Web Security Model

Presented by :

Parv Bharti
Priya Sharma
Pranav Saxena
Sudhanshu Goel
Deepak SIngh Rawat

What is Web Security ?

- **Web security**, also known as ‘Cyber security’, involves protecting website or web application by detecting, preventing and responding to attacks.

- Most businesses that have made the move towards an online presence have experienced some kind of security threat to their business. Since the Internet is a public system in which every transaction can be tracked, logged, monitored and stored in many locations.

Security Threats

- *Unauthorized internal users* who accesses confidential information by using a stolen passwords for the purpose of committing fraud or theft.
- *Former employees of an organization* that maintain access to information resources directly by creating alternative passwords, "back doors into the computer system, or indirectly through former co-workers.
- *Weak access points* in information infrastructure and security that can expose company information and trade secrets.
- *Management* that undermines security is maybe the greatest risk to e-commerce.

Security Main Concepts

- Confidentiality : It allows only authorized parties to read protected information.

- Integrity : It ensures that the data remains as is from the sender to the receiver.

- Availability : It ensures you have access and are authorized to the resources.

Security Features

AUTHENTICATION

- Ensures individual is who he/she claims to be.
- Enforces only user to be allowed to have access of his/her resources.
- Implemented by passwords, biometrics, etc.

AUTHORISATION

- Process of giving individuals access to system objects based on their identity.
- Only authorised user can manipulate his/her resources.
- Implemented by Access Control List (ACL).

Security Features

ENCRYPTION

- Deals with information hiding.
- Translation of data in secret code (cypher text).
- Cypher text is used for communication instead of plain text.
- Increases confidentiality.

AUDITING

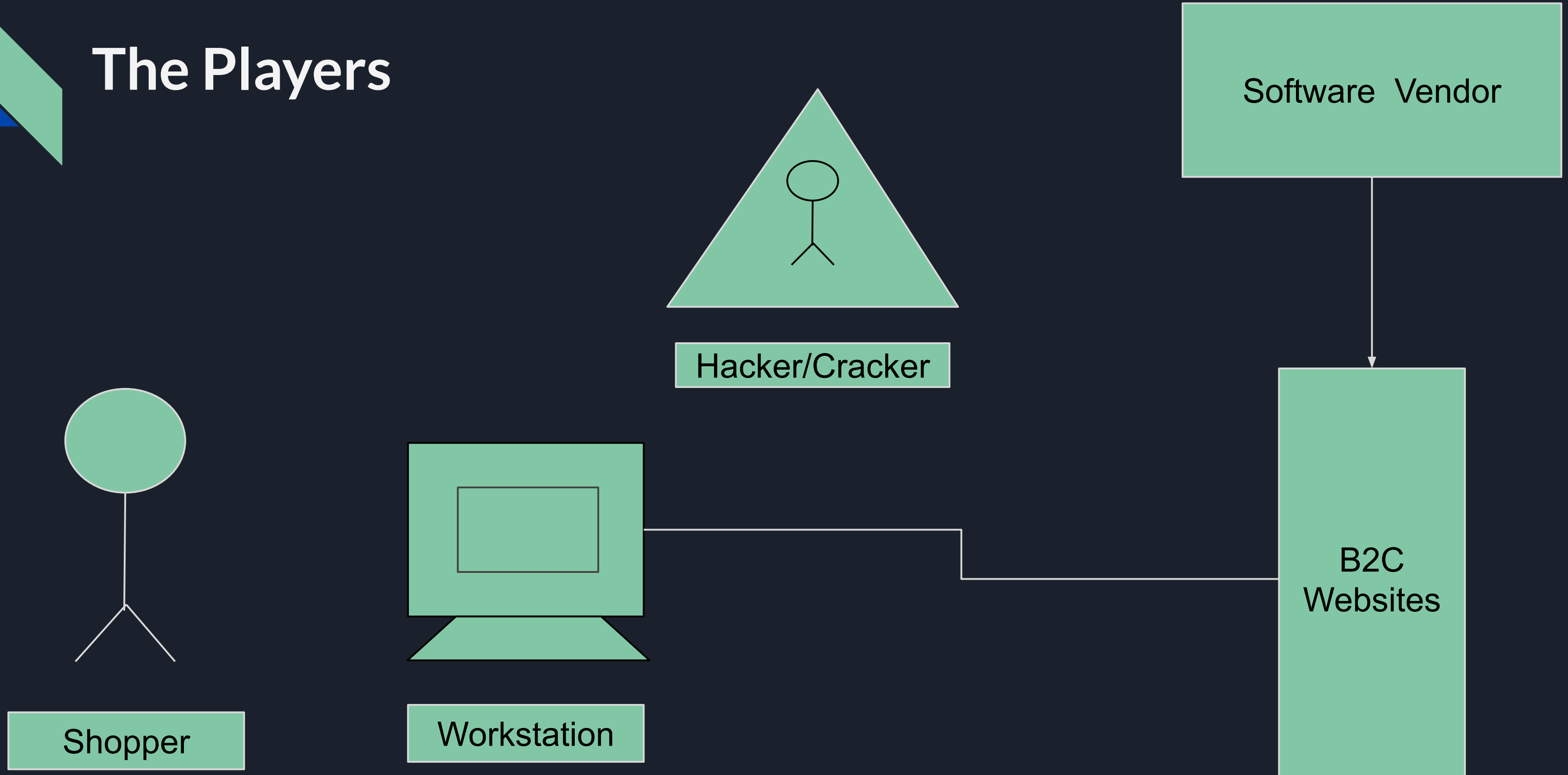
- Systematic and independent evaluation of company’s security systems.
- Accesses security of softwares, information handling processes and user practices.
- Measures how well it conforms to a set of established criteria.

Case Study : E-Commerce Website

- In a typical e-Commerce experience, a shopper proceeds to a Website to browse a catalog and make purchase.
- This simple actively illustrates the four major players in e-Commerce security :-

1. Shoppers
2. Merchants
3. Software vendors
4. Attackers

The Players

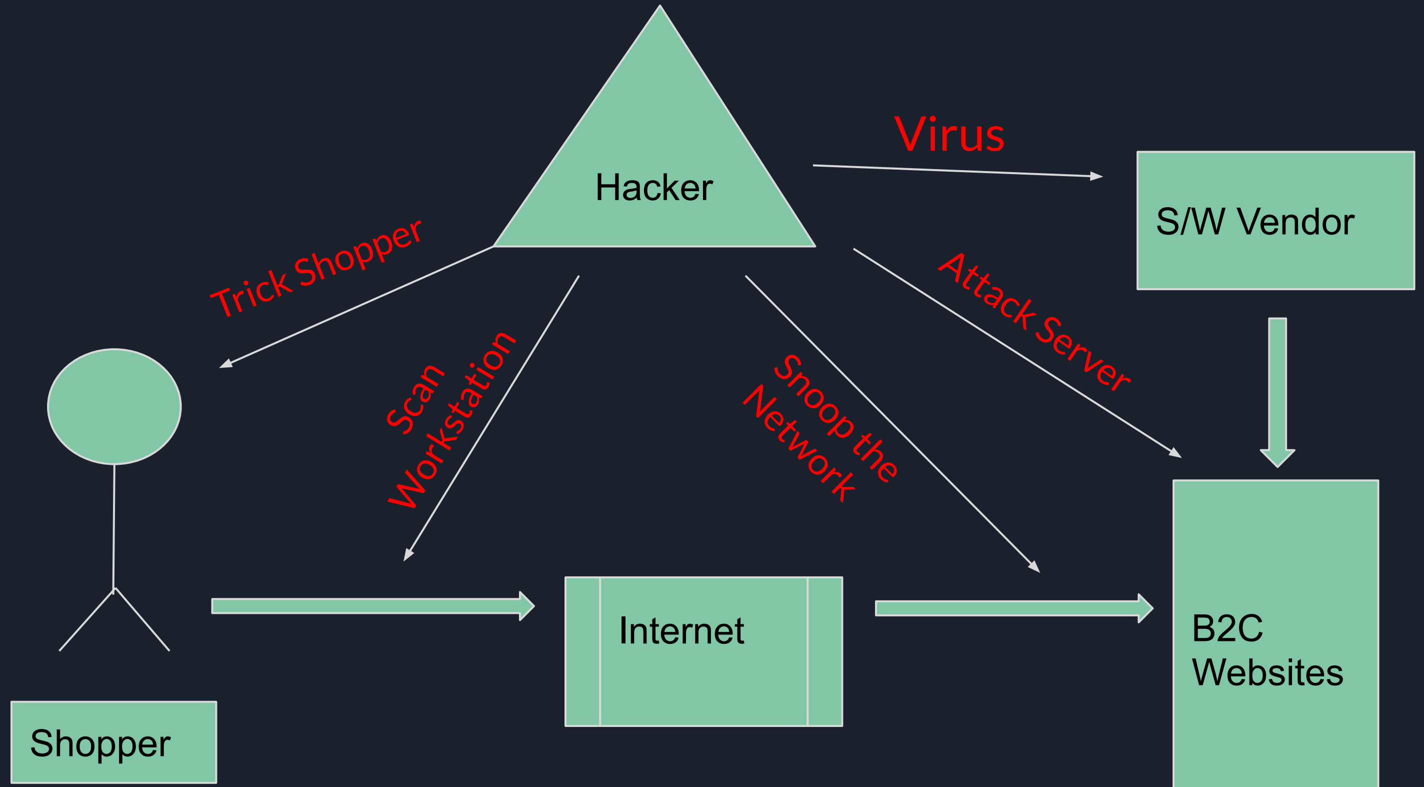


Software Vendor
Hacker/Cracker
Shopper
Workstation
B2C Websites

Criminal Incentive

- Cheap Tools
- Unimaginable Payoff
- Easy to locate the victim
- Anonymous
- Free and Easy Availability of Information

Points The Attacker can Target



ATTACKS

A. TRICKING THE SHOPPER - Some of the easiest and most profitable attacks are based on the shopper, also known as social engineering techniques.

a.) Gathering Information -These attacks involve surveillance of the shopper's behavior, gathering information to use against the shopper

b.)Phishing-Typo pirates play on the names of famous sites to collect authentication and registration information. For example, http://www.ibm.com/shop is registered by the attacker as www.ibn.com/shop

B. SNOOPING THE SHOPPER'S COMPUTER -Software and hardware vendors, in their quest to ensure that their products are easy to install, will ship products with security features disabled.

A popular technique for gaining entry into the shopper's system is to use a tool, such as SATAN, m for personal information, such as passwords.

C. SNIFFING THE NETWORK - In this scheme, the attacker monitors the data between the shopper's computer and the server. He collects data about the shopper or steals personal information, such as credit card numbers.

D. GUESSING PASSWORDS- Another common attack is to guess a user's password. This style of attack is manual or automated. Manual attacks are laborious, and only successful if the attacker knows something about the shopper.
Automated attacks have a higher likelihood of because the probability of guessing a user ID/password becomes more significant as the number of tries increases.

E. USING OF DENIAL OF SERVICE ATTACKS-

a.) The denial of service attack is one of the best examples of impacting site availability. It involves getting the server to perform a large number of mundane tasks, exceeding the capacity of the server to cope with any other task.

b.) Distributed DoS is a type of attack used on popular sites, such as Yahoo!. In this type of attack, the hacker infects computers on the Internet via a virus or other means. The infected computer becomes slaves to the hacker.

CONCLUSION

Current technology allows for secure site design. It is up to the development team to be both proactive and reactive in handling security threats, and up to the shopper to be vigilant when shopping online.

THANK YOU