extraction
- Measurement
- Processing
- Template matching
- Link with applications



33

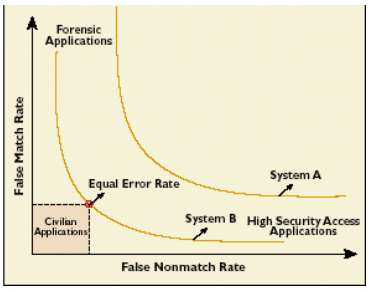
Robustness/performance

- Performance evaluation
  - False Acceptance Ratio or False Match Rate
  - False Rejection Ratio or False Non-Match Rate
- Application dependent



34

Robustness/performance (2)

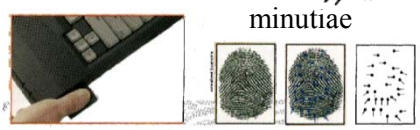


35

Fingerprint

- Used for PC/laptop access
- Widely available
- Reliable and inexpensive
- Simple interface

minutiae



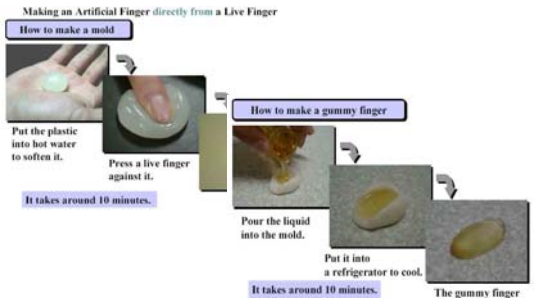
36

Fingerprint (2)

- Small sensor
- Small template (100 bytes)
- Commercially available
  - Optical/thermical/capacitive
  - Liveness detection
- Problems for some ethnic groups and some professions
- Connotation with crime

37

Fingerprint (3): gummy fingers



38

Hand geometry

- Flexible performance tuning
- Mostly 3D geometry
- Example: 1996 Olympics

39

Voice recognition

- Speech processing technology well developed
- Can be used at a distance
- Can use microphone of our gsm
- But tools to spoof exist as well
- Typical applications: complement PIN for mobile or domotica

40

Iris Scan

- No contact and fast
- Conventional CCD camera
- 200 parameters
- Template: 512 bytes
- All etnic groups
- Reveals health status

41

Retina scan

- Stable and unique pattern of blood vessels
- Invasive
- High security

42

Manual signature

- Measure distance, speed, accelerations, pressure
- Familiar
- Easy to use
- Template needs continuous update
- Technology not fully mature

43

Facial recognition

- User friendly
- No cooperation needed
- Reliability limited
- Robustness issues
  - Lighting conditions
  - Glasses/hair/beard/...

44

Comparison

Feature	Uniqueness	Permanent	Performance	Acceptability	Spoofing
Facial	Low	Average	Low	High	Low
Fingerprint	High	High	High??	Average	High??
Hand geometry	Average	Average	Average	Average	Average
Iris	High	High	High	Low	High
Retina	High	Average	High	Low	High
Signature	Low	Low	Low	High	Low
Voice	Low	Low	Low	High	Low

45

Biometry: pros and cons

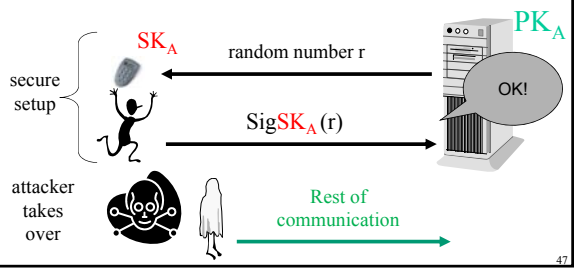
- Real person
- User friendly
- Cannot be forwarded
- Little effort for user
- Secure implementation: derive key in a secure way from the biometric

- Privacy (medical)
- Intrusive?
- Liveliness?
- Cannot be replaced
- Risk for physical attacks
- Hygiene
- Does not work everyone, e.g., people with disabilities
- Reliability
- No cryptographic key

46

Keeping authenticity alive

- Establish who someone is
- Establish that this person is active/liveliness
- But what if the connection is broken after the initial phase?



47

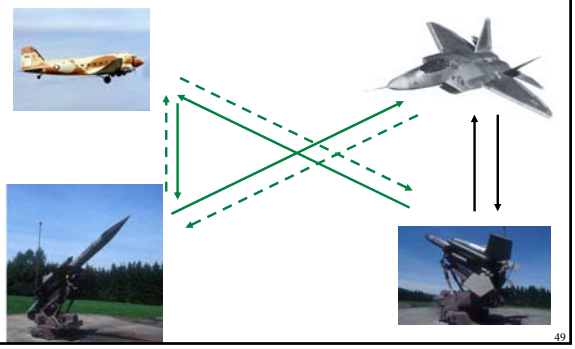
Solution

- Authenticated key agreement

- Run a mutual entity authentication protocol
- Establish a key
- Encrypt and authenticate all information exchanged using this key

48

The mafia fraud
– or the grandmaster chess problem



49

Location-based authentication

- Distance bounding: try to prove that you are physically close to the verifier
- Other uses of "location"
  - Dial-back: can be defeated using fake dial tone
  - IP addresses and MAC addresses can be spoofed
  - Mobile/wireless communications: operator knows access point, but how to convince others?
  - Trusted GPS: Galileo?

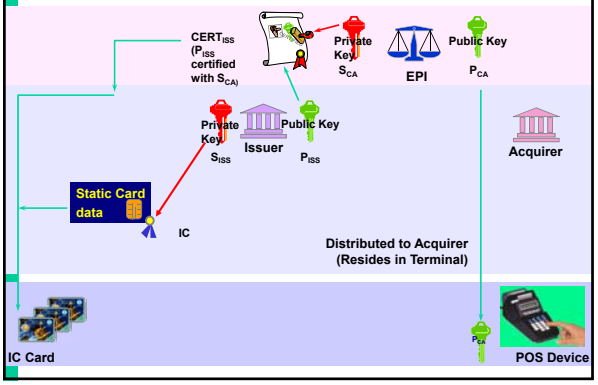
50

Authentication with device

- E.g. smart card, secure login token
- Needs 2 stages
  - Local: user to device
  - Device to rest of the world
- Are these 2 stages connected properly?

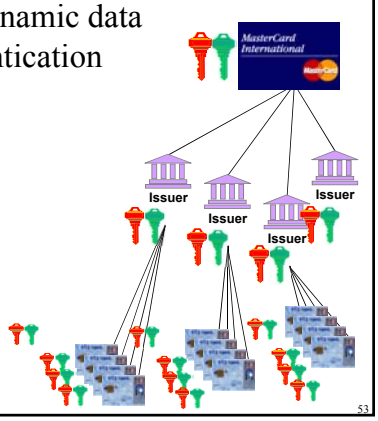
51

EMV Static Data Authentication (SDA)



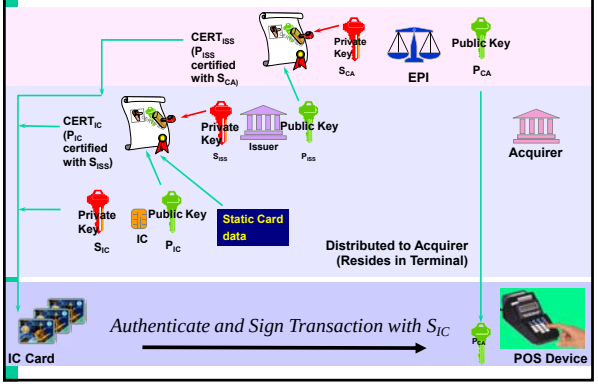
EMV: dynamic data authentication

- Three layers:
  - EPI
  - Issuers
  - Cards



53

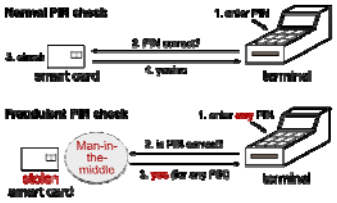
EMV Dynamic Data Authentication



Warning about EMV

http://www.cl.cam.ac.uk/research/security/banking/nopin/oakland10chipbroken.pdf

- **EMV PIN verification "wedge" vulnerability** S.J. Murdoch, S. Drimer, R. Anderson, M. Bond, IEEE Security & Privacy 2010



55

Guidelines

NIST Special Publication 800-63 Version 1.0.2 (2006): Electronic Authentication Guideline: identifies four levels of assurance

http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

See http://csrc.nist.gov/publications/PubsSPs.html for about 120 Special Publications (800 Series) from NIST on computer security and cryptography

56