أمن تكنولوجيا المعلومات وإدارة المخاطر

IT Security and Risk Management

Secure Design and implementation

ا.د. حنان الطاهر الداقيز

h.dagez@uot.edu.ly

خريف 2023

https://t.me/+1iMQn29WU0o0Zjc8

What is VPN security ?

VPN stands for "**Virtual Private Network**" and describes the opportunity to establish a protected network connection when using public networks. VPNs encrypt the bath in internet traffic and the online identity. This makes it more difficult for third parties to track your activities online and steal data. The encryption takes place in **real time**.

Why VPNs?

- How can you connect two networks in geographically separate locations without installing a private connection between them?
- How can you provide remote services to allow users to access corporate services that need to remain protected from the prying eyes of the public Internet?

The answer to both questions is to use a virtual private network (VPN)

Benefits of VPNs ?

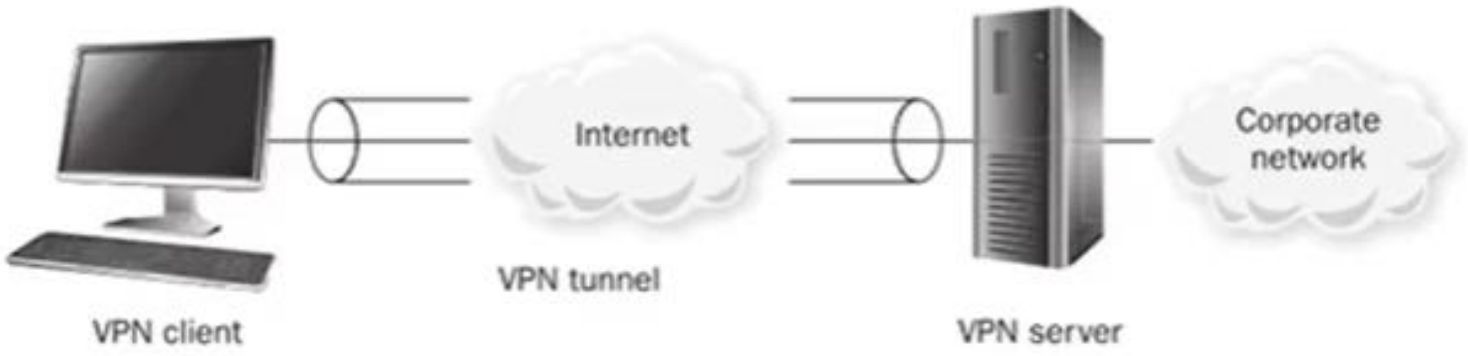
- Benefits of VPNs
  1. Encrypting your web activity.
  2. Hiding your physical location.
  3. Securing the personal information you send and receive while on public Wi-Fi.
  4. Protecting your online data from being used to make you vulnerable to spear-phishing.
  5. Bypass blocking of websites, apps, or services on the Internet.

VPNs security

- VPNs provide virtual network links based on encrypting and isolating traffic at the packet level while using Internet services for transport.
- The two most common uses of VPN are to link branch offices or remote sites together (called LAN-to-LAN tunneling, or L2L) and to provide remote access to office environments (called remote access [RA] VPN).
- L2L tunnels are used widely for private communications between corporate networks and other trusted networks, which could be remote offices or other corporate-controlled networks, or third parties (example, for outsourcing or business-to-business [B2B] data exchange).

How VPNs work?

- The goal of a VPN is to provide a secured communication channel through a network, most commonly a private tunnel through the Internet.
- To do this, the traffic is encapsulated with a header that provides routing information that helps the traffic get to the destination.
- The traffic is also encrypted, which provides integrity, confidentiality, and authenticity.



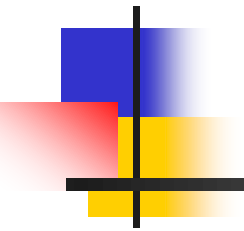
A VPN is referred to as a *tunnel* because the client does not know or care about the actual path between the two endpoints.

VPNs vs Proxy

When comparing proxy vs. VPN capabilities, the difference is that proxies strictly act as a gateway between the internet and users. On the other hand, VPN traffic runs through an encrypted tunnel and the user's device, making VPNs an effective solution for ensuring network security.

- A VPN and Proxy server both mask your IP address.
- VPN encrypt the data you send and receive, something that a proxy server doesn’t do.

So, do you need a proxy if you have a VPN?



Secure Application Design

Important Security Consideration

- Potential security issues and how to solve them are very important for:
  - Development cycle of web applications,
  - Client applications, and
  - Remote administration.
- After an application is written, it is deployed into an environment of some sort, where it remains for an extended period of time with only its original features to defend it from threats, mistakes, or misuse.

Important Security Consideration ..

- A malicious agent in the environment has that same extended period of time to observe the application and tailor its attack techniques until something works.
- At this point, any number of undesirable things could happen such as breach, vulnerability disclosure, or malware exploiting the vulnerability.
- Most of these undesirable things eventually lead to customers who are unhappy with their software vendors, regardless of whether or not the customers were willing to pay for security before the incident occurred.

Important Security Consideration ..

- For that reason, security is becoming more important to organizations that produce software, and building security into the software up front is easier (and cheaper) than waiting until the software is already out in the field and then providing security updates.
- While the deployment environment can help protect the application to some extent, every application must be secure enough to protect itself from whatever meaningful attacks the deployment environment cannot prevent, for long enough for the operator to notice and respond to attacks in progress.

Important Security Consideration ..

- Application security needs to be done right from the start because it's much harder to actively fix security problems in the field than it is to do so in the programmer's chair.
- Training, corporate standards, reviews at the design phase, and formal code reviews can all help ensure that security is integrated from the beginning of any new application.
- Every programmer who isn't focused on security when writing an application, whether web-based or client, can leave the application vulnerable to outside attackers.
- Because application security problems primarily result from human errors and omissions (on the part of the programmers), the best solution is education.
- To produce an application that is secure enough, define **"secure enough"** near the beginning of the development process.

Secure Software Development Lifecycle

- A Secure Software Development Lifecycle (SSDL) is essentially a development process that includes security practices and decision making inputs.
- In some cases, an SSDL is a stand-alone process, but most organizations find that altering their existing practices and processes is easier and more efficient than creating and managing an additional, separate process.
- Typical SSDL affects two to three lifecycles:
  - **The application lifecycle,** in which an application begins as an idea and then is planned, designed, developed, tested, documented (hopefully), released, sometimes deployed and operated, maintained, and eventually "end-of-lifed".
  - **The employee lifecycle,** in which an employee is selected, hired, brought on board, changes job responsibilities, and eventually leaves the organization.
  - **The project or contract lifecycle,** if any development is outsourced, in which a contract is negotiated, results are accepted, and vendors are paid.

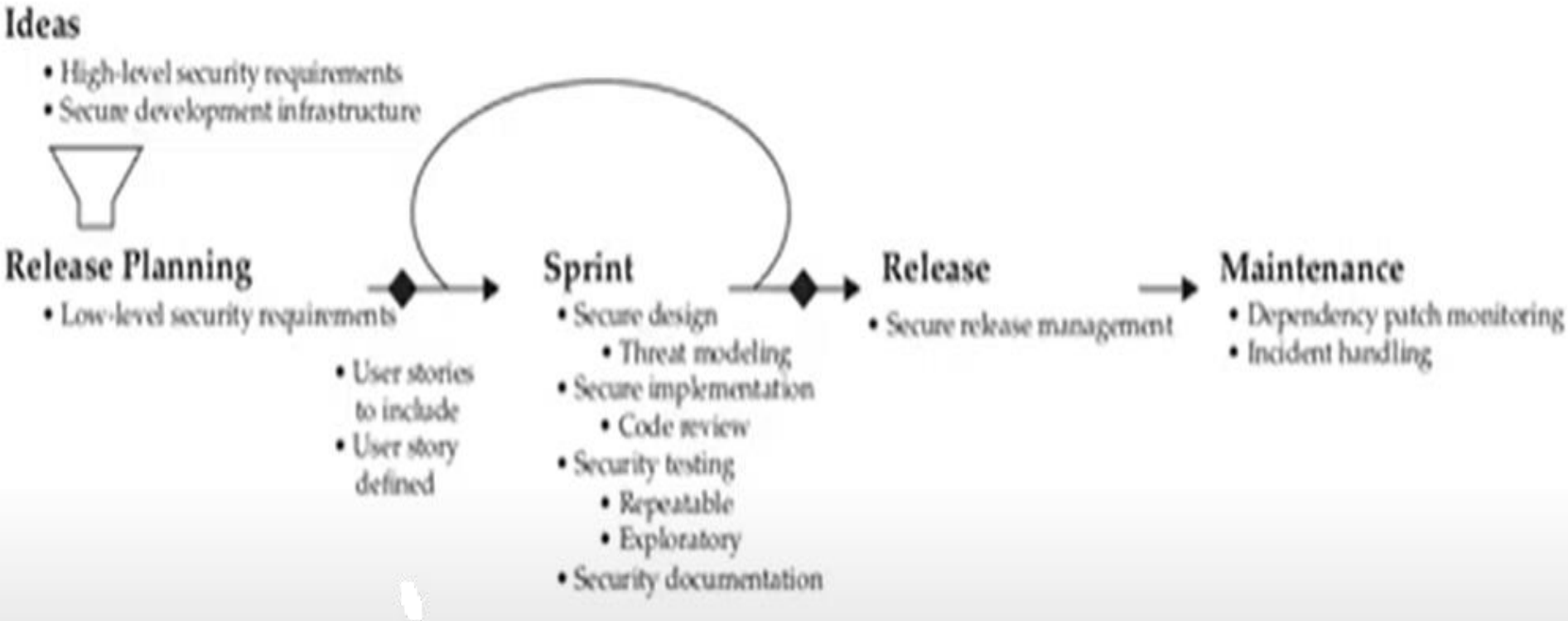
Secure Software Development Lifecycle ..

- The SSDL itself is created, operated, measured, and changed over time following a business process lifecycle.
- Sometimes people call the process of developing and maintaining an SSDL and other application security activities an application security assurance program.
- Typically, an SSDL contains three primary elements:
  - **Security activities** that don't exist at all in the original lifecycle; for instance, threat modeling.
  - **Security modifications** to existing activities; for instance, adding security checks to existing peer reviews of code.
  - **Security criteria** that should affect existing decisions; for instance, the number of open high-severity security issues when a decision to ship is made.

Secure Software Development Lifecycle ..

- Like any other quality, adding security is cheapest if it is included from the beginning of the lifecycle.
- Like other bugs, security vulnerabilities are less expensive to fix the earlier they are resolved, and the cheapest thing to do is to avoid inserting bugs at all.
- The pre-ship activities in an SSDL usually focus on either preventing security bugs in each development deliverable or detecting security bugs in a deliverable that was just produced.
- **Waterfall SDLs** frequently involve a security reviewer from outside the team, who must approve the application at different points in the process.
- **Agile SDLs** frequently provide access to security coaches from outside the team, so that the team has someone to consult when they need security help.

Secure Development Lifecycle ..



Thank you