Cyber Security

Part II

Authentication & Authorization

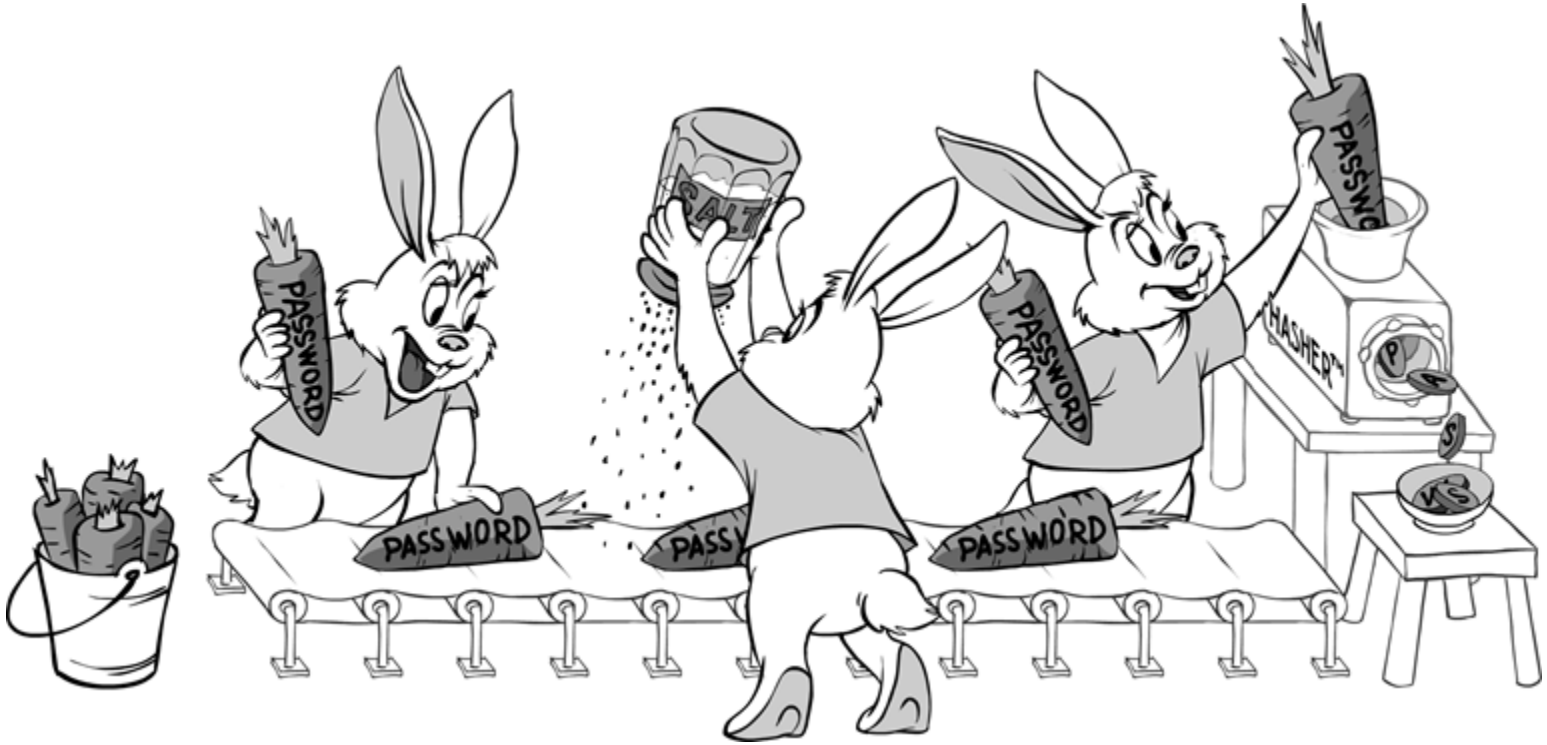
PASSWORDS – FIRST LINE OF DEFENSE

https://www.youtube.com/watch?v=hEMHG13t3YI

Cryptography and it's Significance in security

Hashing

Passwords are usually stored in a hashed format due to the security provided by its one-way-ness. However, even though it isn't possible to reverse the hash process directly, it's possible to reverse-engineer a hash.



Source: [04/01/2019] https://accu.org/index.php/journals/2159

Cryptography and it's Significance in security

Hashing

Characteristics of a hash function are as under:

1. It must be one-way. This means that it is not reversible. Once you hash something, you cannot un-hash it.

2. Variable-length input produces fixed-length output. This means that whether you hash two characters or two million, the hash size is the same.

3. The algorithm must have few or no collisions. This means that hashing two different inputs does not give the same output.

Cryptography and it's Significance in security

Digital Signatures

A digital signature is an electronic mechanism to prove that a message was sent from a specific user (that is, it provides for non-repudiation) and that the message wasn't changed while in transit (it also provides integrity).

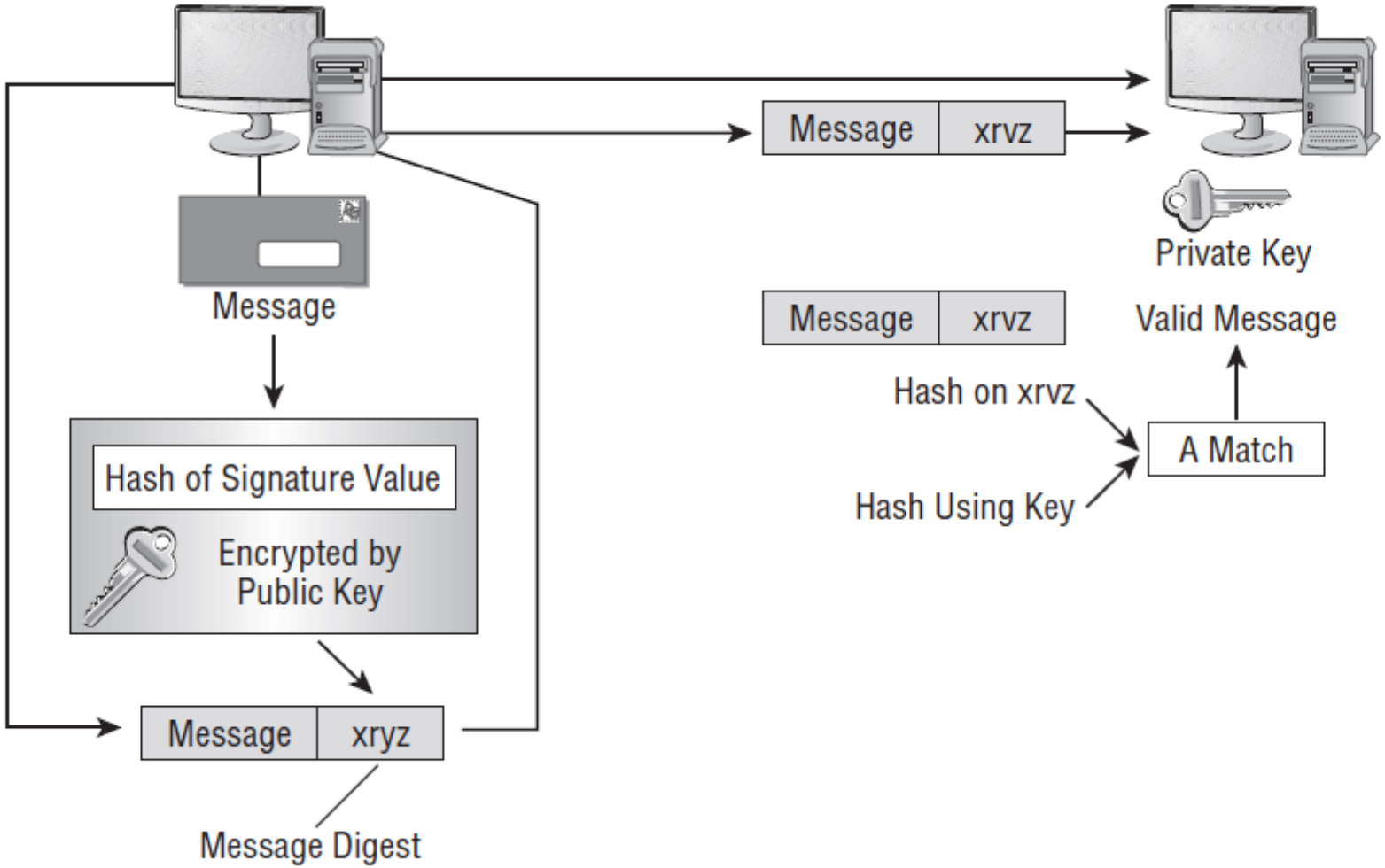
Digital signatures operate using a hashing algorithm and either a symmetric or an asymmetric encryption solution.

The message is encrypted using the encryption system, and a second piece of information, the digital signature, is added to the message.

Most digital signature implementations also use a hash to verify that the message has not been altered, intentionally or accidently, in transit.

Cryptography and it's Significance in security

Digital Signatures



Source: Emmett Dulaney, Chuck Easttom (2014), *CompTIA® Security+™ Study Guide*, Sixth Edition, John Wiley & Sons

Cryptography and it's Significance in security

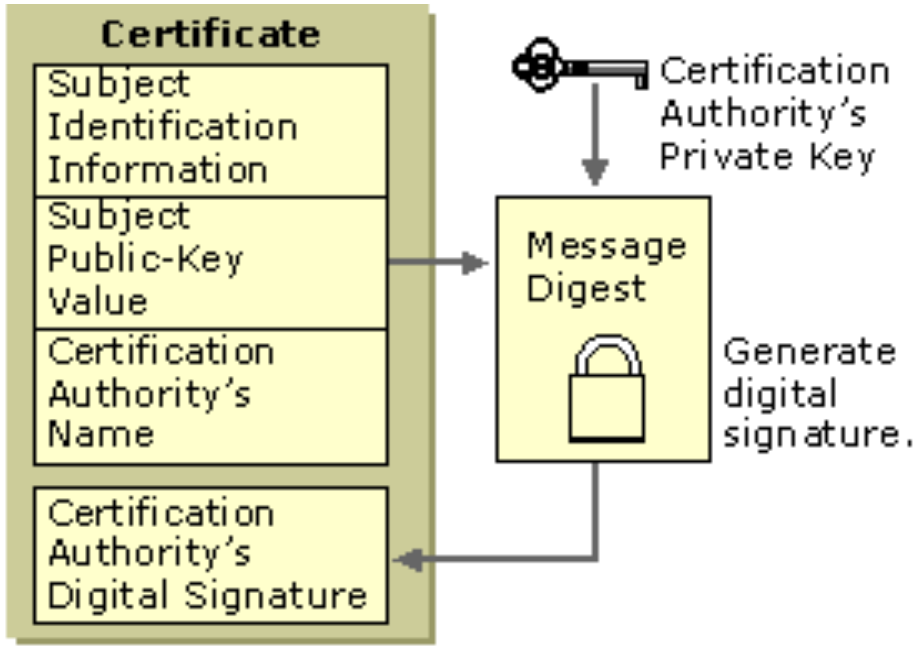
Digital Certificates

A certificate is nothing more than a mechanism that associates the public key with an individual.

Digital certificates serve a single purpose: proving the identity of a user or the source of an object.

They don't provide proof as to the reliability or quality of the object or service to which they're attached; they only provide proof of where that product or service originated.

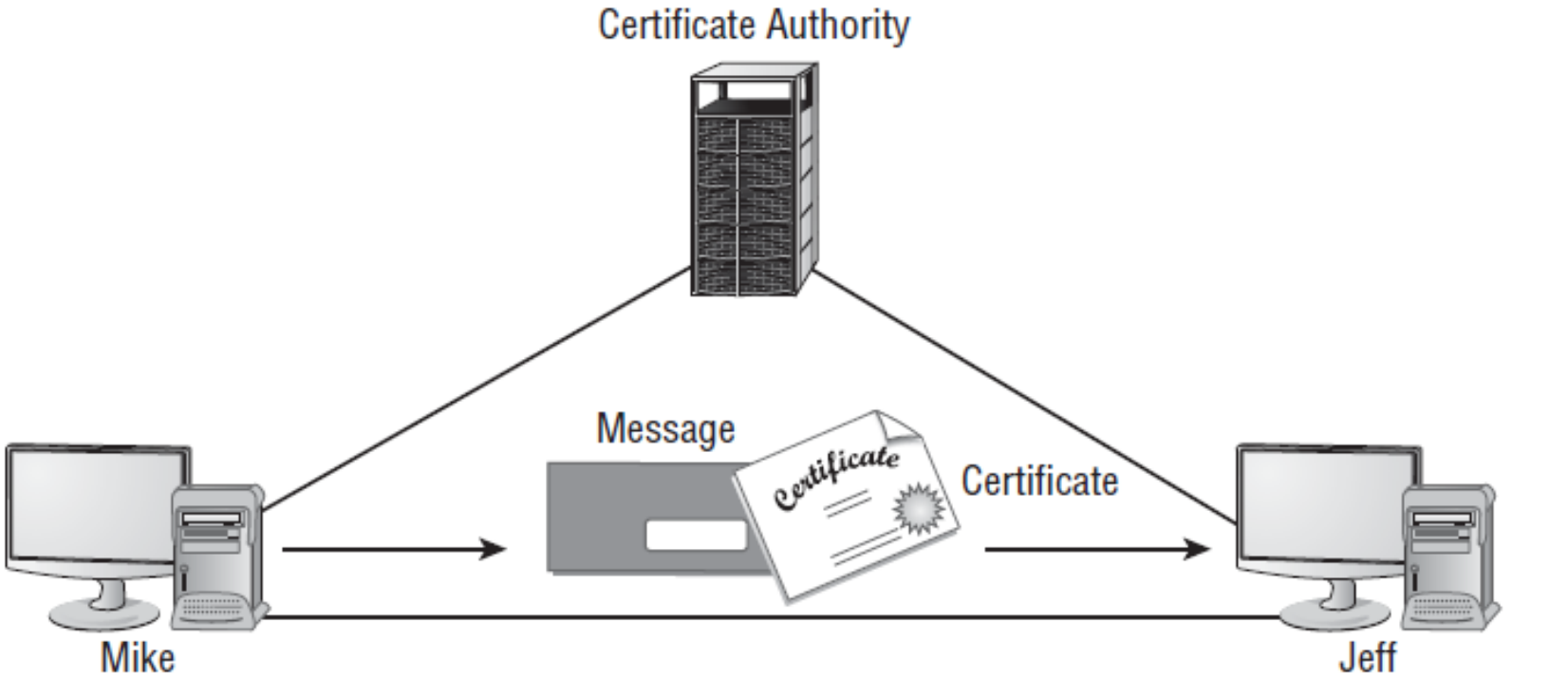
Certificates work under a theory known as the trusted third party. This theory states that if user A trusts user C and user B trusts user C, then user A can trust B and vice versa.



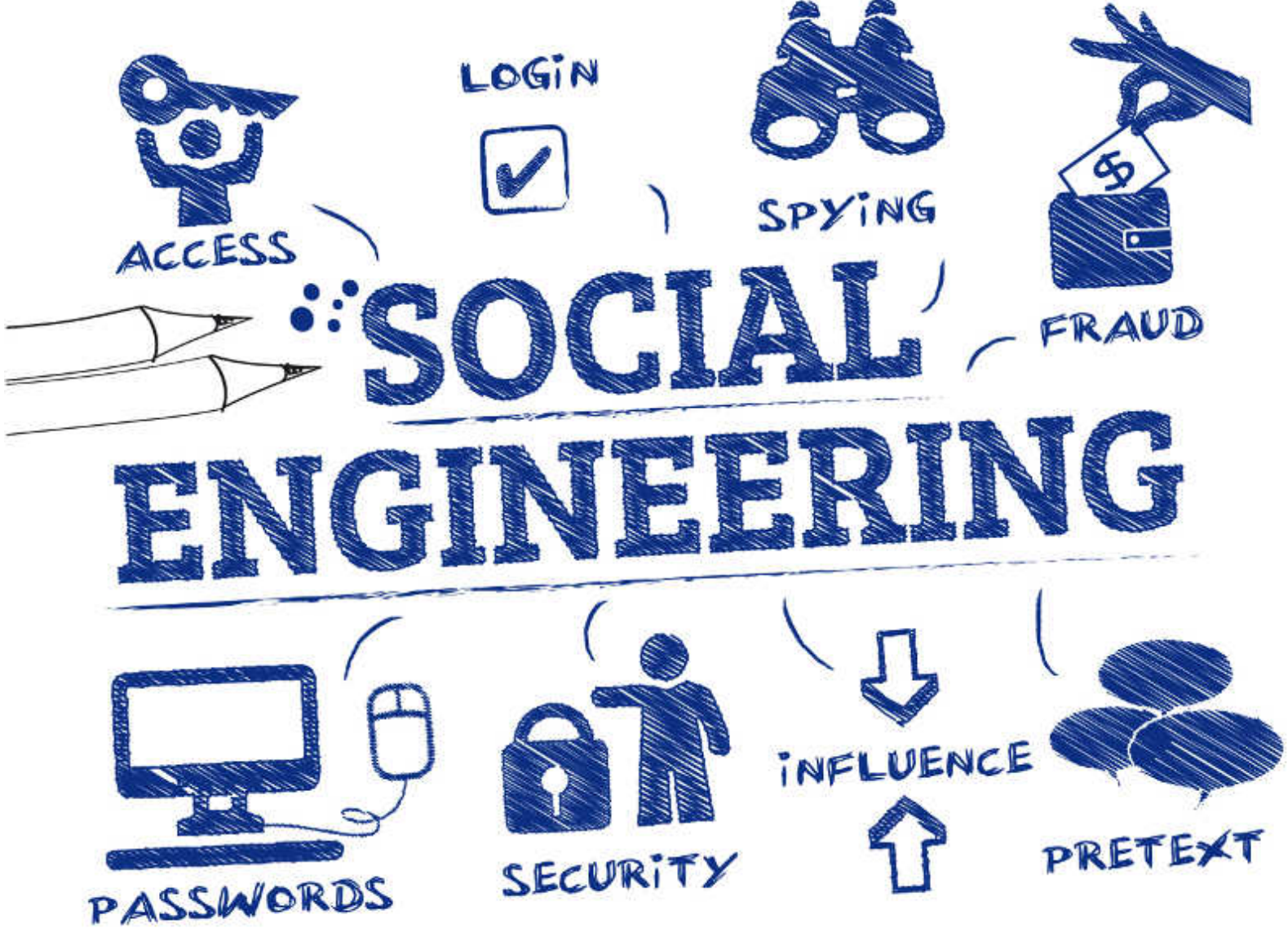
Source: [14/04/2018] https://technet.microsoft.com/en-us/library/cc962029.aspx

Cryptography and it's Significance in security

Digital Certificates

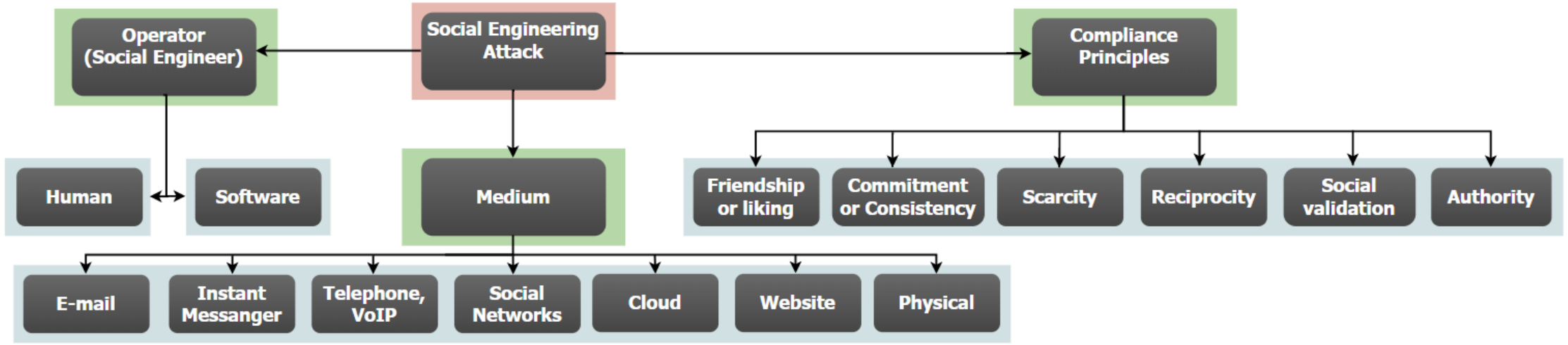


Source: James Michael Stewart (2014), *CompTIA® Security+™ Review Guide*, John Wiley & Sons



***Definition:** Social Engineering is a combination of social, psychological and information gather techniques that are used to manipulate people to gain access to information or locations that the hacker is not authorized to access*

Social Engineering Taxonomy



Attack Vectors

Dumpster Diving | Advanced Persistent Threat | Baiting | Tailgating | Surfing Online Content | Pretexting | Vishing

Phishing | Shoulder Surfing | Reverse Social Engineering | Waterholing | Trojan Horse | Role Playing | Quid Pro Quo

Effects of Social Engineering

Social engineering has serious consequences. Because the objective of social engineering is to coerce someone to provide information that leads to ill-gotten gains, anything is possible

- User passwords.
- Security badges or keys to the building and even to the computer room.
- Intellectual property such as design specifications, source code, and other research-and-development documentation.
- Confidential financial reports.
- Private and confidential employee information.
- Personally identifiable information (PII) such as health records and credit card information.
- Customer lists and sales prospects.

Types of Social Engineering Attacks

Phishing

It is an attempt to acquire sensitive information by masquerading as a trustworthy entity via an electronic communication, usually an email. Such attacks rely on a mix of technical deceit and social engineering practices.

Vishing

Attackers directly involve in a digital conversation to gather information using voice solicitation techniques and digital messaging techniques

Impersonation

Attacker identify a way to enter into your facility like a courier delivery executive or tech staff to check internet connectivity etc. to gather valuable information of organisation

Top 10 Phishing Attack Emails

1. Security Alert – 21%
2. Revised Vacation & Sick Time Policy – 14%
3. UPS Label Delivery 1ZBE312TNY00015011 – 10%
4. BREAKING: United Airlines Passenger Dies from Brain Hemorrhage – VIDEO – 10%
5. A Delivery Attempt was made – 10%
6. All Employees: Update your Healthcare Info – 9%
7. Change of Password Required Immediately – 8%
8. Password Check Required Immediately – 7%
9. Unusual sign-in activity – 6%
10. Urgent Action Required – 6%

Phishing Types

Spear Phishing - Attackers use focuses on specific individuals correlating information found on social media and elsewhere to initiate a pointed attack

Whaling - Attacker concentrate on high value individuals, generally senior management staff of an organisation following spear phishing technique to infiltrate and steal valuable organisation data

Pre-texting – Attacker pretend to be the victim and call organisation helpdesk to gather information or penetrate by asking the IT helpdesk executive to click a link to take control of organisation system and escalate privileges

Vishing Types

Phone Vishing: Attacker directly calling an individual or a group attempting to gain access to account information to penetrate and modify confidential information of an organization

SMSishing: Attacker uses a text or an image or a web link to gain information to victim's digital device to steal valuable personal and organization information

Sextortion

Sextortion is a widely used form of online blackmail where a cyber scammer threatens to reveal intimate images or videos of someone online

often to their friends, family, work colleagues, or social media lists

unless they pay a ransom quickly

De Logan Meyer <hbcarmitaoh@outlook.com>
Sujet **xxxx - 515549** 21/07/2018 21:11
Pour xxxx@xxx-xxxxx.xxx <xxxx@xxx-xxxxx.xxx>
Date Sat, 21 Jul 2018 19:11:59 +0000
Identifiant du message <PS2PR02MB2901ECEF5E49F76CD47263DBB0500@PS2PR02MB2901.apcprd02.prod.outlook.com>
Received from mail-oln040092255060.outbound.protection.outlook.com (HELO APC01-

I do know 515549 one of your passphrase. Lets get straight to point. Absolutely no one has paid me to investigate you. You do not know me and you are probably wondering why you are getting this email?

actually, I actually placed a malware on the adult vids (pornography) web site and do you know what, you visited this web site to experience fun (you know what I mean). When you were viewing video clips, your web browser started out working as a Remote Desktop that has a key logger which provided me accessibility to your display as well as web cam. Immediately after that, my software obtained all of your contacts from your Messenger, FB, and e-mailaccount. After that I created a double-screen video. 1st part displays the video you were watching (you've got a good taste ;)), and second part shows the recording of your web cam, & its u.

You will have 2 options. Shall we understand each of these choices in particulars:

First alternative is to ignore this message. In this case, I am going to send out your recorded material to all of your personal contacts and thus consider concerning the disgrace you feel. And as a consequence should you be in a relationship, how it will eventually affect?

Next alternative is to pay me $1000. Lets describe it as a donation. In this scenario, I will instantly erase your video. You could continue on your life like this never took place and you would never hear back again from me.

You'll make the payment through Bitcoin (if you don't know this, search "how to buy bitcoin" in Google).

BTC Address to send to: 1P6V4q85b7guyEUnAzQDEga3BL2hrVDEPP
[CASE-SENSITIVE copy and paste it]

In case you are making plans for going to the law enforcement officials, very well, this e mail cannot be traced back to me. I have dealt with my actions. I am not trying to demand so much, I simply want to be paid for. You now have one day to pay. I've a special pixel in this e-mail, and at this moment I know that you have read through this message. If I do not get the BitCoins, I will certainly send your video to all of your contacts including friends and family, colleagues, and many others. Nonetheless, if I do get paid, I'll erase the video right away. If you want proof, reply with Yea & I will certainly send your video to your 13 friends. It's a non-negotiable offer so don't waste my personal time and yours by replying to this message.

Get Rid of Sextortion

Don’t panic

Don't communicate further with the criminals

Change your password to the mail id (in case you got mail from your own id)

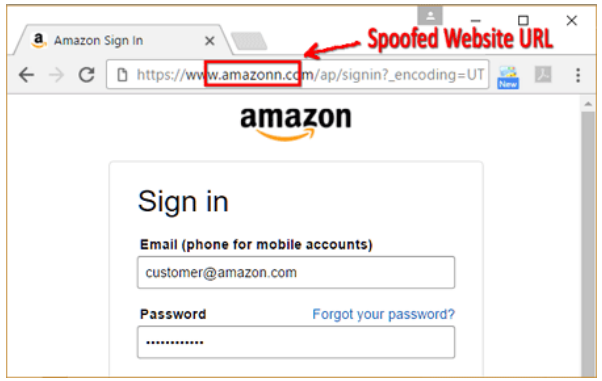
Don't pay

Preserve evidence that was used by the hacker to communicate

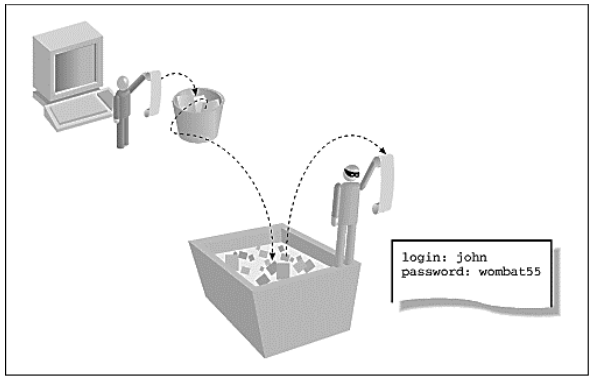
If it is repeated, give a complaint to Cyber Crime cell of Police

Social Engineering and Social Media Security

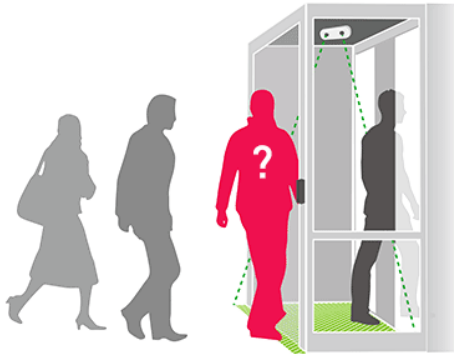
Impersonation



Pharming – Attacker redirects victims to a duplicate website, even if the user correctly entered the intended site



Dumpster Diving – Attacker search the trash of an organisation to gather deleted data in digital environment



Tailgating - Attacker used to gain access to secured areas, that typically involves following a person into an area with access restrictions.

Baiting/Quid pro quo - Attacker would make the victim to grab a digital device that has pre-installed malware to be used in organisation computers to steal information

Social Engineering and Social Media Security

Social Media Security

People accidentally or unknowingly post personally identifiable information (PII) or confidential information on the Internet.

This may include employees sharing information specific to their organizations too.

Additionally, it is also not easy to delete such information once posted on the Internet in most cases.

Source: [04/01/2019] https://www.securitymagazine.com/articles/86902-the-evolution-of-social-media-monitoring-in-corporate-security

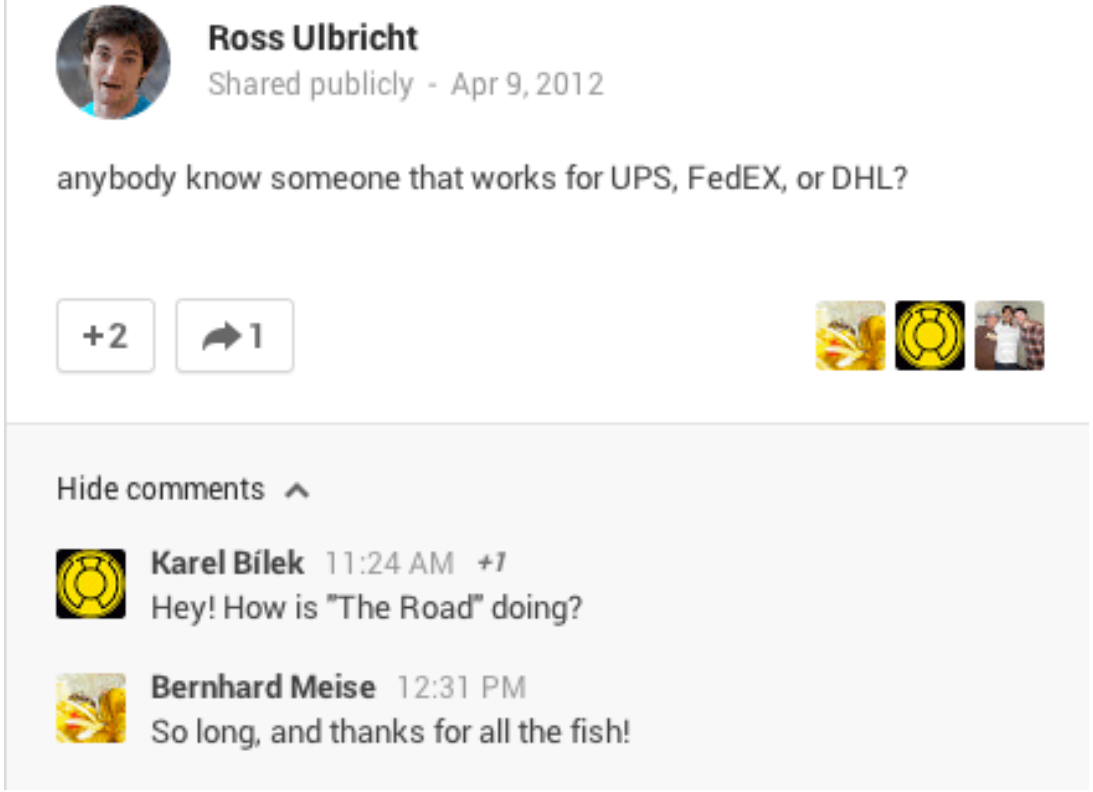
Social Engineering and Social Media Security

Social Media Security

However, this may also apply to attackers and cyber criminals, wherein they post some questions or comment on articles, which could serve as proofs for law enforcement organizations to prosecute them.

This was how “Dread Pirate Roberts”, the infamous head of Silk Road, was caught by the FBI.

First Assignment.
2 pager on Dread Pirate Roberts – case study with your own analysis on threats like this in 2020.
Submission by 10th Sep.

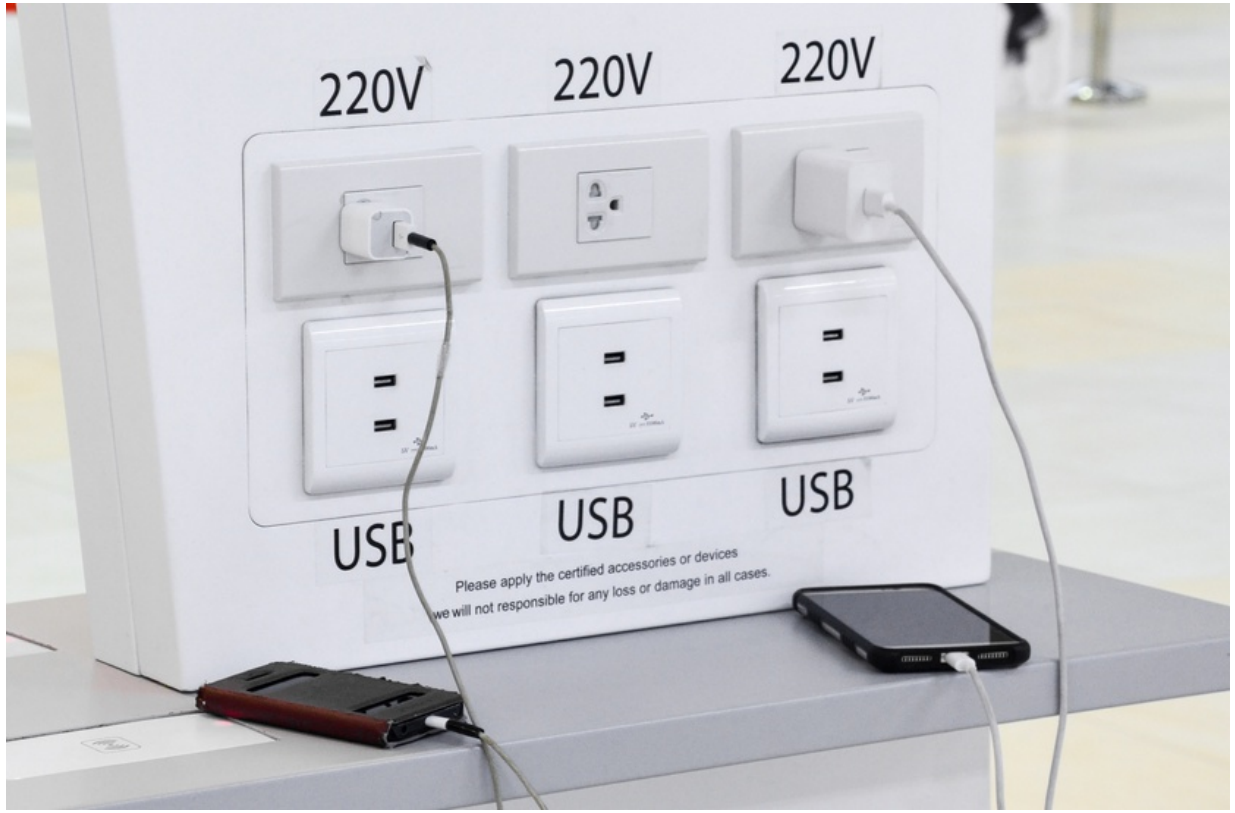


Source: [04/01/2019]
https://siliconangle.com/2013/10/02/fbi-busts-silk-road-operation-and-its-operator-dread-pirate-roberts/

Social Engineering and Social Media Security

Intelligent Hacks

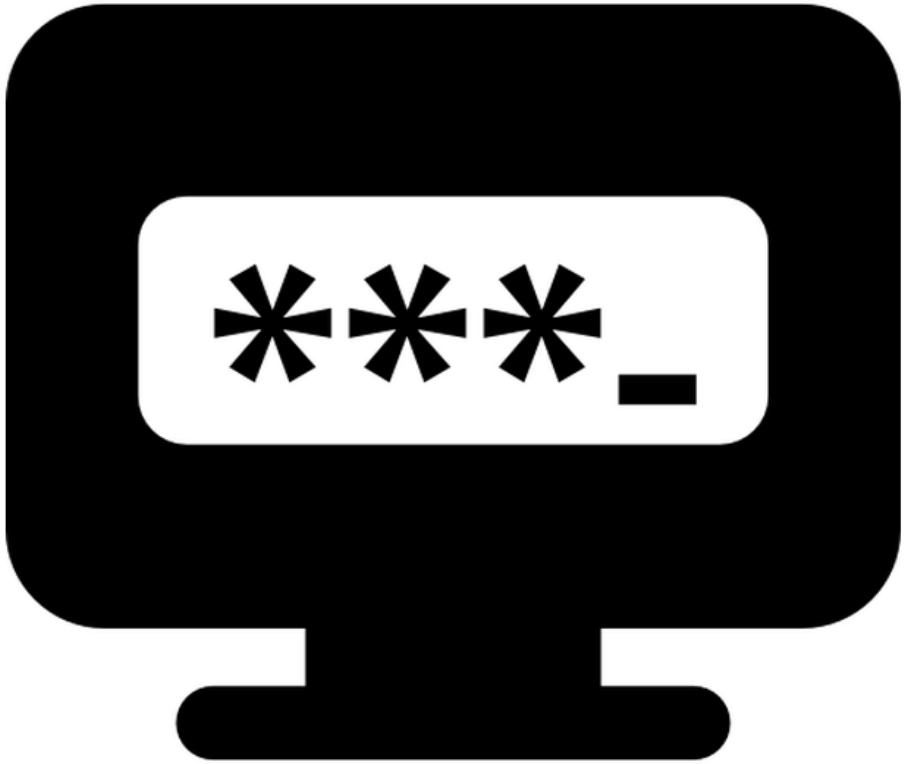
- Use data disabled charger
- Carry you own power bank
- Disable data transfer option in your phone while charging
- May be switching off is a better idea



Juice Jacking

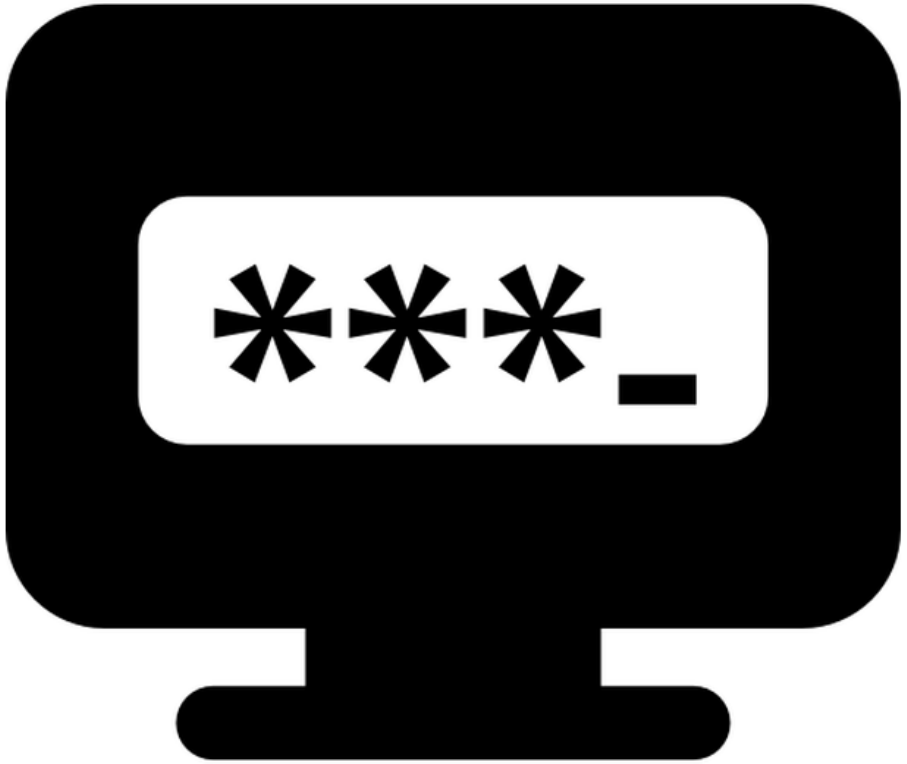
https://www.youtube.com/watch?v=ezy03Y6xbbw

How passwords work: Creation



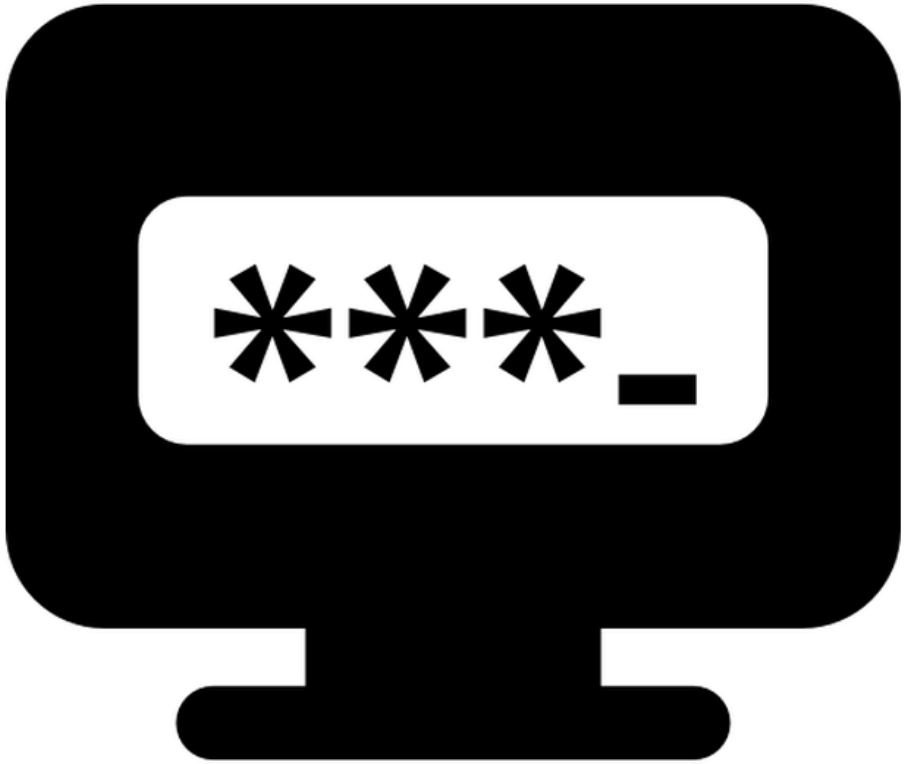
- User enters a password first time (plain text)
- System forces the password to comply with complexity rules
- Ideally password should be transmitted to the system over encrypted channels

How passwords work: Storage



- User entered password is hashed.
- Algorithms used:
  - Linux: MD5, SHA 256, Blowfish etc.
  - Windows: LM, NTLM hashing
  - Recommended: Bcrypt, Scrypt, PBKDF2

How passwords work: Comparison



- User enters a password to authenticate. System takes the password and hashes it
- Compares the hash of what the user entered against the hash stored in the password file
- If they match, allows access. Else declines.

(Watch out for error messages!)

Password Cracking

- Time needed to crack: understanding password strength.

- Mechanisms:
  - Online Brute Forcing
  - Offline Cracking: Via the obtained password hashes (John the ripper)
  - A different approach: using pre-computed hashes (Rainbow tables)

- Prevention: account lockout, captcha, two factor, salting, complex passwords

Authorization

- Authorization is a mechanism of verifying that a particular user is allowed to perform an action that user is attempting
- Does subject S have right R for object O
  - Subject: various users
  - Rights: Read, Write, Execute
  - Objects: Files, programs etc.
- In real world, this is often done as Role Based Access Control (RBAC). Various roles defined, users assigned to those roles, rights granted accordingly