CHAPTER 2

CONTROL, AUDIT AND SECURITY OF INFORMATION SYSTEM

TOPICS TO COVER

CONTROL, AUDIT AND SECURITY OF INFORMATION SYSTEM (5 HOURS)

- **Control of information system**
- **Audit of information system**
- **Security of information system**
- **Consumer layered security strategy**
- **Enterprise layered security strategy**
- **Extended validation and SSL certificate**
- **Remote access authentication**
- **Content control and policy based encryption**
- **Example of security in e-Commerce transaction**

2.1 Control of Information System

- Methods, policies, and procedures
- Ensure protection of organization's assets, accuracy and reliability of records
- Protection of information resources requires a well-designed set of controls.
- Computer systems are controlled by a combination of : **general controls and application controls.**

General Controls

General controls include software controls, physical hardware controls, computer operations controls, data security controls, controls over the systems implementation process.

- **Software controls**
- **Hardware controls**
- **Data security controls**
- I**mplementation controls:** Audit the systems development process at various points to ensure that the process is properly controlled and managed.
- **Administrative controls:** ensure that the organization's general and application controls are properly executed and enforced.

Application Controls

- Application controls include both automated and manual procedures that ensure that **only authorized data are completely and accurately processed by that application.**
- Application controls can be classified as (1) input controls, (2) processing controls, and (3) output controls.
- **Input controls** check data for accuracy and completeness when they enter the system.
- **Processing controls** establish that data are complete and accurate during updating.
- **Output controls** ensure that the results of computer processing are accurate, complete, and properly distributed.

DIGITAL FIRM

- "*A digital firm is one in which nearly all of the organization's significant business relationships with customers, suppliers, and employees are digitally enabled, and key corporate assets are managed through digital means.*"
- Some examples of these technology platforms are :

  Customer Relationship Management (CRM),

  Supply Chain Management (SCM),

  Enterprise Resource Planning (ERP)

Protecting the Digital Firm

- **High-availability computing:** Tools and technologies enabling system to recover from a crash
- **Disaster recovery plan**
- **Load balancing:** Distributes large number of requests for access among multiple servers
- **Mirroring:** Duplicating all processes and transactions of server on backup server to prevent any interruption
- **Clustering:** Linking two computers together so that a second computer can act as a backup to the primary computer or speed up processing

2.2 Audit of information system

- WHAT IS AUDIT?
- The information system audit is conducted to evaluate the information systems
- and suggest measures to improve their value to the business.
- used as an effective tool for evaluation of the information system and controlling the computer abuse.
- Information system audit is carried out by professionals who are not only well versed with the complex information system issues but also know how to relate them to the business.

Process of information system audit

Process of information system audit involves four steps:

- **Measuring vulnerability of information system:**

The first step in the process of information system audit is the identification of the vulnerability of each application.

Where the probability of computer abuse is high, there is a greater need for an information system audit of that application.

- **Identification of sources of threat:**

Most of the threats of computer abuse are from the people. The information system auditor should identify the people who might pose a threat to the information systems.

These people include system analysts, programmers, data entry operators, data providers, users, vendors of hardware, software and services, computer security specialists, PC users, etc.

- **Identification of high risk points:**
  - The next step in the process of information system audit is to identify the occasions, points or events when the information system may be attacked . These points may be when a transaction is added, altered or deleted.
- **Check for computer abuse:**
  - The last step in the process is to conduct the audit of high potential points keeping the view the activities of the people who could abuse the information system for the applications that are highly vulnerable.

Information System Auditors

- **information systems auditor**, is a professional involved in examination of the management controls within an Information technology (IT) infrastructure and business applications.
-
- The evaluation of evidence obtained determines if the information systems are safeguarding assets, maintaining data integrity, and operating effectively to achieve the organization's goals or objectives.

2.3. Security of information system

- Security means protection of data from accidental or intentional modification, destruction or disclosure to unauthorized persons.
- Information systems security, more commonly referred to as **INFOSEC**, refers to the processes and methodologies involved with keeping information confidential, available, and assuring its integrity.
- It also refers to:
  - Access controls, which prevent unauthorized personnel from entering or accessing a system.
  - Protecting information, no matter where that information is, i.e. in transit (such as in an email) or in a storage area.
  - The detection and remediation of security breaches, as well as documenting those events.

THE INFORMATION SECURITY TRIAD: CONFIDENTIALITY, INTEGRITY, AVAILABILITY

Tools for Information Security

- AUTHENTICATION
- ACCESS CONTROL
- ENCRYPTION

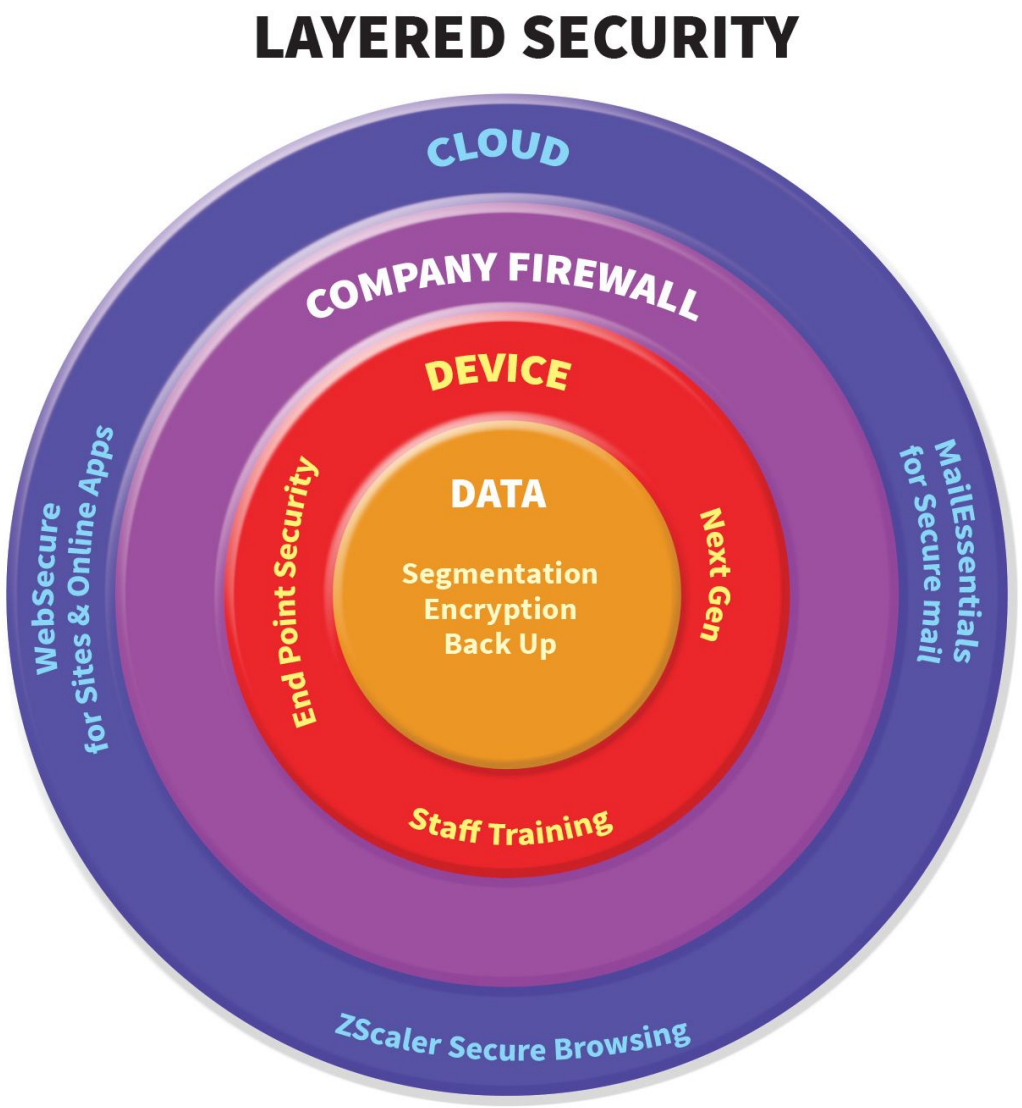
Potential Threats to Security

- Natural disasters such as fire, floods, earthquakes.
- Accidents such as disk crashes, file erasure by inexperienced operators.
- Theft/erasure of data by disgruntled employees.
- Frauds by changing programs, data by employees.
- Industrial espionage.
- Viruses/Worms.
- Hackers who break into systems connected to the internet.
- Denial of service attacks by flooding with mail.

How to Protect Data/programs?

- Regular back up of data bases every day/or week depending on the time criticality and size.
- Incremental back up at shorter intervals.
- Backup copies kept in safe remote location-particularly necessary for disaster recovery.
- Duplicate systems and transactions mirrored
- Physical locks.

- Password system.
- Biometric authentication (e.g. Finger print).
- Encrypting sensitive data/programs.
- Identification of all persons who read or modify data and logging it in a file.
- Training employees on data care/handling and security.
- Antivirus software.
- Firewall protection when connected to internet.



LAYERED SECURITY

- **layered security** is the practice of using many different **security** controls at different levels to protect assets.
- This provides strength and depth to reduce the effects of a threat.
- Your goal is to create redundancies (backups) in case **security** measures fail, are bypassed, or defeated.
- Layered security may also be known as layered defense.

Defense in Depth

- is based on a slightly different idea where multiple strategies and resources are used to slow, block, delay or hinder a threat until it can be completely neutralized.

2.4.CONSUMER LAYERED SECURITY STRATEGIES

Providing layered security to Consumer

- **Backup:** Consider where you would be if your layered security strategy failed. If you've ever lost critical data to a malware infection
- Free backup utilities are readily available
- **Firewall** – is an application designed to block unauthorized access to your computer from the Internet, at the same time permitting authorized communications.

- **Antivirus** – An antivirus application is another critical component in a layered defense strategy to ensure that if a malicious program is detected, it will be stopped dead in its tracks!
- **Web Browser Security** – Install a free Internet Browser add-on such as WOT(Web of Trust). WOT tests web sites you are visiting for spyware, spam, viruses, browser exploits, unreliable online shops, phishing, and online scams, helping you avoid unsafe web sites.

Consumer Layered Security Strategy

- Extended validation (EV) SSL certificates
- Multifactor authentication
- Single sign-on (SSO):enables users to securely authenticate with multiple applications and websites by logging in only once—with just one set of credentials (username and password).
- Fraud detection and risk-based authentication
- Encryption
- Secure Web and e-mail

2.5.ENTERPRISE LAYERED SECURITY STRATEGIES

- •A modern enterprise security strategy uses a layered identity approach as the underpinning of its security.
- •All enterprise systems, applications, information systems, facilities, buildings and rooms are assigned as enterprise risk.
- •As the user digitally or physically approaches higher risk applications or a physical location the stronger authentication is used.
- •As consider the enterprise firewall and the use of Id and passwords for login.

Implementing a Layered Identity Strategy: Enterprise Layered

- •This could take the form of **digital certificates, security tokens, smart cards and biometrics.** It could also take the form of transactional security.
- •The user may successfully use their **Id and password**,
- the transaction security software would examine the IP address that the user is coming in from, their geographic position, the time of day, the type of physical computer the user is using and their **behavioral pattern.**
- •If any of these differ from the past, then system alarm bells may start ringing resulting in the user being asked more personal questions, the action being stopped.

- ***NOTE: A security token is a portable device that authenticates a person's identity electronically by storing some sort of personal information. The owner plugs the security token into a system to grant access to a network service.***

Enterprise Layered Security Strategy

- Workstation application listing
- Workstation system restore solution
- Workstation and network authentication
- File, disk and removable media encryption
- Remote access authentication
- Network folder encryption
- Content control and policy-based encryption

SSL CERTIFICATE

- SSL stands for Secure Socket Layer.
- It is the standard security technology for establishing an encrypted link between a web server and a browser.
- This link ensures that all data passed between the web server and browsers remain private and integral.
- To be able to create an SSL connection a web server requires an SSL Certificate.

- SSL Certificates are small data files that digitally bind a cryptographic key to an organization's details.
- When installed on a web server, it activates the padlock and the https protocol (over port 443) and allows secure connections from a web server to a browser.
- Typically, SSL is used to secure credit card transactions, data transfer and logins, and more recently is becoming the norm when securing browsing of social media sites.

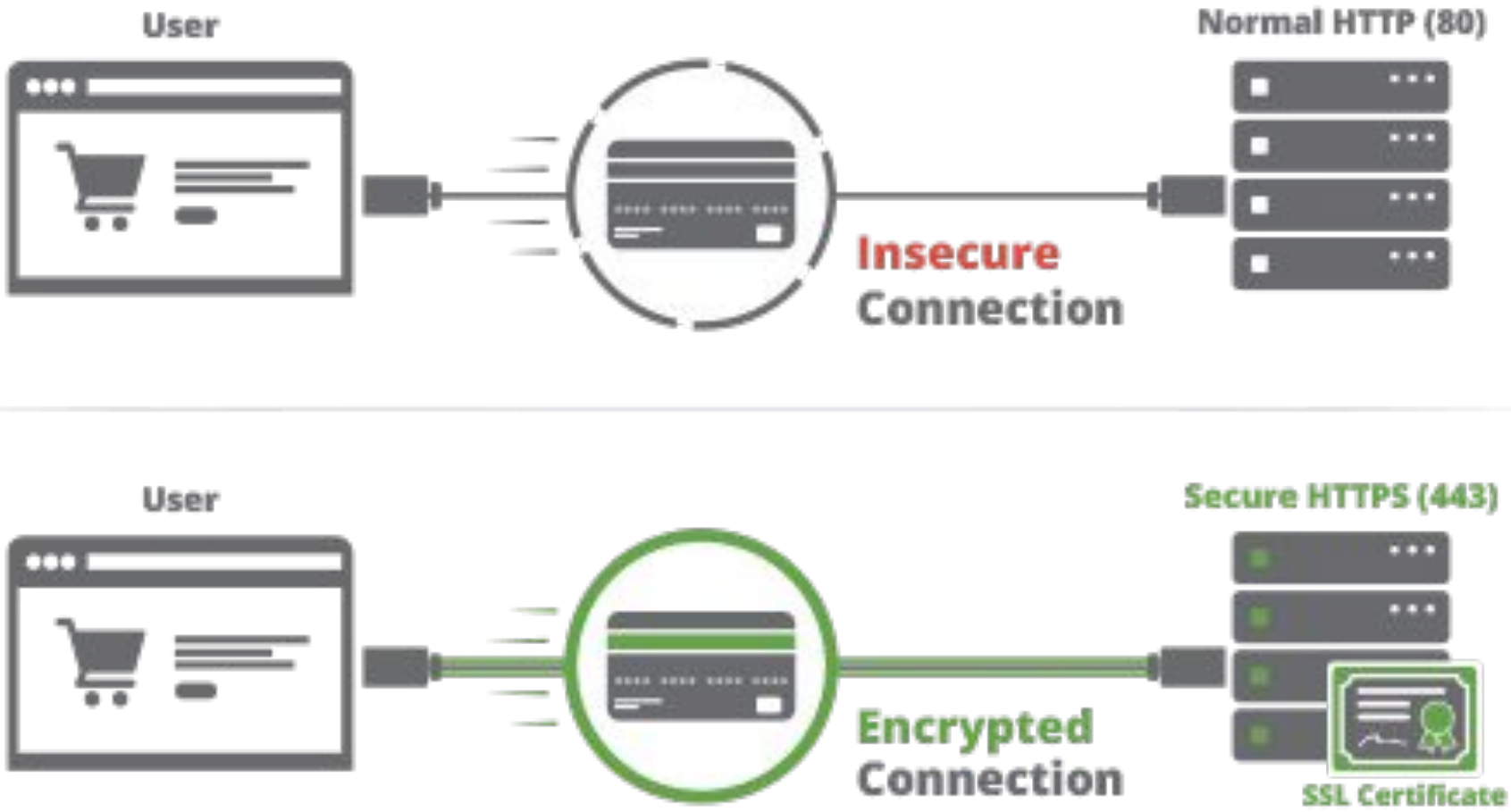
SSL Certificates Binds together:

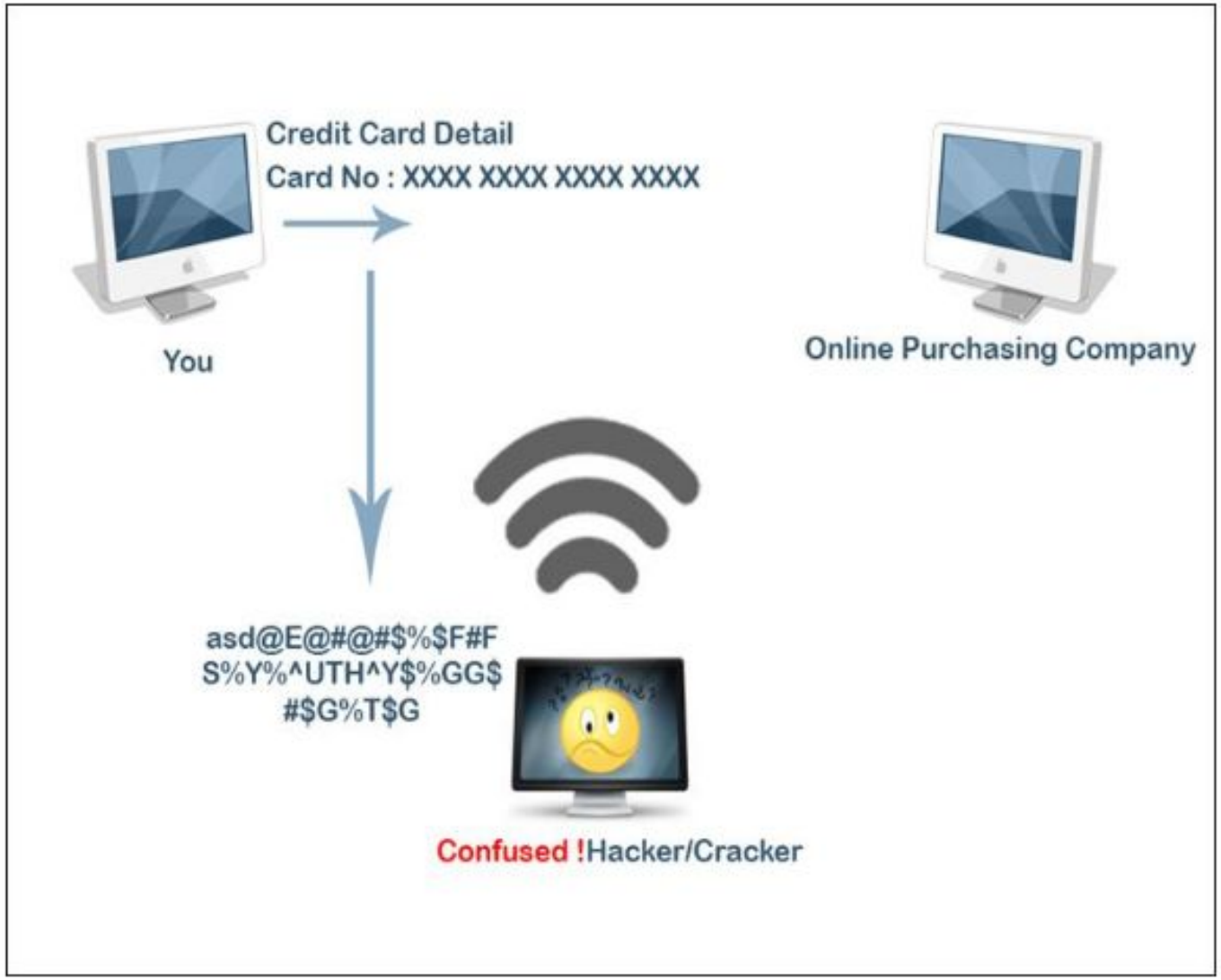
- A domain name, server name or hostname.
- An organizational identity (i.e. company name) and location.
- An organization needs to install the SSL Certificate onto its web server to initiate secure sessions with browsers.

Stages for acquiring SSL Certificate

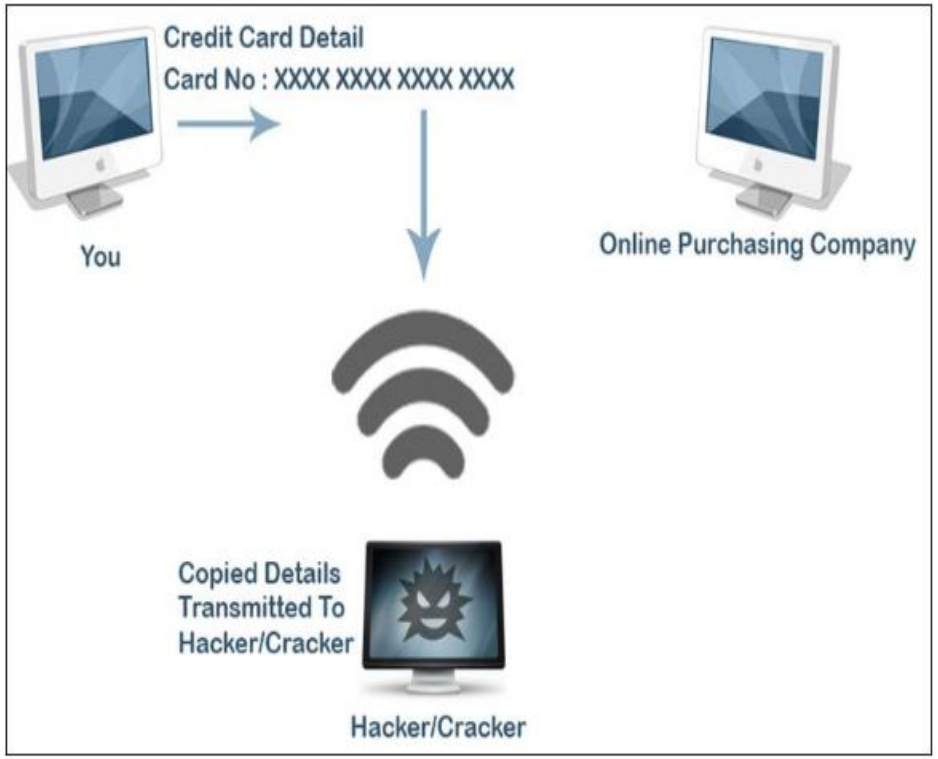
- Depending on the type of SSL Certificate applied for, the organization will need to go through differing levels of examination.
- Once installed, it is possible to connect to the website over https://www.domain.com, as this tells the server to establish a secure connection with the browser.
- Once a secure connection is established, all web traffic between the web server and the web browser will be secure.

HTTP vs HTTPS




Credit Card Detail
Card No : XXXX XXXX XXXX XXXX
You
Online Purchasing Company
asd@E@#@#$%$F#F
S%Y%^UTH^Y$%GG$
#$G%T$G
Confused !Hacker/Cracker

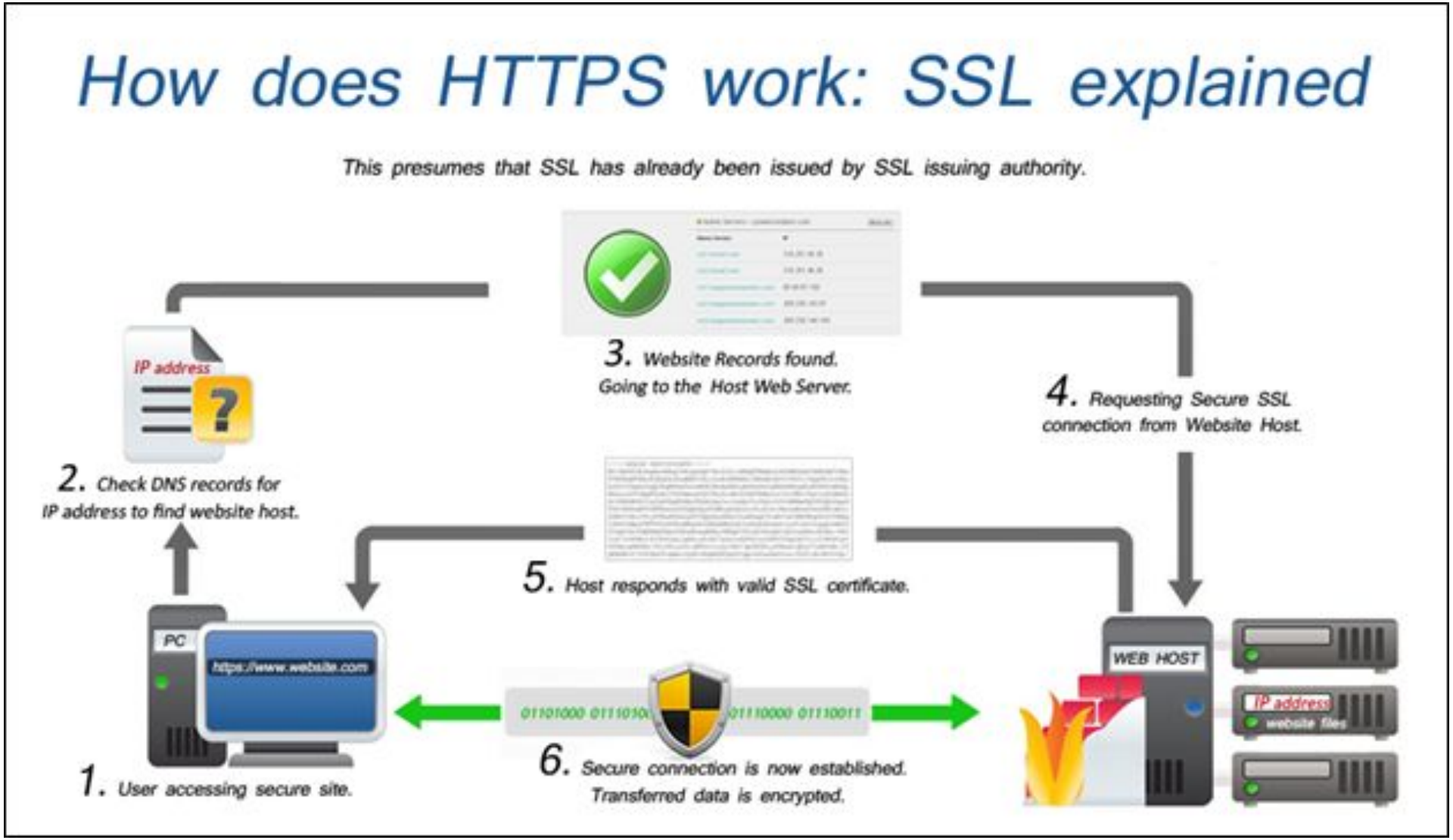

Credit Card Detail
Card No : XXXX XXXX XXXX XXXX
You
Online Purchasing Company


Credit Card Detail
Card No : XXXX XXXX XXXX XXXX
You
Online Purchasing Company
Copied Details
Transmitted To
Hacker/Cracker
Hacker/Cracker

SSL DOC ….go through this article

- https://resources.infosecinstitute.com/ssl-unleashed/#gref

How does HTTPS work: SSL explained



Types of SSL Certificates

- **OV(Organization Validation) SSL Certificates:** This process assures the validity of a Web site by verifying that the applicant is a legitimate business.
- Before issuing the SSL certificate, the CA performs a rigorous validation procedure, including checking the applicant's business credentials (such as the Articles of Incorporation) and verifying the accuracy of its physical and Web addresses.

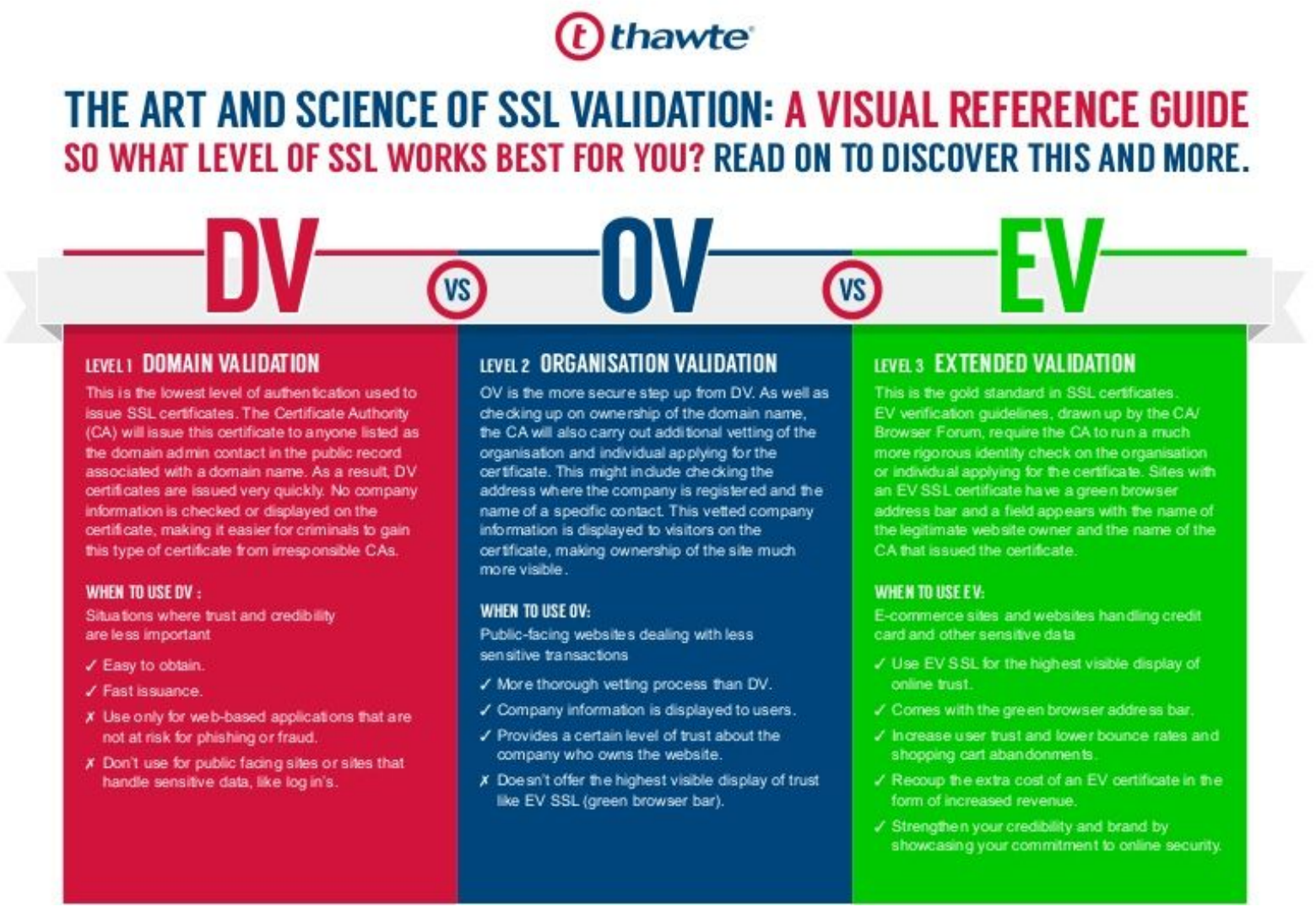
- ■**DV (Domain Validation)SSL Certificates:** The validation procedure is less rigorous for a Domain Validated SSL Certificate.

- When issuing a Domain Validated SSL Certificate, the CA checks only that the applicant's name and contact information matches the registration information in the WHOIS database for the domain name associated with the applied for SSL Certificate.

- ■**EV (Extended Validation)SSL Certificates:** The Certificate application process itself is more thorough and the validation criteria more rigorous for EV certification, whose applicants, at least initially, are limited to certain types of business entities and government agencies.


DV
certificates
Secure
https://yourdomain.com
OV
certificates
Secure
https://yourdomain.com
EV
certificates
Company Name [GB]
https://yourdomain.com

Cert type:	Best for:
DV	Running your own web server for your own personal use Web services (computer talking to internal computer) Development and testing Internal company websites
OV	Small business “brochure ware” website Web services (computer talking to external computer) Blog
EV	E-commerce Banking Medical / highly sensitive information Sites susceptible to phishing


thawte
THE ART AND SCIENCE OF SSL VALIDATION: A VISUAL REFERENCE GUIDE
SO WHAT LEVEL OF SSL WORKS BEST FOR YOU? READ ON TO DISCOVER THIS AND MORE.
DV
VS
OV
VS
EV
LEVEL 1 DOMAIN VALIDATION
This is the lowest level of authentication used to issue SSL certificates. The Certificate Authority (CA) will issue this certificate to anyone listed as the domain admin contact in the public record associated with a domain name. As a result, DV certificates are issued very quickly. No company information is checked or displayed on the certificate, making it easier for criminals to gain this type of certificate from irresponsible CAs.
WHEN TO USE DV :
Situations where trust and credibility are less important
✓ Easy to obtain.
✓ Fast issuance.
✗ Use only for web-based applications that are not at risk for phishing or fraud.
✗ Don't use for public facing sites or sites that handle sensitive data, like log in's.
LEVEL 2 ORGANISATION VALIDATION
OV is the more secure step up from DV. As well as checking up on ownership of the domain name, the CA will also carry out additional vetting of the organisation and individual applying for the certificate. This might include checking the address where the company is registered and the name of a specific contact. This vetted company information is displayed to visitors on the certificate, making ownership of the site much more visible.
WHEN TO USE OV:
Public-facing websites dealing with less sensitive transactions
✓ More thorough vetting process than DV.
✓ Company information is displayed to users.
✓ Provides a certain level of trust about the company who owns the website.
✗ Doesn't offer the highest visible display of trust like EV SSL (green browser bar).
LEVEL 3 EXTENDED VALIDATION
This is the gold standard in SSL certificates. EV verification guidelines, drawn up by the CA/ Browser Forum, require the CA to run a much more rigorous identity check on the organisation or individual applying for the certificate. Sites with an EV SSL certificate have a green browser address bar and a field appears with the name of the legitimate website owner and the name of the CA that issued the certificate.
WHEN TO USE EV:
E-commerce sites and websites handling credit card and other sensitive data
✓ Use EV SSL for the highest visible display of online trust.
✓ Comes with the green browser address bar.
✓ Increase user trust and lower bounce rates and shopping cart abandonments.
✓ Recoup the extra cost of an EV certificate in the form of increased revenue.
✓ Strengthen your credibility and brand by showcasing your commitment to online security.

EV (Extended Validation) SSL Certificates

- Extended Validation, or EV SSL, raises the bar on standard SSL validation processes, incorporating some of the highest standards in identity assurance to establish the legitimacy of online entities.
- Certificate Authorities put applicant websites through rigorous evaluation procedures and documentation checks to confirm their authenticity and ownership.

- This systematic authentication process, also known as the Extended Validation Standard, is **based on a set of guidelines** prescribed for CAs to adhere to when they receive a request for a digital certificate from an organization or business entity.
- The objective of the EV issuance process is to enable users to distinguish legitimate websites from phishing sites, building their trust in online commercial transactions and increasing participation.

These guidelines include:

- ■Establishing the legal, physical and operational existence of the entity
- ■Verifying that the entity's identity matches official records like incorporation and business licensing information
- ■Confirming that the entity owns or has exclusive rights to use the domain mentioned in the application for certification
- ■Confirming that the request for an EV certificate has been authorized by the entity


Your customers see the green address bar
whenever somone visits your site
https://www.yourcompanywebsite.com
Your Company, Inc [US]
https://www.yourcompanywebsite.com
Comodo CA Ltd [GB]
The right side of the green bar alternates between
your company name and the certificate authority.

Remote Based Authentication (RBA)

- Remote access is the ability to get access to a computer or a network from a remote distance through wired or wireless connection.
- Authentication is the method of proving the subject's identity. E.g.: Password, Passphrase, PIN
- **Why is RBA used?**
  - To prevent accessing private data and information transferring between server and users i.e. Channel attack.
  - Direct attacks from hackers into network.
  - Brute force, software attacks

Authentication Methods:

- **Biometrics**
- **Passwords**
- **Cognitive Passwords**
- **Card Based**
- A smart card, chip card, or integrated circuit card (ICC) is a physical electronic authorization device, used to control access to a resource.
- **One-Time or Dynamic Passwords (token based)**
- OTP security tokens are microprocessor-based smart cards or pocket-size key fobs that produce a numeric or alphanumeric code to authenticate access to the system or transaction.
- This secret code changes every 30 or 60 seconds.

Importance Today?

- Today everything is electronics and internet based like e-banking, e-commerce, e-learning, e-governance, m-banking etc.
- Companies have many branches worldwide so data and information are distributed among branches offices.
- User do transaction remotely using internet using different handheld devices.
- All information of enterprises is centralized at server which is shared/distributed remotely among concerned people worldwide.

https://www.ibm.com/docs/en/spectrumvirtualsoftw/8.2.x?topic=authentication-configuring-remote

2.11Content Control and Policy Based Encryption

- *Content encryption helps to protect the confidentiality of content that you add to a storage area in case the content is accessed by an outsider* .

- This encryption pertains only to the storage of content in the storage area: when Content Platform Engine retrieves and passes content to a client in response to a client request, the content is automatically decrypted.

- For example : Services for the security of email content in an organization are called content control.
- Email content like: credit card no., account information, organization vital information and customer vital information needs to be protected.

Policy Based Encryption (PBE)

- *Policy Based Encryption encrypts specific emails based on a policy.*
- *That is, a set of rules that are designed to analyze all email, and encrypt any email that matches the predefined conditions.*

- Policy-Based Encryption is account-wide. Messages sent from each mailbox are forwarded through the gateway.
- Internal messages (messages, sent from one user on the account to another one) do not get encrypted. It's considered safe since internal mail never actually leaves the server.
- All changes to the policies and other settings are made through the administrative interface.
- Policy-Based Encryption does not require any software to be installed on the client computer.
- Message encryption and decryption is performed on the servers the message was routed to.

Policy Based Encryption Benefits

- Automatically applies email encryption based on the organization's email security policies.
- Data loss prevention and email messages security policies are consistently and accurately applied.
- Eliminates email encryption key management, backup and administration burdens.

PRACTICAL GUIDE ON PBE

https://support.intermedia.com/app/articles/detail/a_id/10941/type/KB

Example of security in e-Commerce transaction

- Electronic commerce or ecommerce is a term for any type of business, or commercial transaction that involves the transfer of information across the Internet.
- E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction.
- **Dimensions of E-Commerce Security**
- **INTEGRITY**
- **NON REPUDIATION**
- **AUTHENTICITY**
- **CONFIDENTIALITY**
- **PRIVACY**
- **AVAILABILITY**

Threat to Ecommerce

- Financial Frauds
- Spam
- Phishing
- Bots
- DDoS Attack
- Brute Force Attack
  - These attacks target your online store's admin panel in an attempt to figure out your password by brute-force. It uses programs that establish a connection to your website and use every possible combination to crack your password. You can protect yourself against such attacks by using a strong, complex password. Do remember to change it regularly.

- SQL Injections
  - SQL injections are cyber-attacks intended to access your database by targeting your query submission forms. They inject malicious code in your database, collect the data and then delete it later on.
- Trojan Horses
  - Admins and customers might have Trojan Horses downloaded on their systems. It is one amongst the worst network security threats where attackers use these programs to swipe sensitive information from their computers with ease.

Ecommerce Security Solutions

- 1. Switch to HTTPS
- 2. Secure Your Servers and Admin Panels
- Most ecommerce platforms come with default passwords that are ridiculously easy to guess. And if you don't change them you are exposing yourself to preventable hacks. Use complex password(s) and usernames and change them frequently.
- 3. Payment Gateway Security
- You can use third-party payment processing systems to carry out the process off-site. Popular options include PayPal, Stripe, Skrill, and Wordplay.

- 4. Antivirus and Anti-Malware Software
- Hackers can use stolen credit card information to place orders from anywhere in the world. An antivirus or an anti-fraud software can help you with this serious ecommerce issue.
- 5. Use Firewalls
- Another effective ecommerce recommendation is to use firewall software and plugins that are pocket-friendly yet effective. They keep untrusted networks at bay and regulate traffic that enters and leaves your site.
- 6. Secure your website with SSL certificates

- 7. Employ Multi-Layer Security
- 8. Backup Your Data
- 9. Train Your Staff Better

PRACTICE QUESTIONS

- 1.What are different security threats while deploying Information System over extranet of a business firm? What are the technologies for mitigating the security risks in Information System?
- 2.What are different threats to Information System in terms of security? Discuss different controls and security measures (including physical and logical) that are to be applied to protect information system?
- 3.Explain the security component in IS. Explain.
- 4.Explain Enterprise Layered security strategy with its types in detail. Why audit and control in information are important.
- 5.What is multi layer security strategy? Discuss how multi layer security strategy can be applied to protect e- commerce system.
- 6.Define physical and logical security that can be applied in Information system. What is the key threat and vulnerabilities against with any information system should be protected? What are different controls that can be applied to protect information system against such threats?
- 7.How do you define cyber crime and theft of intellectual property right? Discuss with suitable example.
- 8.List and describe the most common threats against contemporary information system. What are different physical and logical security measures that organization can apply to protect information system for different threats.
- 9.Define security and control of information. Explain the technologies and tools for protecting information resources.
- 10.Explain SSL certificates for client server connection over the web. What do you mean by Extended Validation?
- 11.What is an Information audit? What benefits will you obtain after going through Information audit?

CASE STUDY 2

What is SSL and its types ? How is SSL certificate obtained? Is there any SSL Service Provider in Nepal?

- **DISCUSS ABOUT ANY ONE SSL SERVICE PROVIDER:**
- 1. Comodo SSL
- 2. DigiCert
- 3. Entrust Datacard
- 4. GeoTrust
- 5. GlobalSign
- 6. GoDaddy
- 7. Network Solutions
- 8. RapidSSL
- 9. SSL.com
- 10. Thawte

- Discuss about the real world scenario for using above SSL certificate for below area (you can also choose your own area):
- School Gives Parents Secure Web Based Access to Student Data with SSL Certificates
- Travel Company Uses SSL Certificates to Build Trust with Customers and Grow Business Online
- Healthcare Portal Secures Medical Data with SSL Certificates to Build Trust with Patients and Providers
- New E-commerce Site Quickly Builds Customer Confidence with SSL Certificates
- **Each topic should include:**
- Industry Name
- Key Challenges
- Solution using any one SSL service provider.
- Result