Hochschule Konstanz
Fakultät Informatik

Introduction to IT Security

WIN+AIN

Hanno Langweg

03 Authentication

Authentication

- Access control = **authentication** + authorisation
- Identification: **claiming** an identity
- Authentication: **verifying** claimed identity
- Initial/repeated authentication
- Based on
  - something you know (e.g. PIN/password)
  - something you have (e.g. physical token)
  - something you are/do (biometrics)
- Differentiate: human to machine, machine to machine (➔ network security)

Something you know

- Username and password
  - Used for entity authentication
  - Entity authentication vs. message authentication
- Password is shared secret between user and computer system
  - Limits: human memory and password input

Attacks against passwords

- **Intercept** password when new account is created
- **Guess** password
- Obtain from user by **phishing**, **spoofing**, **keylogging**
- Obtain from system by reading password file or by **social engineering**

Sniffing and key loggers

- **Password sniffing on the local network** used to be a major problem; mostly solved by cryptographic authentication:
  - SSH, SSL, HTTP Digest Authentication, MS-CHAPv2
- **Key logger**: software or hardware that stores all key strokes typed on a computer
  - Used to be a problem in public-access computers e.g. at libraries and cafes
  - Now can be **malware** on any computer
  - Why do some bank web sites ask you to use the mouse to enter the PIN code?

http://www.keelog.com/hardware-keylogger/

Schritt 1 von 5: Anmelden am Wahlsystem

Willkommen bei der Präsidiumswahl 2014 der Gesellschaft für Informatik e.V. (GI)

Bitte geben Sie GI-Mitgliedsnummer und Wahl-PIN (unter dem Rubbelfeld im Wahlschreiben) ein. Nutzen Sie dazu das Tastenfeld oder über den Button "Anmeldung über Tastatur" Ihre Tastatur.

GI-Mitgliedsnummer:

Wahl-PIN:

Password recovery

- Humans prone to forget things ➔ need a process to **recover from password loss**
- Recovery mechanisms often enable new attacks
- *What are the advantages and disadvantages of the following recovery mechanisms?*
  - Security question or memorable secret, e.g. birth place, mother's maiden name, pet's name
  - Emailing password to another user account
  - Physical visit to helpdesk
  - Yellow sticker on the back of the keyboard
  - USB memory stick with a password recovery file

Password reuse

- How many different user accounts and passwords do you have? ***Ever used the same password on two accounts?***
- Using the same or related passwords on multiple accounts means that one **compromised system or account** can lead to compromise of other accounts

Password reuse

- Administrative countermeasures:
  - Passwords chosen by service, not set by users
  - Exotic password format requirements
  - Single sign-on to enable just one password
- Personal countermeasures:
  - Generating service-specific passwords from one master password
  - Password wallet (e.g. on phone) encrypted with a master password

12. Passwort

Zur Erstregistrierung benutzen Sie Ihre Kreditkartennummer und das Passwort, das Ihnen zugesandt wurde. Dieses Passwort ist nur einmal gültig! Aus Sicherheitsgründen müssen Sie sich sofort ein neues Passwort einrichten. Hierfür gelten die folgenden Regeln:
Das neue Passwort muss zwischen sieben und zehn Zeichen umfassen und mindestens eine Ziffer und einen Buchstaben enthalten (z.B. az39kpx). Das neue Passwort darf nicht einem der letzten vorherigen Passworte entsprechen (Passwort-History). Sonder- und Leerzeichen sowie Buchstaben ä, ö, ü und ß sind nicht zugelassen. Bitte beachten Sie, dass eine Unterscheidung zwischen Groß- und Kleinbuchstaben erfolgt, d.h. "Wort" ist nicht gleich "wort". Geben Sie bitte zuerst das alte und dann zweimal das neue Passwort ein. Mit <ändern> geben Sie die Änderung frei. Die erfolgreiche Änderung Ihres Passwortes wird Ihnen sofort am Bildschirm angezeigt.

Sofern Sie über ein Kreditkarten-Doppel verfügen, gilt ein Passwort für beide Karten. Sie sollten sicherheitshalber Ihr Passwort regelmäßig ändern. Wählen Sie hierzu aus dem Menü auf der linken Bildschirmseite den Punkt "Passwort" aus. Verfahren Sie wie zuvor beschrieben.

kreditkartenbanking.de,
HTWG,
Uni Duisburg-Essen

Das Passwort sollte aus Buchstaben und Ziffern bestehen. Bei Passwörtern ist die Groß- und Kleinschreibung zu beachten.
Das Passwort muss mindestens 8 Zeichen lang sein.

Tipps für ein sicheres Passwort

Das Passwort muss mindestens 8 und höchstens 12 Zeichen umfassen.

- Es sollte mindestens 2 Sonderzeichen, eine Zahl, einen Kleinbuchstaben und einen Großbuchstaben enthalten.
- Für das Passwort sind folgende Zeichen erlaubt:
  Kleinbuchstaben (a - z)
  Großbuchstaben (A - Z)
  Ziffern (0 - 9)
  die Sonderzeichen ( ) [ ] { } ? ! $ % & / = * + ~ , . ; : < > - _

Goal: High number of possible passwords

- Examples:
  - Random 4 digits PIN: 10^4
  - Random 10 characters alphanumeric passwords: $(26+26+10)^{10} = 839,299,365,868,340,224 \approx 8 \times 10^{17}$
  - Passphrase with 5 words:
    $(250,000)^5 \approx 9 \times 10^{26}$
    $(5,000)^5 \approx 3 \times 10^{18}$ – individual vocabulary in active use could be just several thousand words

The Second Edition of the 20-volume *Oxford English Dictionary* contains full entries for 171,476 words in current use, and 47,156 obsolete words. To this may be added around 9,500 derivative words included as subentries. Over half of these words are nouns, about a quarter adjectives, and about a seventh verbs; the rest is made up of exclamations, conjunctions, prepositions, suffixes, etc. And these figures don't take account of entries with senses for different word classes (such as noun and adjective).

https://en.oxforddictionaries.com/explore/how-many-words-are-there-in-the-english-language

  - Problem: are passwords chosen at random, i.e., do all passwords have the same probability of being chosen?

Length beats alphabet size

- Longer passwords better than complicated ones
  (Long complicated passwords better than only long passwords)
- Size >2^{100} recommended for password space
  BSI TR-02102 "Cryptographic mechanisms: recommendations and key lengths"
- $2^{100} \approx 10^{30}$
  - 30 digit PIN chosen from [0..9]
  - 21 character password chosen from [A..Z]
  - 17 character password chosen from [A..Za..z0..9]

Schneier on Security

← Another Failed Copy-Protection System

Security Alert Humor →

Write Down Your Password

Microsoft's Jesper Johansson urged people to write down their passwords.

This is good advice, and I've been saying it for years.

Simply, people can no longer remember passwords good enough to reliably defend against dictionary attacks, and are much more secure if they choose a password too complicated to remember and then write it down. We're all good at securing small pieces of paper. I recommend that people write their passwords down on a small piece of paper, and keep it with their other valuable small pieces of paper: in their wallet.

https://www.schneier.com/blog/archives/2005/06/write_down_your.html

Password guessing

- **Dictionary attack** and other intelligent guessing vs. **brute force** trials
- Countermeasures against guessing
  - Limit the number or rate of login attempts
  - Minimum password length and complexity, password quality check
  - Preventing reuse of old passwords
  - System-generated random passwords
  - Password aging, i.e. mandatory periodic password changes (e.g. several times a year)

Dictionary

https://github.com/danielmiessler/SecLists/blob/master/Passwords/darkweb2017-top10000.txt

1. 123456
2. 123456789
3. 111111
4. password
5. qwerty
6. abc123
7. 12345678
8. password1
9. 1234567
10. 123123

Distribution: Top 10 14%, top 100 40%, top 1,000 91%

Brute force

- http://project-rainbowcrack.com/table.htm

SHA1 Rainbow Tables

Table ID	Charset	Plaintext Length	Key Space	Success Rate	Table Size
sha1_ascii-32-95#1-7	ascii-32-95	1 to 7	70,576,641,626,495	99.9 %	64 GB
sha1_ascii-32-95#1-8	ascii-32-95	1 to 8	6,704,780,954,517,120	96.8 %	576 GB
sha1_mixalpha-numeric#1-8	mixalpha-numeric	1 to 8	221,919,451,578,090	99.9 %	160 GB
sha1_mixalpha-numeric#1-9	mixalpha-numeric	1 to 9	13,759,005,997,841,642	96.8 %	864 GB
sha1_loweralpha-numeric#1-9	loweralpha-numeric	1 to 9	104,461,669,716,084	99.9 %	80 GB
sha1_loweralpha-numeric#1-10	loweralpha-numeric	1 to 10	3,760,620,109,779,060	96.8 %	396 GB

Offline/online guessing attacks

- **Offline attack:** cracking the password from a known hash (or other function) of the password
  - E.g. MS-CHAPv2 or HTTP digest authentication without SSL
  - Unlimited number of guesses ➔ **attacker can perform an exhaustive brute force search**
- **Online guessing:** attacker tries to login many times
  - E.g. PIN entry on a phone
  - E.g. network login to an authenticated server over SSH or SSL
  - System can **limit the number or rate of guesses**

Offline vs. online guessing

- Big difference in the required password strength:
  - **Online** guessing success probability
    ≈ number of allowed guesses / number of possible passwords
  - **Offline** attack requires **cryptographic strength** from the password, e.g. 128-bit entropy, to prevent exhaustive search

Storing passwords on server

- Assume that password database becomes **public**
  - Attackers often manage to read files or database tables on a web server e.g. with SQL injection
- How to store passwords in a public file?
  - Store a hash i.e. one-way function of the password; when user enters a password, hash and compare
  - Use a **slow hash** (many iterations of a hash function)
  - Include random account-specific "**salt**":
    `slow_hash( password | salt)`
    to prevent **simultaneous brute force cracking** of many passwords, **pre-computation** attacks, and **equality comparison** between passwords

Other threats

- No system is perfectly secure:
  system designers have a specific threat model in mind, but the attacker can break these rules
- Some other attacks against PINs and passwords:
  - Phishing and social engineering
  - User mistakes: using wrong password
  - Camera to record key presses
  - Heat camera to detect pressed keys
  - Acoustic emanations from the keyboard
  - etc.

Physical security tokens

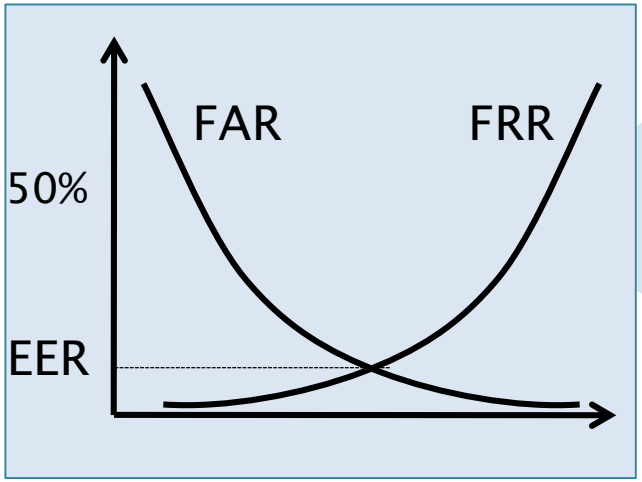
- Smart card is a typical physical security token
  - Holds **cryptographic keys** to prove its identity
  - **Tamperproof:** secret keys will stay inside
- Used for door keys, computer login, ATM
- Other security token implementations: smart button, USB dongle, mobile phone
- **Two factor authentication:** require also PIN
  - Attacker needs to both steal the card and learn the PIN
    ➔ clear qualitative increase in security

Issues with security tokens

- Physical tokens require **distribution**
- Computers (or doors etc.) must have **readers**
- It is not easy to integrate cryptographic tokens to all systems
  - E.g. how to use a physical token if the application requires cached credentials (password) on the client or on a proxy server
- Process needed for **recovering** from the loss of tokens
- Are smart card + PIN really two factors?

Biometric authentication

- Biometric authentication means verifying some physical feature of the user
  - **Physiological** characteristic: picture, signature, face geometry, fingerprint, iris scan, DNA
  - **Behavioural** characteristic: voice, typing, gait
- Biometrics are **not 100% reliable**:
  - **False acceptance** rate FAR
  - **False rejection** rate FRR
  - Equal error rate EER



Issues with biometrics

- Biometrics require **enrollment** and **readers**
- Big difference in the security of **unsupervised** vs. **supervised** readers
  - E.g. fingerprint reader on computer vs. iris scanner at immigration check point
- Suitability for security architectures:
  - Are biometric characteristics secrets?
  - Can they be copied?
  - How to revoke biometrics?
- What if enrollment fails?
  - Some people have no fingerprints, or no fingers

Summary

- Something you know, e.g. PIN/password
  - Widely used, well-researched, integration support
  - In practice often not randomly chosen
- Something you have, e.g. token, smart card, phone
  - Widely used, well-researched
  - Cost of integration
- Something you are/do, e.g. fingerprint
  - Ease of use, cannot forget, cannot lose/misplace
  - Accuracy, false match/non-match
  - System integration, enrolment failures, privacy
- Multi-factor authentication combines different methods