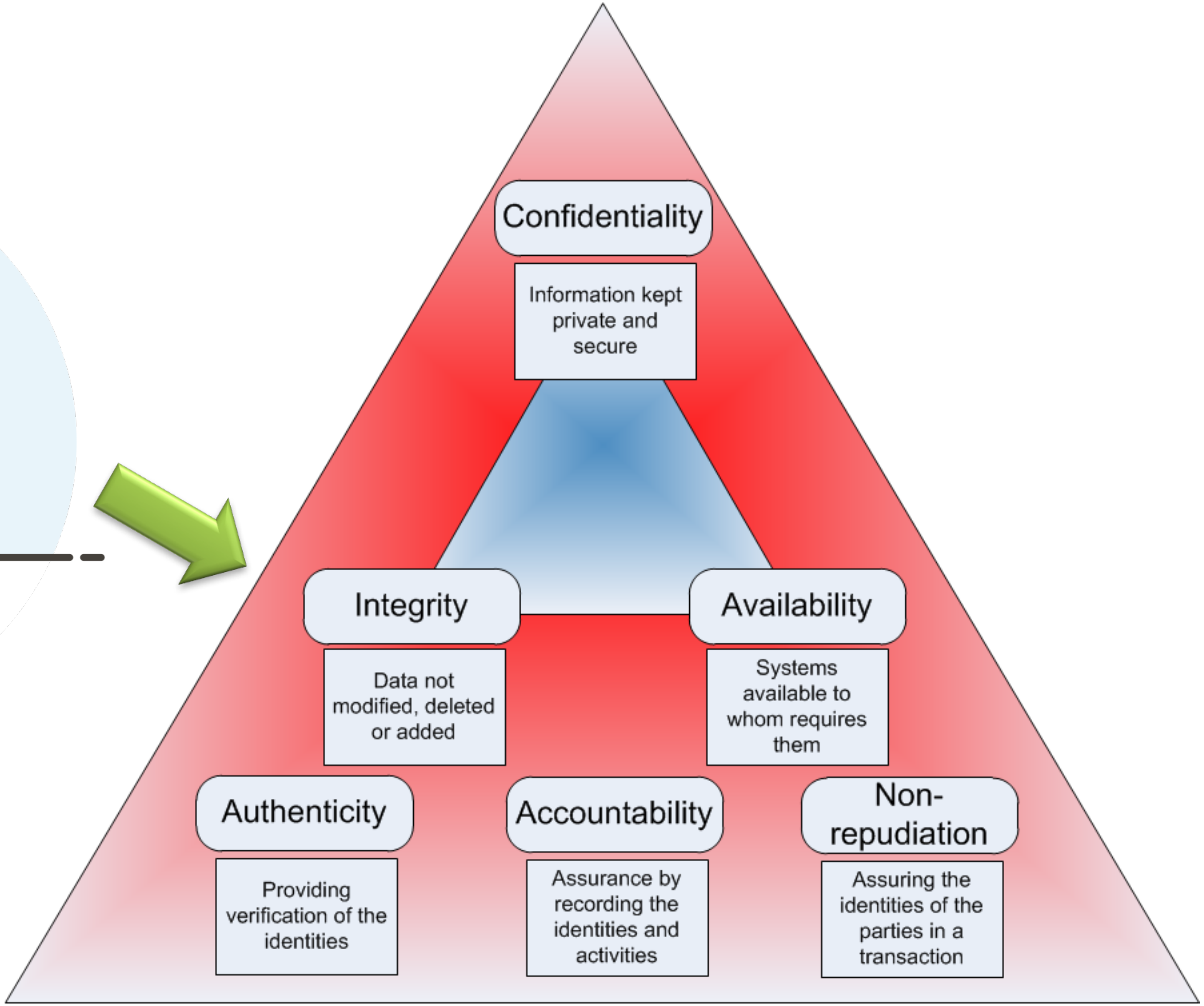
Introduction & Overview

Cyber Security

Part I

CIA Triad

The CIA Triad



Confidentiality

Information kept private and secure

Integrity

Data not modified, deleted or added

Availability

Systems available to whom requires them

Authenticity

Providing verification of the identities

Accountability

Assurance by recording the identities and activities

Non-repudiation

Assuring the identities of the parties in a transaction

Source: [04/01/2019] http://keywordsuggest.org/gallery/151304.html

Formal Definition: CIA Triad

Confidentiality

Confidentiality is the property, that information is not **accessible** (made available or disclosed) to **unauthorized** individuals, entities, or processes. In ensures sensitive data does not land in wrong hands.

Integrity

Integrity means that data cannot be **modified** in an **unauthorized** or **undetected** manner. It provides assurance over accuracy and completeness over entire data life cycle.

Availability

Availability means relevant information is readily accessible to those authorized to view it at all times. It ensures information is available when needed.

Layers of Security

- Physical security
- Personal security
- Operations security
- Communications security
- Computer security
- Network security
- Information security

Source: [27/12/2016] https://www.pinterest.com/homecontrols/home-security/

Physical Security

New age warfare does not require missiles or bombs

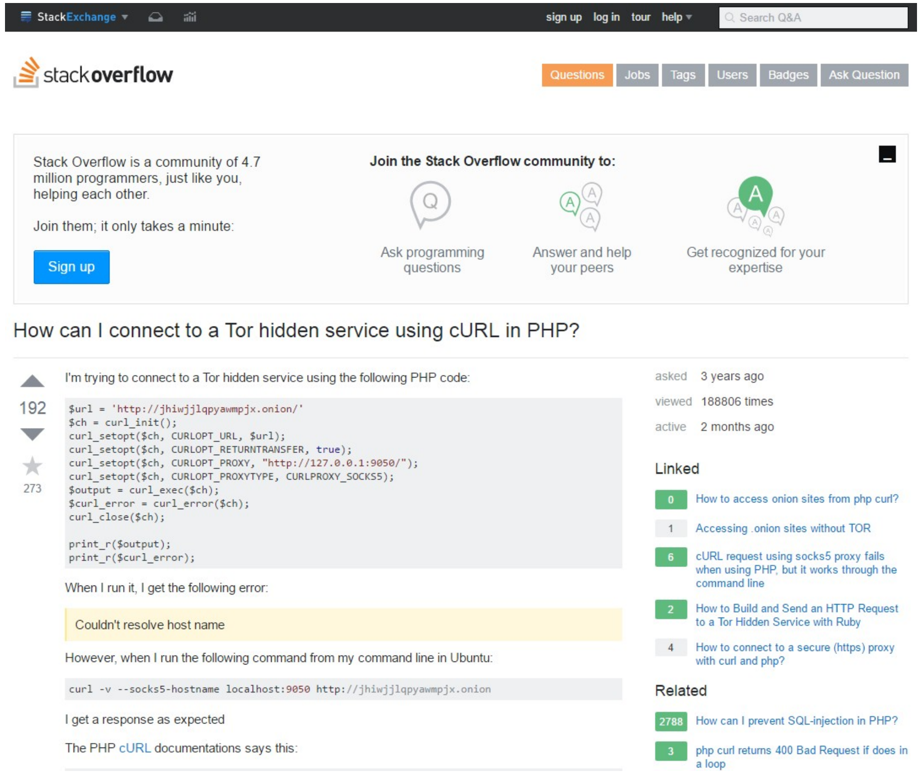
How malware was used to destroy a nuclear reactor

Social Media Security

Story of Uncle C: Sir John Sawers

Are employees accidentally revealing confidential data on Social Media?

Social Media Security



Stack Overflow is a community of 4.7 million programmers, just like you, helping each other.

Join them; it only takes a minute:

Sign up

Join the Stack Overflow community to:

Ask programming questions

Answer and help your peers

Get recognized for your expertise

How can I connect to a Tor hidden service using cURL in PHP?

192

273

I'm trying to connect to a Tor hidden service using the following PHP code:

```
$url = 'http://jhiwjjlqpyawmpjx.onion/'
$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, $url);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
curl_setopt($ch, CURLOPT_PROXY, "http://127.0.0.1:9050/");
curl_setopt($ch, CURLOPT_PROXYTYPE, CURLPROXY_SOCKS5);
$output = curl_exec($ch);
$curl_error = curl_error($ch);
curl_close($ch);

print_r($output);
print_r($curl_error);
```

When I run it, I get the following error:

> Couldn't resolve host name

However, when I run the following command from my command line in Ubuntu:

```
curl -v --socks5-hostname localhost:9050 http://jhiwjjlqpyawmpjx.onion
```

I get a response as expected

The PHP cURL documentations says this:

asked	3 years ago
viewed	188806 times
active	2 months ago

Linked

0	How to access onion sites from php curl?
1	Accessing .onion sites without TOR
6	cURL request using socks5 proxy fails when using PHP, but it works through the command line
2	How to Build and Send an HTTP Request to a Tor Hidden Service with Ruby
4	How to connect to a secure (https) proxy with curl and php?

Related

2788	How can I prevent SQL-injection in PHP?
3	php curl returns 400 Bad Request if does in a loop

- People accidentally post confidential information on the Internet
- Not easy to delete such information
- Story of Dread Pirate Roberts: Silk Road

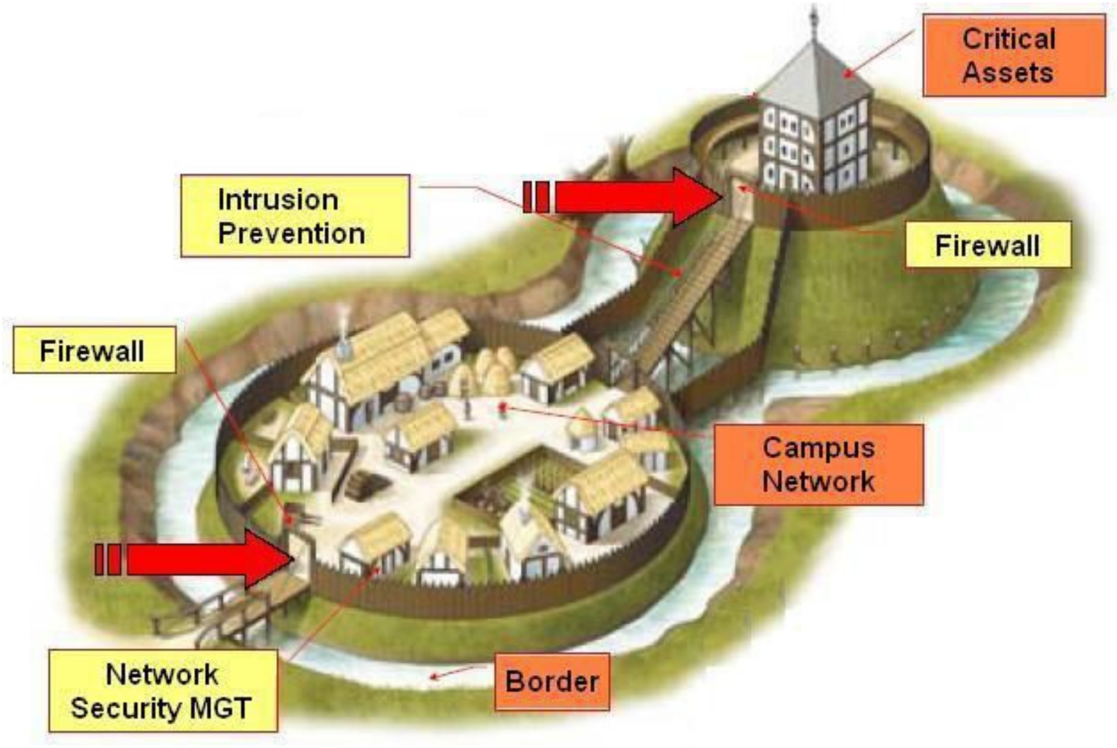
Phishing

- What happened at RSA
- Most likely vector that attackers will be used to compromise an organization's users
- Protecting yourself from Phishing

Defense in Depth – Classical Military

Information Security draws idea from conventional military doctrine

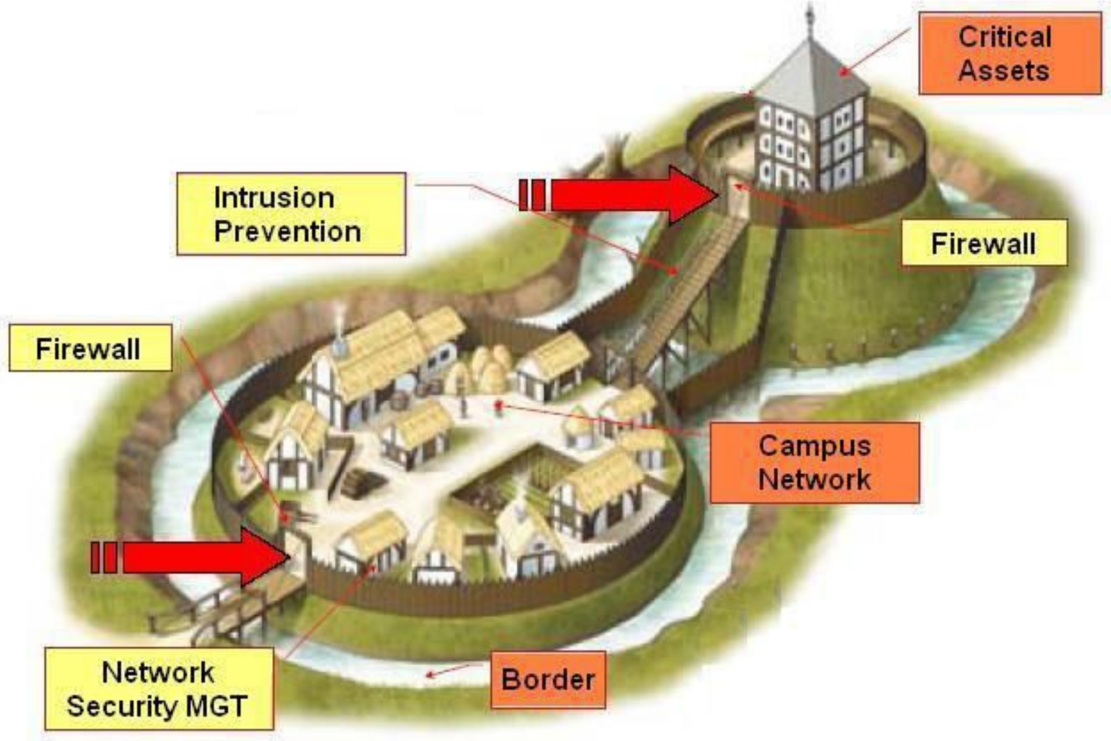
Defense in depth:
•Moat (with moat monsters)
•Drawbridge (with spikes)
•Protective walls, narrow stairs
•Offensive Security: Archers, Soldiers with boiling oil etc.



Defense in Depth – Information Security

Defense in depth:

- DMZ
- Firewalls + WAF
- Privileged Identity Management
- IDS / IPS
- AV & Anti-malware
- Anti-APT
- Honeypots
- Hardened Systems

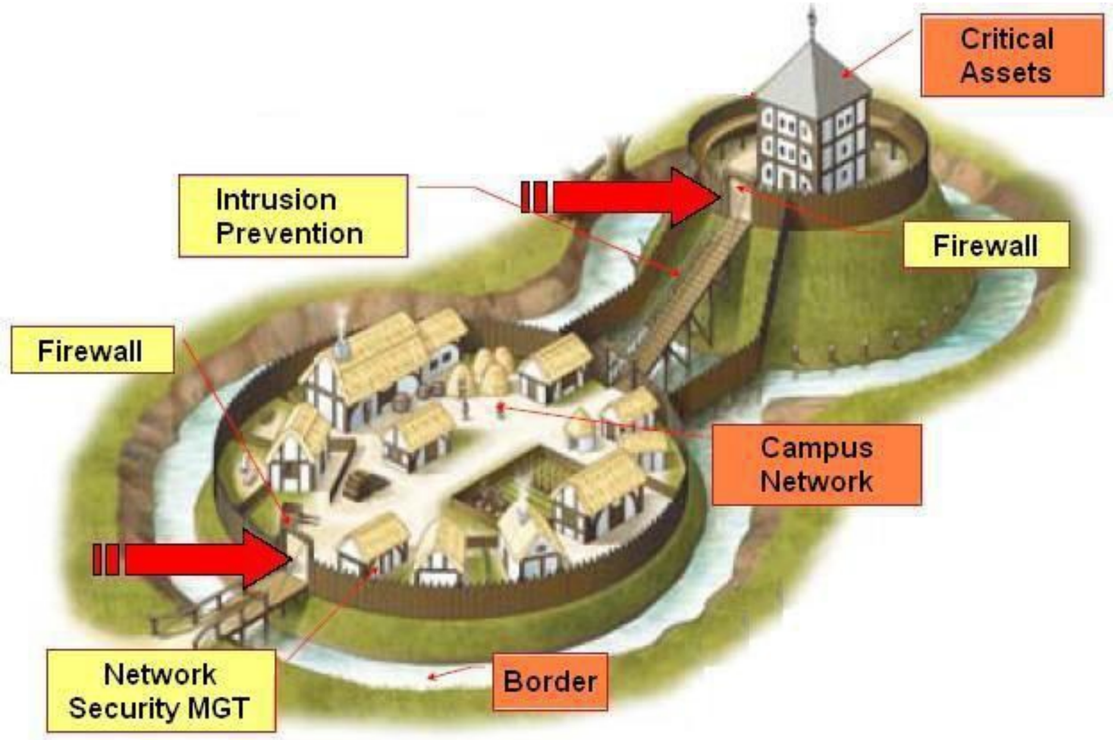


Question – Differences?

What are some of the differences when we compare classical military strategy with cybersecurity differences?

Key differences from classical military:

- Loss of strength gradient (inverse)
- Lack of counter attack / deterrents(?)
- Attribution (close to impossible)



Defense in Depth

Network Security Gateway (MGT)

- Network Security Gateway is a combination of two or more security solutions that prevents unsecured traffic from entering an internal network of an organization

Firewall (Network + WAF)

- A device that forwards packets between the less secure and more secure parts of the network, applying rules that determine which packets are allowed to pass, and which are not

Intrusion Detection & Prevention Systems (IDS / IPS)

- A security function that examines more complex traffic patterns against attack signatures/pattern, and alert administrators about an attack on the network and can prevent (IPS) the initial packet from entering the network

Honeypots

- A system designed to look like something that an intruder can hack. Normally built for many purposes, but the overriding purpose is to deceive attackers and learn their tools and methods

Hardened Systems (secured with Anti-virus & Anti-malware)

- Network devices and end points in an organization which carries the critical information and generally equipped with host based security solutions

Part II

Authentication

First Line of Defense: Authentication

Authentication is a process of **proving** you are who you claim to be.

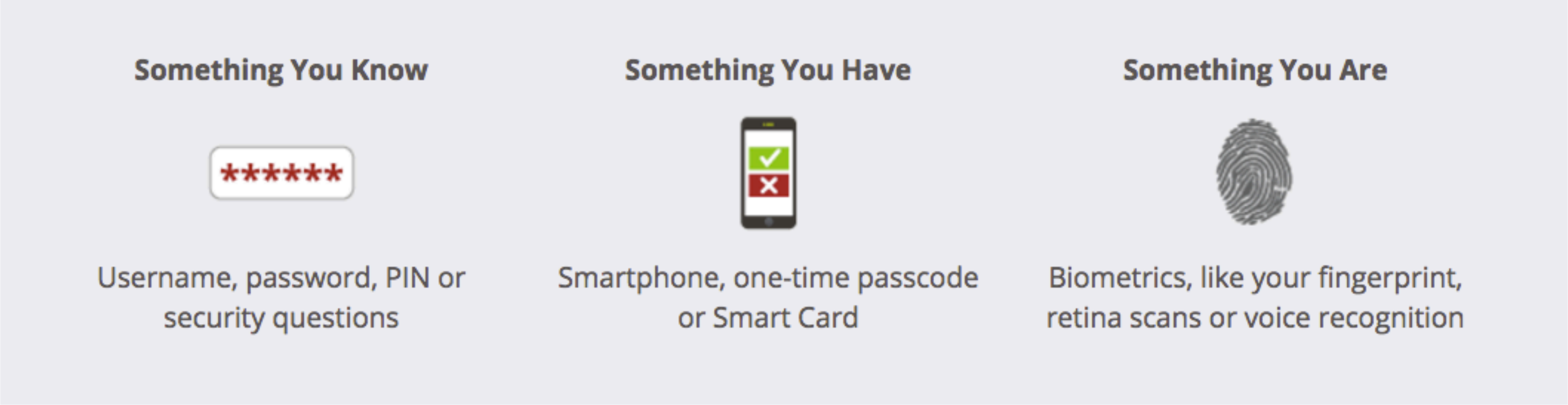
Mechanisms:

- Something you know (Passwords)
- Something you have (Tokens)
- Something you are (Biometrics)

Authentication & Authorization – Passwords

Authentication

Authentication is a process of **proving** you are who you claim to be.



Something You Know

Username, password, PIN or security questions

Something You Have

Smartphone, one-time passcode or Smart Card

Something You Are

Biometrics, like your fingerprint, retina scans or voice recognition

Source: [04/01/2019] https://blog.centrify.com/sfa-mfa-difference/

Authentication & Authorization – Passwords

What are Passwords?

A password consists of a sequence of characters or numbers or both used to verify the identity of a user in order to access various resources in a computing system, which are generally not accessible without a valid password.

Good passwords are the first line of defense against malicious attackers.

Source: [10/01/2018] https://now.avg.com/how-to-make-a-strong-password-in-3-easy-steps/

Passwords

Good passwords are the first line of defense against malicious attackers.

What makes a good password?

Authentication & Authorization – Passwords

What makes a Good Password?

It should be at least 10 characters long.

It should not contain user name, real name, institution name.

It should not contain any complete word or dictionary word.

It should contain characters from each of the following categories:

- Uppercase letters (eg. A,B,C,D)
- Lowercase letters (eg. a,b,c,d)
- Special characters (eg. @,!,#,$,*)
- Numbers (eg. 1,2,3,4,5)

Solid Password - suggestion

J&Jw^dh2fapofH2O

Jfd&bh^^&Jcta2

T2l*?Iw?Ur!

You can be innovative in making it complex – yet simple to remember !

Authentication & Authorization – Passwords

Password Security Implications

- Personal Information in Passwords
- Use of Default Passwords
- Use of Weak Passwords
- Sharing passwords with stranger
- Falling into the Phishing trap and revealing password details
- Write passwords on pieces of paper
- Repeat passwords across sites