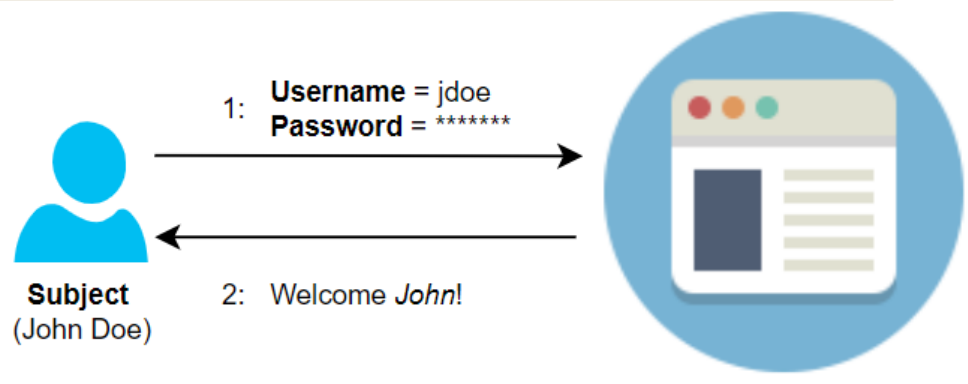
University of Stavanger

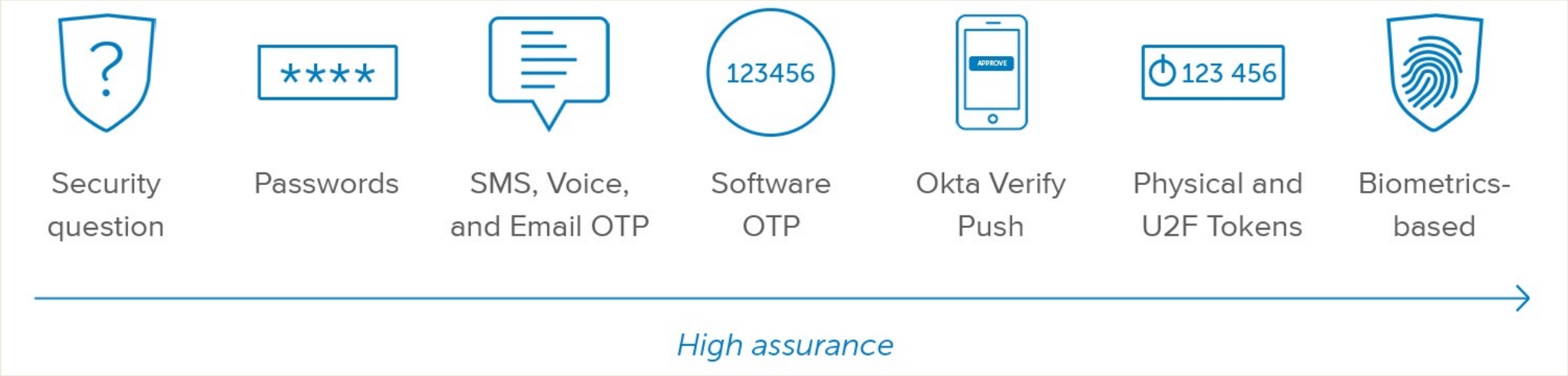
DAT250 Informasjons- og programvaresikkerhet

Broken Authentication

What is Authentication?

- the process of verifying that a user is who they claim to be.



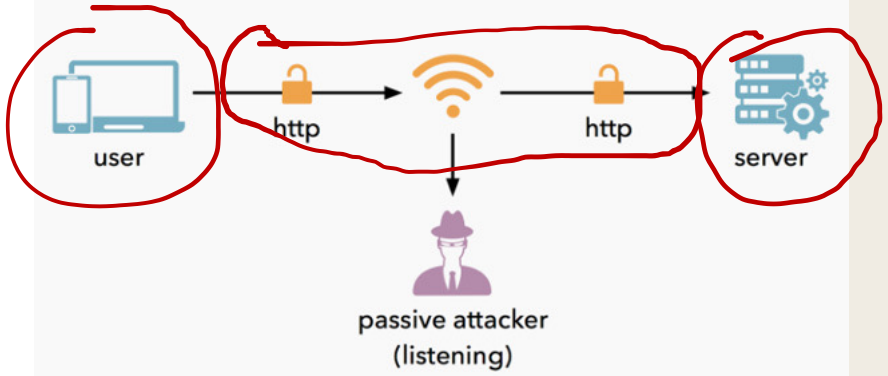


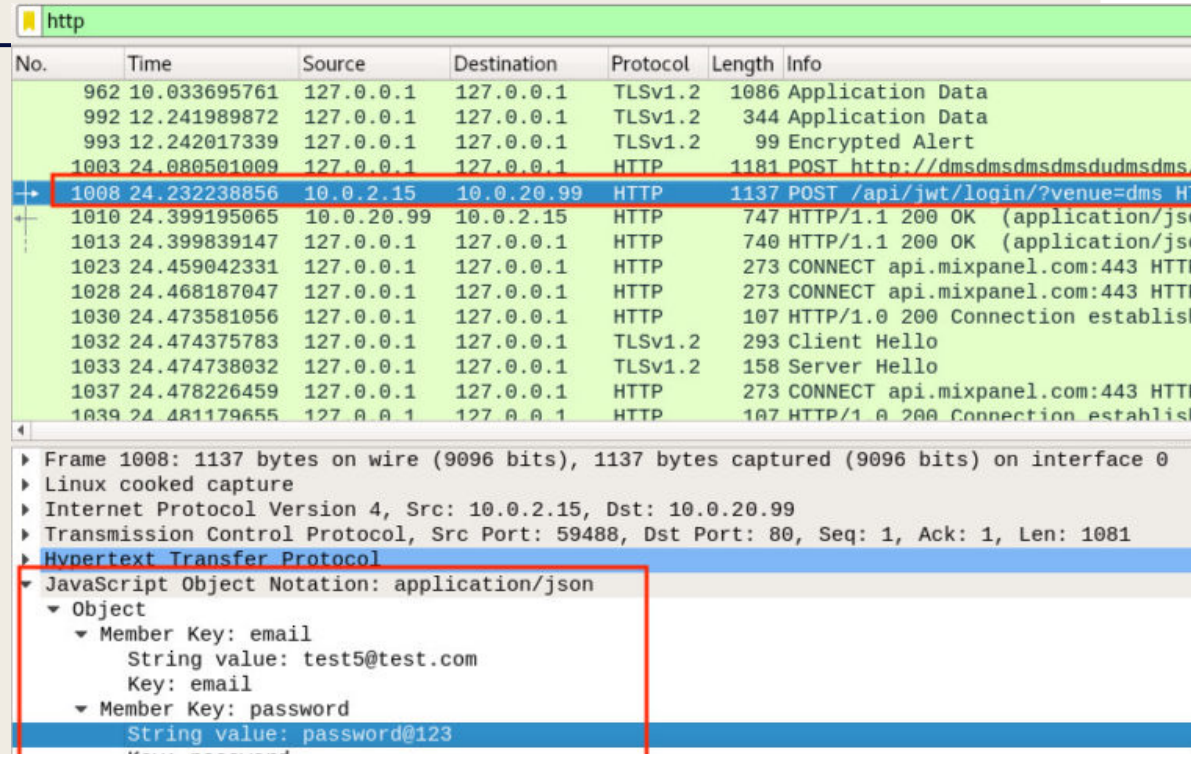
Authentication Types

- HTTP Authentication:
  - Basic:
    - prompt Username/Password
    - send it to Server in an HTTP Header
  - Digest:
    - Hash of username/password/ a nonce (a random number)
    - Server checks the hash
- Certificate-Based Authentication
  - This type uses an x.509 certificate
  - public/private key technology.
- Token-Based Authentication
  - A token, such as BankID, is a hardware device that displays an authentication code for 60 seconds;
  - a user uses this code to log into a network.
- Biometric Authentication
  - physical characteristic such as fingerprint, eye iris, or handprint to authenticate the user.

HTTP Authentication Basic - Problems

- It is simple and vulnerable
- eavesdrop on the communication can capture everything over this channel, including passwords.
- Don’t use it in your apps



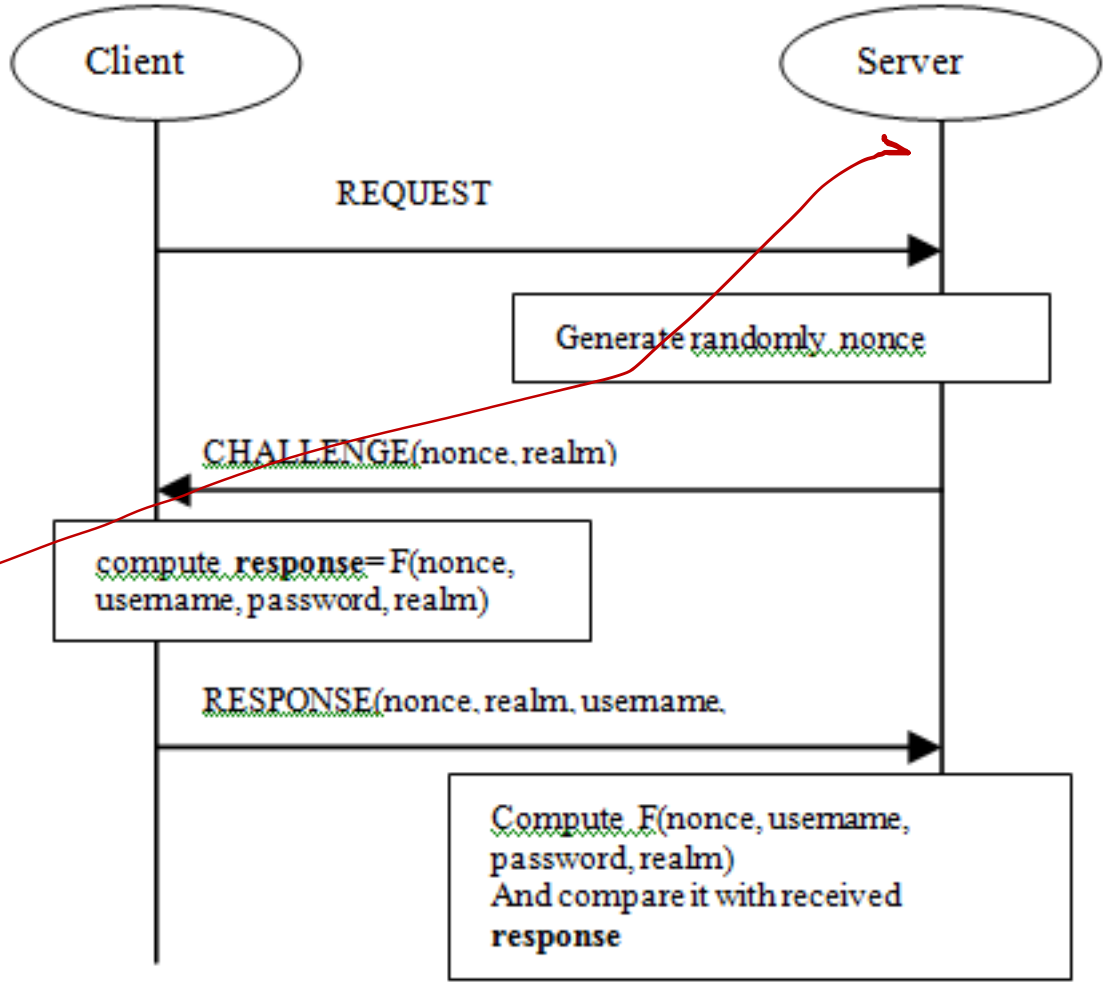


Syntax of basic Authentication

```
Value = username:password
Encoded Value =  base64(Value)
Authorization Value = Basic <Encoded Value>
//at last Authorization key/value map added to http header as follows
Authorization: <Authorization Value>
```

HTTP Authentication Digest

- Still vulnerable for the Man In The Middle Attack
- HTTP Digest prevents use of the strong password encryption, meaning the passwords stored on the server could be hacked



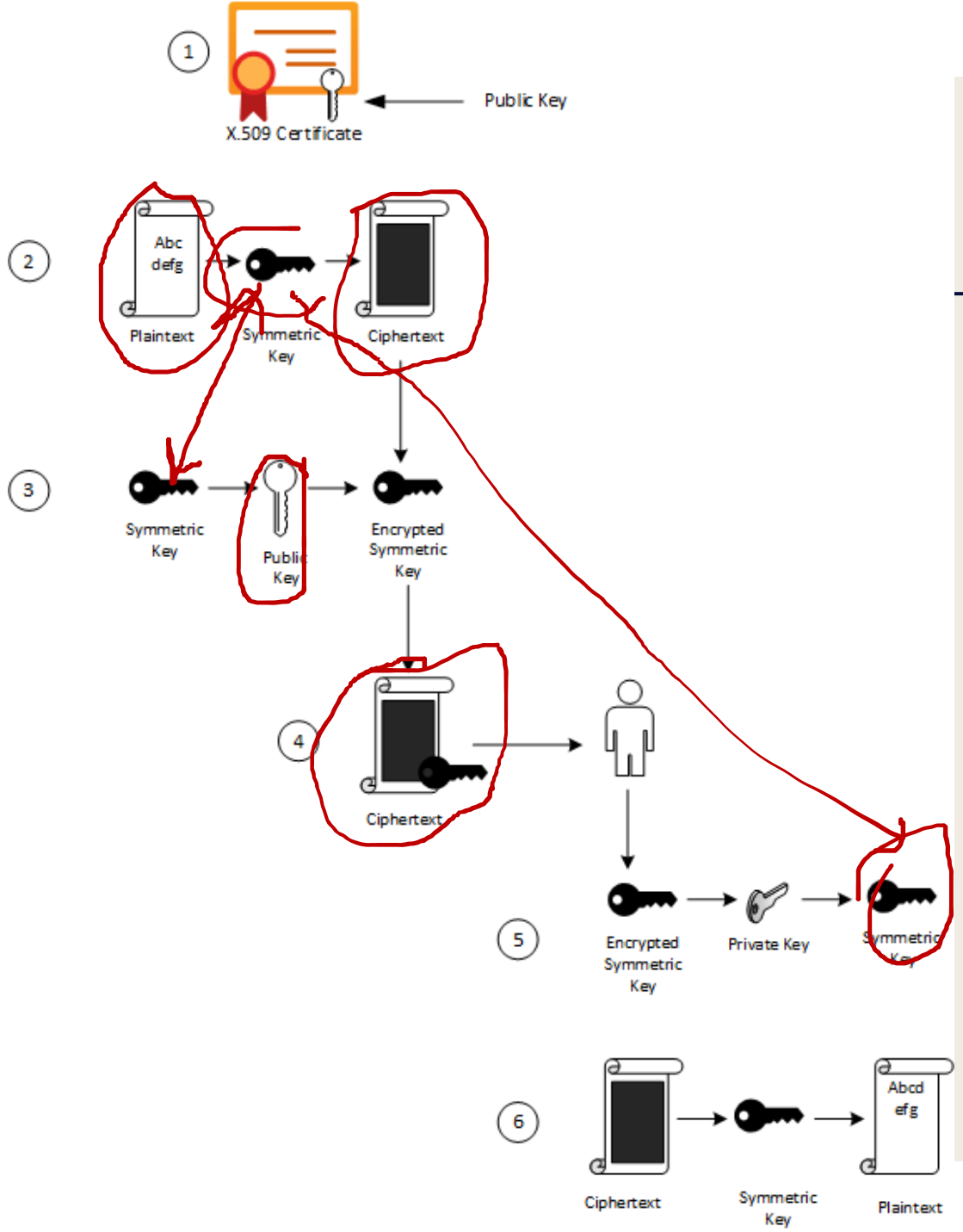
RFC 2069 Digest Access Authentication Syntax

```
Hash1=MD5(username:realm:password)
Hash2=MD5(method:digestURI)
response=MD5(Hash1:nonce:Hash2)
```

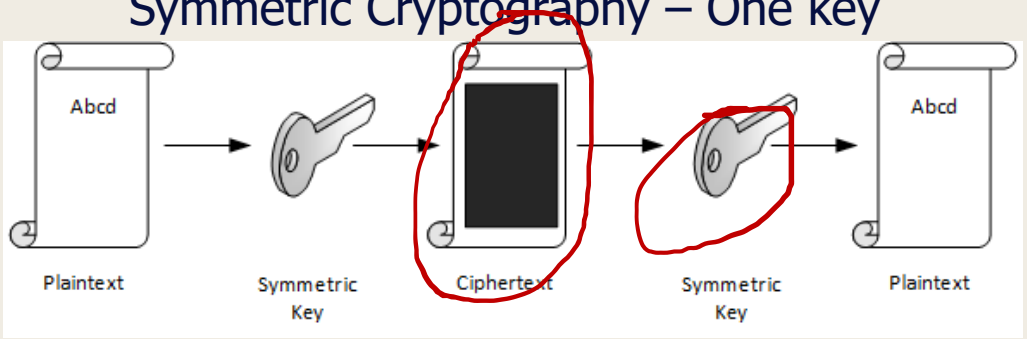
Certificate-Based Authentication

- Uses digital certificates to verify the identity of a user or device.
- A digital certificate is a file: information about the user or device
  - Name
  - Email
  - Public key
- Certificate Authority (CA):
  - A certificated is signed by a trusted authority
  - verify that the information in the certificate is accurate.

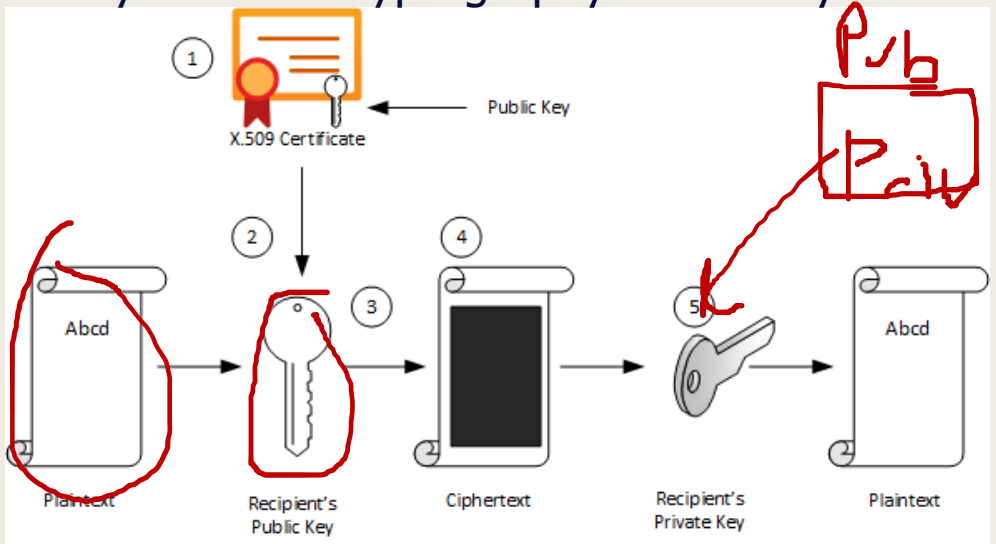
Certificate-Based Authentication



Symmetric Cryptography – One key



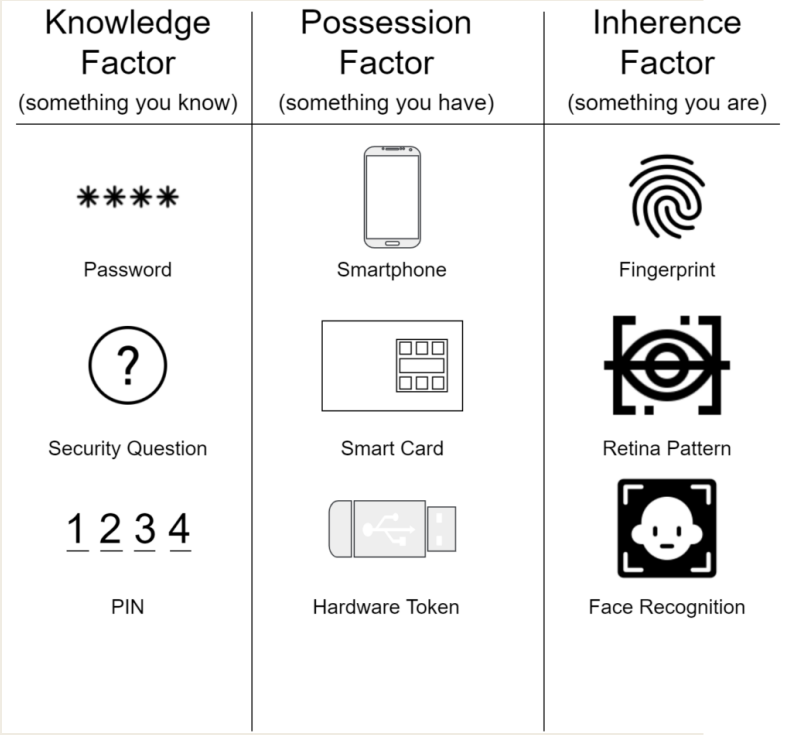
Asymmetric Cryptography – Two keys



https://docs.microsoft.com/en-us/azure/iot-hub/tutorial-x509-introduction

Authentication Factors

- **Something you know:** a password, a PIN, or a pattern.
- **Something you have:** a physical token like a key, or a virtual token like a one-time code from a hardware device.
- **Something you are:** a biometric like a fingerprint or iris.

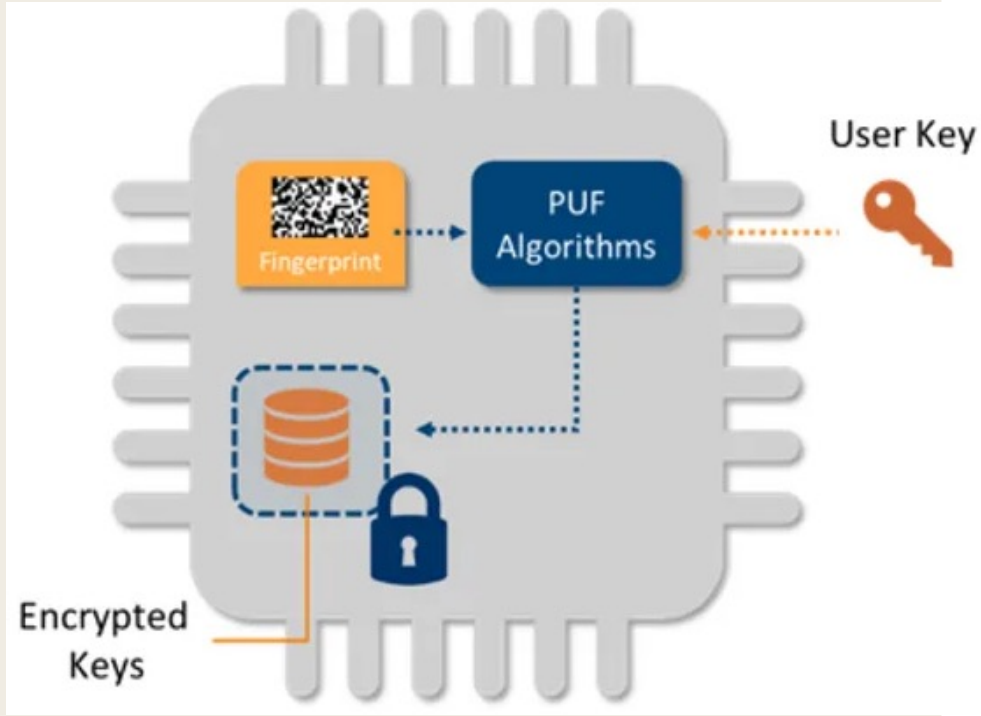


- Strong authentication: Two or more factors
  - Password + fingerprint > Password + Security question

PUF – Physical Unclonable Functions

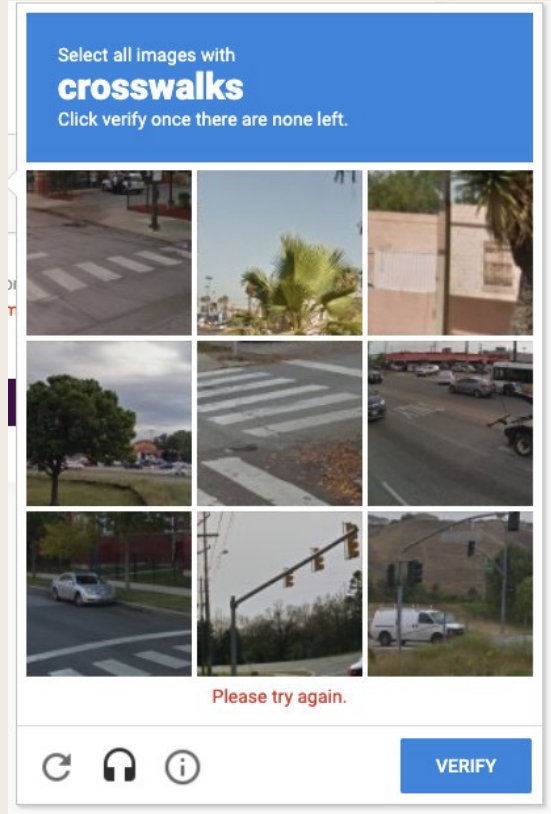
- A type of security measure that uses the physical properties of a device to create a unique **fingerprint**.
- Use the fingerprint to verify the **identity of the device.**
- **Example Scenario**
  - a PUF could be used to verify that a USB drive is the authorized device for accessing a encrypted file.
  - bind cryptographic keys to hardware devices, so that the keys cannot be extracted from the device.
  - **Chip-to-Cloud Authentication**

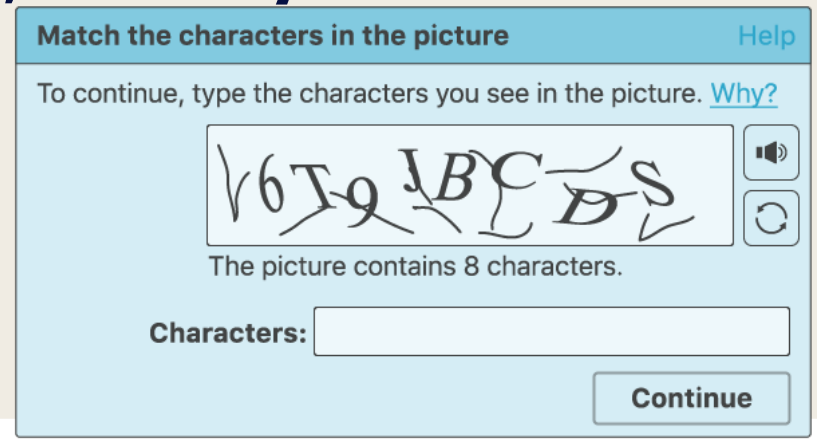
unique identifier for any given IC.
silicon fingerprint = human biometric



CAPTCHA

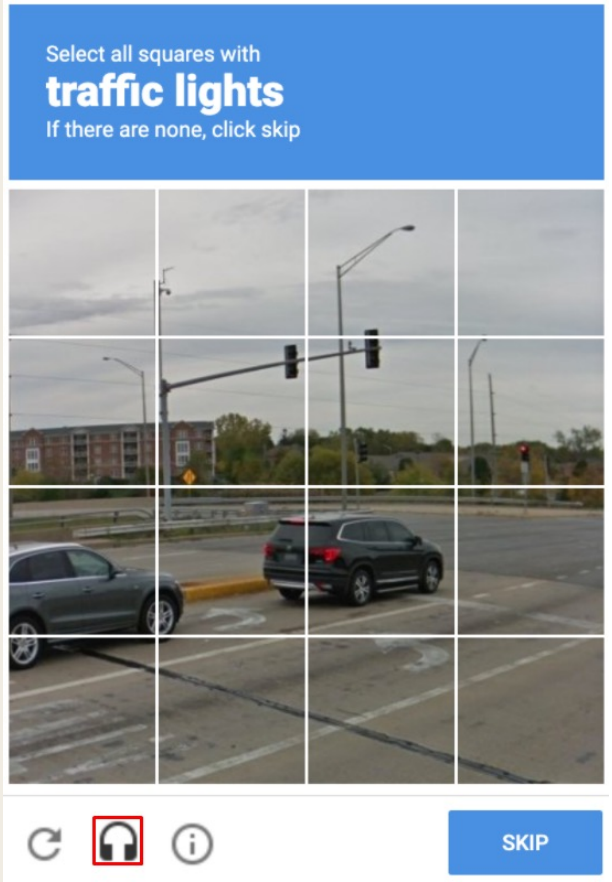
- Completely Automated Public Turing test to tell Computers and Humans Apart.
- User type the letters of a distorted image or the result of a simple math problem.
- can prevent bots from creating spam accounts on websites or submitting spam comments on blogs.
- **difficult for computers to solve, but easy for humans.**
- bypass
  - OCR or guessing common words





reCAPTCHA v3

- Two main tasks
  - Find tiles containing object in photo
  - Pick all photos containing an object
- Difficulty increased through lowering resolution or blurring the photos



Pros and Cons of CAPTCHA

- Pros:
  - CAPTCHA can protect websites from automated attacks.
  - CAPTCHA can be used to prevent spam comments on blogs.
  - CAPTCHA can be used to prevent bots from creating spam accounts on websites.

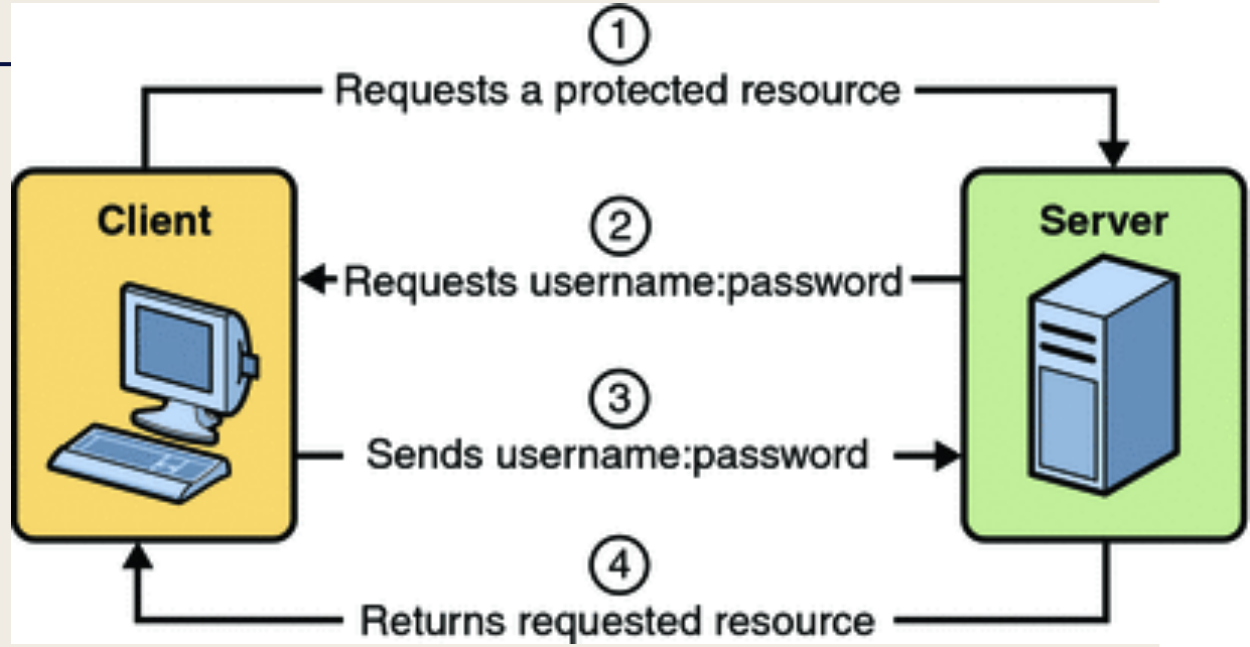
- Cons:
  - CAPTCHA can be difficult for humans to solve, especially if the images are distorted or the letters are in a foreign language.
  - CAPTCHA bypass methods are constantly evolving, so CAPTCHA designers must continually update the tests to stay ahead of the attackers.
  - CAPTCHA tests are not perfect, and they can sometimes be frustrating for users.

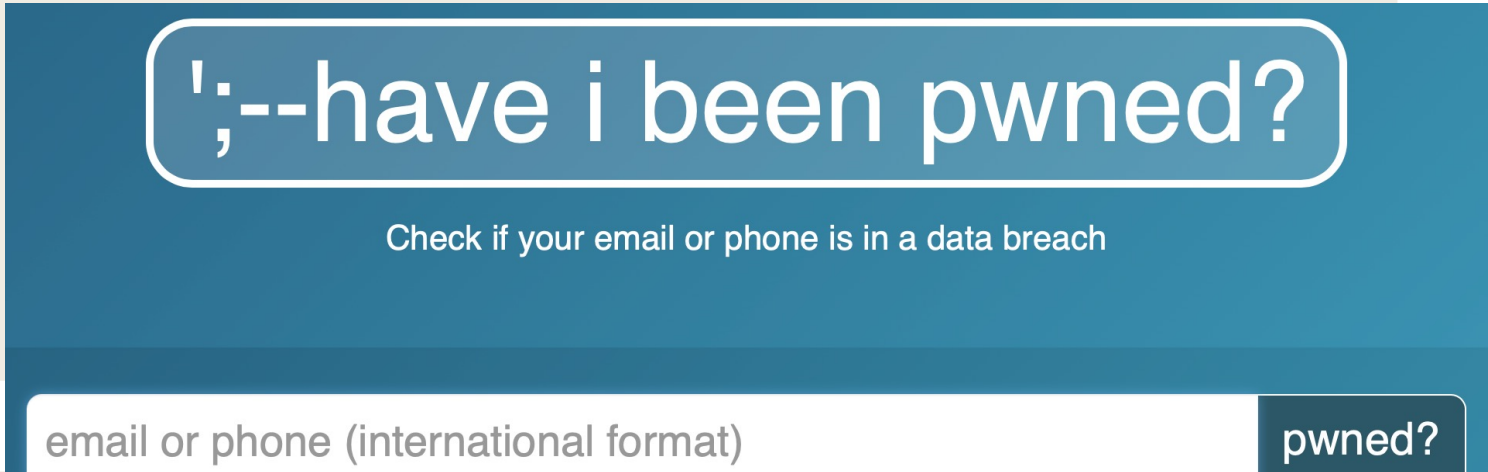
demo

- Open Burpsuite
- DVWA -> Insecure Captcha
- Enable Proxy on the browser
- Check the fields
- Modify and send

Username/Password based Authentication

- the user provides their username and password to the system in order to authenticate
- Verify credentials
- Simple, easy to implement
- Is not secure. Have I been pwned?
- Social Engineering Attacks?



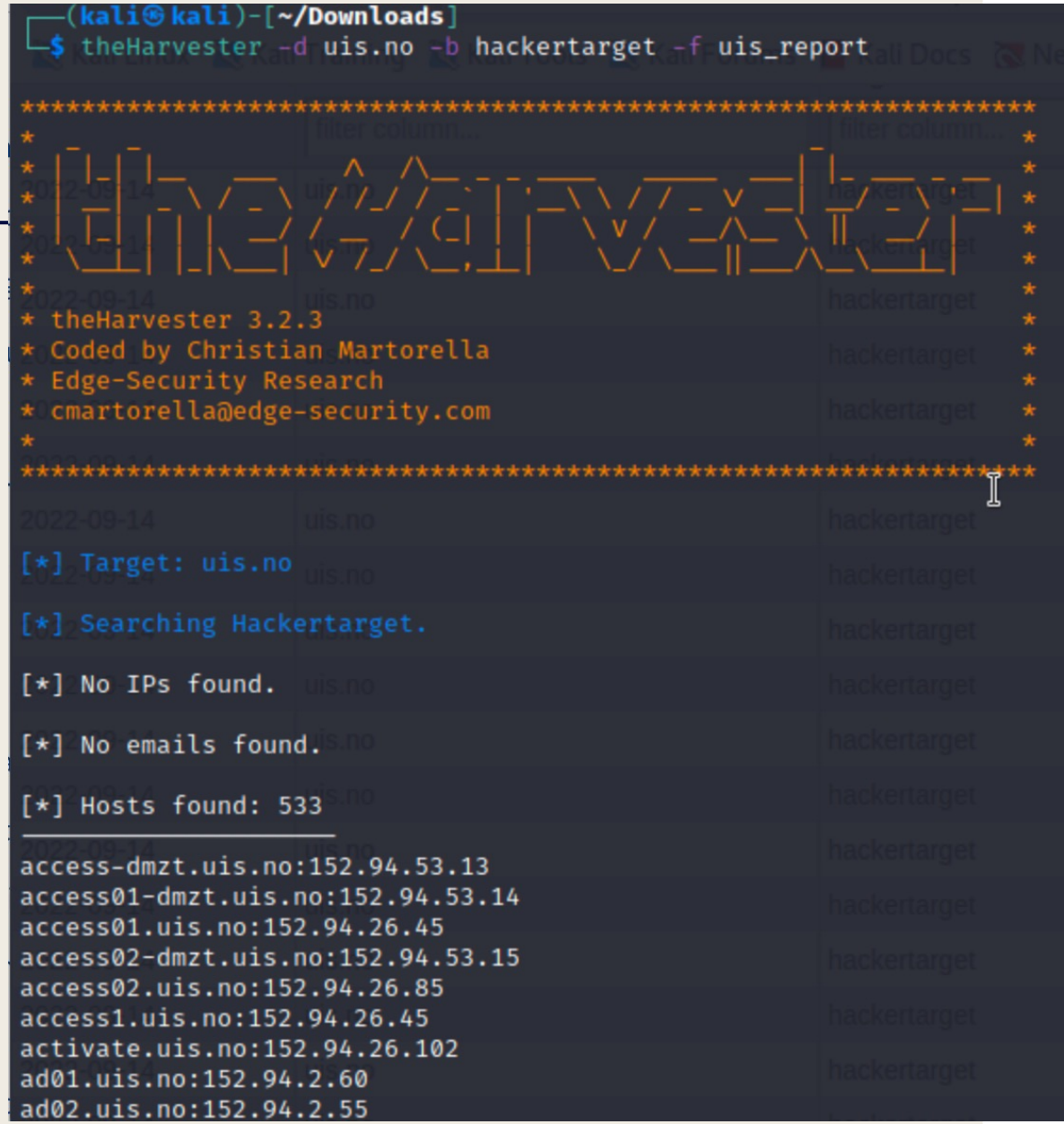


Social Engineering Attacks

The art of manipulation.	Steal sensitive information	Common methods	They may pose as a trusted individual	Challenging to detect
• **Psychological attack**	• **login credentials** • **credit card numbers** • **install malware** Attackers use social engineering techniques to trick victims into revealing information they would not normally divulge.	• **phishing emails** • **fake websites** • **phone calls**.	• a customer service representative • technical support agent	• rely on human interaction • often exploit people's natural trust

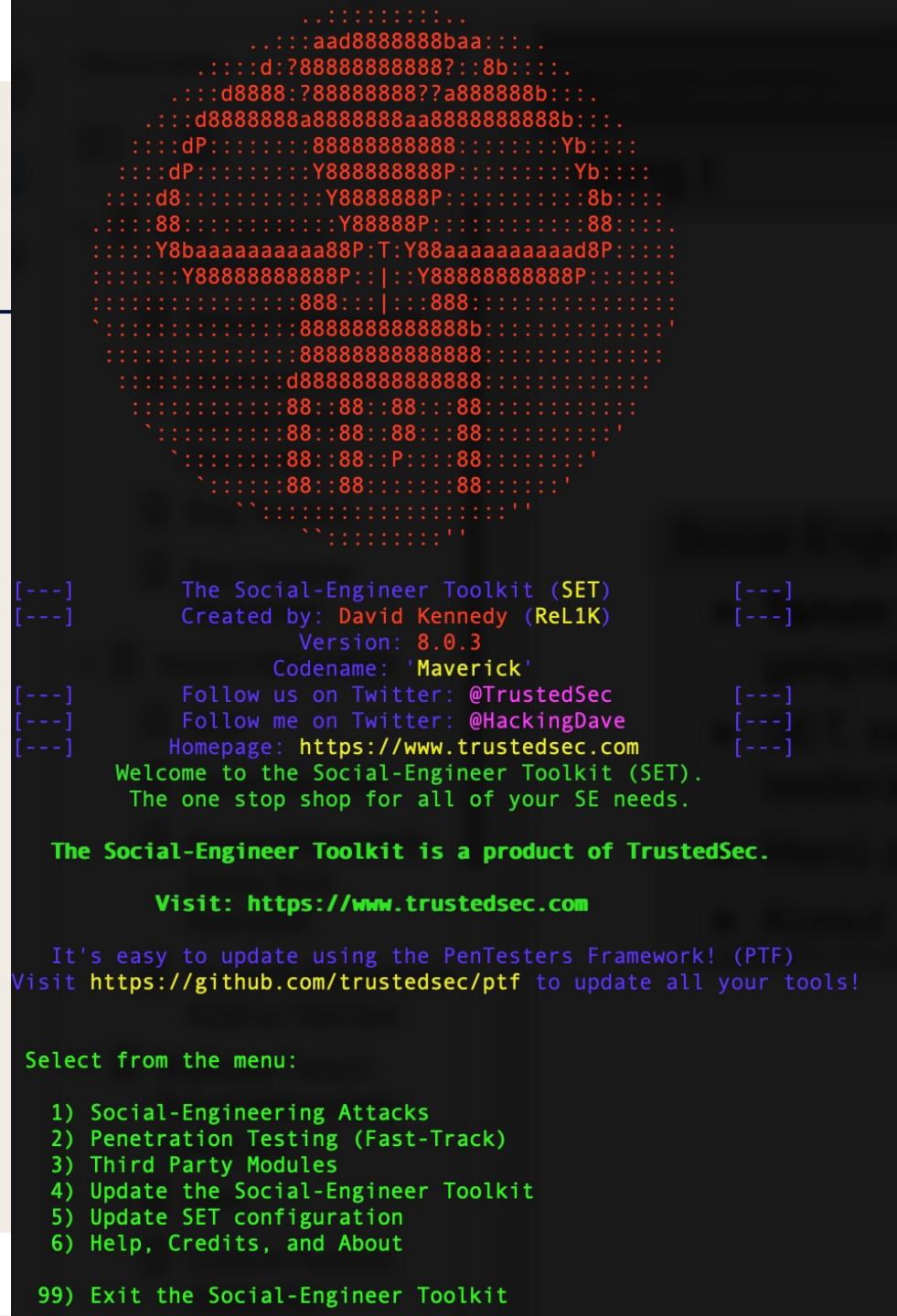
Collecting E-mails

- To collect information about a target system.
- like usernames, email addresses, and IP addresses.
- often used to collect data that can be used to brute force passwords or gain access to other systems.

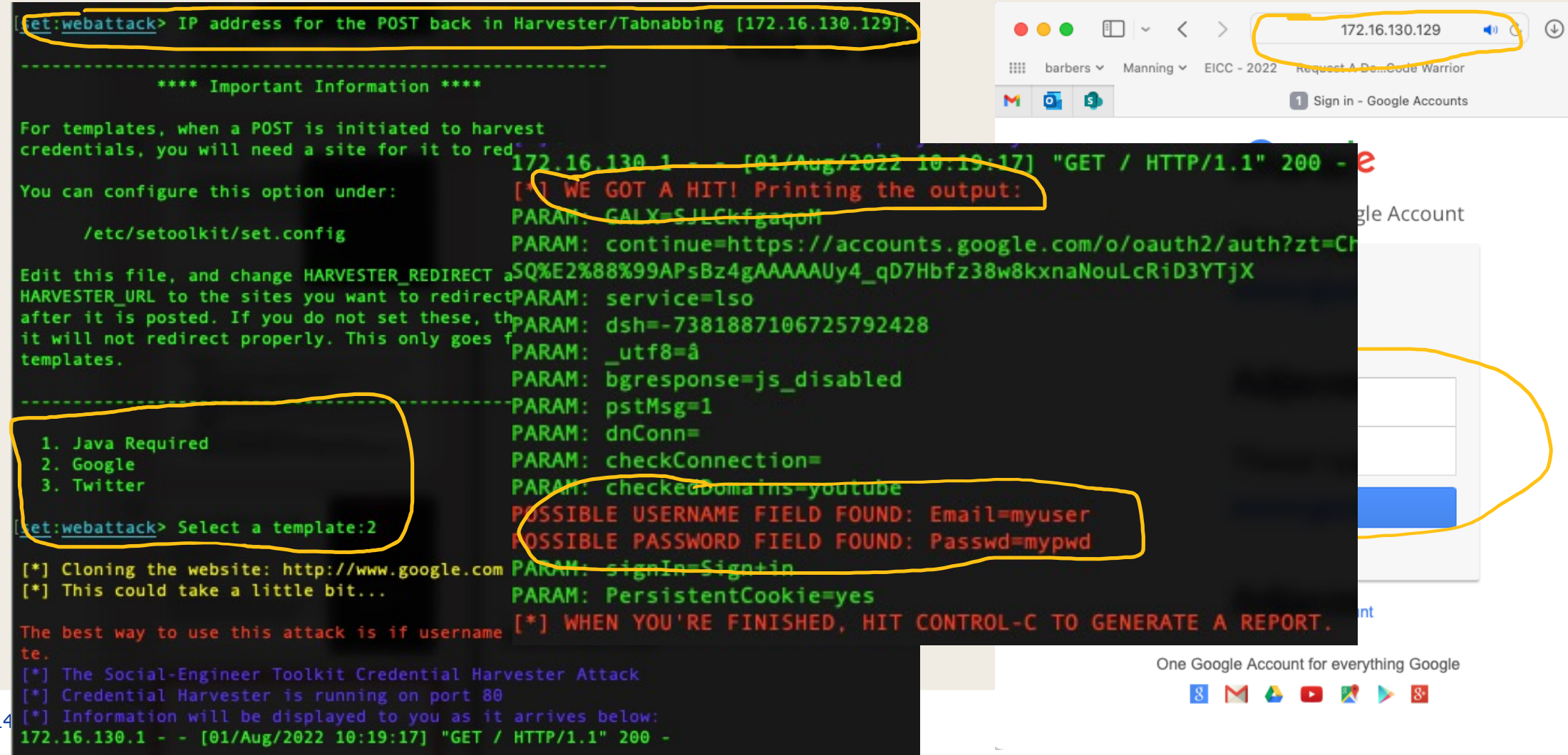


Social Engineering Toolkit

- The Social Engineering Toolkit (SET) is a powerful open-source toolkit used by ethical hackers to perform social engineering attacks.
- SET was designed to be used in penetration testing engagements to demonstrate the risk posed by social engineering attacks.
- SET can be used to launch a variety of different attacks, including
  - phishing attacks
  - credential harvesting attacks
  - web-based attacks.
- SET is a part of the Kali Linux distribution and can be installed by running the following command:
- It can be launched by running the setoolkit command. SET will then present a menu of options, as shown in the following screenshot:
- The options in the SET menu can be used to launch different types of attacks. For example, option 1 can be used to launch a phishing attack, option 2 can be used to launch a credential harvesting attack, and option 3 can be used to launch a web-based attack.
- SET can be a handy tool for ethical hackers. It can be used to demonstrate the risks posed by social engineering attacks and can also be used to launch real-world attacks.



Social Engineering Toolkit

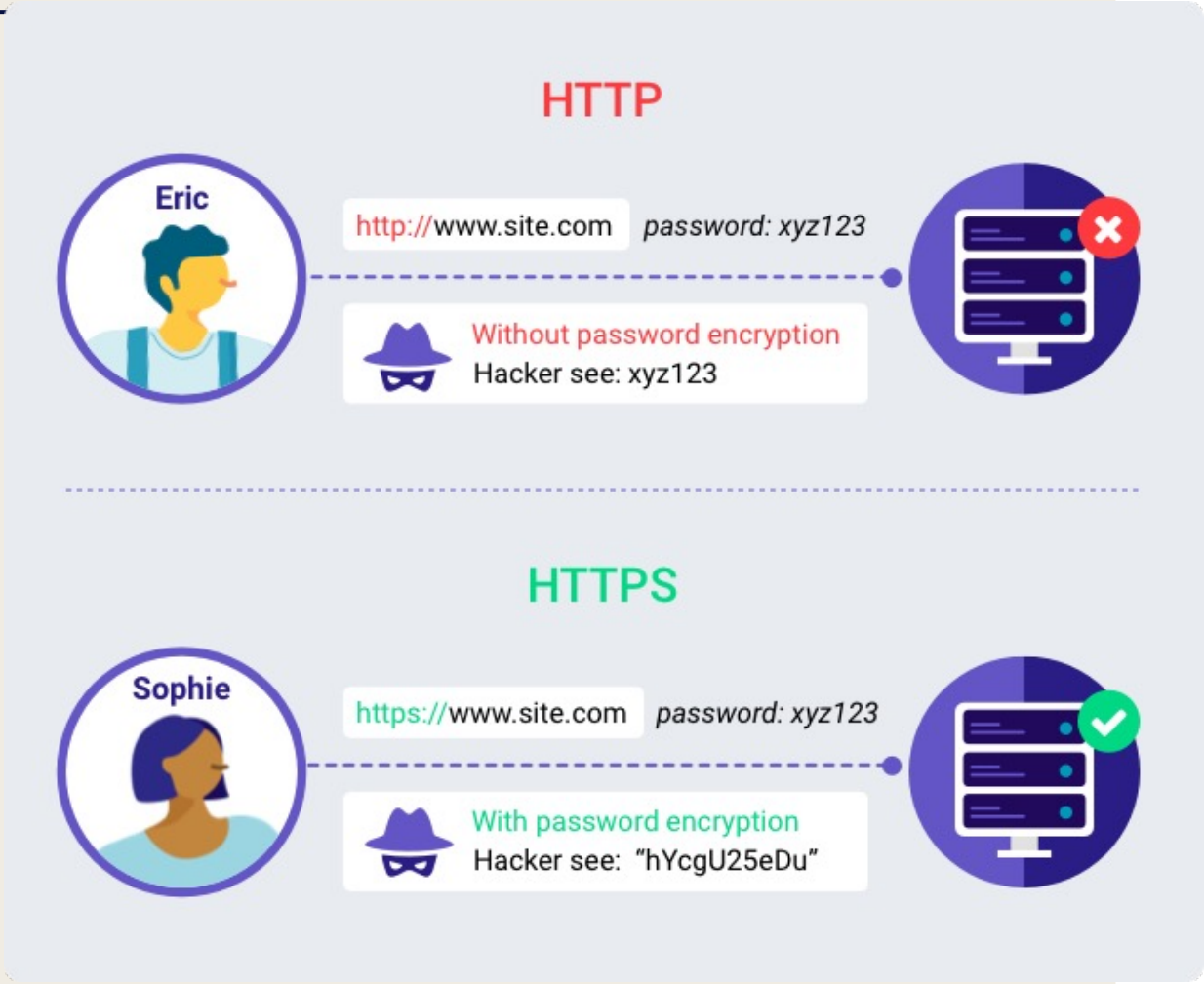


Demo

- The harvester collect the emails (usernames) from Google/Linkedin/HackerTarget
  - theHarvester –d domain.no –b hackertarget –f report_file
- Check login pages
- Get Passwords
  - Method 1: Social engineering Toolkit
    - setoolkit (Credential Harvester Attack)
    - Google
    - Clone login page
  - Method 2: Recon-ng
    - Workspace create NAME
    - Workspace search hibp
    - Marketplace install HIBP_BREACH_FULL_PATH
    - modules load hibp_breach
    - Info
    - Options set SOURCE EMAIL_ADDRESS
    - run

Credential Transport over Encrypted Channel

- TLS, or Transport Layer Security, is a cryptographic protocol designed to provide communication security over the Internet.
- TLS is used by a wide variety of applications,
- No protection of authentication process
  - HTTP
- Protection unclear
  - Verification needed
- Transport Layer Security (TLS)
  - A combination of symmetric and asymmetric cryptography to encrypt and authenticate data.



Default Credentials

- Passwords that are assigned to an account or computer by the manufacturer or system administrator.
- Applications not configured
  - Default credentials for initial authentication and configuration are never changed
- New accounts are created with default passwords
  - Password not changed on first access
- Well known among penetration testers and malicious attackers
- **Purpose:**
  - Gain access to various applications
- **Cause:**
  - Inexperienced IT personnel, programmers leaving back doors and forget to remove them, built-in default accounts, no enforcing of change of credentials

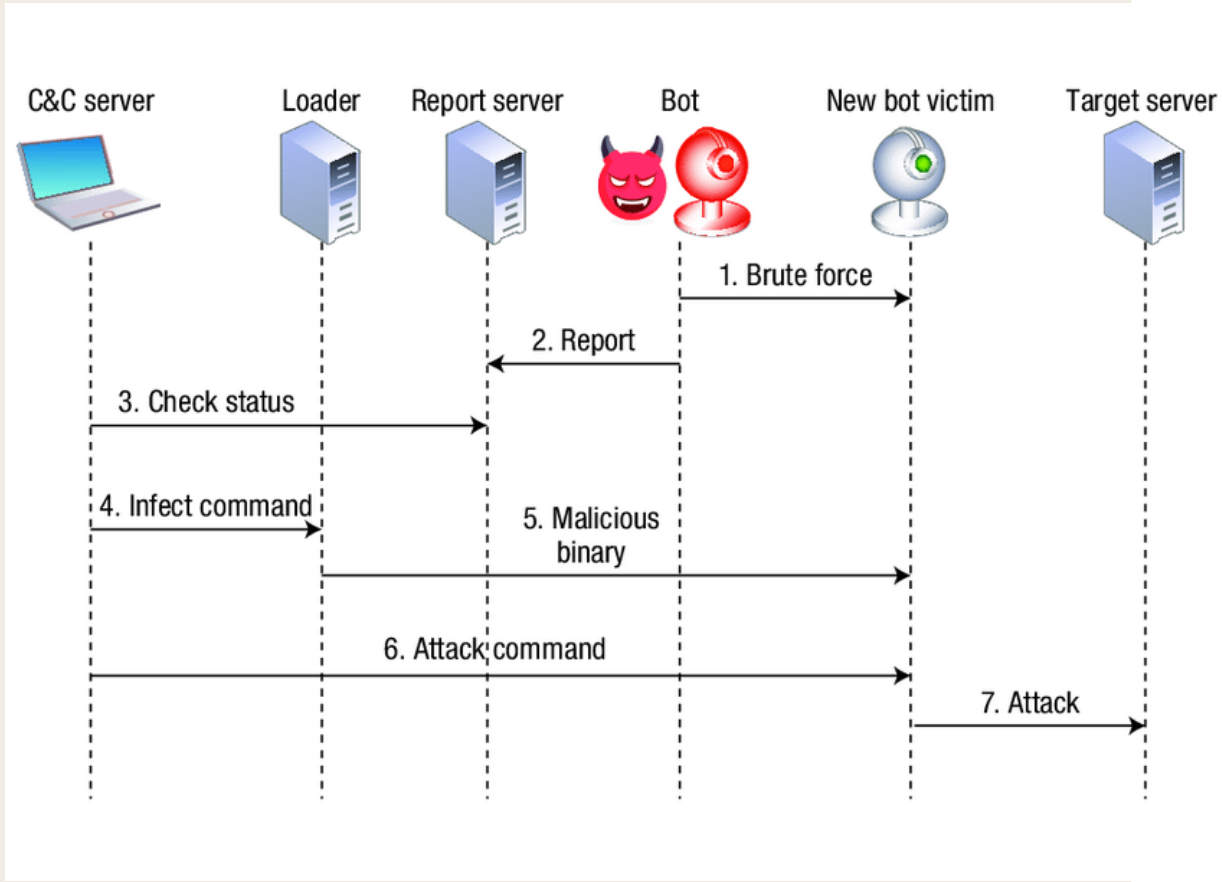
Example: MIRAI DDoS Attack

- It uses a botnet of infected devices to target a single victim.
- The Mirai botnet is created by infecting devices with a malicious piece of code that allows the attacker to take control of the device.
- The best defense against a Mirai DDoS attack is to ensure that all devices on your network are properly secured. This includes ensuring that all devices have strong passwords and that any devices that are not needed are turned off or removed from the network.

Username/Password	Manufacturer	Link to supporting evidence
admin/123456	ACTi IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-
root/anko	ANKO Products DVR	http://www.cctvforum.com/viewtopic.php?f=3&t=44250
root/pass	Axis IP Camera, et. al	http://www.cleancss.com/router-default/Axis/0543-001
root/vizxv	Dahua Camera	http://www.cam-it.org/index.php?topic=5192.0
root/888888	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/666666	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/7ujMko0vizxv	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
root/7ujMko0admin	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
666666/666666	Dahua IP Camera	http://www.cleancss.com/router-default/Dahua/DH-IPC-H
root/dreambox	Dreambox TV receiver	https://www.satellites.co.uk/forums/threads/reset-root-pa
root/zlxx	EV ZLX Two-way Speaker?	?
root/juantech	Guangzhou Juan Optical	https://news.ycombinator.com/item?id=11114012
root/xc3511	H.264 - Chinese DVR	http://www.cctvforum.com/viewtopic.php?f=56&t=34930
root/hi3518	HiSilicon IP Camera	https://acassis.wordpress.com/2014/08/10/i-got-a-new-h
root/klv123	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff04735
root/klv1234	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff04735
root/jvbzd	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff04735
root/admin	IPX-DDK Network Camera	http://www.ipxinc.com/products/cameras-and-video-serv
root/system	IQinVision Cameras, et. al	https://ipvm.com/reports/ip-cameras-default-passwords-
admin/meinsm	Mobotix Network Camera	http://www.forum.use-ip.co.uk/threads/mobotix-default-p
root/54321	Packet8 VOIP Phone, et. al	http://webcache.googleusercontent.com/search?q=cach
root/00000000	Panasonic Printer	https://www.experts-exchange.com/questions/2619439
root/realtek	RealTek Routers	
admin/1111111	Samsung IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-
root/xmhdipc	Shenzhen Anran Security Camera	https://www.amazon.com/MegaPixel-Wireless-Network-S
admin/smcadmin	SMC Routers	http://www.cleancss.com/router-default/SMC/ROUTER
root/ikwb	Toshiba Network Camera	http://faq.surveillixdvrsupport.com/index.php?action=artil
ubnt/ubnt	Ubiquiti AirOS Router	http://setuprouter.com/router/ubiquiti/airos-airgrid-m5hp/
supervisor/supervisor	VideoIQ	https://ipvm.com/reports/ip-cameras-default-passwords-
root/<none>	Vivotek IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-
admin/1111	Xerox printers, et. al	https://atyourservice.blogs.xerox.com/2012/08/28/loggin
root/Zte521	ZTE Router	http://www.ironbugs.com/2016/02/hack-and-patch-your-z

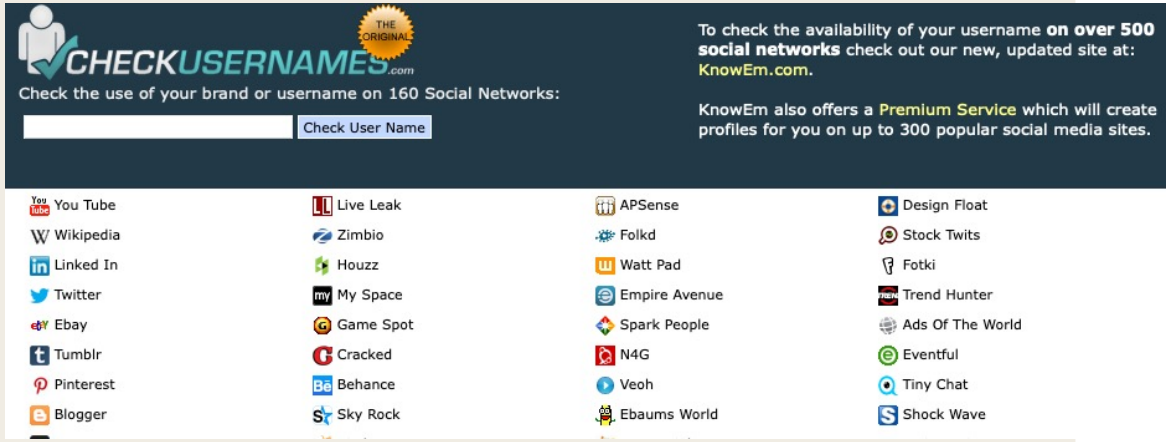
Example

1. Mirai scans random public IP addresses through TCP ports 23 or 2323.
2. Attemp to log in with a list of 62 common factory default usernames/passwords.
3. If successfully logs in, sends the device a copy of itself
4. Mirai also opens a backdoor
5. Continuously scans for new devices to infect.
6. When instructed by the command and control server, the devices in the botnet can be used to launch DDoS attacks.



User enumeration, Brute force, Exposed Passwords

- User enumeration
  - Guess usernames of valid users. E-mails?
  - Using OSINT: social media accounts, common usernames (root/admin/test/user etc)
- Target organization: company website directory, Linkedin profiles, Google
- Motivation
  - gain access to systems and data
  - launch targeted attacks against specific users
- Look for different error codes
  - Valid user but bad password
  - Invalid user and password
  - In error messages, url/pages, recovery services



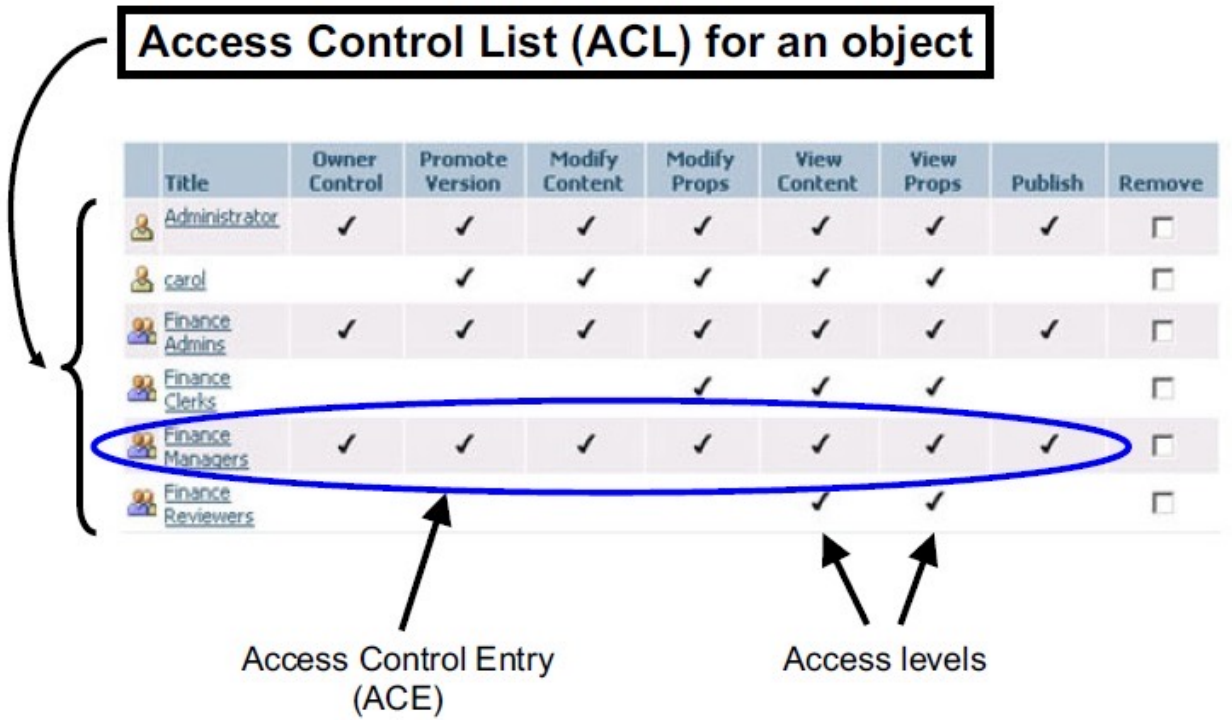
Authorization

Authorization

- The process of granting or denying access to a resource
  - Determining whether a user or computer process has the right to access a resource.
- Resources
  - Computer systems
  - Applications
  - Data
  - APIs

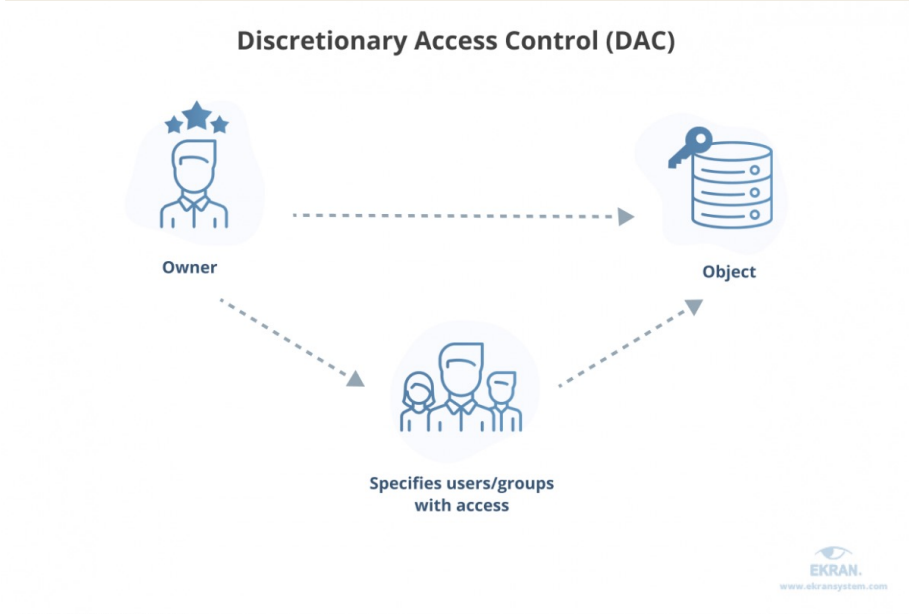
Access Control List (ACL)

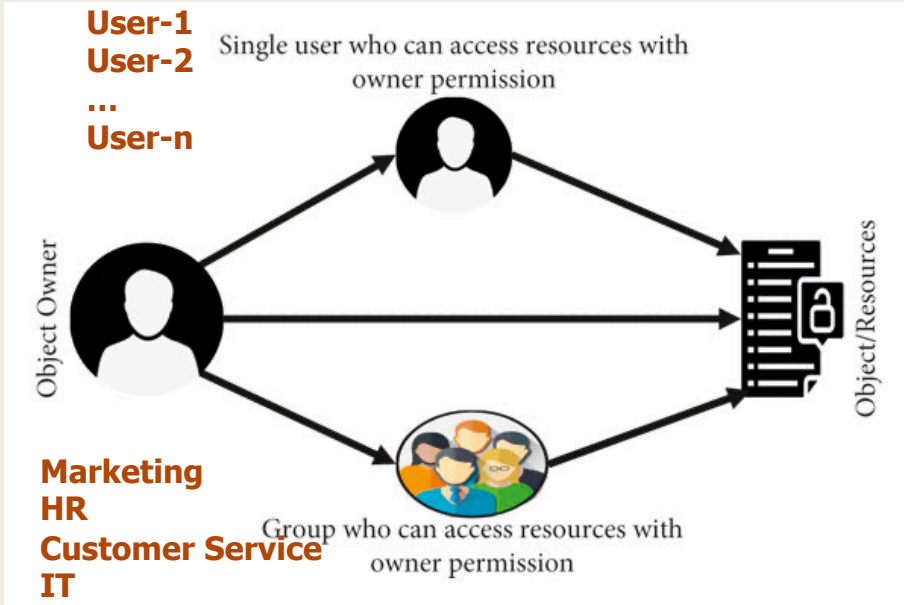
- List of rules
  - Which users/systems/apps -> granted/denied to object/database/server/file (resource)
- Access Control Types
  - Mandatory Access Control (MAC)
  - Discretionary Access Control (DAC)
  - Role-Based Access Control (RBAC)
  - Attribute-Based Access Control (ABAC)



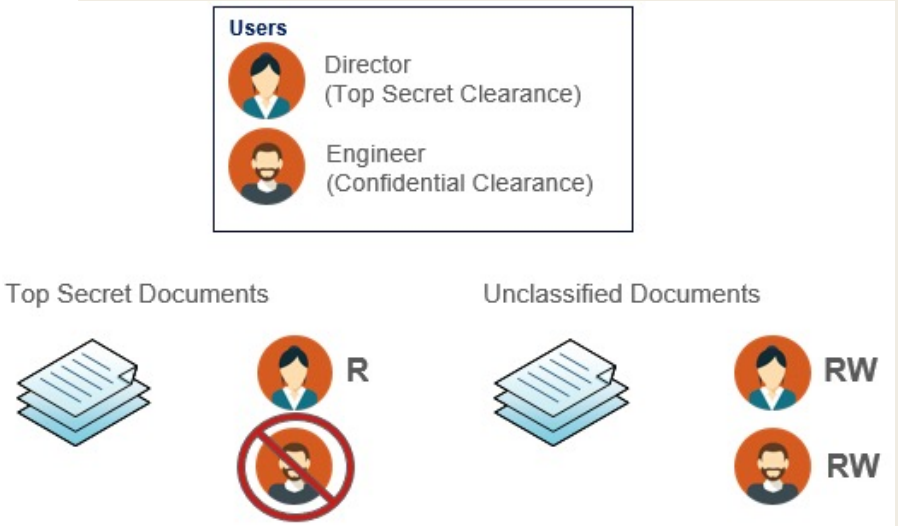
Discretionary Access Control (DAC)

- Restricting access to objects based on the identity of the subject
- implemented using ACL
  - If the user has permission to access the resource
  - users who can access the resource and the authority (such as read or update)





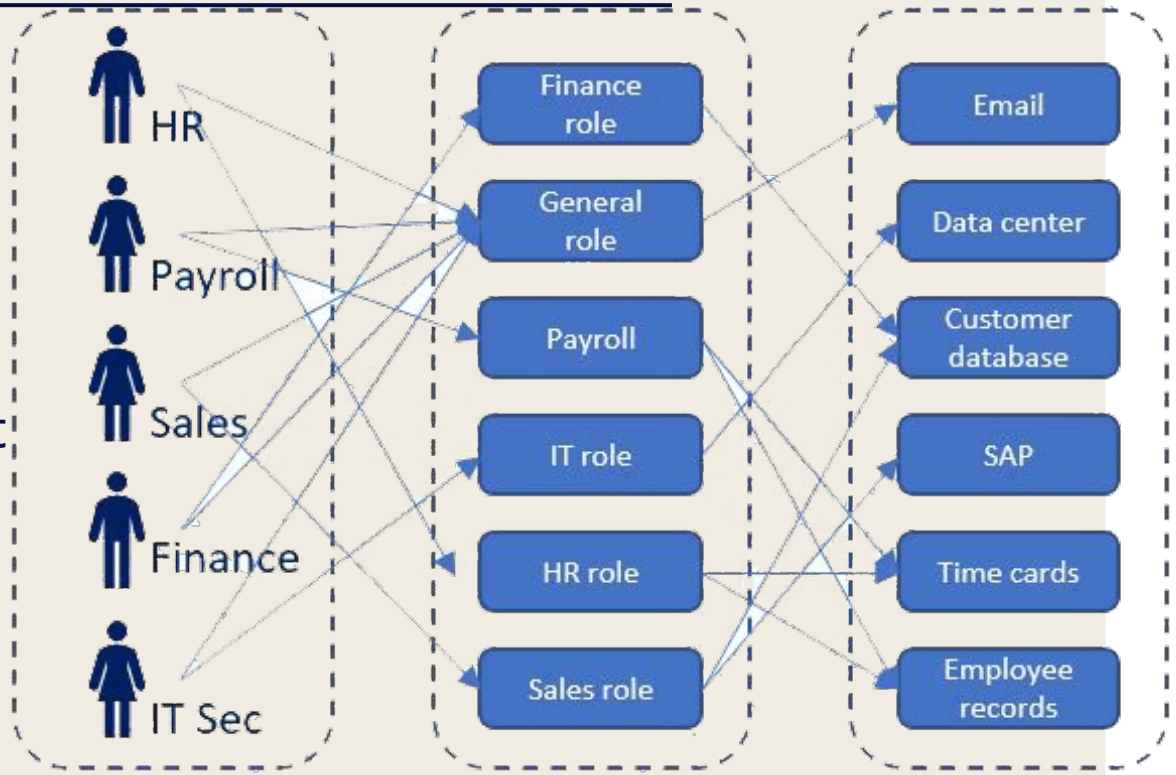
Mandatory Access Control (MAC)



- limiting access to resources based on
  - the sensitivity of the information
  - the authorization of the user to access information with that level of sensitivity.
- Sensitivity: define by means of a security label: **Unclassified**, **Restricted, Confidential, Secret, Top Secret**
- Users can access only the information in a resource to which their security labels entitle them.

Role-Based Access Control (RBAC)

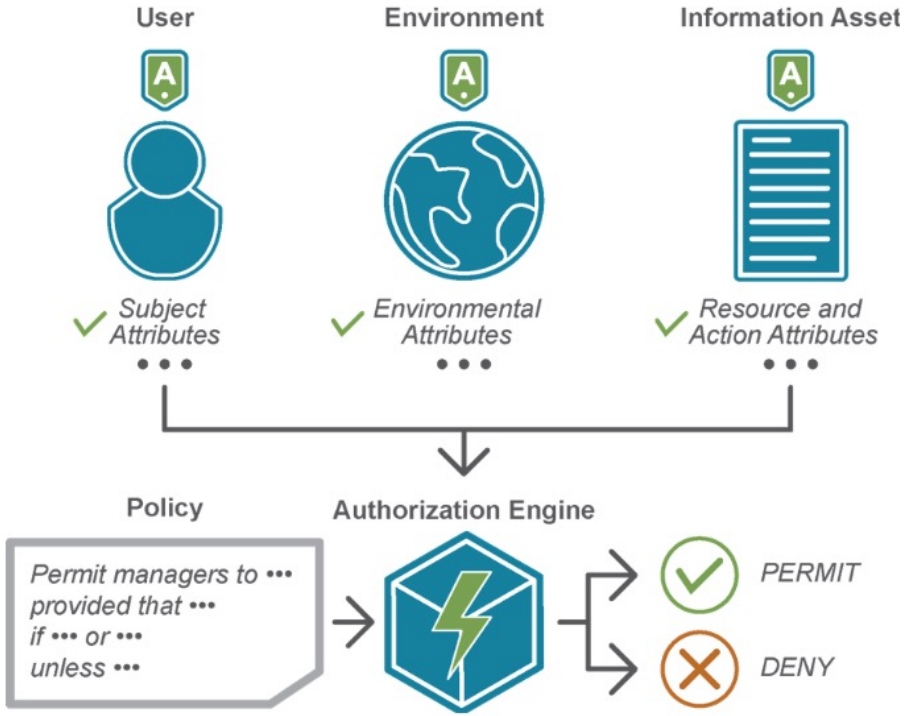
- Restricts access to resources based on the roles assigned to users.
- Flexible and Scalable security model
- Well-suited for large organizations
- Advantages
  - easily **grant** or **revoke** access to multiple users at once
  - granularly control access to resources:
    - financial analysts granted read-only access to financial data
    - accounting managers granted read/write access.
- Disadvantages
  - Can be complex to manage with thousands users
  - Security breach



Attribute-Based Access Control (ABAC)

- Subjects and objects are related to each other through attributes.
- **RBAC**: a user with the role "manager" would be given access to the object "payroll."
- **ABAC**: a user with the attribute "employee" would be given access to the object "payroll".

Object Attributes	Subject Attributes	Environment Conditions Attributes
• Type • Author • Owner • Date Created • Last Updated • Classification	• Name • Employee # • Designation • Department/ Affiliation • Clearance	• Location • Time Zone • Current time • Current Day

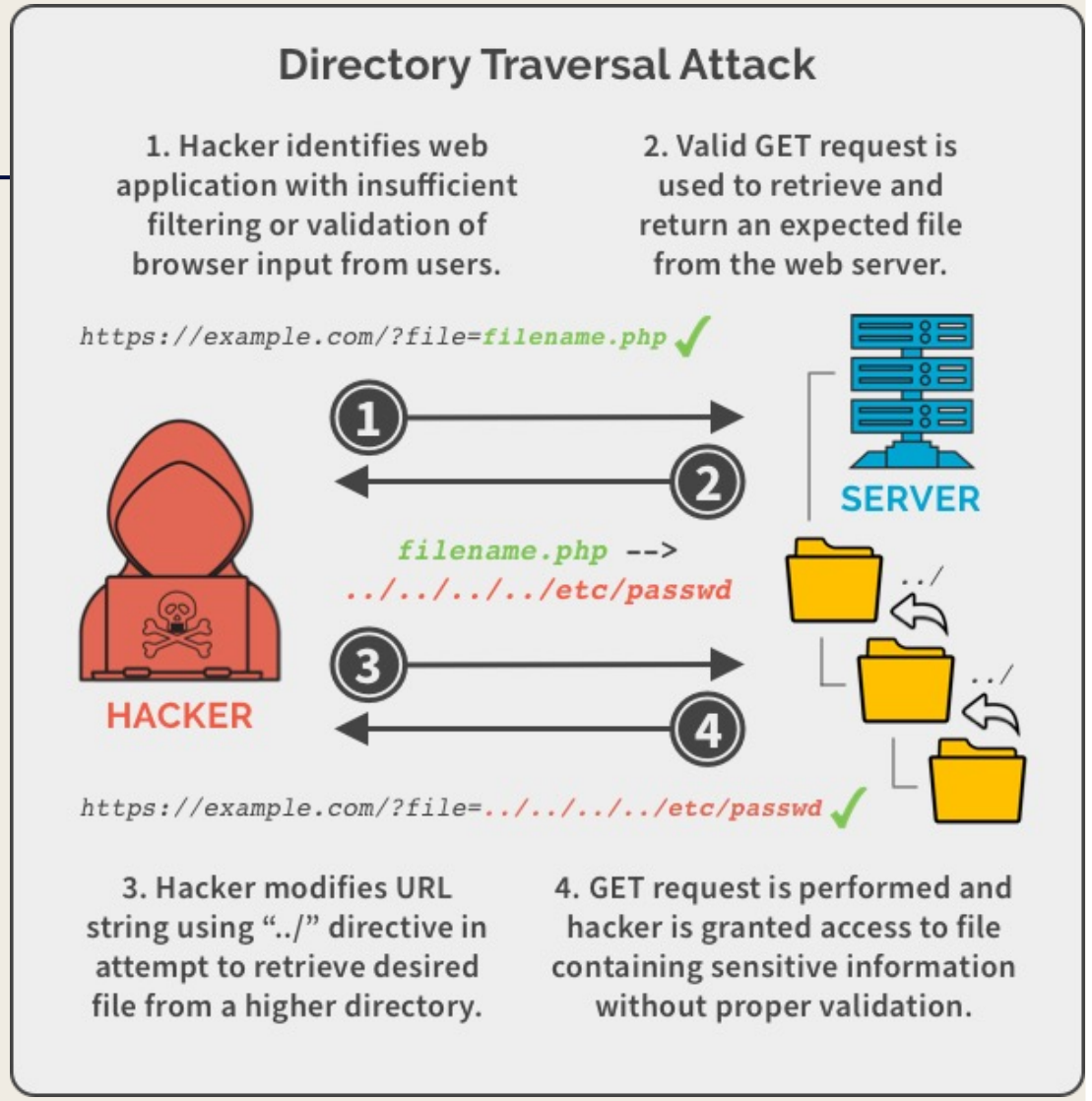


Allowing only users who are **type=employees** and have **department=HR** to access the **HR/Payroll system** and only **during business hours** within the **same timezone** as the company.

Attacks

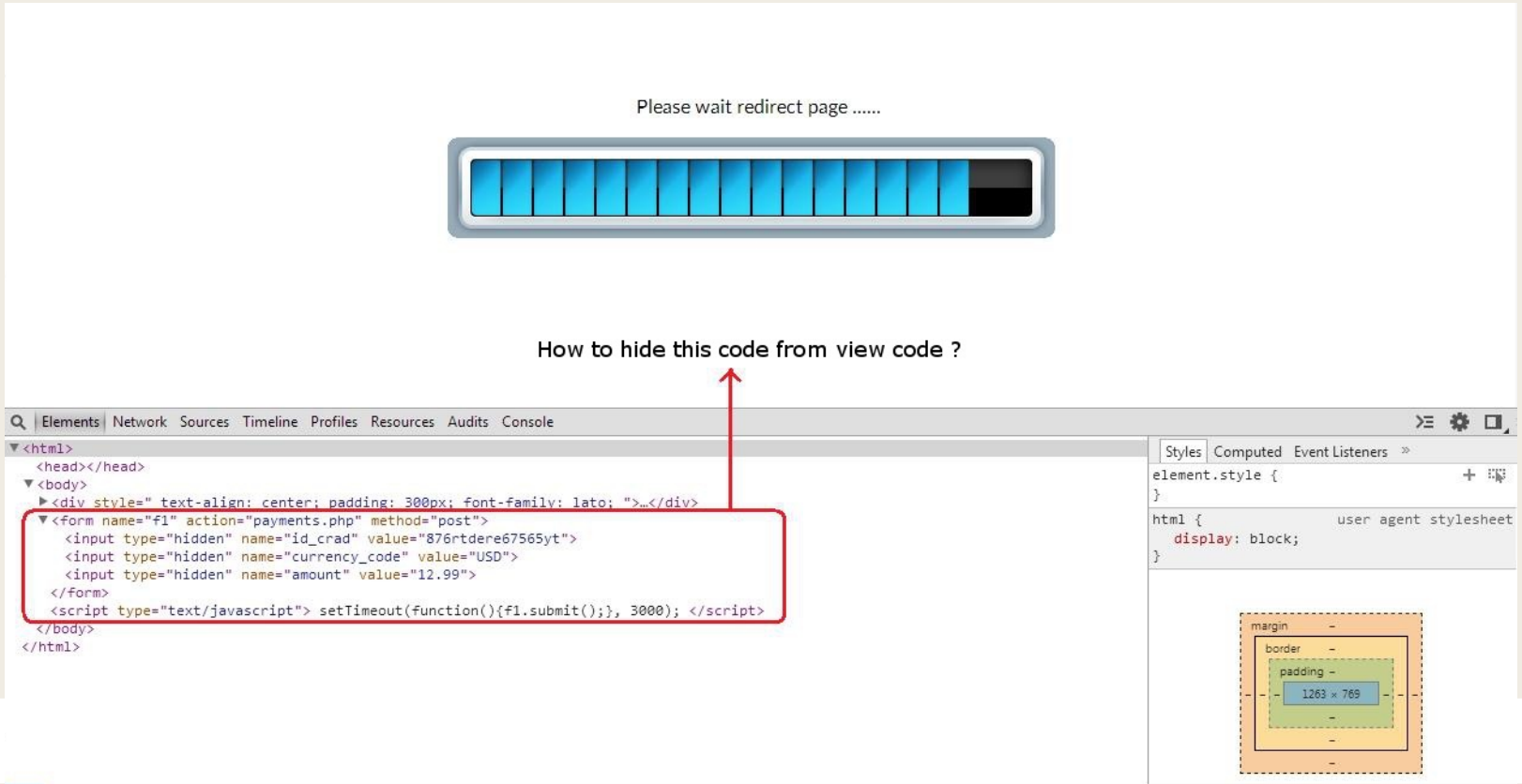
Path Traversal

- An exploit: the attacker attempts to access files and directories that are outside of the web root directory.
- Often used to gain access to the server's file system.
- URL Encoding
  - Dot: %252e
  - Forward slash: %252f
  - Backslash: %255
- **Demo: DVWA – File Inclusion**



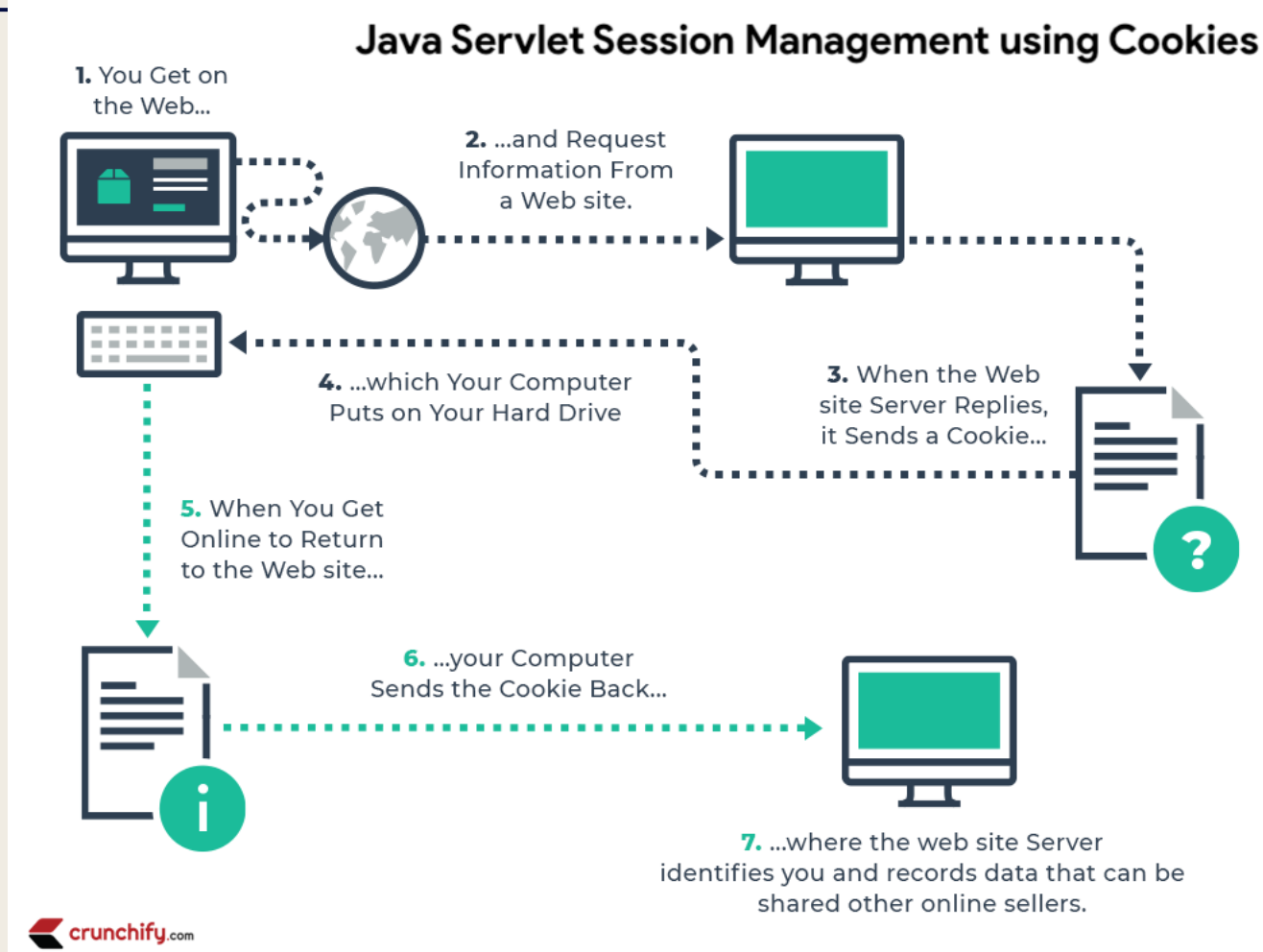
Manipulating Hidden Fields

- HOW: Look for hidden fields within forms, analyze what they are used for, and try to change their values in ways that would benefit an attacker
  - Source code – look for ”hidden”



Cookie Tampering

- Cookie: small text file that web application creates on client machine
  - sessionId
  - Username
  - User preferences
  - Etc.
- HOW:
  - Directly modify the file
    - Stored in predefined location
    - Browser extensions
    - Burp Suite
    - Owasp ZAP



Session hijacking

- An attacker takes control of a user's web session by stealing their session cookie.
- access the victim's account and perform any actions that the user is able to do.
- Allows bypass authentication and authorization checks
  - gain access to sensitive information: financial data or personal information.
- **Demo:**

Steal another user’s session ID

Session hijacking - Mitigations

- Ensure that all users get a ”clean” sessionID by regenerating the sessionID whenever a user logs in
- Set the ”**HttpOnly**” flag on all cookies
  - Protect against XSS. Javascript cannot read these
- Set the ”**secure**” flag on all cookies
  - transmitted using a secure connection (SSL/HTTPS).
- Enforce strong policies for sessionID creation an
  - Never use userID as sessionID
  - Never use sequential sessionIDs
- Use a content security policy (CSP) to prevent cross-site scripting (XSS) attacks
- **DVWA - Weak Session IDs**
  - **Low: increasing**
  - **Medium: Sequencer, copy**
  - **High: copy 3 session id**
    - **Hashcat –a 3 –m 0 hash.txt –increment**
      - **-m : hashtype: 0 – MD5**
      - **-a attack mode: 3-Brute-Force attack**
      - **--increment: incremental 1?-> 2? -> 3? …**

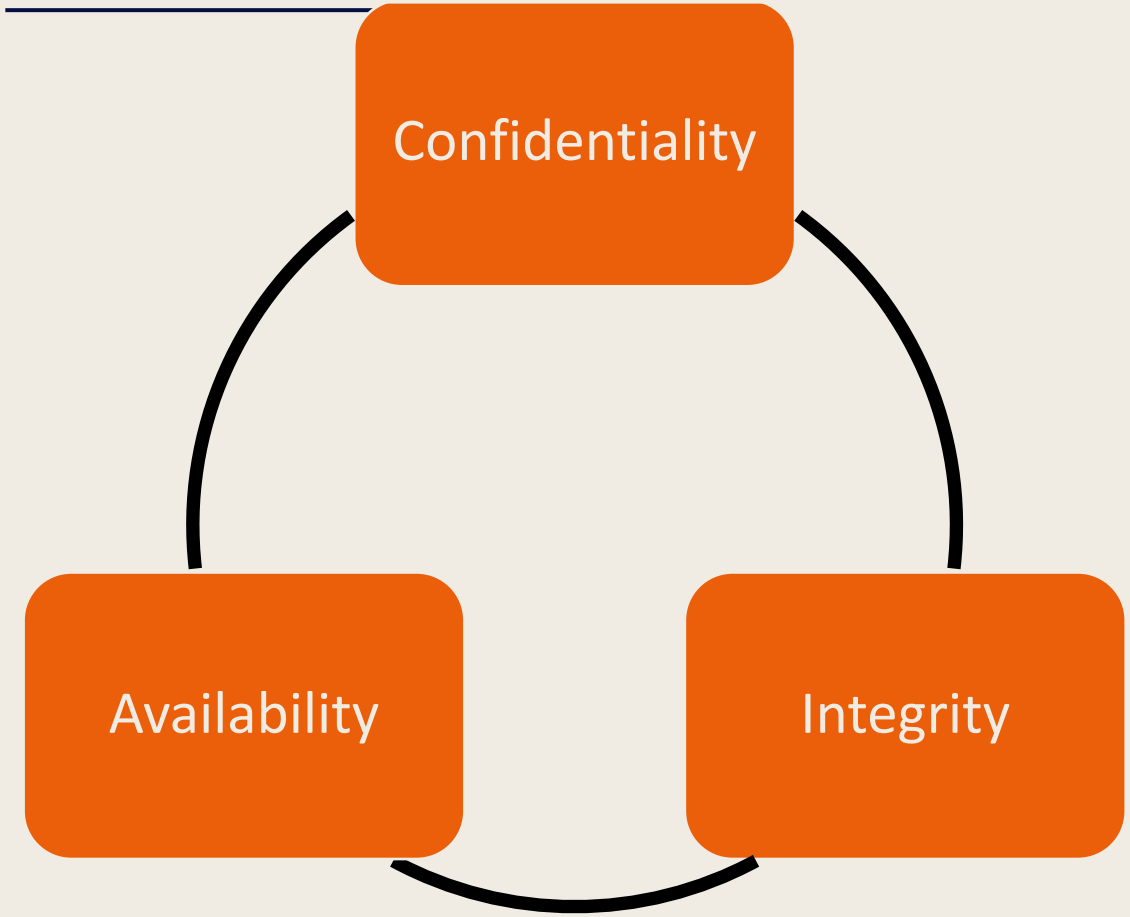
```
Set-Cookie: sessionid=QmFieWxvbiA1; HttpOnly
```

```
Set-Cookie: sessionid=QmFieWxvbiA1; HttpOnly; Secure
```

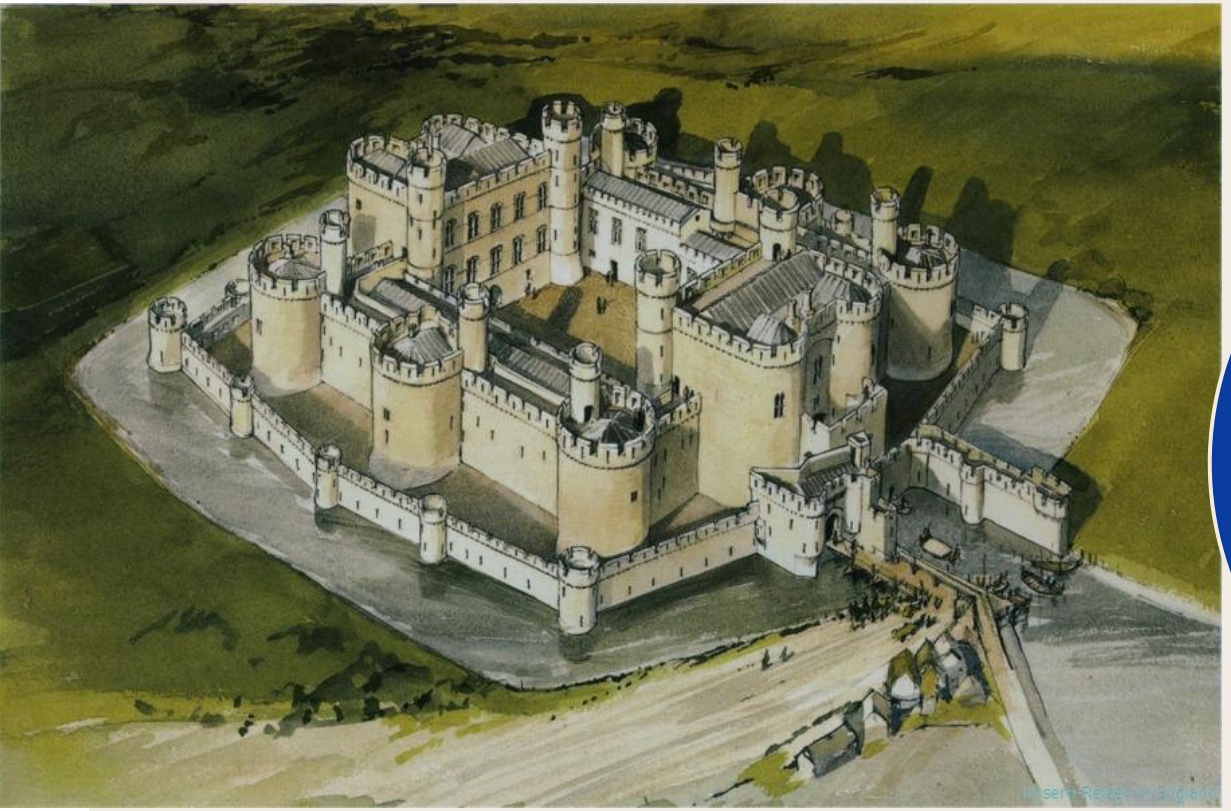
Security Protocols

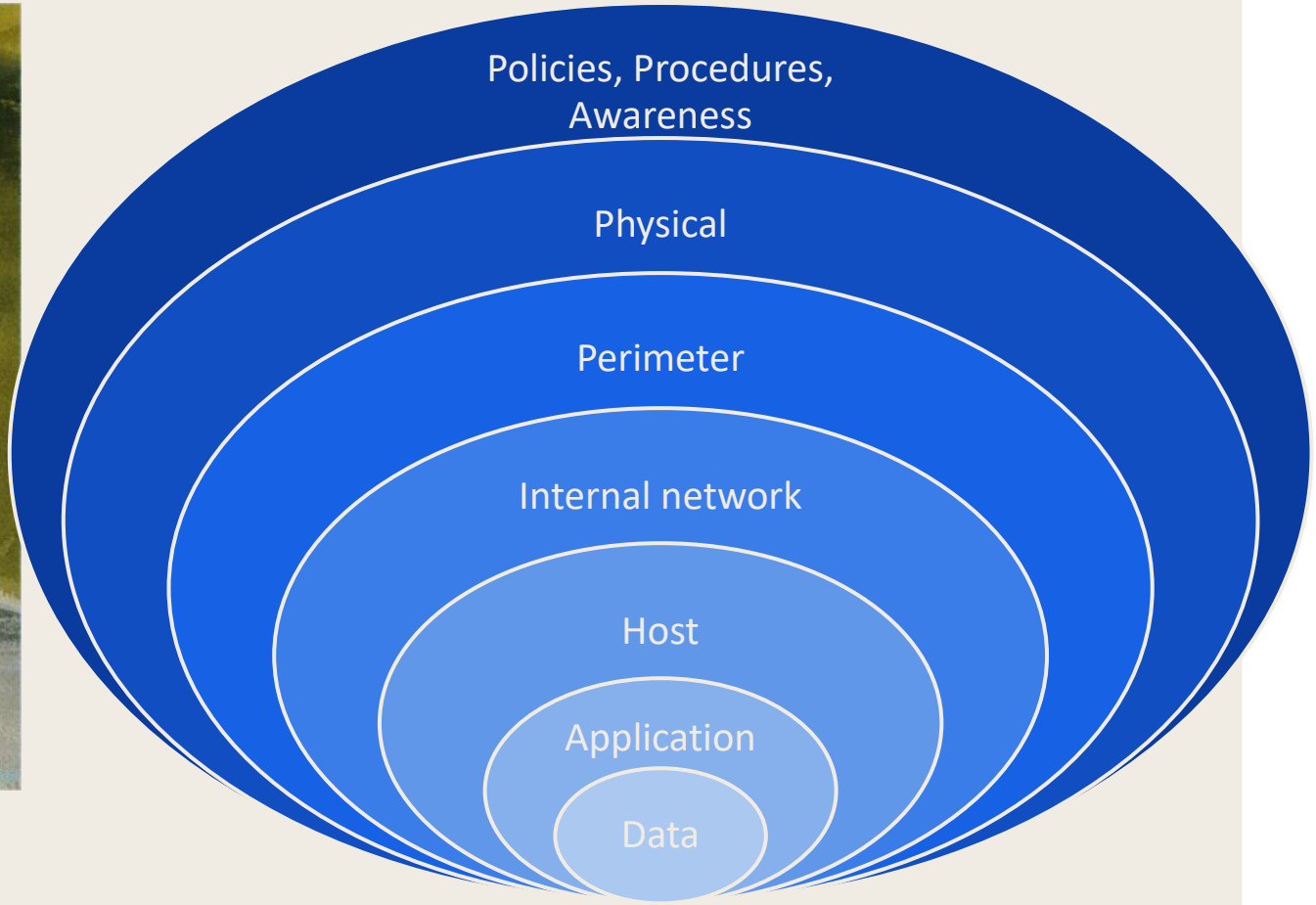
Elements of Information Security (CIA-Triad)

- a security model that is used to guide security efforts
- the three pillars of security
- Confidentiality:



Defense-in-Depth





Click to add text