Computer security Lecture 2

Identification and Authentication

Ingo Hölscher

LINKÖPING UNIVERSITY

User authentication

- Authentication is the process of **verifying the identify** of a user
- There are two reasons to do this:
  - To make access control decisions
  - To enable audit trails
- Authorization is sometimes based on role, not identity
- Accountability is based on identity, since group accountability is ineffective

Authentication procedure

- The most common procedure is as follows:
  - An individual arrives at a checkpoint (login dialog, door, . . .)
  - The individual claims an identity (username, Smart Card, token,. . .)
  - The individual presents the item needed to prove the identity (password, PIN, . . .)

"On the Internet, nobody knows you're a dog."

Authentication of users can use

- **Something you know** (passwords, PIN, . . .)
- **Something you have** (keys, badges, tokens, smart card, . . .)
- **Something you are** biometrics (handwriting, fingerprints, retina patterns, . . .)

Authentication of users can use

- **Something you know** (passwords, PIN, . . .)
- **Something you have** (keys, badges, tokens, smart card, . . .)
- **Something you are** biometrics (handwriting, fingerprints, retina patterns, . . .)
- Something you do (handwriting, . . .)
- Where you are

“Where you are”?

- does not verify identity, unless only one person can enter that location
- could reduce the number of possible identities
- but should rather be thought of as access restriction, than an authentication mechanism

Authentication of users can use

- **Something you know** (passwords, PIN, . . .)
- **Something you have** (keys, badges, tokens, smart card, . . .)
- **Something you are** biometrics (handwriting, fingerprints, retina patterns, . . .)
- Something you do (handwriting, . . .)
- Where you are

Authentication modes

- **Something you know**
  (passwords, PIN, . . .)
- **Something you have**
  (keys, badges, tokens, smart card, . . .)
- **Something you are**
  biometrics (handwriting, fingerprints, retina patterns, . . .)

Something you know: Passwords

- Username+password is the standard first line of defense
- Widely accepted, not too difficult to implement
- Can be expensive to manage password securely
- Obtaining a valid password is a common attack

Maintaining passwords

- People can't remember infrequently used, frequently changed, many similar items
- We can't forget on demand
- Recall is harder than recognition
- Non-meaningful words are more difficult to remember

Ways for an attacker to obtain a valid password

- Intercept it at creation
- Guess it
- Steal the note where it is written down
- Watch user enter it, or use a keylogger
- Eavesdrop on transmission
- Find it in a memory buffer

Ways for an attacker to obtain a valid password

- Find it through a spoofing program, through phishing, or more general social engineering
- Find it reused in another system
- Password recovery

Ways for an attacker to obtain a valid password

Keylogger

Ways for an attacker to obtain a valid password

Guessing passwords

- Exhaustive search
- Intelligent search
  dictionary
  words associated with user

Password management

- Requires proper routines for issuing
- Requires properly trained staff, maybe round-the-clock helpdesk
- This can become a cost factor that needs to be taken into account

LiUs password policy:

http://liu.se/insidan/it/irt/losenord?l=en&sc=true

Selecting a secure password

In general, when you want to protect something, you lock it up with a key. Houses, cars and bicycle locks all have physical keys; protected files have encryption keys; bank cards have PIN numbers; and email accounts have passwords. All of these keys, physical and electronic, have one thing in common: they open their respective locks just as effectively in the hands of somebody else. You can install advanced firewalls, secure email accounts, and encrypted disks, but if your password is weak, or if you allow it to fall into the wrong hands, they will not do you much good.

Selecting a secure password

Common advice on passwords

Passwords should

- be long enough, and
- …have enough variation to make guessing hard
- be easy to remember, without violating the points above
- be changed at reasonable intervals

Should not

- be anything you reveal outside authentication
- be the same for two sites
- if one site is more sensitive
- if one site is less trusted
- be stored in plaintext
- be sent in plaintext
- be connectable to you

Selecting a secure password

Common advice on passwords

Passwords should

- be long enough, and
- …have enough variation to make guessing hard
- be easy to remember, without violating the points above
- be changed at reasonable intervals

Should not

- be anything you reveal outside authentication
- be the same for two sites
- if one site is more sensitive
- if one site is less trusted
- be stored in plaintext
- be sent in plaintext
- be connectable to you

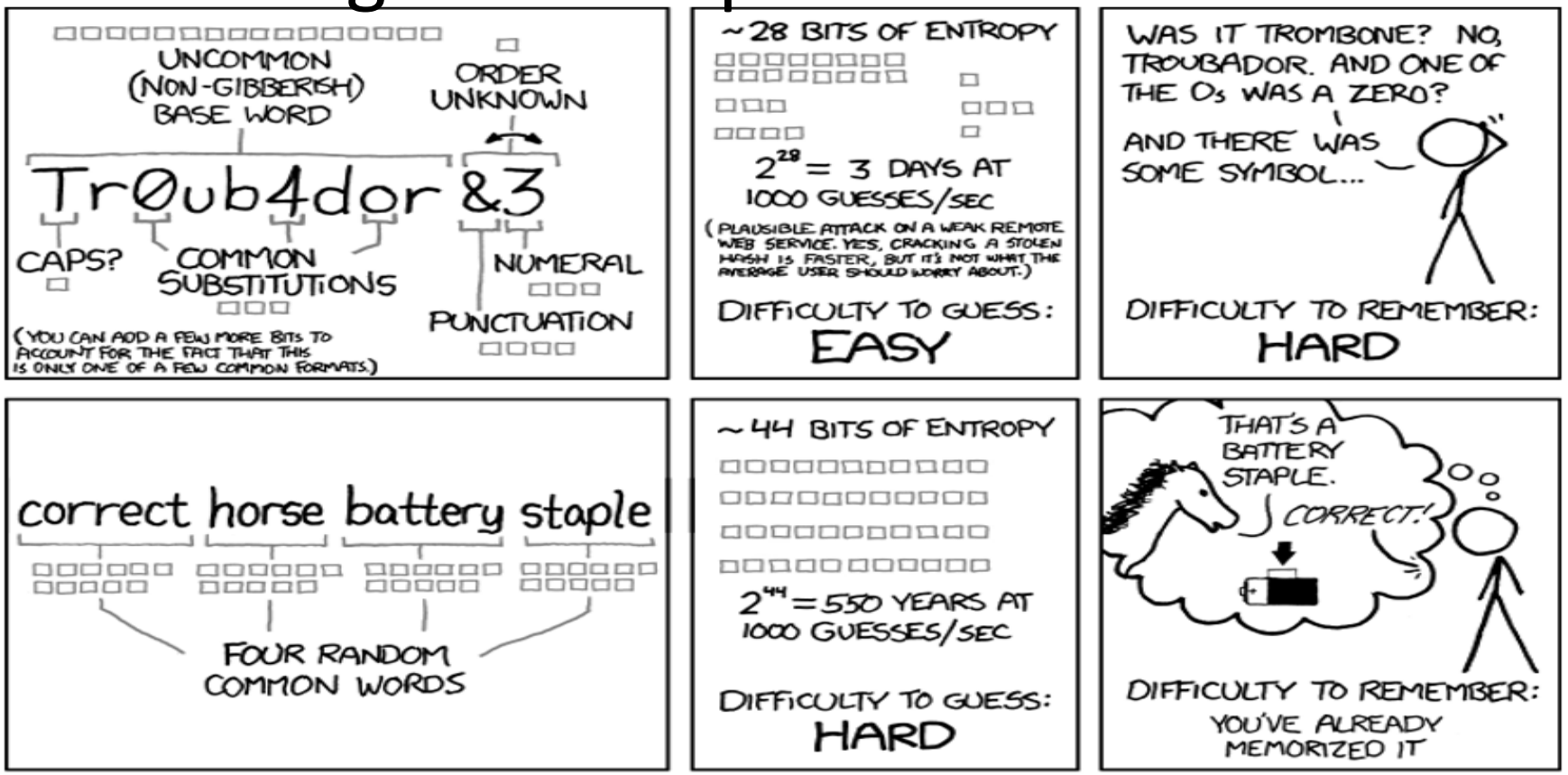
Choose a password you can't remember and don't write it down

Selecting a secure password

Schneier

1. Generate (a real) random password
2. Write it on a piece of paper
3. Keep the now valuable piece of paper with the other valuable pieces of paper you own in your wallet

Selecting a secure password



xkcd.org

Selecting a secure password

Is naive password choice really a problem?

(Yes!)

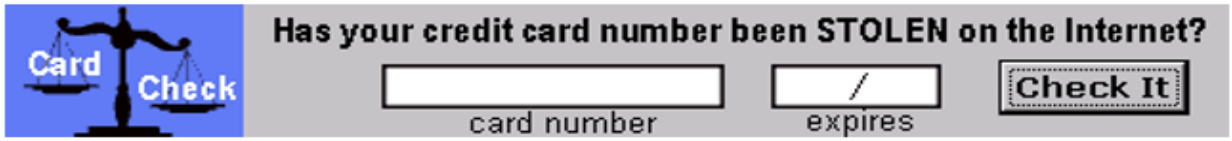
- An old study by D. Klein found that 25% of passwords could be guessed, roughly
  Dictionary words: 7.4%
  Common names: 4%
  Combination of user and account name: 2.7%
  …
- Frequent password changes often backfire
  monthly changes: alice01, alice02, …
  checking against old passwords: rapid changes until the old password can be used
  post-it notes on the screen
  …

Something you know: PIN

- Financial PINs are often four digits
- Some banks force PIN on the user, other allows you to choose
- Avoid 1111, 2222, and 1234, 2345, or birthdates and suchlike
- Many systems allow three attempts before locking card, giving a 0.06% chance of guessing it
- PIN generation through the IBM 3624 standard uses the account number to generate the PIN (through encryption)
- Despite the encryption key being secret, the connection to the account number allows guessing the PIN on the average in 15 attempts (Zielinski and Bond, 2002)

Ways for an attacker to obtain a PIN

- Phishing: Ask user for login and password under false pretense
- Spoofing: Present false but genuine-looking login screen
- Other social engineering: Directed personal attacks aimed to extract password, often aimed at support staff



- One problem is that even big banks (or indeed PayPal) train customers in unsafe behaviour

How to avoid phishing, spoofing and social engineering

Educate users, or even better: don't miseducate them

- Check the English (better English)
- Look for the lock symbol (use TLS or put a lock symbol on the page)
- Look for the last four numbers in your account number (put the first four numbers there)
- Don't click on URLs but pictures are OK (hide executables under pictures)
- Use mouse hover to show the real URL (insert nonprinting chars, or use extremely long URLs)

How to avoid phishing, spoofing and social engineering

The need for repeated authentication

- Some systems require repeated authentication
- This is to stop attackers from using an already logged-in computer, later
- This can also be used to authenticate again when a user wants to perform a security-critical operation
- The book mentions TOCTTOU, time-of-check-to-time-of-use

Authentication modes

- **Something you know** (passwords, PIN, . . .)
- **Something you have** (keys, badges, tokens, smart card, . . .)
- **Something you are** biometrics (handwriting, fingerprints, retina patterns, . . .)

Something you have

- can be stolen
- can be found by others, if lost
- can be copied, if you know their correct properties
  - Skimming
  - guessing valid properties
  - radio eavesdropping on RFID
  - taking photos of metal key
    http://www.flir.se/

Something you have

Secure object: Yubikey

- Connects as a USB keyboard or via NFC
- Issues one-time passwords
- Contains secret AES key used to encrypt a counter
- The AES key cannot be retrieved, so the key cannot be copied
- Slightly better security than a physical, ordinary key

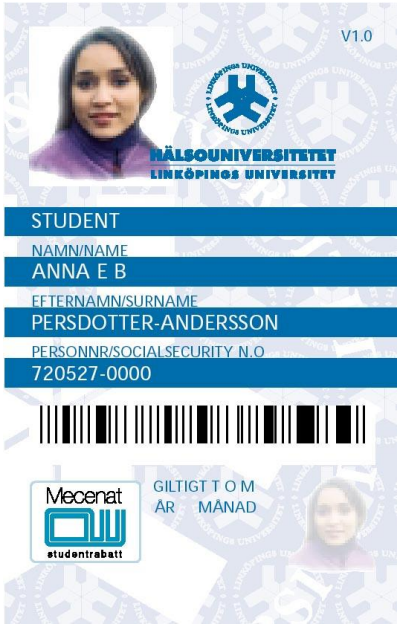
Something you have

Other secure objects

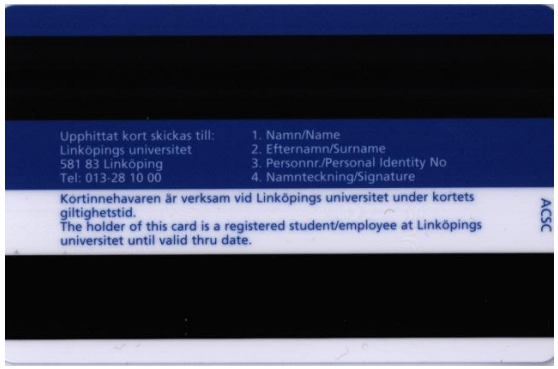
- Modern car keys
- Passports
- Credit cards
- Mobile phone SIM
- Mobile BankID
- Identity cards
- Smart card
- Bank identification device (“bankdosa”)

LiU-card

The beginning:



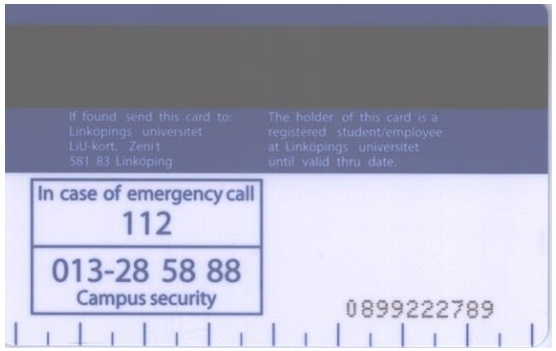
LiU-card


Upphittat kort skickas till:
Linköpings universitet
581 83 Linköping
Tel: 013-28 10 00
1. Namn/Name
2. Efternamn/Surname
3. Personnr./Personal Identity No
4. Namnteckning/Signature
Kortinnehavaren är verksam vid Linköpings universitet under kortets giltighetstid.
The holder of this card is a registered student/employee at Linköpings universitet until valid thru date.
ACSC


LINKÖPINGS UNIVERSITET
v 2.0
STUDENT
FÖRNAMN
EFTERNAMN
801122-3344
Mecenat
studentrabatt
GILTIGT T O M
VALID THRU
Å/Y M/M
04 02
© LiU-kort


1 FÖRNAMN
2 EFTERNAMN
3 801122-3344
ANSTÄLLD
LiU
TFK
05 02
© LiU-kort

LiU-card


If found send this card to:
Linköpings universitet
LiU-kort, Zenit
581 83 Linköping
The holder of this card is a registered student/employee at Linköpings universitet until valid thru date.
In case of emergency call
112
013-28 58 88
Campus security
0899222789


LINKÖPINGS UNIVERSITET
v 4.0
STUDENT
FÖRNAMN
EFTERNAMN
801122-3344
9752249611111
VALID THRU
Year/Month
0702
LinTek
Mecenat


LINKÖPINGS UNIVERSITET
v 4.0
ANNA
SVENSSON
801122-3344
STUDENT HU
9752249600002

LiU-card


LINKÖPINGS UNIVERSITET
STUDENT
LINNEA
BOHR
930124-1620
VALID THRU
YEAR/MONTH
17/02
Mecenat
SJ

Two-factor authentication 2FA

- Today, secure applications are moving to two-factor authentication
- All online banks today use this
- Also, ranked computer games, online Bitcoin wallets, hospital systems (SITHS-card), etc.
- Often password + a device
- Gives some protection against phishing and simple password capture
- Still vulnerable to man-in-the-middle attacks

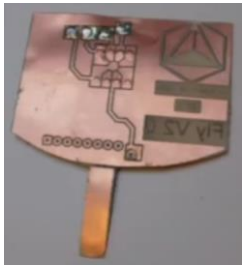
Two-factor authentication 2FA

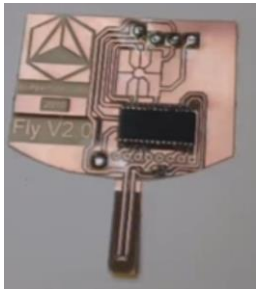
- Today, secure applications are moving to two-factor authentication
- All online banks today use this
- Also, ranked computer games, online B… wallets, hospital systems (SITHS …
- Often pass… device
- G… some protection against phishing and simple password capture
- Still vulnerable to **man-in-the-middle** attacks

Bruce Schneier, 2005: "Too Little, Too Late"

Ways for an attacker to obtain a PIN

Example EMV and PIN broken





DEFCON 19: Chip & PIN is Definitely Broken
https://youtu.be/6lI56XXeV8g
https://dev.inversepath.com/download/emv/emv_2011.pdf

Ingo Hölscher

IT-avdelningen APP

www.liu.se

LINKÖPINGS UNIVERSITET