Quiz 2

Solution

Q1: According to NIST SP 800-63-3 (*Digital Authentication Guideline*, October 2016) what is definition of user authentication

"The process of establishing confidence in user identities that are presented electronically to an information system."

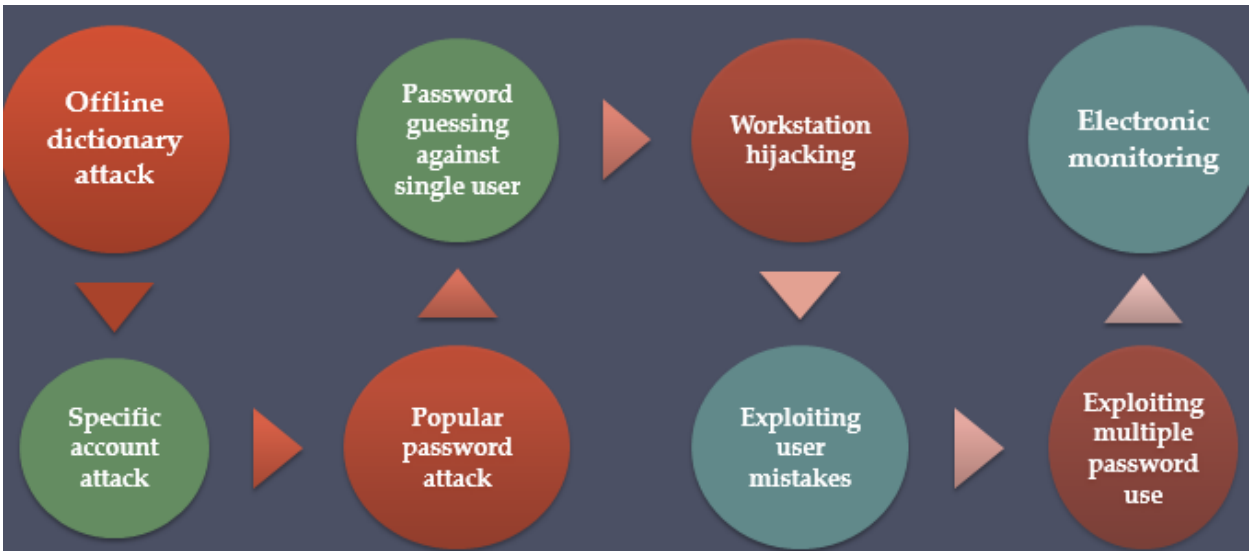
Q2: What are the two basic security requirements for user authentication explain with example

	Basic Security Requirements:
1	Identify information system users, processes acting on behalf of users, or devices.
2	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

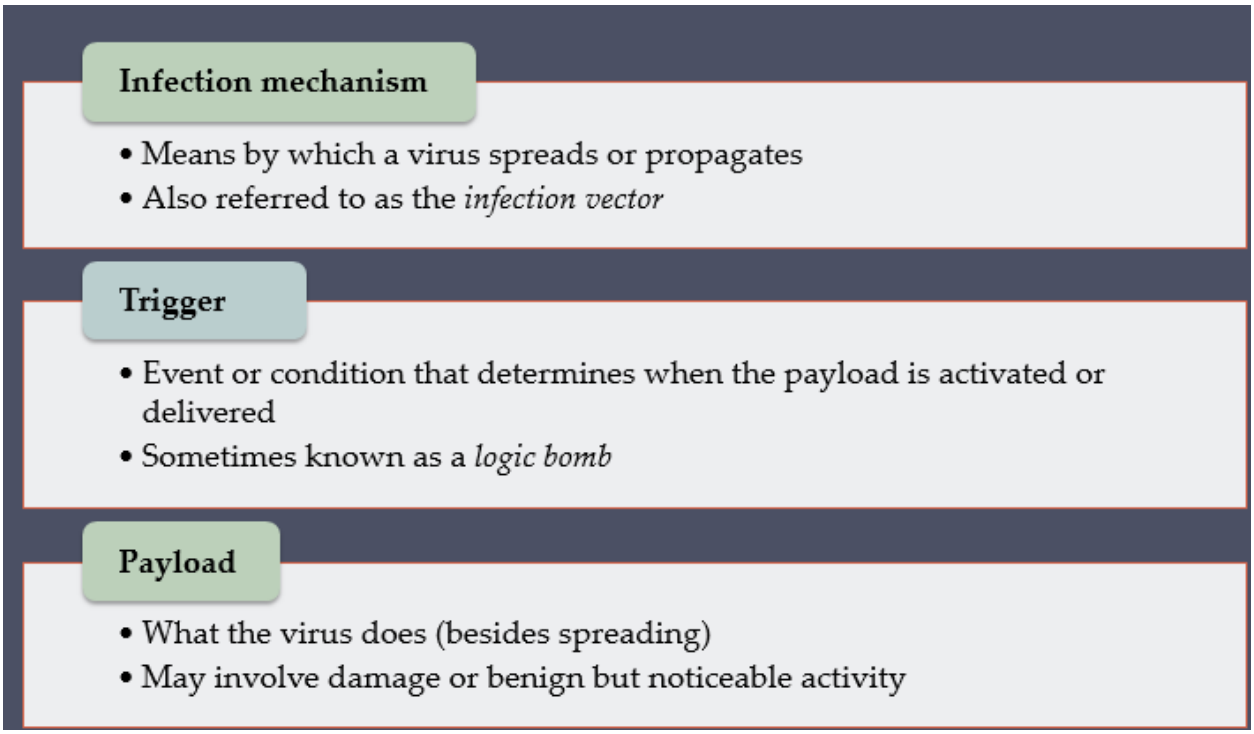
Q3: One of the four means of authenticating user identity is "Something the individual knows" Give example

PIN Numbers

Q4: List at least five password vulnerability



Q5:What are the virus component



Q6: IoT will allow self-driving vehicles to better interact with the transportation system around them through bidirectional data exchanges while also providing essential data to the riders. Self-driving cars need always-on, reliable communications and data from other transportation-related sensors to reach their full potential. Connected roadways are associated with both the driver and driverless cars fully integrating with the surrounding transportation infrastructure. Figure-1 shows a self-driving car designed by Google. Necessary sensors reside in cars already. They monitor oil pressure, tire pressure, temperature, and other operating conditions and provide data around the core car functions. From behind the steering wheel, the driver can access this data while also controlling the car using equipment such as a steering wheel, pedals, etc. The need for all this

sensory information and control is obvious. The driver must understand, handle, and make critical decisions while concentrating on driving safely. The Internet of Things is replicating this concept on a much larger scale. Today, we see automobiles produced with thousands of sensors to measure everything from fuel consumption to the location to the entertainment your family is watching during the ride. As automobile manufacturers strive to reinvent the driving experience, these sensors become IP-enabled to allow easy communication with other systems both inside and outside the car. New sensors and communication technologies are being developed to let vehicles "talk" to other cars, traffic signals, school zones, and other transportation infrastructure elements. We are now starting to realize a truly connected transportation solution.

What are the current security challenges being address in the Upper user case .Explain it with some supportive examples

Challenge	Description	IoT Architectural Change Required
Devices and networks constrained by power, CPU, memory, and link speed	Due to the massive scale and longer distances, the networks are often constrained, lossy, and capable of supporting only minimal data rates (tens of bps to hundreds of Kbps).	New last-mile wireless technologies are needed to support constrained IoT devices over long distances. The network is also constrained, meaning modifications need to be made to traditional network-layer transport mechanisms.
The massive volume of data generated	The sensors generate a massive amount of data on a daily basis, causing network bottlenecks and slow analytics in the cloud.	Data analytics capabilities need to be distributed throughout the IoT network, from the edge to the cloud. In traditional IT networks, analytics and applications typically run only in the cloud.
Support for legacy devices	An IoT network often comprises a collection of modern, IP-capable endpoints as well as legacy, non-IP devices that rely on serial or proprietary protocols.	Digital transformation is a long process that may take many years, and IoT networks need to support protocol translation and/or tunneling mechanisms to support legacy protocols over standards-based protocols, such as Ethernet and IP.
The need for data to be analyzed in real time	Whereas traditional IT networks perform scheduled batch processing of data, IoT data needs to be analyzed and responded to in real-time.	Analytics software needs to be positioned closer to the edge and should support real-time streaming analytics. Traditional IT analytics software (such as relational databases or even Hadoop), are better suited to batch-level analytics that occur after the fact.