Prezentare

Securitatea spatiului cybernetic
(Cybersecurity)

Fundamentarea cursului:

- Curs CISCO *Introduction to Cybersecurity (2016)*
  - Necesitatea securității spațiului cybernetic
  - Atacuri: concepte și tehnici
  - Protejarea echipamentelor si a datelor
  - Protejarea organizațiilor
  - Vor exista in viitor locuri de angajare in cybersecurity?

Fundamentarea cursului:

- Curs CISCO *Cybersecurity Essentials (2016):*
  - Lumea criminalității cibernetice
  - Securitatea informatiei modelul “*McCumber Cube”*
  - Vulnerabilități și atacuri în spațiul cybernetic
  - Arta protejarii secretelor
  - Tehnici de asigurare a integritatii datelor
  - Domeniul celor cinci "nouari" (uptime 99.999%)
  - Securizarea domeniului de activitate
  - Introducerea în lumea specialiștilor din spațiul cibernetic

Examen

- Curs
- Laborator

- Promovare - daca la oricare dintre cele 2 componente se obtin note >4;

Introducere:

- De la introducerea internetului prin intermediul unui proiect dezvoltat in perioada 1960, mediul on-line a cunoscut o extindere constanta ajungand in prezent ca peste 2.5 miliarde de utilizatori sa desfasoare diferite activitati on-line;
- Scopul cursului este de a prezenta structura internetului din punct de vedere al amenintariilor pe care acesta le poate aduce utilizatorilor
- Va propun sa ne schimpam perspectiva din care privim mediul on-line plecand de la urmatoarea transformare:

www - *World Wide Web -> Wild Wild West*

*(“**The cyberworld is the Wild Wild West — to some degree we’re asked to be the sheriff**”)*

Introducere:

- Cat de mult va influenteaza viata internetul? Cat de mult depinde viata dumneavoastra de mediul on-line?

- Ce considerati ca va modela mai mult societatea «revolutia din industrie» sau «revolutia tehnologiei informatiei»?

- Prezentare STUXNET

Notiuni generale

Securitatea spatiului cybernetic
(CyberSecurity Fundamentals)

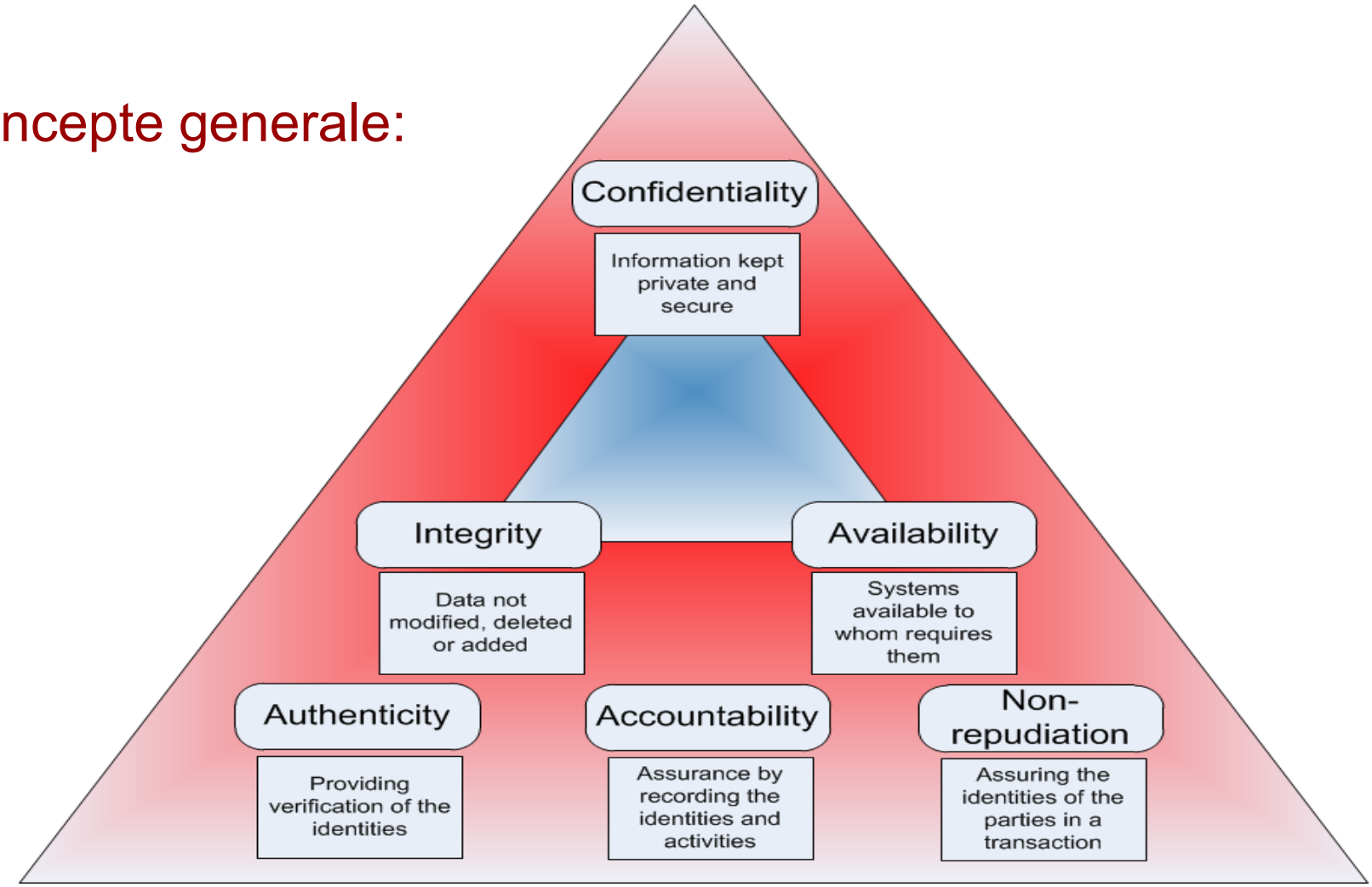
Concepte generale:

- In timpul dezvoltarii unui sistem de cele mai multe ori sunt folositi termenii:

  - Autentificare
  - Autorizare => Securitatea sistemului
  - Nerepudiere

  - Confidentialitate
  - Integritate => “*CIA triad*”
  - Disponibilitate

Concepte generale:

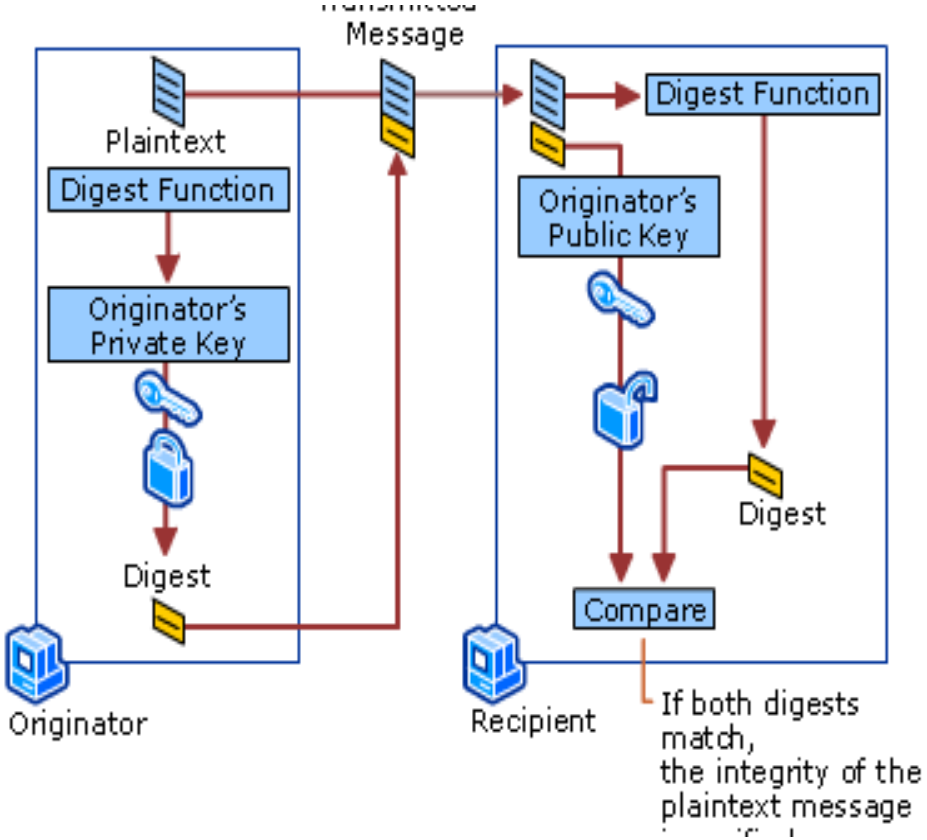


Definitii (eng. provin din "*National Information Assurance Glossary*")

- Autentificare: proces important in securitatea unui sistem deoarece permite verificarea sursei unui mesaj sau ca o persoana este ceea ce pretinde
- Authentication: "security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information."
- De obicei procesul de autentificare consta in lansarea unei provocari/intrebari la care persoana care doreste sa se autentifice trebuie sa participe/raspunda
- Exemple: un cod PIN, un stick de memorie, amprenta, scanarea retinei etc;
- Sunt impartite in 3 categorii: «ceva ce stii», «ceva ce ai», «ceva ce te identifica»

Observatie: o combinatie de 2 sau mai multe "chei" de acelasi tip nu creste securitatea unui sistem

Definitii:



Deoarece vorbim de autentificare si intre doua sisteme (2 servere de mail) nu se mai pot folosi parametrii biometrici si de obicei se folosesc semnaturi digitale (cheie sau un hash al mesajului generat cu o cheie secreta)

Fara un proces de autentificare solid nu putem vorbi despre securitatea unui sistem

Definitii:

- Autorizare: proces prin care determin ce drepturi are un utilizator
- Authorization : “access privileges granted to a user, program, or process.”
- Exemplu: intr-un sistem bancar dupa autentificarea unui utilizator trebuie sa ii fie atasate conturile pe care le controleaza;
- Non-repudiere: procesul prin care 2 entitati pot sa dovedeasca implicarea fiecareia la un schimb de informatii (exemplu: contract de vanzare-cumparare)
- Nonrepudiation: “assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender’s identity, so neither can later deny having processed the data.”

Observatie: un sistem informatic foloseste, de obicei, criptarea asimetrica pentru a implementa aceasta cerinta;

Definitii:

- Confidentialitate: proces prin care se asigura confidenta datelor
- Confidentiality: “assurance that information is not disclosed to unauthorized individuals, processes, or devices.”
- Pentru a asigura confidenta datelor sunt parcursi 3 pasi: informatia nu trebuie sa fie publica, sa existe o serie de drepturi/privilegii, un sistem de autentificare trebuie sa fie deja implementat;
- **Autentificare + Autorizare <= Confidentialitate => Protejarea informatiei**
- Confidentialitatea poate fi realizata prin stocarea informatiei intr-un loc secret, iar pentru informatia din Internet se foloseste criptarea datelor si/sau VPN

Exemplu: https://core.ac.uk/download/pdf/6245917.pdf

Definitii:

- Integritate: proces prin care se asigura acuratetea datelor (nu au suferit modificari din partea unor persoane neautorizate)
- Integrity: “Quality of an IS (Information System) reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, **in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information**.”
- **Autentificare + Autorizare + Non-repudiere <= Integritate**

Exemplu: SQL injection

Definitii:

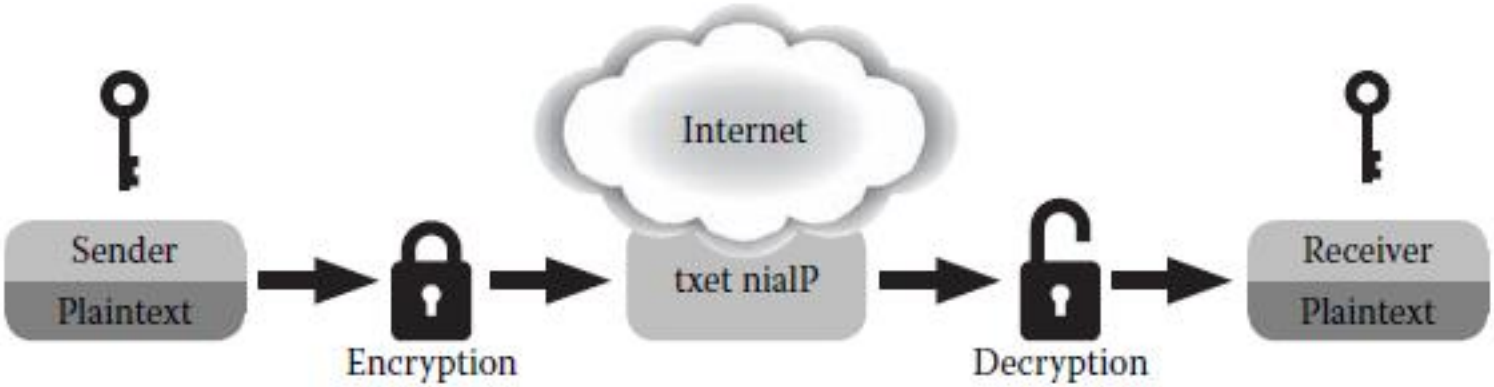
- Disponibilitate: proces prin care este asigurat accesul la informatii; un sistem care raspunde greu la cereri poate produce brese de securitate
- Availability: “timely, reliable access to data and information services for authorized users“
- Cele mai cunoscute atacuri de acest tip poarta numele de “denial of service (DoS)” si constau in restrictionarea accesului la informatie, utilizatorilor care au acest drept
- Vizeaza in general resurse de tipul: latimea de banda a retelei, numarul de conexiuni, memoria disponibila etc.

Observatie: existenta unei vulnerabilitati la oricare dintre componentele prezentate poate duce la compromiterea sistemului

Notiuni elementare de criptografie

Definitii:

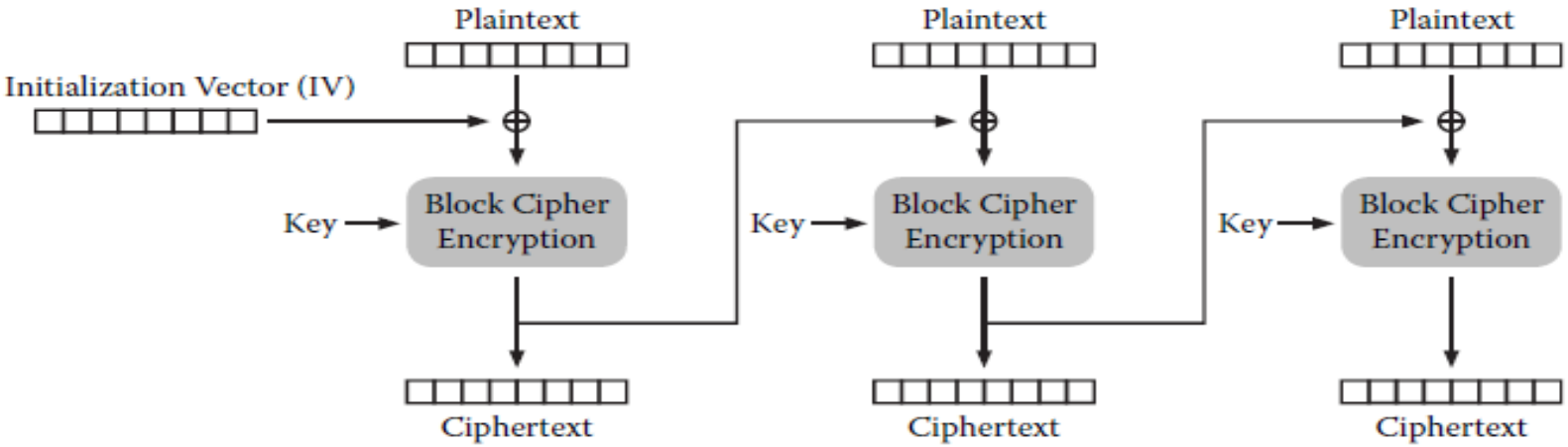
- «cryptography» =«hidden writing»
- Criptosisteme elementare: substitutie (Caesar) <= vulnerabile la analiza frecventei literelor;
- Criptosisteme “one-time pads” <= cheia de aceeasi lungime cu mesajul (imposibil de descifrat)
- Criptosisteme simetrice => **foarte usor de folosit**



Notiuni elementare de criptografie

Definitii:

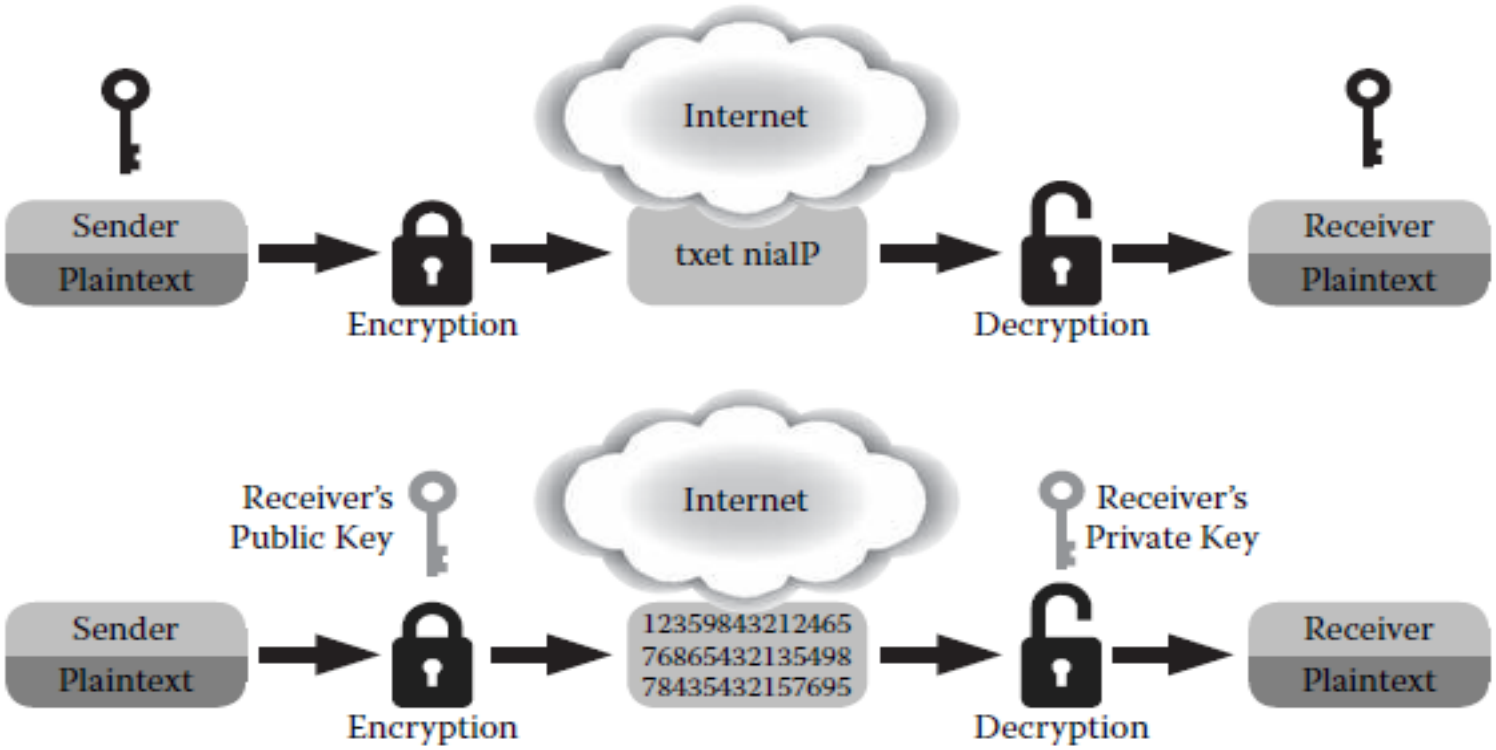
- Criptosisteme simetrice care cripteaza fiecare caracter pastreaza "*pattern-uri*" din textul clar => sunt vulnerabile la analiza textului
- Criptosisteme simetrice care impart textul in blocuri: 1977 - DES, 1991 - IDEA, 1993 - Blowfish, 1994 - RC5, 1998 - Triple DES, 1998 - AES



Notiuni elementare de criptografie

Definitii:

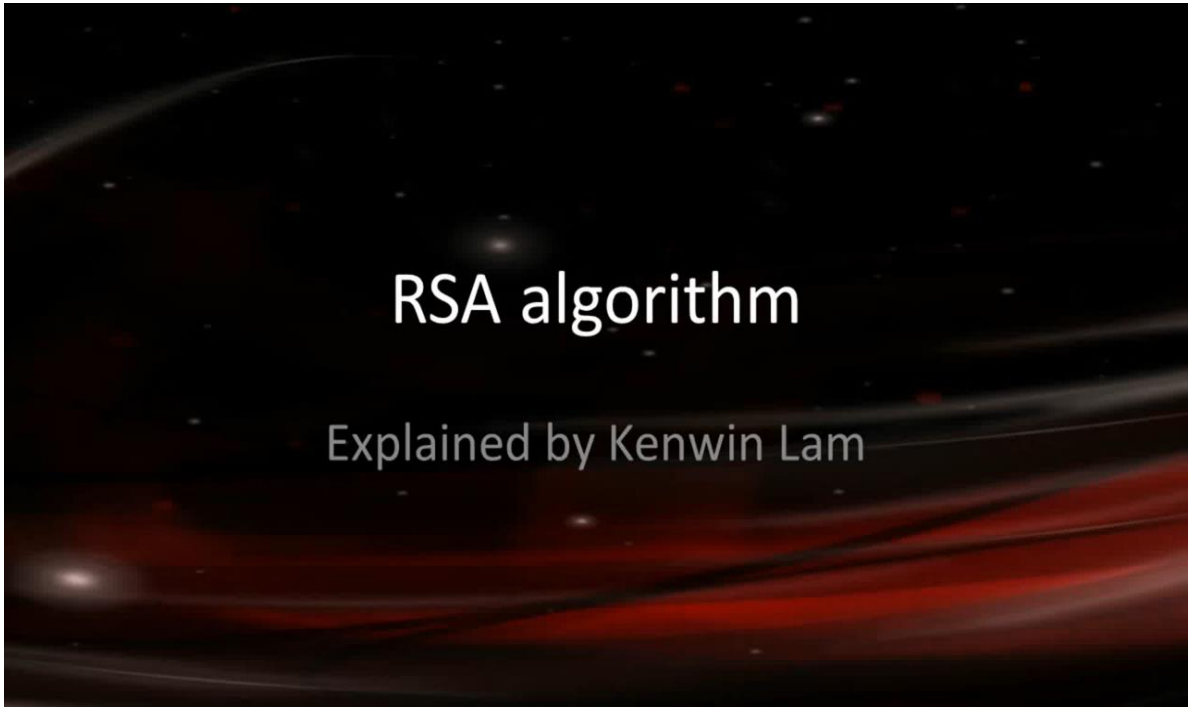
- Criptosisteme asimetrice = criptare cu cheie publica



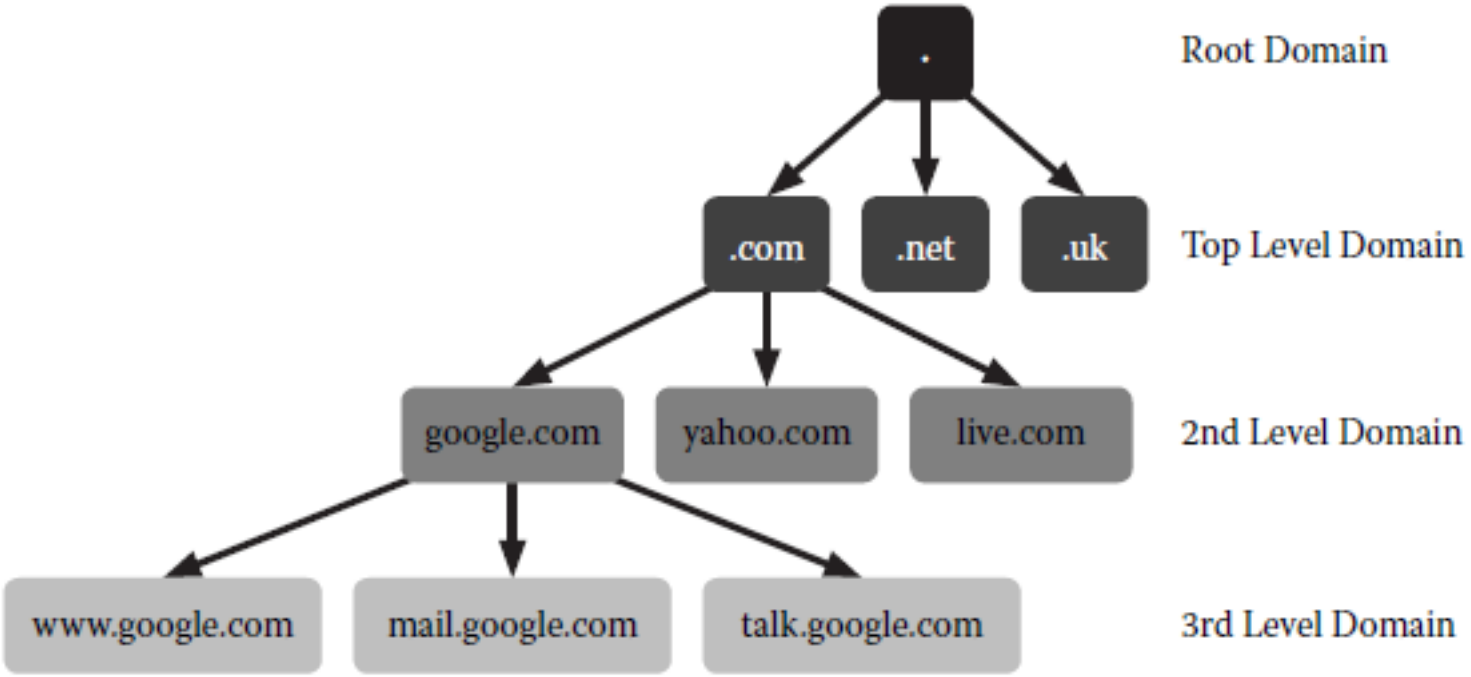
Notiuni elementare de criptografie

Definitii:

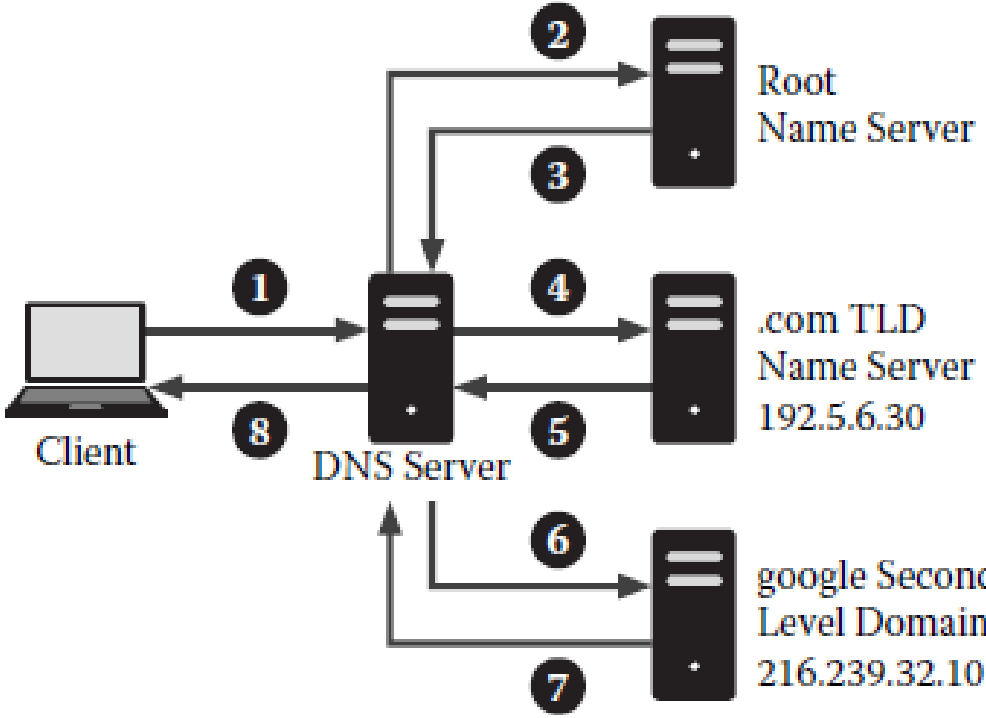
- Criptosisteme asimetrice:
  - Whitfield Diffie, Martin Hellman - 1976
  - Ron Rivest, Adi Shamir, and Leonard Adleman - 1979



Domain Name System (DNS)



Procesul de identificare al unui domeniu



1. What is google.com's IP Address
2. What is .com's Name Server IP Address
3. 192.5.6.30
4. What is google's Name Server IP Address
5. 216.239.32.10
6. What is google's IP Address?
7. 74.125.45.100
8. 74.125.45.100

Securitatea spatiului cybernetic
(Vulnerability and Exploits)

Analyzing a Cyberattack

Cisco | Networking Academy®
Mind Wide Open™

Security Vulnerability and Exploits

- Software vulnerability
  - Errors in OS or application code
  - Project Zero
  - What can you do to protect yourself from software vulnerability?
- Hardware vulnerability
  - Hardware design flaws
  - RAM memory example: Rowhammer

    (https://www.youtube.com/watch?v=5dx0zWZvh6g

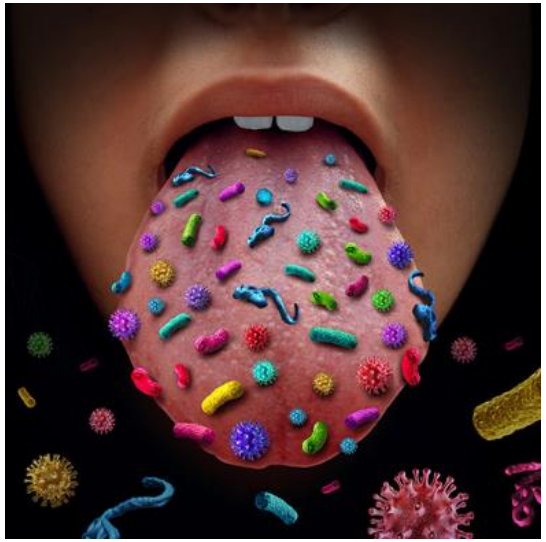
    https://www.youtube.com/watch?v=0U7511Fb4to)
  - What can you do to protect yourself from hardware vulnerability?

Types of Security Vulnerabilities

- Buffer Overflow
  - Data is written beyond the limits of a buffer
- Non-validated Input
  - Force programs to behave in an unintended way
- Race Conditions
  - Improperly timed events
- Weaknesses in Security Practices
  - Protect sensitive data through authentication, authorization, and encryption
- Access-control Problems
  - Access control to equipment and resources
  - Security practices

Types of Malware and Symptoms

- Types of Malware
  - Spyware
  - Bot
  - Ransomware
  - Scareware
  - Rootkit
  - Man-in-The Middle
- Symptoms of Malware
  - Deleted files
  - Modified files
  - Can you list more symptoms?

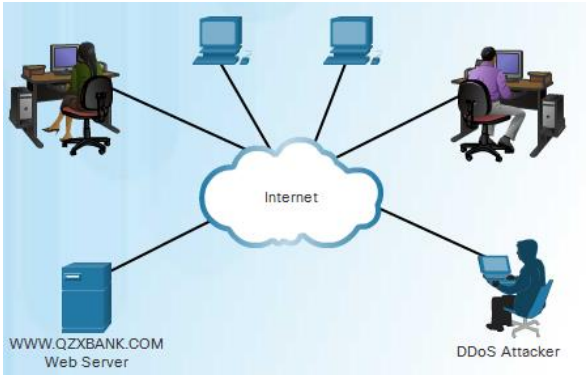


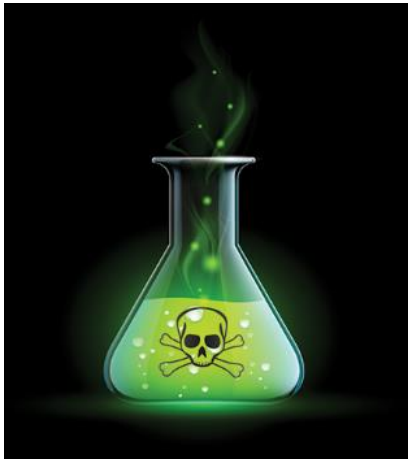
Methods of Infiltration

- Social Engineering – manipulation of individual
  - Pretexting
  - Tailgating
  - Something for something (Quid pro quo)
- Wi-Fi Password Cracking – Password discovery
  - Social engineering
  - Brute-force attacks
  - Network sniffing
- Phishing – sends fraudulent emails to trick users
- Vulnerability Exploitation – scan to find vulnerability to exploit

Denial of Service

- DoS – disruption of network services
  - Overwhelming quantity of traffic
  - Maliciously formatted packets
- DDoS
  - Similar to DoS
  - Originates from multiple, coordinated sources
- SEO Poisoning
  - Increase traffic to malicious sites
  - Force malicious sites to rank higher





Blended Attack

- What is a Blended Attack?
  - Uses multiple techniques to compromise a target
  - Worms, Trojan horses, spyware, keyloggers, spam and phishing schemes
  - Examples: Nimbda, BugBear, and Conficker

Impact Reduction

- What is a Impact Reduction?
  - Communicate the issue
  - Be sincere and accountable
  - Provide details
  - Understand the cause of the breach
  - Take steps to avoid another similar breach in the future
  - Ensure all systems are clean
  - Educate employees, partners and customers

Protecting Your Devices and Network

- Protect Your Computing Devices
  - Keep the Firewall on
  - Use Antivirus and antispyware
  - Manage Your Operating System and Browser
- Use Wireless Networks Safely
  - Use caution when using public Wi-Fi hotspots
  - Turn off Bluetooth when not in use
- Use Unique Passwords for Each Online Account
  - Prevents criminals from accessing all your online accounts using one stolen credentials
  - Use password managers
- Use Passphrase Rather Than a Password

Data Maintenance

- Encrypt Your Data
  - Encrypted data can only be read with the secret key or password
  - Prevent unauthorized users from reading the content
- Back up Your Data
  - Local vs. Online (Cloud)
- Deleting Your Data Permanently
  - Use available tools to delete permanently: SDelete and Secure Empty Trash, for example
  - Delete the online versions

Strong Authentication

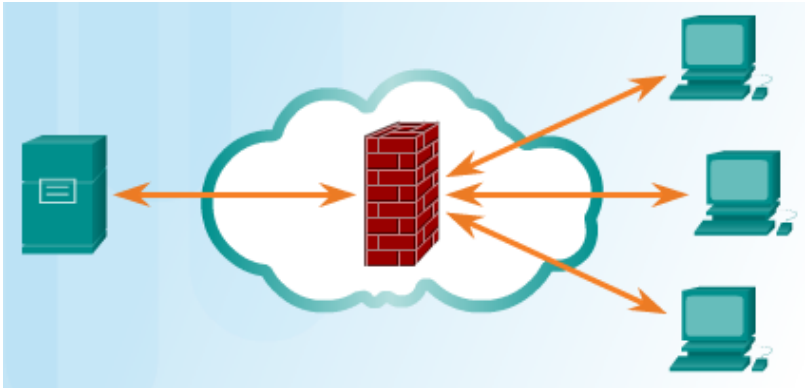
- Two Factor Authentication
  - Physical object
  - Biometric scan
- OAuth 2.0 (Open Authentication)
  - open standard protocol
  - allows an end user's credentials to access third party applications without exposing the user's password.
  - acts as the middle man to decide whether to allow end users access to third party applications.

Sharing Too Much Information?

- Do Not Share Too Much on Social Media
  - Share as little as possible
  - Answer secret questions with false answers
- Email and Web Browser Privacy
  - Encrypt you emails
  - Use in-private browsing mode on your web browser

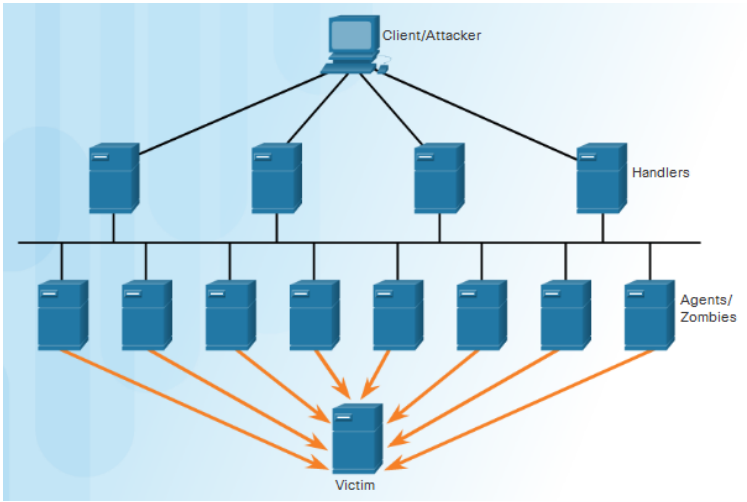
Firewall Types

- Firewall Types
  - Control or filter incoming or outgoing communications on a network or device
  - Can you name a few types of firewalls?
- Port Scanning
  - Process of probing a computer, server or other network hosts for open ports
  - Port numbers are assigned to each running application on a device.
  - Reconnaissance tool to identify running OS and services



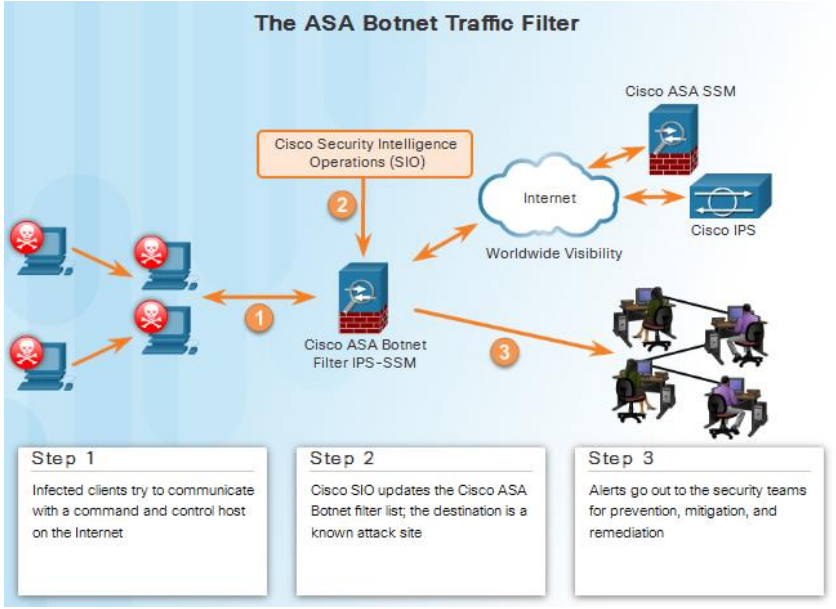
Detecting Attacks in Real Time

- Detect and response to zero-day attacks
- Real Time Scanning from Edge to Endpoint
  - Actively scan for attacks using firewall and IDS/IPS network devices
  - Malware detection
  - Detect network anomalies using context-based analysis and behavior detection
- DDoS Attacks requires real time response and detection



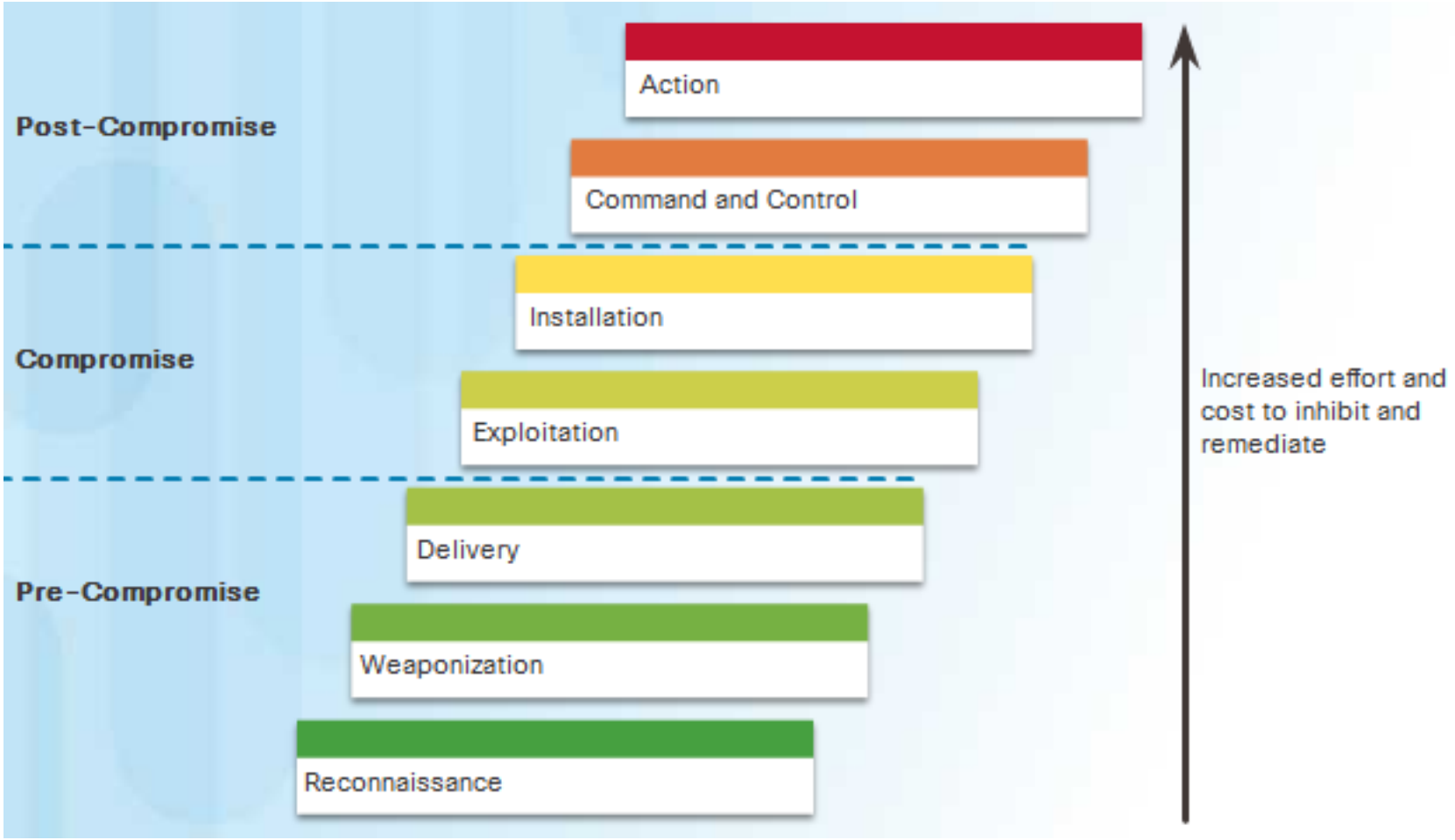
Botnet

- Botnet
  - A group of bots connect through the Internet
  - Controlled by malicious individuals or groups
- Bot
  - Typically infected by visiting a website, opening an email attachment, or opening an infected media file



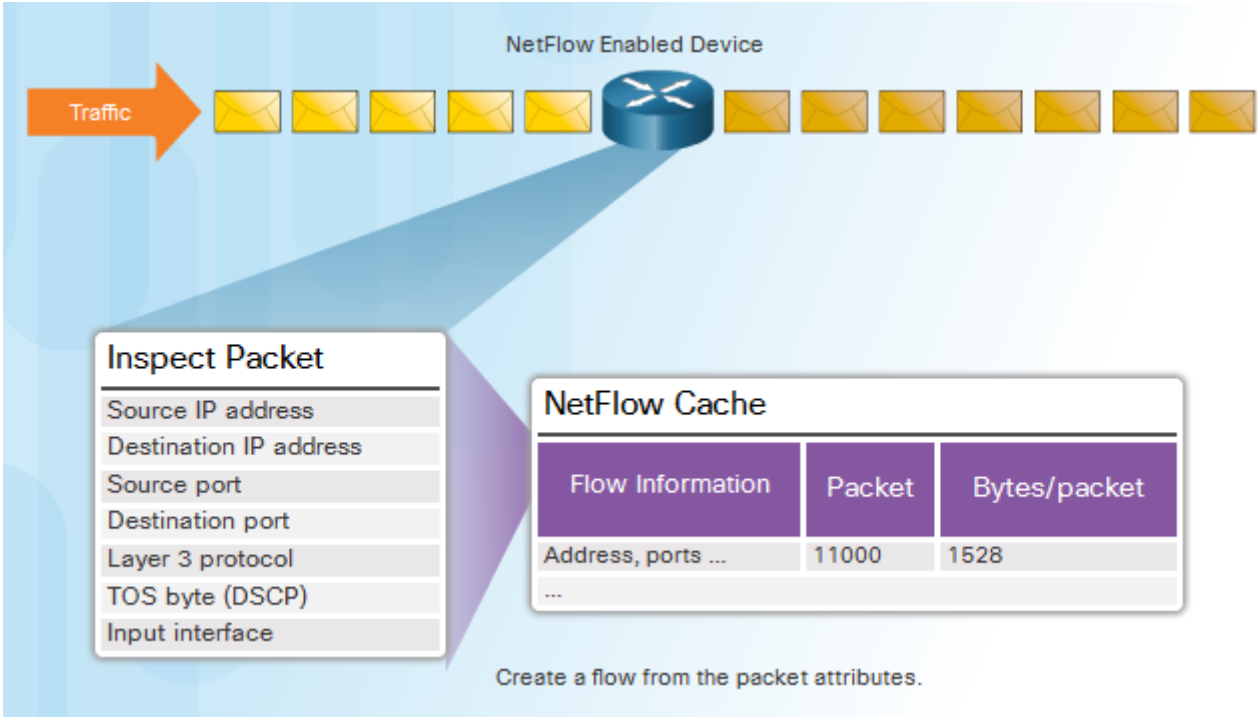
Kill Chain

- What are the stages in a Kill Chain?



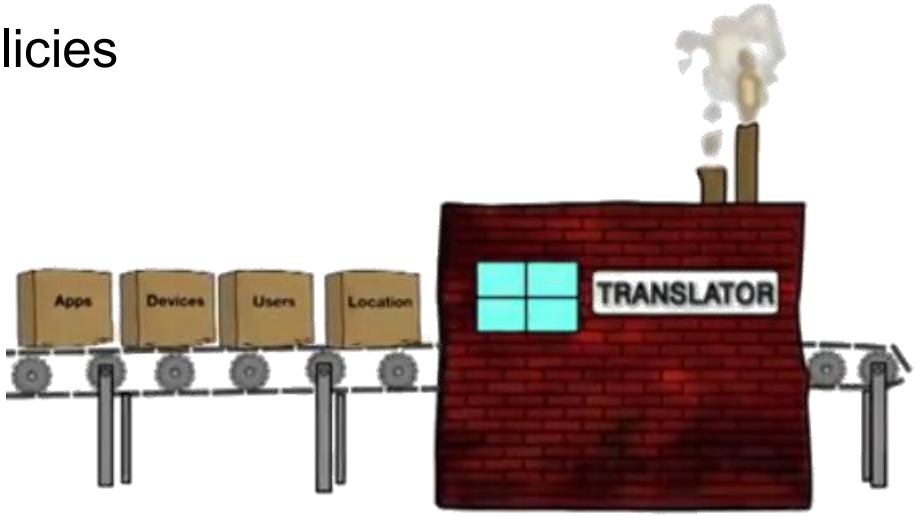
NetFlow and Cyberattacks

- NetFlow
  - Gather information about data flowing through a network
  - Important components in behavior-based detection and analysis
  - Establish baseline behaviors



Tools for Incident Prevention and Detection

- SIEM – Security Information and Event Management
  - Software that collects and analyzes security alerts, logs and other real time and historical data from security devices on the network
- DLP – Data Loss Prevention
  - Stops sensitive data from being stolen or escaped from the network
  - Designs to monitor and protect data in three different states
- Cisco Identity Services Engine (Cisco ISE) and TrustSec
  - Uses role-based access control policies



Infractiunile informatice prevazute de legea 161/2003 (art. 34 – 67)

- http://www.euroavocatura.ro/articole/164/Infractiunile_informatice_prevazute_de_legea_161_2003
- LEGE nr161 din 2003.pdf

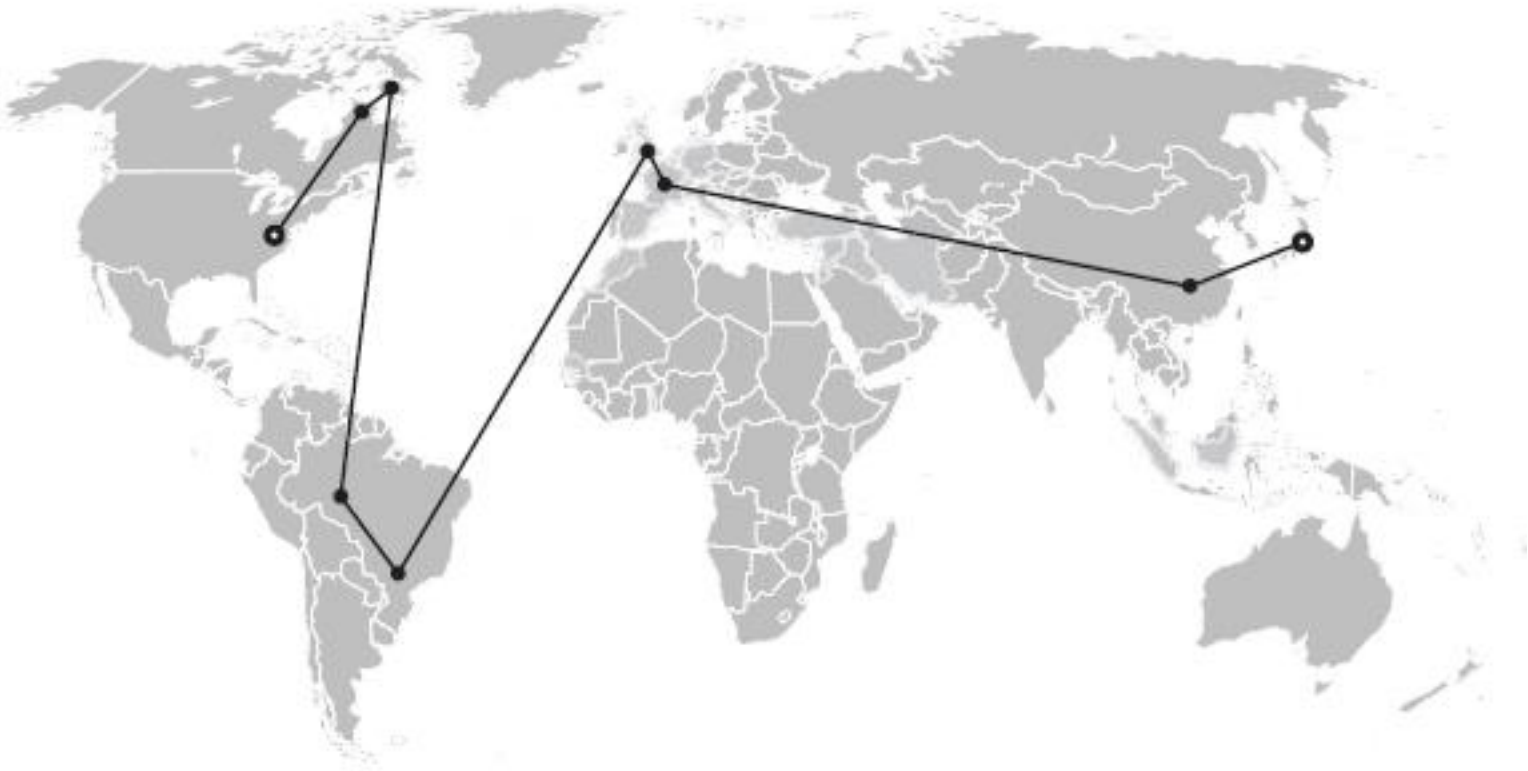
- DDOS
- Real time: http://www.digitalattackmap.com/
- How many providers: https://www.safeskyhacks.com/Forums/showthread.php?39-Top-10-DDoser-s-(Booters-Stressers)
- How difficult it is: https://www.youtube.com/watch?v=ITV6ke036Z4
- Games: https://www.consumer.ftc.gov/sites/default/files/games/off-site/ogol/_invasion-wireless-hakers.html

Tehnici de atac si motivatii
(Attacker Techniques and Motivations)

Cum un atacator “reuseste” sa isi acopere identitatea

- Ascunderea IP-ului sursa este considerata deja o tehnica standard pentru initierea unui atac
- Un **proxy bine configurat** ofera o metoda destul de robusta pentru ascunderea identitatii
- Un proxy are rolul de a transmite traficul de la un IP prin intermediul unui server dedicat
- Se folosesc serverele de proxy deoarece adresa IP poate fi localizata
- In “practica” sunt folsoite mai multe adrese de proxy pentru a redirecta traficul, astfel cererea este greu de localizat (la sursa este vizibila doar ultima adresa utilizata)

Cum un atacator “reuseste” sa isi acopere identitatea



Cum un atacator “reuseste” sa isi acopere identitatea

- Exista multe site-uri care “ofera” posibilitatea de a redirecta traficul
- Un exemplu “negativ” este AnonProxy:

http://anonproxyserver.sourceforge.net/

- De obicei un proxy local modifica hederul pachetelor sau se instaleaza ca un add-on in brower

- In foarte multe situatii aceste programe au si o **componenta ce salveaza datele confidentiale**

Serverele de proxy locale sunt mult mai dificil de identificat deoarece pot sa deschida/foloseasca porturi aleatoriu (la fiecare initializare folosesc un alt port)

SQL Injection

Privire de ansamblu

„Știința se răzbună ca o femeie,
nu când o ataci, ci când o negliezi.”
Grigore C. Moisil

Introducere

- Majoritatea dezvoltatorilor subestimează riscul atacurilor cu SQL Injection ce afectează aplicațiile cu baze de date Oracle în spate.
- Se pare că mulți dezvoltatori de aplicații nu înțeleg în întregime riscul atacurilor cu SQL Injection și nici tehnicile folosite pentru prevenirea unor astfel de atacuri.
- Scopul este sublinierea riscurilor atacurilor cu SQL Injection și demonstrarea premiselor de vulnerabilitate ale aplicațiilor web.
- Nu se vrea a fi un tutorial pentru realizarea de atacuri SQL și nici nu oferă nici instrucțiuni în această privință.

Privire de ansamblu asupra SQL Injection

- SQL Injection este un atac de bază folosit fie pentru obținerea accesului neautorizat la o bază de date, fie pentru extragerea informațiilor direct din baza de date.
- Orice program sau aplicație pot fi vulnerabile la SQL Injection, inclusiv procedurile stocate executate în mod direct printr-o conexiune la o bază de date, aplicații în Oracle Forms, aplicații web, etc.
- Numeroase vulnerabilități au fost descoperite în pachetele standard Oracle Database cum ar fi DBMS_DATAPUMP, DBMS_REGISTRY și DBMS_METADATA (vezi update-ul de importanță critică din ianuarie 2006).
- Aplicațiile web prezintă cel mai mare risc al acestor atacuri de vreme ce un atacator poate exploata vulnerabilitățile la SQL Injection de la distanță fără autentificare la nivel de bază de date sau la nivel de aplicație.

Privire de ansamblu asupra SQL Injection

- Aplicațiile web care au în spate o bază de date Oracle sunt mai vulnerabile la atacurile cu SQL Injection decât ar crede majoritatea dezvoltatorilor. În urma unor auditări de aplicații au fost descoperite multe aplicații web vulnerabile la SQL Injection.
- Atacurile SQL Injection pe baza funcțiilor reprezintă cea mai mare preocupare, de vreme ce aceste atacuri nu necesită informații despre aplicație și pot fi ușor automatizate.
- Atacurile SQL Injection sunt ușor de combătut prin anumite procedee de codare.
- Orice parametru transmis oricărui enunț SQL dinamic trebuie validat, sau trebuie folosite variabile legate.

SQL Injection: Oracle versus alte sisteme

- Oracle se descurcă bine în general împotriva atacurilor SQL Injection de vreme ce nu există suport pentru cereri SQL multiple (SQL Server și PostgreSQL), nu există cererea EXECUTE (SQL Server), și nu există funcția INTO OUTFILE (MySQL) – toate acestea fiind metode de exploatare a vulnerabilităților la SQL Injection.
- Utilizarea variabilelor legate în mediile Oracle din motive de performanță oferă cea mai eficientă protecție împotriva atacurilor SQL Injection.

SQL Injection

„Răutatea calculată este
cea mai ascuțită dintre toate răutățile.”
Honore de Balzac

Introducere

- Atacurile prin SQL Injection sunt în esență simple – un atacator strecoară un șir de caractere în aplicație în speranța că va reuși să manipuleze cererea SQL în avantajul său.
- Complexitatea atacului implică exploatarea unei cereri SQL care poate fi necunoscută atacatorului.
- Aplicațiile open-source și cele comerciale livrate alături codul sursă sunt mai vulnerabile de vreme ce atacatorul poate descoperi potențiale vulnerabilități înaintea atacului.

Categoriile de atacuri cu SQL Injection

- Sunt patru categorii principale pentru atacurile SQL Injection împotriva bazelor de date Oracle:

  - Manipularea SQL
  - Injectarea codului
  - Injectarea apelurilor de funcții
  - Supraîncărcarea bufferelor.

Ce este și ce nu este vulnerabil

- O aplicație este vulnerabilă la SQL Injection dintr-un singur motiv – inputul de stringuri nu este validat corespunzător și este trecut către o cerere SQL dinamică fără vreo astfel de validare.
- Din cauza lipsei de „memorie” a multor aplicații web, este frecventă scrierea datelor în baza de date sau stocarea acestora prin alte mijloace între paginile web.
- Cererile SQL care folosesc variabile legate sunt în general protejate împotriva SQL Injection de vreme ce baza de date folosește valoarea variabilei legate exclusiv și nu interpretează variabila în niciun fel. PL/SQL și JDBC permit variabile legate. Variabilele legate ar trebui să fie utilizate pe scară largă din rațiuni de securitate și performanță.

Tipuri de SQL Injection

„Răutatea este neîmblânzită,
chiar dacă îi faci cel mai mare bine.”
Aesop

Manipularea codului SQL

- Manipularea codului SQL reprezintă cea mai raspândită metodă de atac de tip SQL Injection. Cel mai adesea, această metodă presupune modificarea instrucţiunii SQL prin adăugarea de elemente clauzei WHERE sau extinderea instrucţiunii cu ajutorul operatorilor UNION, INTERSECT, sau MINUS
- O aplicație web ar putea să facă autentificarea unui utilizator prin executarea query-ului de mai jos și apoi verificarea daca acesta a întors vreun rezultat:

```
SELECT * FROM users
WHERE username = 'bob' and PASSWORD = 'mypassword'
```

Manipularea codului SQL

- Manipulând instrucțiunea de mai sus, ca în exemplul de mai jos, bazându-se pe precendența operatorilor, clauza WHERE poate deveni adevarată pentru orice linie, astfel atacatorul primind acces la datele aplicației.

```
SELECT * FROM users
WHERE username = 'bob' and PASSWORD =
'mypassword'
        or 'a' = 'a'
```

- Operatorul pentru mulțimi, UNION, este folosit adesea în atacurile de tip SQL Injection, scopul fiind acela de a manipula o instrucțiune SQL astfel încât să returneze rânduri dintr-un alt tabel.

```
SELECT product_name FROM all_products
WHERE product_name like '%Chairs'
UNION
SELECT username FROM dba_users
WHERE username like '%'
```

Code Injection

- Atacurile de tip code injection încearcă adăugarea unor instrucţiuni sau comenzi SQL adiţionale. Acest tip de atac este utilizat adesea împotriva aplicaţiilor de tip Microsoft SQL Server, dar funcţionează rar în cazul aplicaţiilor ce folosesc o bază de date Oracle. Instrucţiunea *EXECUTE* folosită de SQL Server reprezintă o ţintă frecventă a atacurilor de tip SQL Injection, Oracle neavând însă o instrucţiune corespunzătoare acesteia.
- atacul de mai jos nu va funcţiona într-o aplicaţie PL/SQL sau Java ce are în spate o bază de date Oracle, şi va returna o eroare:

```
SELECT * FROM users
WHERE username = 'bob' and PASSWORD = 'mypassword';
DELETE FROM users
WHERE username = 'admin';
```

- Însă există limbaje de programare sau diferite API-uri care permit executarea instrucţiunilor SQL multiple.
- Un atacator ar putea să încerce manipularea blocului PL/SQL astfel:

```
BEGIN ENCRYPT PASSWORD('bob', 'mypassword');
DELETE FROM users
WHERE upper(username) = upper('admin'); END;
```

Injectare cu apel funcție

- Orice instrucțiune SQL dinamică este vulnerabilă, astfel încât chiar și cele mai simple instrucțiuni SQL pot fi exploatate, așa cum arată exemplul de mai jos.

```
SELECT TRANSLATE('user input',
'0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ',
'0123456789') FROM dual;
```

- . Atacatorul poate manipula instrucțiunea SQL astfel încât să se execute ca mai jos, ceea ce va duce la executarea cererii de afișare a unei pagini de pe un server web. De asemenea atacatorul ar putea manipula URL-ul pentru a include și alte funcții ce ar putea returna informații din baza de date ce vor fi apoi trimise serverului web din cadrul URL-ului.

```
SELECT TRANSLATE('' ||
UTL_HTTP.REQUEST('http://192.168.1.1/') || '',
'0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ',
'0123456789')
FROM dual;
```

Injectare cu apel funcție

- Întrucât este permisă executarea funcțiilor custom și funcțiilor din pachete custom, acest lucru face ca anumite instrucțiuni SQL să fie vulnerabile. Un exemplu este reprezentat de o aplicație ce are definită o funcție ADDUSER în pachetul custom MYAPPADMIN. Funcția a fost marcată *"PRAGMA TRANSACTION"*, pentru a putea fi executată în orice situație specială ce ar putea apărea. Datorită acestui lucru, această funcție poate face scrieri în baza de date chiar și din cadrul unei instrucțiuni *SELECT*, cum se observă în exemplul de mai jos în care atacatorul poate crea noi utilizatori ai aplicației.

```
SELECT TRANSLATE('
      ' || myappadmin.adduser('admin', 'newpass') ||
'',
     '0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ',
'0123456789')
FROM dual;
```

Supraîncărcarea bufferului

- Atacurile de forma supraîncărcarea bufferului sunt folosite pentru a corupe execuţia unei aplicaţii. Prin trimiterea unor date de intrare atent construite, un atacator poate face ca aplicaţia să execute cod arbitrar, şi poate duce de asemenea la oprirea funcţionării aplicaţiei.
- Anumite funcţii standard Oracle sunt vulnerabile la supraîncărcarea bufferului, lucru ce poate fi exploatat de către un atac SQL Injection. Printre funcţiile standard Oracle vulnerabile se numără: BFILENAME (Oracle8i, Oracle9i), FROM_TZ (Oracle9i), NUMTODSINTERVAL (Oracle8i, Oracle9i), NUMTOYMINTERVAL (Oracle8i, Oracle9i), TO_TIMESTAMP_TZ (Oracle9i), TZ_OFFSET (Oracle9i).
- Pentru a împiedica atacurile de acest gen, este recomandat ca pachetele neesenţiale lucrului cu baze de ate (DBMS_*, UTL_*) să nu fie accesibile utilizatorilor aplicaţiei.

PL/SQL

„Binele trebuie făcut așa cum încercăm să facem răul: pe ascuns.”

John Petit

Instrucțiunea *execute immediate*

- Un exemplu de instrucțiune ***execute immediate*** ce este vulnerabilă atacurilor SQL injection poate arăta astfel:

```
CREATE OR REPLACE PROCEDURE demo(name IN VARCHAR2) AS
   sqlstr VARCHAR2(1000);
   code VARCHAR2(100);
BEGIN
...
sqlstr := 'SELECT postal-code FROM states WHERE state-name = '' ||
   name || '';
EXECUTE IMMEDIATE sqlstr INTO code;
IF code = 'IL' THEN ...
...
END;
```

Instrucțiunea *execute immediate*

- Pentru a preveni atacurile SQL Injection și pentru a îmbunătăți performanța aplicației, ar trebui folosite întotdeauna cereri parametrizate.

```
CREATE OR REPLACE PROCEDURE demo(name IN VARCHAR2)
  AS
  sqlstr VARCHAR2(1000);
  code VARCHAR2(100);
BEGIN
...
sqlstr := 'SELECT postal-code FROM states WHERE
  state-name = :name';
EXECUTE IMMEDIATE sqlstr USING name INTO code;
IF code = 'IL' THEN ...
...
END;
```

Instrucțiunea *execute immediate*

- Instrucțiunea ***execute immediate*** poate utiliza și blocuri PL/SQL anonime, ceea ce o face vulnerabilă la atacuri SQL Injection întrucât un atacator ar putea încerca inserarea mai multe instrucțiuni SQL.

```
CREATE OR REPLACE PROCEDURE demo(value IN
  VARCHAR2) AS
BEGIN
...
-- vulnerable
EXECUTE IMMEDIATE 'BEGIN updatepass(''' || value
  || '''); END;'; -- not vulnerable
cmd := 'BEGIN updatepass(:1); END;';
EXECUTE IMMEDIATE cmd USING value;
...
END;
```

Pachetul DBMS_SQL

- Procedura prezentată mai jos folosește pachetul DBMS_SQL și este vulnerabilă la atacuri:

```
CREATE OR REPLACE PROCEDURE demo(name IN VARCHAR2) AS
  cursor_name INTEGER;
  rows_processed INTEGER;
  sqlstr VARCHAR2(150);
  code VARCHAR2(2);
BEGIN
...
sqlstr := 'SELECT postal-code FROM states WHERE state-name
  = ''' || name || '''';
cursor_name := dbms_sql.open_cursor;
DBMS_SQL.PARSE(cursor_name, sqlstr, DBMS_SQL.NATIVE);
  DBMS_SQL.DEFINE_COLUMN(cursor_name, 1, code, 10);
  rows_processed :=
        DBMS_SQL.EXECUTE(cursor_name);
  DBMS_SQL.CLOSE_CURSOR(cursor_name);
...
END;
```

Pachetul DBMS_SQL

- În schimb, aceeaşi procedură care foloseşte cereri parametrizate nu mai este susceptibilă atacurilor, cum se vede în exemplul de mai jos:

```
CREATE OR REPLACE PROCEDURE demo(name IN VARCHAR2) AS
cursor_name INTEGER;
rows_processed INTEGER;
sqlstr VARCHAR2;
code VARCHAR2;
BEGIN
...
sqlstr := 'SELECT postal-code FROM states WHERE state-name
  = :name'; cursor_name := dbms_sql.open_cursor;
DBMS_SQL.PARSE(cursor_name, sqlstr, DBMS_SQL.NATIVE);
  DBMS_SQL.DEFINE_COLUMN(cursor_name, 1, code, 10);
  DBMS_SQL.BIND_VARIABLE(cursor_name, ':name', name);
  rows_processed :=     DBMS_SQL.EXECUTE(cursor_name);
  DBMS_SQL.CLOSE_CURSOR(cursor_name);
...
END;
```

Cursoare dinamice

- PL/SQL permite folosirea cursoarelor statice și a celor dinamice. La fel ca și instrucțiunea ***execute immediate*** sau instrucțiunile DBMS_SQL, instrucțiunile cursor pot fi vulnerabile la atacuri cum se vede în exemplul de mai jos. Însă ele pot fi generate în mod dinamic prin folosirea cererilor parametrizate, ceea ce le protejează de atacurile SQL Injection.

```
CREATE OR REPLACE PROCEDURE demo(name IN VARCHAR2) AS
sqlstr VARCHAR2;
...
BEGIN
...
sqlstr := 'SELECT * FROM states WHERE state-name = ''' || name ||
  '''';
OPEN cursor_states FOR sqlstr;
LOOP
  FETCH cursor_states INTO rec_state
  EXIT WHEN cursor_states%NOTFOUND;
  ...
 END LOOP;
CLOSE cursor_status;
...
END;
```

JDBC

„Lenevia, ca și rugina,
roade viața mai mult decât munca.”
Benjamin Franklin

PreparedStatement

- O instrucțiune *PreparedStatement* care e vulnerabilă la SQL Injection este prezentată în exemplul de mai jos:

```
String name = request.getParameter("name");
PreparedStatement pstmt =
conn.prepareStatement("insert into EMP (ENAME) values ('" +
  name + "')"); pstmt.execute();
 pstmt.close();
```

- Pentru a preveni SQL Injection, o variabilă de legătură trebuie să fie folosită:

```
PreparedStatement pstmt =
conn.prepareStatement ("insert into EMP (ENAME) values (?)");
String name = request.getParameter("name");
pstmt.setString (1, name);
pstmt.execute();
pstmt.close();
```

CallableStatement

- Procedura stocată

```
            prepareCall( "{call proc (?,?)}" );
    Bloc PL/SQL anonim
            prepareCall("begin proc1(?,?); ? :=
  func1(?);
                                    ...; end;");
```

- Mai jos este prezentat un bloc PL/SQL anonim, care este vulnerabil la atacuri:

```
String name = request.getParameter("name");
String sql = "begin ? := GetPostalCode('" + name +
  "'); end;";
CallableStatement cs = conn.prepareCall(sql);
cs.registerOutParameter(1, Types.CHAR);
cs.executeUpdate();
String result = cs.getString(1);
cs.close();
```

CallableStatement

- În cadrul unui atac, inputul ar putea fi cu mult diferit față de cel așteptat de către dezvoltator:

```
begin ? := GetPostalCode('Illinois'); end;
begin ? := GetPostalCode(''); delete from users; commit;
  dummy(''); end;
begin ? :=
  GetPostalCode(''||UTL_HTTP.REQUEST('http://192.168.1.1/'
  )||''); end;
```

- Cea mai simplă metodă de a preveni acest lucru este de a folosi cereri parametrizate:

```
String name = request.getParameter("name");
CallableStatement cs = conn.prepareCall ("begin ? :=
                    GetStatePostalCode(?); end;");
  cs.registerOutParameter(1,Types.CHAR);
cs.setString(2, name);
cs.executeUpdate();
String result = cs.getString(1);
cs.close();
```

Prevenirea *SQL Injection* în Oracle

„Anticiparea nenorocirilor viitoare atenuează sosirea lor, căci le vedem cu mult înainte de a veni.”

Marcus Tullius Cicero

Prevenirea *SQL Injection* în Oracle

- Cereri parametrizate
  - Interogările parametrizate tratează datele introduse ca pe niște valori făcând parte din comenzile SQL, în acest fel făcând imposibil ca serverul să trateze interogările parametrizate ca și cod executabil. Chiar dacă se utilizează procedurile stocate, parametrizarea inputului este necesară, pentru că procedurile stocate nu oferă protecție împotriva *SQL Injection*.
  - Cererile parametrizate trebuie folosite pentru fiecare comandă SQL indiferent de când sau unde este executată această comandă.
- **Validarea datelor de intrare**
  - Orice date de intrare introduse de către utilizatori, fie direct în aplicația web sau deja stocate, trebuie să fie validate după tipul serverului, lungime sau format, înainte de a fi trimise mai departe.
  - În cazul bazelor de date Oracle, caracterul ce ar putea pune în pericol securitatea bazei de date, este apostroful. Oracle interpretează ghilimelele simple consecutive ca un literal SQL, iar cea mai simplă metodă de a rezolva această problemă este de a le elimina.

Prevenirea *SQL Injection* în Oracle

- **Securitatea funcțiilor apelate**
  - Oracle are la bază sute de funcții standard, care implicit, pot avea acordate drepturi *PUBLIC*. Aplicația trebuie să conțină funcții suplimentare care să execute operații precum schimbarea parolelor sau crearea unor useri care ar putea să fie exploatați printr-un eventual atac.
  - Toate funcțiile care nu sunt absolut necesare aplicației ar trebui limitate.
- Mesajele de eroare
  - Acesta este punctul de plecare pentru cele mai populare atacuri *SQL Injection*.
  - Însă, ascunderea mesajelor de eroare nu are ca efect oprirea atacului. În cazul în care un atac eșuează, atacatorul poate utiliza informația din mesajele de eroare furnizate de server sau aplicație, pentru a lansa un alt atac.
  - Un atac ce utilizează vulnerabilitatea *SQL Injection* ar putea dezvălui structura unui tabel, a bazei de date, sau să expună logica de interogare, și posibil chiar parole sau informații sensibile utilizate în interogare.

Prevenirea *SQL Injection* în Oracle

- Pentru a evita un atac *SQL Injection* bazat pe mesajele de eroare primite de la serverul aplicației, programatorul trebuie să aibă în vedere:
  - mesajele de eroare să conțină cât mai puține de detalii cu privire la baza de date, care pot fi utilizare pentru a compromite întreg sistemul.
  - mesajele de eroare nu trebuie să conțină numele metodelor, funcțiilor în care a avut loc eroarea.
  - mesajele de eroare trebuie păstrate într-un fișier log, însă trebuie restricționat accesul la ele pentru a evita un posibil nou atac.
  - în fișierele log nu trebuie reținute informații precum parolele userilor.
  - mesajele de eroare nu trebuie să conțină informații privind evenimente interne ale sistemului, ca de exemplu, în caz de logare nereușită, utilizatorul nu trebuie să fie informații dacă există sau nu userul respectiv, ci doar că autentificarea nu a fost posibilă.

Excepții

„Nu există norme. Toți oamenii
sunt excepții ale unei legi care nu există.”
Fernando Pessoa

Excepții

- **Nume de tabele dinamice**
  - Orice tabel dinamic sau nume de coloană trebuie să fie validate, iar toate caracterele invalide ar trebui eliminate, în special apostrofurile. Pentru aceasta, în PL/SQL, poate fi utilizată funcția *TRANSLATE*:

```
translate ( upper ( <input string> ),
  'ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890_#$@.
  `~!%^*()-=+{}[];":''?/><,|\',
'ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890_#$@.');
```

Excepții

- **Clauza LIKE**
  - Următoarea concatenare nu ar trebui utilizată:

```
String name = request.getParameter("name");
conn.prepareStatement("SELECT id
    FROM users
    WHERE name LIKE '%" + name + "%'");
```

  - Mai degrabă se folosesc comenzi multiple și o cerere parametrizată pentru a crea în mod corespunzător o instrucțiune SQL

```
String name = request.getParameter("name");
name = query.append("%").append(name).append("%");
pstmt = conn.prepareStatement("SELECT id
FROM users
WHERE name LIKE ?");
pstmt.setString (1, name);
```

Funcții Oracle

„Nu este îndeajuns să ai o minte bună.
Scopul principal e să o folosești bine.”
Rene Descartes

Funcții Oracle

- **Determinarea privilegiilor funcțiilor**
  - Toate funcțiile disponibile PUBLIC pot fi găsite prin următoarea cerere:

```
SELECT *
FROM dba_tab_privs p, all_arguments a
WHERE grantee = 'PUBLIC'
AND privilege = 'EXECUTE'
AND p.table_name = a.package_name
AND p.owner = a.owner
AND a.position = 0
AND a.in_out = 'OUT'
ORDER BY p.owner, p.table_name, p.grantee;
```

- **Restricționarea accesului la funcții**
  - Accesul la o anumită funcție dintr-un pachet nu poate fi restricționat, ci doar accesul la întreg pachetul. Pentru a restricționa accesul PUBLIC la un pachet se folosește următoarea comandă:

```
REVOKE EXECUTE ON <package_name> FROM public;
```

Funcții Oracle

- **Funcții standard**
  - Supraîncărcarea bufferelor a fost descoperită în câteva funcții standard ORACLE: BFILENAME, TZ_OFFSET, TO_TIMESTAMP_TZ, FROM_TZ, NUMTOYMINTERVAL, și NUMTODSINTERVAL.
  - Aceste funcții aparțin pachetului STANDARD și nu există nici o modalitate de a restricționa accesul la ele.
- **Funcții oferite de ORACLE**
  - Oracle oferă sute de funcții în pachetele bazei de date standard. Majoritatea acestor pachete sunt prefixate de DBMS_ și UTL_. Dacă un anumit pachet nu este folosit de aplicație, accesul la el ar trebui limitat.

Exemple reale - SQL Injection

„Lumea e atât de tare ocupată cu aparența,
încât prea puțin îi pasă de realitate.”
Oxenstierna

Exemple reale - SQL Injection

- **1 noiembrie 2005** : un elev de liceu a folosit o inserție SQL pentru a pătrunde în site-ul unei reviste de securitate taiwaneze și a fura informațiile clienților.
- **13 ianuare 2006** : un grup de infractori ruși au pătruns într-un site al guvernului Rhode Island, și se presupune că a furat datele cărților de credit de la persoane care au făcut afaceri online cu agențiile de stat.
- **2 martie 2007** : Sebastian Bauer a descoperit un defect de inserție SQL în pagina de login knorr.de.
- **29 iunie 2007** : un infractor a neutralizat site-ul Microsoft din Marea Britanie folosind SQL Injection. Un purtător de cuvânt al Microsoft a recunoscut problema site-ului *The Register* din U.K..

Exemple reale - SQL Injection

- **ianuarie 2008** : zeci de mii de PC-uri au fost infectate de un atac *SQL Injection* automat, care a exploatat o vulnerabilitate în codul aplicațiilor ce utilizează Microsoft SQL Server pentru stocarea bazei de date.
- **17 august 2009** : Departamentul de Justiție al Statelor Unite au acuzat un cetățean american, Albert Gonzalez și doi ruși anonimi de furtul a 130 milioane de numere de cărți de credit folosind un atac *SQL Injection*. În relatările presei apare că "cel mai mare caz de furt de identitate din istoria Statelor Unite", omul a furat carduri de la un număr de victime corporative după cercetarea sistemelor de prelucrare a plății. Printre companiile lovite se numără: procesorul de sisteme de plată *Heartland Payment Systems*, lanțul de magazine economice *7-Eleven* și lanțul de supermarketuri *Hannaford Brothers*.
- **decembrie 2009** : un atacator a pătruns într-o bază de date RockYou! prin utilizarea unui atac *SQL Injection,* care conținea în format text numele de utilizator și parolele necriptate pentru aproximativ 32 milioane de utilizatori.
- ...

Exemple reale - SQL Injection

- **25 octombrie 2018 :**
- The Wordfence Web Application Firewall has blocked 134 attacks over the last 10 minutes. Below is a sample of these recent attacks:

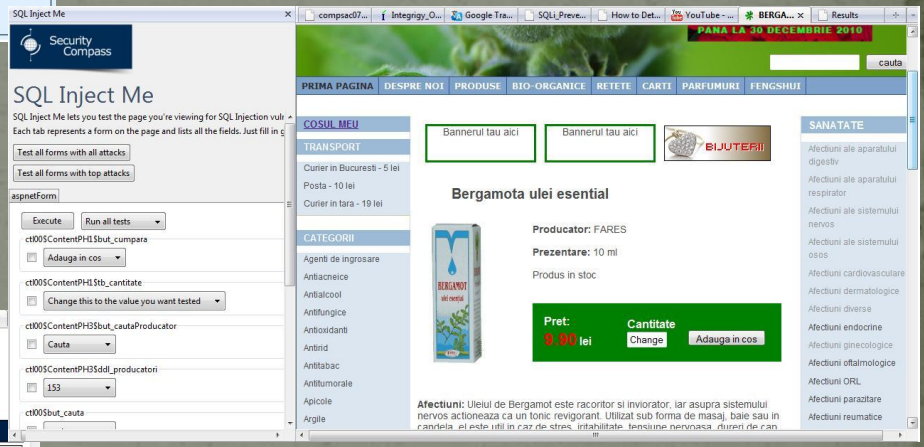
- octombrie 25, 2018 5:07pm 5.101.40.234 (Russian Federation) Blocked for SQL Injection in query string: full=1%' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL#
- octombrie 25, 2018 5:07pm 5.101.40.234 (Russian Federation) Blocked for SQL Injection in query string: full=1%' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL#
- octombrie 25, 2018 5:07pm 5.101.40.234 (Russian Federation) Blocked for SQL Injection in query string: full=1%' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL#
- octombrie 25, 2018 5:07pm 5.101.40.234 (Russian Federation) Blocked for SQL Injection in query string: full=1%' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL#
- octombrie 25, 2018 5:07pm 5.101.40.234 (Russian Federation) Blocked for SQL Injection in query string: full=1%' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL#
- octombrie 25, 2018 5:07pm 5.101.40.234 (Russian Federation) Blocked for SQL Injection in query string: full=1%' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL#
- octombrie 25, 2018 5:07pm 5.101.40.234 (Russian Federation) Blocked for SQL Injection in query string: full=1%' UNION ALL SELECT NULL,NULL,NULL,NULL#
- octombrie 25, 2018 5:07pm 5.101.40.234 (Russian Federation) Blocked for SQL Injection in query string: full=1%' UNION ALL SELECT NULL,NULL,NULL#
- octombrie 25, 2018 5:07pm 5.101.40.234 (Russian Federation) Blocked for SQL Injection in query string: full=1%' UNION ALL SELECT NULL,NULL#
- octombrie 25, 2018 5:07pm 5.101.40.234 (Russian Federation) Blocked for SQL Injection in query string: full=1%' UNION ALL SELECT NULL#

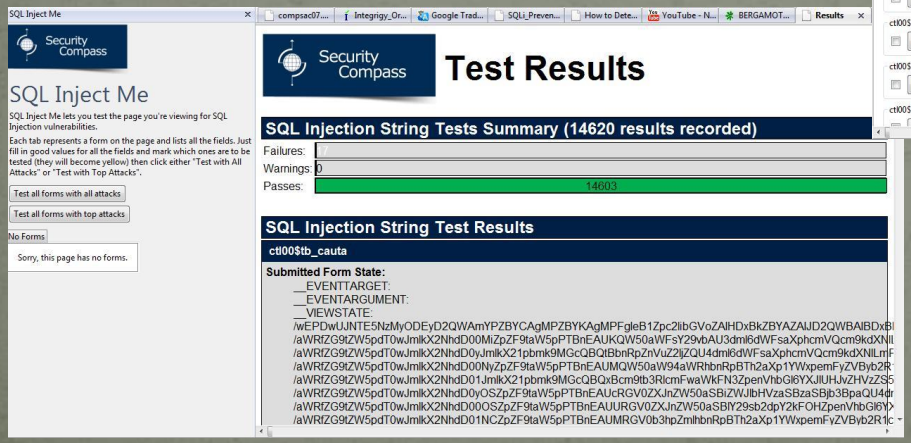
Aplicatii si tool-uri pentru detectarea SQL Injection

SQL Injection me (Firefox Add-on)

- In browser in meniul Tools -> SQL Inject Me -> Open SQL Inject Me Sidebar
- se selecteaza testele care urmeaza a fi rulate (Run all test, Run top 9 tests)
- de asemenea, exista posibilitatea de a testa toate formularele din site-ul web cu toate tipurile de atac sau toate formularele cu cele mai frecvente 9 tipuri de atac
- dupa executarea testelor se va deschide o noua pagina web care va contine un raport al executiei testelor


Add-ons for Firefox > Extensions > SQL Inject Me
SQL Inject Me 0.4.5
by Security Compass
Security Compass
SQL Injection vulnerabilites can cause a lot of damage to a web application. A malicious user can possibly view records, delete records, drop tables or gain access to your server. SQL Inject-Me is Firefox Extension used to test for SQL Injection vulnerabilities.
Continue to Download
Add to collection
Share this Add-on
Updated May 5, 2010
Website http://labs.securitycompass.com/index.php/exploit-me/
Works with Firefox 2.0.0.8 - 3.7a1pre
Rating 12 reviews
Downloads 162,223


SQL Inject Me
Security Compass
SQL Inject Me
Test all forms with all attacks
Test all forms with top attacks
Execute
Run all tests
PANA LA 30 DECEMBRIE 2010
PRIMA PAGINA
DESPRE NOI
PRODUSE
BIO-ORGANICE
RETETE
CARTI
PARFUMURI
FENGSHUI
COSUL MEU
TRANSPORT
CATEGORII
Bannerul tau aici
Bergamota ulei esential
Producator: FARES
Prezentare: 10 ml
Produs in stoc
Pret:
9.90 lei
Cantitate
Change
Adauga in cos
SANATATE


SQL Inject Me
Security Compass
SQL Inject Me
Test all forms with all attacks
Test all forms with top attacks
No Forms
Sorry, this page has no forms.
Test Results
SQL Injection String Tests Summary (14620 results recorded)
Failures: 0
Warnings: 0
Passes: 14603
SQL Injection String Test Results
ctl00$tb_cauta
Submitted Form State:
__EVENTTARGET:
__EVENTARGUMENT:
__VIEWSTATE:

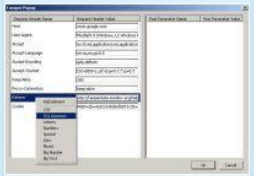
Tamper Data (Firefox Add-on)

- Pentru a utiliza acest add-on trebuie urmati pasii de mai jos:
  - se downloadeaza si se instaleaza add-on-ul Tamper Data
  - se porneste browserul Firefox
  - se selecteaza meniul Tools -> Tamper Data
  - se apasa Start Tamper
  - din browser se fac request-uri catre un site web
  - requesturile sunt inregistrate in Tamper Data – Ongoing requests (imaginea de mai jos)
  - intr-un textbox se introduce o valoare si se apasa butonul submit
  - o fereastra de tip pop-up este deschisa din Tamper Data, unde se specifica actiunea dorita: se trimite requestul mai departe catre server cu datale introduse de utilizator (Submit), se opreste cererea catre server (Abort request) sau se pot schimba parametrii cererii (Tamper)
  - daca se apasa butonul Tamper se pot vedea si schimba parametrii requestului respectiv; daca totul este in regula si nu a fost detectat un input malitios se apasa butonul Ok (imaginea de mai jos)

Add-ons for Firefox > Extensions > Tamper Data

Tamper Data 11.0.1

by Adam Judson



Use tamperdata to view and modify HTTP/HTTPS headers and post parameters...

Continue to Download ›

Updated	February 11, 2010
Website	http://tamperdata.mozde
Works with	Firefox 3.5 - 3.6.*
Rating	★★★★★ 79 reviews
Downloads	3,432,430

Add to collection

Share this Add-on

Tamper Data - Ongoing requests

Start Tamper | Stop Tamper | Clear | Options | Help

Filter | Show All

Time	Duration	Total Duration	Size	Method	Status	Content Type	URL	Load Flags
17:17:03.5...	426 ms	426 ms	40702	GET	200	text/html	http://gr...	LOAD_DOCUM...
17:17:03.9...	0 ms	0 ms	unknown	GET	pending	unknown	http://gr...	LOAD_NORMAL
17:17:04.0...	0 ms	0 ms	unknown	GET	pending	unknown	http://gr...	LOAD_NORMAL
17:17:06.8...	n/a ms	n/a ms	unknown	GET	Cancelled	unknown	http://gr...	LOAD_NORMAL
17:17:07.7...	n/a ms	n/a ms	unknown	GET	Cancelled	unknown	http://gr...	LOAD_NORMAL
17:17:18.8...	n/a ms	n/a ms	unknown	GET	Cancelled	unknown	http://s....	LOAD_NORMAL

Request Header Name	Request Header Value

Response Header Name	Response Header Value

Tamper Popup

http://greenmedica.ro/search.aspx?cuvant=1+and+1%3d1

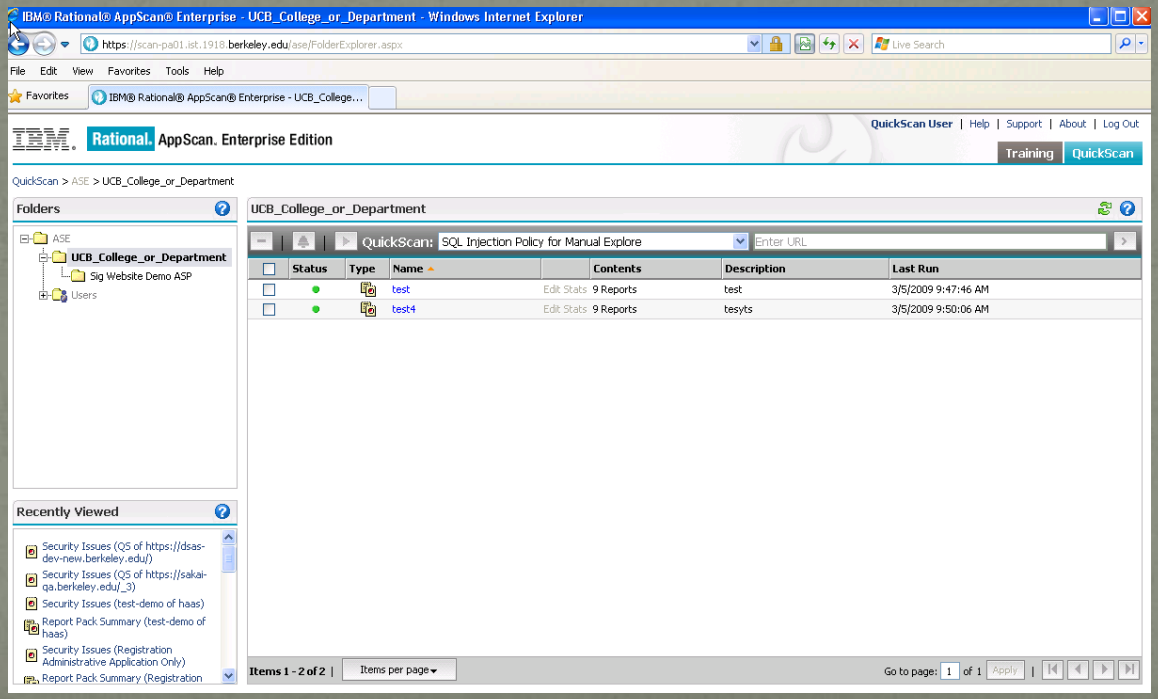
Request Header Name	Request Header Value
Host	greenmedica.ro
User-Agent	Mozilla/5.0 (Windows; U; Windows NT 6
Accept	text/html,application/xhtml+xml,applic
Accept-Language	en-gb,en;q=0.5
Accept-Encoding	gzip,deflate
Accept-Charset	ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive	300
Connection	keep-alive
Referer	http://greenmedica.ro/search.aspx?cuv

Post Parameter Name	Post Parameter Value
__VIEWSTATE	%2FwEPDwUINDM3MjI0MjUP
__EVENTTARGET	
__EVENTARGUMENT	
__EVENTVALIDATION	%2FwEWuAEC%2B4Su6QkCkf
ctl00%24tb_cauta	1+and+1%3D1
ctl00%24but_cauta	cauta
ctl00%24ContentPH3%24ddl_producatori	153

OK | Cancel

AppScan – Application Vulnerability Scanner

- Parcurge o aplicatie web pentru a gasi punctele vulnerabile ale acesteia. Scannerul va cauta vulnerabilitati des intalnite, cum ar fi cross-site scripting, sql injection sau session hijacking.

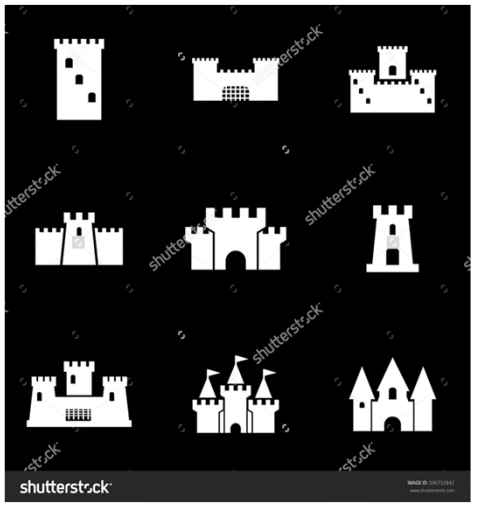


1.1 The Cybersecurity World

Cisco | Networking Academy®
Mind Wide Open™

Overview of the Kingdoms

- Websites and Power of Data
  - Great businesses have been created by collecting and harnessing the power of data and data analytics
  - These businesses have the responsibility to protect this data from misuse and unauthorized access
  - The growth of data has created great opportunities for cybersecurity specialists
- Kingdoms
  - Business large and small have recognized the power of big data and data analytics
  - Organizations like Google, LinkedIn, Amazon provide important services and opportunity for their customers
  - The growth in data collection and analytics poses great risks to individuals and modern life if precautions are not taken to protect sensitive data from criminals or others who have intent to harm



Overview of the Kingdoms (Cont.)

- Cyber wizards now have the technology to track worldwide weather trends, monitor the oceans, and track the movement and behavior of people, animals and objects in real time.
- New technologies, such as Geospatial Information Systems (GIS) and the Internet of Everything (IoE), have emerged. Each depends on collecting and analyzing tremendous amounts of data.
- This growing collection of data can help people save energy, improve efficiencies, and reduce safety risks.

1.2 Cyber Criminals versus Cyber Professionals

Cisco | Networking Academy®
Mind Wide Open™

Cybersecurity Criminals

- **Hackers** – This group of criminals breaks into computers or networks to gain access for various reasons.

  White hat attackers break into networks or computer systems to discover weaknesses in order to improve the security of these systems.

  Gray hat attackers are somewhere between white and black hat attackers. The gray hat attackers may find a vulnerability and report it to the owners of the system if that action coincides with their agenda.

  Black hat attackers are unethical criminals who violate computer and network security for personal gain, or for malicious reasons, such as attacking networks.

Cybersecurity Criminals (Cont.)

Criminals come in many different forms. Each have their own motives:

- **Script Kiddies** - Teenagers or hobbyists mostly limited to pranks and vandalism, have little or no skill, often using existing tools or instructions found on the Internet to launch attacks.
- **Vulnerability Brokers** - Grey hat hackers who attempt to discover exploits and report them to vendors, sometimes for prizes or rewards.
- **Hacktivists -** Grey hat hackers who rally and protest against different political and social ideas. Hacktivists publicly protest against organizations or governments by posting articles, videos, leaking sensitive information, and performing distributed denial of service (DDoS) attacks.

Cybersecurity Criminals (Cont.)

Criminals come in many different forms. Each have their own motives:

- **Cyber Criminals** - These are black hat hackers who are either self-employed or working for large cybercrime organizations. Each year, cyber criminals are responsible for stealing billions of dollars from consumers and businesses.
- **State Sponsored Hackers -** Depending on a person's perspective, these are either white hat or black hat hackers who steal government secrets, gather intelligence, and sabotage networks. Their targets are foreign governments, terrorist groups, and corporations. Most countries in the world participate to some degree in state-sponsored hacking.

Cybersecurity Specialists

Thwarting the cyber criminals is a difficult task, company, government and international organizations have begun to take coordinated actions to limit or fend off cyber criminals. The coordinated actions include:

- **Vulnerability Database**: The Nation Common Vulnerabilities and Exposures (CVE) database is an example of the development of a national database. The CVE National Database was developed to provide a publicly available database of all know vulnerabilities. http://www.cvedetails.com/
- **Early Warning Systems**: The Honeynet project is an example of creating Early Warning Systems. The project provides a HoneyMap which displays real-time visualization of attacks. https://www.honeynet.org/node/960
- **Share Cyber Intelligence**: InfraGard is an example of wide spread sharing of cyber intelligence. The InfraGard program is a partnership between the and the private sector. The participants are dedicated to sharing information and intelligence to prevent hostile cyberattacks. https://www.infragard.org/

Cybersecurity Specialist (Cont.)

- **ISM Standards**: The ISO 27000 standards are an example of Information Security Management Standards. The standards provide a framework for implementing cybersecurity measures within an organization. http://www.27000.org/
- **New Laws**: The ISACA group track law enacted related to cyber security. These laws can address individual privacy to protection of intellectual property. Examples of these laws include: Cybersecurity Act, Federal Exchange Data Breach Notification Act and the Data Accountability and Trust Act. http://www.isaca.org/cyber/pages/cybersecuritylegislation.aspx

Tools for Thwarting Cybercrime

1.3 Threats to the Kingdom

Cisco | Networking Academy®
Mind Wide Open™

Threats to the Kingdom

Threat Arenas

- The term cyber wizards refers to the innovators and visionaries that build the cyber kingdom
- Cyber wizards possess the insight to recognize the influence of data and harness that power to build great organizations, provide services and protect people from cyberattacks
- Cyber wizards recognize the threat that data poses if used against people
- A cybersecurity threat is the possibility that a harmful event, such as an attack, will occur
- Cyber vulnerability is a weakness that makes a target susceptible to an attack
- Cyber threats are particularly dangerous to certain industries and the type of information they collect and protect

Threat Arenas (Cont.)

The following examples are just a few sources of data that can come from established organizations:

- **Personal Information**
- **Medical Records**
- **Education Records**
- **Employment and Financial Records**

Threat Arenas (Cont.)

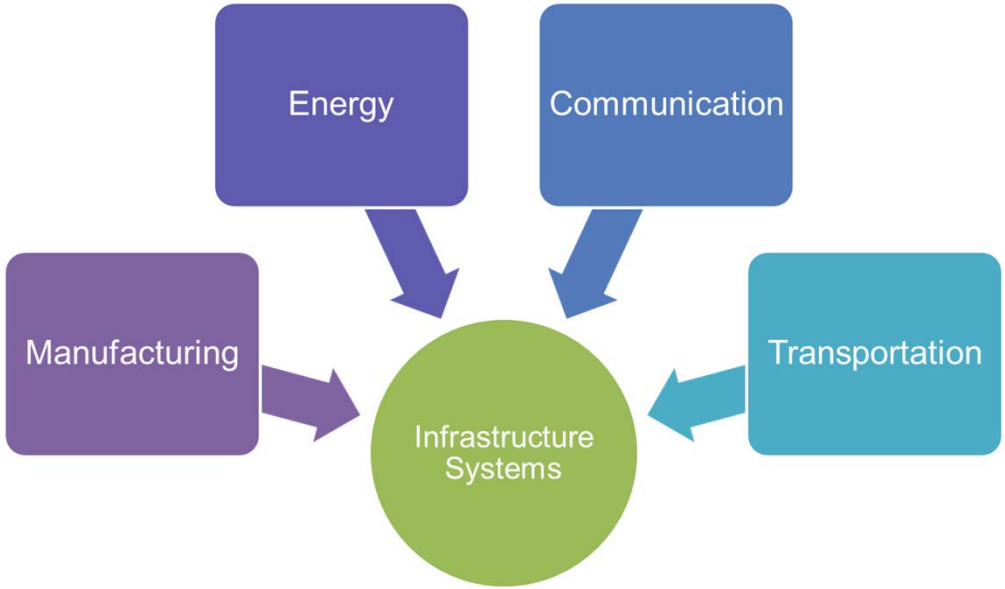
Network services like DNS, HTTP and Online Databases are prime targets for cyber criminals.

- Criminals use packet-sniffing tools to capture data streams over a network. Packet sniffers work by monitoring and recording all information coming across a network.
- Criminals can also use rogue devices, such as unsecured Wi-Fi access points.
- Packet forgery (or packet injection) interferes with an established network communication by constructing packets to appear as if they are part of a communication.

Threat Arenas (Cont.)

Sectors of the kingdom include:

- Manufacturing
  - Industry Controls
  - Automation
  - SCADA
- Energy Production and Distribution
  - Electrical Distribution and Smart Grid
  - Oil and Gas
- Communication
  - Phone
  - Email
  - Messaging
- Transportation systems
  - Air Travel
  - Rail
  - Over the Road



Threat Arenas (Cont.)

- On a personal level, everyone needs to safeguard his or her identity, data, and computing devices.
- At the corporate level, it is the employees' responsibility to protect the organization's reputation, data, and customers.
- At the state level, national security and the citizens' safety and well-being are at stake.
- In the U.S., the National Security Agency (NSA) is responsible for intelligence collection and surveillance activities.
- The efforts to protect people's way of life often conflicts with their right to privacy.

1.4 The Dark Forces of Cybersecurity

Cisco | Networking Academy®
Mind Wide Open™

The Spread of the Dark Forces

Attacks can originate from within an organization or from outside of the organization, as shown in the figure.

Internal Security Threats

- An internal user, such as an employee or contract partner, can accidently or intentionally
- Internal threats have the potential to cause greater damage than external threats because internal users have direct access to the building and its infrastructure devices. Internal attackers typically have knowledge of the corporate network, its resources, and its confidential data. They may also have knowledge of security countermeasures, policies and higher levels of administrative privileges.

External Security Threats

- External threats from amateurs or skilled attackers can exploit vulnerabilities in networked devices, or can use social engineering, such as trickery, to gain access.
- External attacks exploit weaknesses or vulnerabilities to gain access to internal resources.

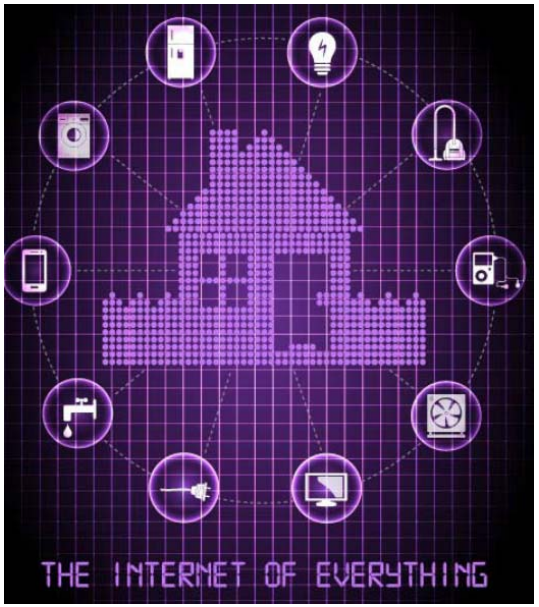
The Spread of the Dark Forces (Cont.)

Vulnerabilities of Mobile Devices - In the past, employees typically used company-issued computers connected to a corporate LAN.

- Today, mobile devices such as iPhones, smartphones, tablets, and thousands of other devices, are becoming powerful substitutes for, or additions to, the traditional PC.
- More and more people are using these devices to access enterprise information. Bring Your Own Device (BYOD) is a growing trend.
- The inability to centrally manage and update mobile devices poses a growing threat to organizations that allow employee mobile devices on their networks.

The Spread of the Dark Forces (Cont.)

- **Emergence Internet-of-Things** - The Internet of Things (IoT) is the collection of technologies that enable the connection of various devices to the Internet.
- IoT technologies enable people to connect billions of devices to the Internet. These devices include appliances, locks, motors, and entertainment devices, to name just a few.
- This technology affects the amount of data that needs protection. Users access these devices remotely, which increases the number of networks requiring protection.
- With the emergence of IoT, there is much more data to be managed and secured. All of these connections, plus the expanded storage capacity and storage services offered through the Cloud and virtualization, has led to the exponential growth of data.



The Spread of the Dark Forces (Cont.)

Impact of Big Data – Big data is the result of data sets that are large and complex, making traditional data processing applications inadequate. Big data poses both challenges and opportunities based on three dimensions:

- The volume or amount of data
- The velocity or speed of data
- The variety or range of data types and sources

There are numerous examples of big corporate hacks in the news. As a result, enterprise systems require dramatic changes in security product designs and substantial upgrades to technologies and practices. Additionally, governments and industries are introducing more regulations and mandates that require better data protection and security controls to help guard big data.

The Sophistication of the Dark Forces

Advanced Weapons

- Advanced persistent threat (APT) is a continuous computer hack that occurs under the radar against a specific object. Criminals usually choose an APT for business or political motives.
- Algorithm attacks can track system self-reporting data, like how much energy a computer is using, and use that information to select targets or trigger false alerts. Algorithmic attacks are more devious because they exploit designs used to improve energy savings, decrease system failures, and improve efficiencies.
- Intelligent selection of victims. In the past, attacks would select the low hanging fruit or most vulnerable victims. Many of the most sophisticated attacks will only launch if the attacker can match the signatures of the targeted victim.

Broader Scope and Cascade Effect

- Federated identity management refers to multiple enterprises that let their users use the same identification credentials gaining access to the networks of all enterprises in the group. The goal of federated identity management is to share identity information automatically across castle boundaries.
- The most common way to protect federated identity is to tie login ability to an authorized device.

The Sophistication of the Dark Forces (Cont.)

Safety Implications

- There are many safety implication associated with the dark forces of cyber security including emergency call centers in the U.S. are vulnerable to cyberattacks that could shut down 911 networks, jeopardizing public safety.
- A telephone denial of service (TDoS) attack uses phone calls against a target telephone network tying up the system and preventing legitimate calls from getting through.
- The next generation 911 call centers are vulnerable because they use Voice-over-IP (VoIP) systems rather than traditional landlines.

Heightened Recognition of Cybersecurity Threats

- The defenses against cyberattacks at the start of the cyber era were low. A smart high school student or script kiddie could gain access to systems.
- Now, countries across the world have become more aware of the threat of cyberattacks. The threat posed by cyberattacks now head the list of greatest threats to national and economic security in most countries.

1.5 Creating More Heroes

Cisco | Networking Academy®
Mind Wide Open™

Creating More Heroes

A Workforce Framework for Cybersecurity

Addressing the Shortage of Cybersecurity Specialists

- In the U.S., the National Institute of Standards and Technologies (NIST) created a framework for companies and organizations in need of cybersecurity professionals. The framework enables companies to identify the major types of responsibilities, job titles, and workforce skills needed.

The Seven Categories of Cybersecurity Wizards

The Workforce Framework categorizes cybersecurity work into seven categories.

- **Operate and Maintain** includes providing the support, administration, and maintenance required to ensure IT system performance and security
- **Protect and Defend** includes the identification, analysis, and mitigation of threats to internal systems and networks
- **Investigate** includes the investigation of cyber events and/or cyber crimes involving IT resources
- **Collect and Operate** includes specialized denial and deception operations and the collection of cybersecurity information

A Workforce Framework for Cybersecurity (Cont.)

- **Analyze** includes highly specialized review and evaluation of incoming cybersecurity information to determine if it is useful for intelligence
- **Oversight and Development** provides for leadership, management, and direction to conduct cybersecurity work effectively
- **Securely Provision** includes conceptualizing, designing, and building secure IT systems

Within each category, there are several specialty areas. The specialty areas then define common types of cybersecurity work.

2.1 The Cybersecurity Sorcery Cube

Cisco | Networking Academy®
Mind Wide Open™

The Three Dimensions

The Principles of Security

- The first dimension of the cybersecurity sorcery cube identifies the goals to protect the cyber world. The goals identified in the first dimension are the foundational principles of the cybersecurity world.
- These three principles are confidentiality, integrity and availability.
- The principles provide focus and enable the cyber wizard to prioritize actions in protecting the cyber world.
- Use the acronym CIA to remember these three principles.

The States of Data

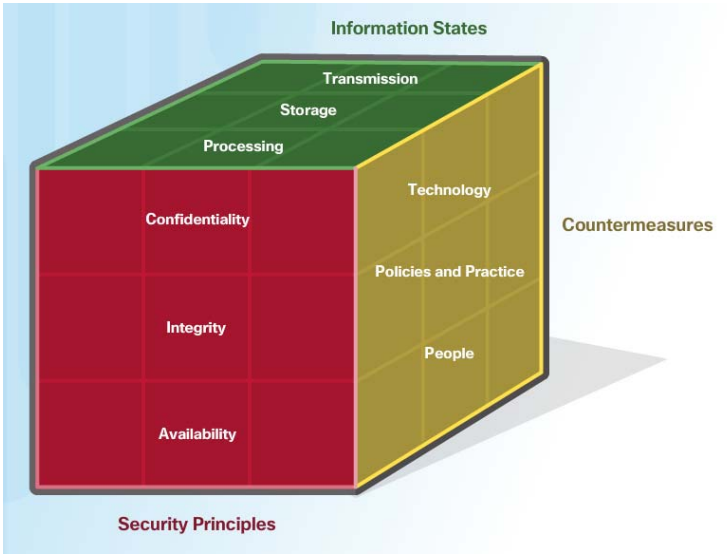
- The cyber world is a world of data; therefore, cyber wizards focus on protecting data. The second dimension of the cybersecurity sorcery cube focuses on the problems of protecting all of the states of data in the cyber world. Data has three possible states:

  1) Data at rest or in storage 2) Data in transit 3) Data in process

The Three Dimensions (Cont.)

Cybersecurity Safeguards

- The third dimension of the cybersecurity sorcery cube defines the types of powers used to protect the cyber world. The sorcery cube identifies the three types of powers:
- **Technologies -** devices, and products available to protect information systems and fend off cyber criminals.
- **Policies and Practices -** procedures, and guidelines that enable the citizens of the cyber world to stay safe and follow good practices.
- **People -** Aware and knowledgeable about their world and the dangers that threaten their world.



2.2 CIA TRIAD

Cisco | Networking Academy®
Mind Wide Open™

Confidentiality

The Principle of Confidentiality

- Confidentiality prevents the disclosure of information to unauthorized people, resources and processes. Another term for confidentiality is privacy.
- Organizations need to train employees about best practices in safeguarding sensitive information to protect themselves and the organization from attacks.
- Methods used to ensure confidentiality include data encryption, authentication, and access control.

Protecting Data Privacy

- Organizations collect a large amount of data and much of this data is not sensitive because it is publicly available, like names and telephone numbers.
- Other data collected, though, is sensitive. Sensitive information is data protected from unauthorized access to safeguard an individual or an organization.

Confidentiality (Cont.)

Controlling Access

Access control defines a number of protection schemes that prevent unauthorized access to a computer, network, database, or other data resources. The concepts of AAA involve three security services: Authentication, Authorization and Accounting. ***Authentication*** verifies the identity of a user to prevent unauthorized access. Users prove their identity with a username or I.D.

Authorization services determine which resources users can access, along with the operations that users can perform. Authorization can also control when a user has access to a specific resource.

Accounting keeps track of what users do, including what they access, the amount of time they access resources, and any changes made.

Confidentiality (Cont.)

Confidentiality and privacy seem interchangeable, but from a legal standpoint, they mean different things.

- Most privacy data is confidential, but not all confidential data is private. Access to confidential information occurs after confirming proper authorization. Financial institutions, hospitals, medical professionals, law firms, and businesses handle confidential information.
- Confidential information has a non-public status. Maintaining confidentiality is more of an ethical duty.
- Privacy is the appropriate use of data. When organizations collect information provided by customers or employees, they should only use that data for its intended purpose.

U.S. Laws

- Privacy Act of 1974
- Freedom of Information ACT (FOIA)
- Family Education Records and Privacy Act (FERPA)
- U.S. Computer Fraud and Abuse Act (CFAA)
- U.S. Children's Online Privacy Protection Act (COPPA)
- Video Privacy Protection Act (VPPA)
- Health Insurance Portability & Accountability Act
- Gramm-Leach-Bliley Act (GLBA)
- California Senate Bill 1386 (SB 1386)
- U.S. Banking Rules and Regulations
- Payment Card Industry Data Security Standard (PCI DSS)
- Fair Credit Reporting Act (FCRA)

Integrity

Principle of Data Integrity

- Integrity is the accuracy, consistency, and trustworthiness of data during its entire life cycle.
- Another term for integrity is quality.
- Methods used to ensure data integrity include hashing, data validation checks, data consistency checks, and access controls.

Need for Data Integrity

- The need for data integrity varies based on how an organization uses data. For example, Facebook does not verify the data that a user posts in a profile.
- A bank or financial organization assigns a higher importance to data integrity than Facebook does. Transactions and customer accounts must be accurate.
- Protecting data integrity is a constant challenge for most organizations. Loss of data integrity can render entire data resources unreliable or unusable.

Integrity Checks

- An integrity check is a way to measure the consistency of a collection of data (a file, a picture, or a record). The integrity check performs a process called a hash function to take a snapshot of data at an instant in time.

Availability

Data availability is the principle used to describe the need to maintain availability of information systems and services at all times. Cyberattacks and system failures can prevent access to information systems and services.

- Methods used to ensure availability include system redundancy, system backups, increased system resiliency, equipment maintenance, up-to-date operating systems and software, and plans in place to recover quickly from unforeseen disasters.
- High availability systems typically include three design principles: eliminate single points of failure, provide for reliable crossover, and detect failures as they occur.

Organizations can ensure availability by implementing the following:

1. Equipment maintenance
2. OS and system updates
3. Test backups
4. Plan for disasters
5. Implement new technologies
6. Monitor unusual activity
7. Test to verify availability

2.3 States of Data

Cisco | Networking Academy®
Mind Wide Open™

Data at Rest

- Stored data refers to data at rest. Data at rest means that a type of storage device retains the data when no user or process is using it.
- A storage device can be local (on a computing device) or centralized (on the network). A number of options exist for storing data.
- Direct-attached storage (DAS) is storage connected to a computer. A hard drive or USB flash drive is an example of direct-attached storage.

Data at Rest (Cont.)

- Redundant array of independent disks (RAID) uses multiple hard drives in an array, which is a method of combining multiple disks so that the operating system sees them as a single disk. RAID provides improved performance and fault tolerance.
- A network attached storage (NAS) device is a storage device connected to a network that allows storage and retrieval of data from a centralized location by authorized network users. NAS devices are flexible and scalable, meaning administrators can increase the capacity as needed.
- A storage area network (SAN) architecture is a network-based storage system. SAN systems connect to the network using high-speed interfaces allowing improved performance and the ability to connect multiple servers to a centralized disk storage repository.

Data In Transit

Data transmission involves sending information from one device to another. There are numerous methods to transmit information between devices including:

- **Sneaker net** – uses removable media to physically move data from one computer to another
- **Wired networks** – uses cables to transmit data
- **Wireless networks** – uses the airwaves to transmit data

The protection of transmitted data is one of the most challenging jobs of a cybersecurity professional. The greatest challenges are:

- **Protecting data confidentiality** – cyber criminals can capture, save and steal data in-transit.
- **Protecting data integrity** – cyber criminals can intercept and alter data in-transit.
- **Protecting data availability** - cyber criminals can use rogue or unauthorized devices to interrupt data availability.

Data In Process

The third state of data is data in process. This refers to data during initial input, modification, computation, or output.

- Protection of data integrity starts with the initial input of data.
- Organizations use several methods to collect data, such as manual data entry, scanning forms, file uploads, and data collected from sensors.
- Each of these methods pose potential threats to data integrity.
- Data modification refers to any changes to the original data such as users manually modifying data, programs processing and changing data, and equipment failing resulting in data modification.
- Processes like encoding/decoding, compression/decompression and encryption/decryption are all examples of data modification. Malicious code also results in data corruption.

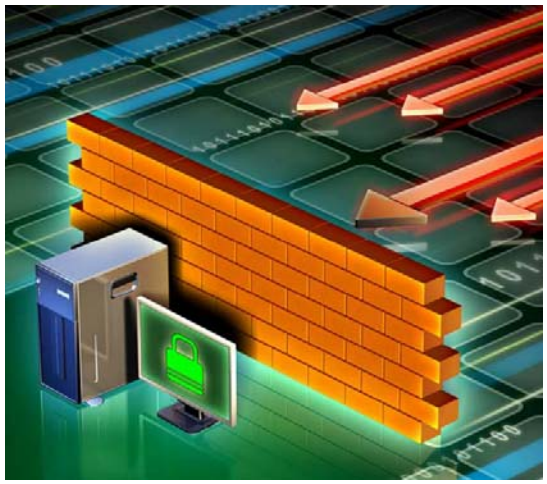
2.4 Cybersecurity Countermeasures

Cisco | Networking Academy®
Mind Wide Open™

Technologies

Software-based Technology Safeguards

- Software safeguards include programs and services that protect operating systems, databases, and other services operating on workstations, portable devices, and servers. There are several software-based technologies used to safeguard an organization's assets.



Hardware-based Technology Safeguards

- Hardware based technologies are appliances that are installed within the network faculties. They can include: Firewall appliances, Intrusion Detection Systems (IDS),Intrusion Prevention Systems (IPS) and Content filtering systems.

Technologies

Network-based Technology Safeguards

Technological countermeasures can also include network-based technologies.

- **Virtual Private Network (VPN)** is a secure virtual network that uses the public network (i.e., the Internet). The security of a VPN lies in the encryption of packet content between the endpoints that define the VPN.
- **Network access control (NAC)** requires a set of checks before allowing a device to connect to a network. Some common checks include up-to-data antivirus software or operating system updates installed.
- **Wireless access point security** includes the implementation of authentication and encryption.

Technologies

Cloud-based Technology Safeguards

- Technological countermeasures now also include cloud-based technologies. Cloud-based technologies shift the technology component from the organization to the cloud provider.
- **Software as a Service (SaaS)** allows users to gain access to application software and databases. Cloud providers manage the infrastructure. Users store data on the cloud provider's servers.
- **Infrastructure as a Service (IaaS)** provides virtualized computing resources over the Internet. The provider hosts the hardware, software, servers, and storage components.
- **Virtual security appliances** run inside a virtual environment with a pre-packaged, hardened operating system running on virtualized hardware.

Implementing Cybersecurity Education and Training

A security awareness program is extremely important for an organization. An employee may not be purposefully malicious but just unaware of what the proper procedures are.

There are several ways to implement a formal training program:

- Make security awareness training a part of the employee's onboarding process
- Tie security awareness to job requirements or performance evaluations
- Conduct in-person training sessions
- Complete online courses

Security awareness should be an ongoing process since new threats and techniques are always on the horizon.

Cybersecurity Policies and Procedures

- A security **policy** is a set of security objectives for a company that includes rules of behavior for users and administrators and specifies system requirements. These objectives, rules, and requirements collectively ensure the security of a network, the data, and the computer systems within an organization.
- **Standards** help an IT staff maintain consistency in operating the network. Standards provide the technologies that specific users or programs need in addition to any program requirements or criteria that an organization must follow.
- **Guidelines** are a list of suggestions on how to do things more efficiently and securely. They are similar to standards, but are more flexible and are not usually mandatory. Guidelines define how standards are developed and guarantee adherence to general security policies.
- **Procedure** documents are longer and more detailed than standards and guidelines. Procedure documents include implementation details that usually contain step-by-step instructions and graphics.

3.1 Malware and Malicious Code

Cisco | Networking Academy®
Mind Wide Open™

Types of Malware

Cyber criminals target user's end devices through the installation of malware.

Viruses - A virus is malicious executable code attached to another executable file, such as a legitimate program. Most viruses require end-user initiation, and can activate at a specific time or date.

Worms - Worms are malicious code that replicates by independently exploiting vulnerabilities in networks. Worms usually slow down networks. Whereas a virus requires a host program to run, worms can run by themselves. Other than the initial infection, worms no longer require user participation.

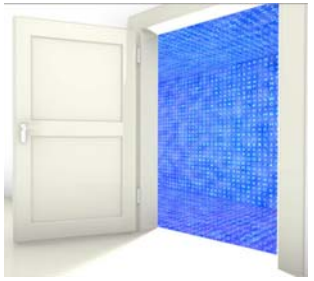
Trojan horse - A Trojan horse is malware that carries out malicious operations under the guise of a desired operation such as playing an online game. This malicious code exploits the privileges of the user that runs it. A Trojan horse differs from a virus because the Trojan binds itself to non-executable files, such as image files, audio files, or games.

Types of Malware (Cont.)

- **Logic Bomb** - A logic bomb is a malicious program that uses a trigger to awaken the malicious code. For example, triggers can be dates, times, other programs running, or the deletion of a user account. The logic bomb remains inactive until that trigger event happens. Once activated, a logic bomb implements a malicious code that causes harm to a computer.

- **Ransomware** - Ransomware holds a computer system, or the data it contains, captive until the target makes a payment. Ransomware usually works by encrypting data in the computer with a key unknown to the user.

- **Backdoors and Rootkits** - A backdoor or rootkit refers to the program or code introduced by a criminal who has compromised a system. The backdoor bypasses the normal authentication used to access a system. A rootkit modifies the operating system to create a backdoor. Attackers then use the backdoor to access the computer remotely.



Email and Browser Attacks (Cont.)

Email is a universal service used by billions worldwide. As one of the most popular services, email has become a major vulnerability to users and organizations.

Spam - Spam, also known as junk mail, is unsolicited email. In most cases, spam is a method of advertising. However, spam can send harmful links, malware, or deceptive content.

Spyware - Spyware is software that enables a criminal to obtain information about a user's computer activities. Spyware often includes activity trackers, keystroke collection, and data capture. In an attempt to overcome security measures, spyware often modifies security settings.

Email and Browser Attacks (Cont.)

Adware - Adware typically displays annoying pop-ups to generate revenue for its authors. The malware may analyze user interests by tracking the websites visited. It can then send pop-up advertising pertinent to those sites.

Scareware - Scareware persuades the user to take a specific action based on fear. Scareware forges pop-up windows that resemble operating system dialogue windows.

Email and Browser Attacks (Cont.)

Phishing - Phishing is a form of fraud. Cyber criminals use email, instant messaging, or other social media to try to gather information such as login credentials or account information by masquerading as a reputable entity or person. Phishing occurs when a malicious party sends a fraudulent email disguised as being from a legitimate, trusted source. The message intent is to trick the recipient into installing malware on his or her device or into sharing personal or financial information.

Spear phishing - Spear phishing is a highly targeted phishing attack. While phishing and spear phishing both use emails to reach the victims, spear phishing sends customized emails to a specific person.

Email and Browser Attacks (Cont.)

Vishing - Vishing is phishing using voice communication technology. Criminals can spoof calls from legitimate sources using voice over IP (VoIP) technology. Victims may also receive a recorded message that appears legitimate.

Pharming - Pharming is the impersonation of a legitimate website in an effort to deceive users into entering their credentials.

Whaling - Whaling is a phishing attack that targets high profile targets within an organization such as senior executives.

Email and Browser Attacks (Cont.)

Plugins - The Flash and Shockwave plugins from Adobe enable the development of interesting graphic and cartoon animations that greatly enhance the look and feel of a web page. Plugins display the content developed using the appropriate software.

SEO Poisoning - Search engines such as Google work by ranking pages and presenting relevant results based on users' search queries. Depending on the relevancy of web site content, it may appear higher or lower in the search result list. SEO, short for Search Engine Optimization, is a set of techniques used to improve a website's ranking by a search engine. While many legitimate companies specialize in optimizing websites to better position them, SEO poisoning uses SEO to make a malicious website appear higher in search results.

Browser Hijacker - A browser hijacker is malware that alters a computer's browser settings to redirect the user to websites paid for by the cyber criminals' customers. Browser hijackers usually install without the user's permission and is usually part of a drive-by download.

3.2 Trickery

Cisco | Networking Academy®
Mind Wide Open™

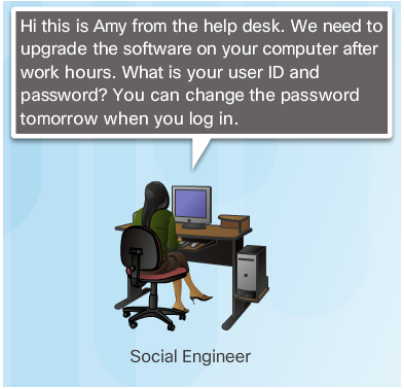
The Art of Trickery

Social Engineering - Social engineering is a completely non-technical means for a criminal to gather information on a target. Social engineering is an attack that attempts to manipulate individuals into performing actions or divulging confidential information.

Social engineers often rely on people's willingness to be helpful but also prey on people's weaknesses. These are some types of social engineering attacks:

Pretexting - This is when an attacker calls an individual and lies to them in an attempt to gain access to privileged data. An example involves an attacker who pretends to need personal or financial data in order to confirm the identity of the recipient.

Something for Something (Quid pro quo) - This is when an attacker requests personal information from a party in exchange for something, like a gift.



Types of Trickery

Shoulder Surfing and Dumpster Diving – refers to picking up PINs, access codes or credit card numbers. An attacker can be in close proximity to his victim or the attacker can use binoculars or closed circuit cameras to shoulder surf.

Impersonation and Hoaxes - Impersonation is the action of pretending to be someone else. For example, a recent phone scam targeted taxpayers. A criminal, posing as an IRS employee, told the victims that they owed money to the IRS.

Piggybacking and Tailgating - Piggybacking occurs when a criminal tags along with an authorized person to gain entry into a secure location or a restricted area. Tailgating is another term that describes the same practice.

Online, Email, and Web-based Trickery - Forwarding hoax emails and other jokes, funny movies, and non-work-related emails at work may violate the company's acceptable use policy and result in disciplinary actions.

3.3 Attacks

Cisco | Networking Academy®
Mind Wide Open™

Types of Cyber Attacks

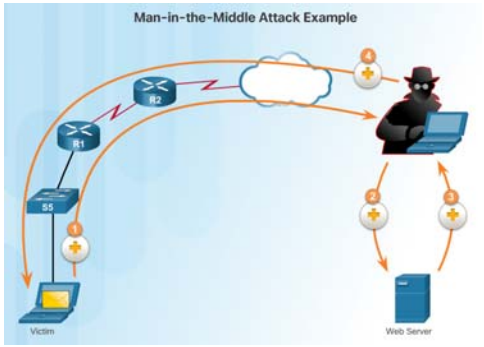
Denial-of-Service (DoS) Attacks - are a type of network attack. A DoS attack results in some sort of interruption of network services to users, devices, or applications. DoS attacks are a major risk because they can easily interrupt communication and cause significant loss of time and money. These attacks are relatively simple to conduct, even by an unskilled attacker.

Sniffing - Sniffing is similar to eavesdropping on someone. It occurs when attackers examine all network traffic as it passes through their NIC, independent of whether or not the traffic is addressed to them or not. Criminals accomplish network sniffing with a software application, hardware device, or a combination of the two.

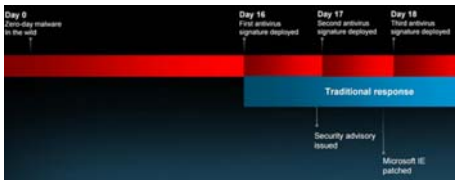
Spoofing - Spoofing is an impersonation attack, and it takes advantage of a trusted relationship between two systems. If two systems accept the authentication accomplished by each other, an individual logged onto one system might not go through an authentication process again to access the other system.

Types of Cyber Attacks

Man-in-the-middle - A criminal performs a man-in-the-middle (MitM) attack by intercepting communications between computers to steal information crossing the network. The criminal can also choose to manipulate messages and relay false information between hosts since the hosts are unaware that a modification to the messages occurred. MitM allows the criminal to take control over a device without the user's knowledge.



Zero-Day Attacks - A zero-day attack, sometimes referred to as a zero-day threat, is a computer attack that tries to exploit software vulnerabilities that are unknown or undisclosed by the software vendor. The term zero hour describes the moment when someone discovers the exploit.



Keyboard Logging - Keyboard logging is a software program that records or logs the keystrokes of the user of the system. Criminals can implement keystroke loggers through software installed on a computer system or through hardware physically attached to a computer. The criminal configures the key logger software to email the log file. The keystrokes captured in the log file can reveal usernames, passwords, websites visited, and other sensitive information.

Wireless and Mobile Attacks (Cont.)

Grayware and SMiShing

- Grayware includes applications that behave in an annoying or undesirable manner. Grayware may not have recognizable malware concealed within, but it still may pose a risk to the user. Grayware is becoming a problem area in mobile security with the popularity of smartphones.
- SMiShing is short for SMS phishing. It uses Short Message Service (SMS) to send fake text messages. The criminals trick the user into visiting a website or calling a phone number. Unsuspecting victims may then provide sensitive information such as credit card information. Visiting a website might result in the user unknowingly downloading malware that infects the device.

Wireless and Mobile Attacks (Cont.)

Rogue Access Points - A rogue access point is a wireless access point installed on a secure network without explicit authorization. A rogue access point can be set up in two ways.

RF Jamming - Wireless signals are susceptible to electromagnetic interference (EMI), radio-frequency interference (RFI), and may even be susceptible to lightning strikes or noise from fluorescent lights. Wireless signals are also susceptible to deliberate jamming. Radio frequency (RF) jamming disrupts the transmission of a radio or satellite station so that the signal does not reach the receiving station.

Bluejacking and Bluesnarfing - Bluejacking is the term used for sending unauthorized messages to another Bluetooth device. Bluesnarfing occurs when the attacker copies the victim's information from his device. This information can include emails and contact lists.

Wireless and Mobile Attacks (Cont.)

WEP and WPA Attacks

Wired Equivalent Privacy (WEP) is a security protocol that attempted to provide a wireless local area network (WLAN) with the same level of security as a wired LAN. Since physical security measures help to protect a wired LAN, WEP seeks to provide similar protection for data transmitted over the WLAN with encryption.

- WEP uses a key for encryption.
- There is no provision for key management with WEP, so the number of people sharing the key will continually grow.

Wi-Fi Protected Access (WPA) and then WPA2 came out as improved protocols to replace WEP. WPA2 does not have the same encryption problems because an attacker cannot recover the key by observing traffic.

- WPA2 is susceptible to attack because cyber criminals can analyze the packets going between the access point and a legitimate user.
- Cyber criminals use a packet sniffer and then run attacks offline on the passphrase.

Wireless and Mobile Attacks (Cont.)

Defending Against Wireless and Mobile Device Attacks

There are several steps to take to defend against wireless and mobile device attacks.

- Most WLAN products use default settings. Take advantage of the basic wireless security features such as authentication and encryption by changing the default configuration settings.
- Restrict access point placement with the network by placing these devices outside the firewall or within a demilitarized zone (DMZ) which contains other untrusted devices such as email and web servers.
- WLAN tools such as NetStumbler may discover rogue access points or unauthorized workstations. Develop a guest policy to address the need when legitimate guests need to connect to the Internet while visiting. For authorized employees, utilize a remote access virtual private network (VPN) for WLAN access.

Application Attacks

Cross-site scripting (XSS) - is a vulnerability found in web applications. XSS allows criminals to inject scripts into the web pages viewed by users. This script can contain malicious code. Cross-site scripting has three participants: the criminal, the victim, and the website. The cyber-criminal does not target a victim directly. The criminal exploits vulnerability within a website or web application. Criminals inject client-side scripts into web pages viewed by users, the victims.

Code Injections Attacks - One way to store data at a website is to use a database. There are several different types of databases such as a Structured Query Language (SQL) database or an Extensible Markup Language (XML) database. Both XML and SQL injection attacks exploit weaknesses in the program such as not validating database queries properly.

Buffer Overflow - A buffer overflow occurs when data goes beyond the limits of a buffer. Buffers are memory areas allocated to an application. By changing data beyond the boundaries of a buffer, the application accesses memory allocated to other processes. This can lead to a system crash, data compromise, or provide escalation of privileges.

Application Attacks

Remote Code Executions vulnerabilities allow a cybercriminal to execute malicious code and take control of a system with the privileges of the user running the application. Remote code execution allows a criminal to execute any command on a target machine.

ActiveX Controls and Java controls provide the capability of a plugin to Internet Explorer.

- ActiveX controls are pieces of software installed by users to provide extended capabilities. Third parties write some ActiveX controls and they may be malicious. They can monitor browsing habits, install malware, or log keystrokes. Active X controls also work in other Microsoft applications.
- Java operates through an interpreter, the Java Virtual Machine (JVM). The JVM enables the Java program's functionality. The JVM sandboxes or isolates untrusted code from the rest of the operating system. There are vulnerabilities, which allow untrusted code to go around the restrictions imposed by the sandbox.

Application Attacks

Defending Against Application Attacks

- The first line of defense against an application attack is to write solid code.
- Regardless of the language used, or the source of outside input, prudent programming practice is to treat all input from outside a function as hostile.
- Validate all inputs as if they were hostile.
- Keep all software including operating systems and applications up to date, and do not ignore update prompts.
- Not all programs update automatically, so at the very least, always select the manual update option.

4.1 Cryptography

Cisco | Networking Academy®
Mind Wide Open™

Cryptography
Overview

Cryptology is the science of making and breaking secret codes. Cryptography is a way to store and transmit data so only the intended recipient can read or process it. Modern cryptography uses computationally secure algorithms to make sure that cyber criminals cannot easily compromise protected information.

The history of cryptography started in diplomatic circles thousands of years ago. Messengers from a king's court took encrypted messages to other courts. Occasionally, other courts not involved in the communication, attempted to steal messages sent to a kingdom they considered an adversary. Not long after, military commanders started using encryption to secure messages.

Each encryption method uses a specific algorithm, called a cipher, to encrypt and decrypt messages. A cipher is a series of well-defined steps used to encrypt and decrypt messages. There are several methods of creating ciphertext:

- Transposition
- Substitution
- One-time pad

Overview (Cont.)

Two Types of Encryption

There are two classes of encryption algorithms:

- **Symmetric algorithms** - These algorithms use the same pre-shared key, sometimes called a secret key pair, to encrypt and decrypt data. Both the sender and receiver know the pre-shared key before any encrypted communication begins.
- **Asymmetric algorithms** - Asymmetrical encryption algorithms use one key to encrypt data and a different key to decrypt data. One key is public and the other is private. In a public-key encryption system, any person can encrypt a message using the public key of the receiver, and the receiver is the only one that can decrypt it using his private key. Parties exchange secure messages without needing a pre-shared key. Asymmetric algorithms are more complex. These algorithms are resource intensive and slower to execute.

Private-Key Encryption

Symmetrical Encryption Process - Symmetric algorithms use pre-shared key to encrypt and decrypt data, a method also known as private-key encryption. Numerous encryption systems use symmetric encryption. Some of the common encryption standards that use symmetric encryption include the following:

- **3DES (Triple DES):** Digital Encryption Standard (DES) is a symmetric block cipher with 64-bit block size that uses a 56-bit key. Triple DES encrypts data three times and uses a different key for at least one of the three passes, giving it a cumulative key size of 112-168 bits.
- **IDEA:** The International Data Encryption Algorithm (IDEA) uses 64-bit blocks and 128-bit keys. IDEA performs eight rounds of transformations on each of the 16 blocks that results from dividing each 64-bit block. IDEA was the replacement for DES, and now PGP (Pretty Good Privacy) uses it.
- **AES:** The Advanced Encryption Standard (AES) has a fixed block size of 128-bits with a key size of 128, 192, or 256 bits. The National Institute of Standards and Technology (NIST) approved the AES algorithm in December 2001. The U.S. government uses AES to protect classified information.

Public-Key Encryption

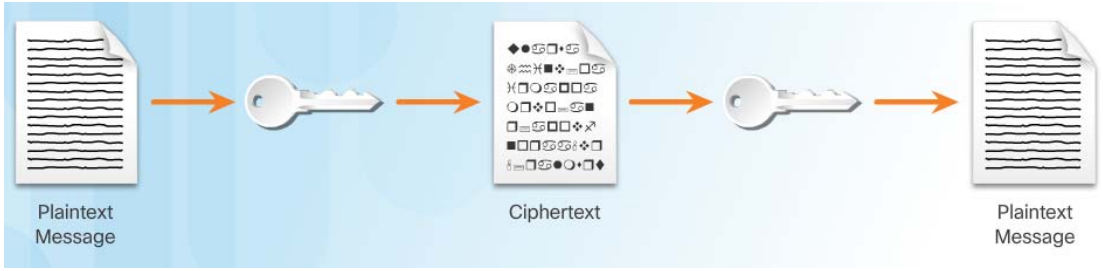
Asymmetrical Encryption Process - Asymmetric encryption, also called public-key encryption, uses one key for encryption that is different from the key used for decryption. A criminal cannot calculate the decryption key based on knowledge of the encryption key, and vice versa, in any reasonable amount of time. The asymmetric algorithms include:

- **RSA (Rivest_Shamir-Adleman)** - uses the product of two very large prime numbers with an equal length of between 100 and 200 digits. Browsers use RSA to establish a secure connection.
- **Diffie-Hellman** - provides an electronic exchange method to share the secret key. Secure protocols, such as Secure Sockets Layer (SSL), Transport Layer Security (TLS), Secure Shell (SSH), and Internet Protocol Security (IPsec), use Diffie-Hellman.
- **ElGamal** - uses the U.S. government standard for digital signatures. This algorithm is free to use because no one holds the patent.
- **Elliptic Curve Cryptography (ECC)** - uses elliptic curves as part of the algorithm. In the U.S., the National Security Agency uses ECC for digital signature generation and key exchange.

Symmetrical versus Asymmetrical Encryption

Comparing Encryption Types

- It is important to understand the differences between symmetric and asymmetric encryption methods. Symmetric encryption systems are more efficient and can handle more data. However, key management with symmetric encryption systems is more problematic and harder to manage.
- Asymmetric cryptography is more efficient at protecting the confidentiality of small amounts of data, and its size and speed make it more secure for tasks such as electronic key exchange which is a small amount of data rather than encrypting large blocks of data.



Symmetrical versus Asymmetrical Encryption

Application

There are many applications for both symmetric and asymmetric algorithms. A one-time password-generating token is a hardware device that uses cryptography to generate a one-time password. A one-time password is an automatically generated numeric or alphanumeric string of characters that authenticates a user for one transaction of one session only. The number changes every 30 seconds or so. The session password appears on a display and the user enters the password.

- The electronic payment industry uses 3DES.
- Operating systems use DES to protect user files and system data with passwords.
- Most encrypting file systems, such as NTFS, use AES.

Symmetrical versus Asymmetrical Encryption

Application

Four protocols use asymmetric key algorithms:

- Internet Key Exchange (IKE), which is a fundamental component of IPsec Virtual Private Networks (VPNs).
- Secure Socket Layer (SSL), which is a means of implementing cryptography into a web browser.
- Secure Shell (SSH), which is a protocol that provides a secure remote access connection to network devices.
- Pretty Good Privacy (PGP), which is a computer program that provides cryptographic privacy and authentication to increase the security of email communications.

Symmetrical versus Asymmetrical Encryption

Application

A VPN is a private network that uses a public network, usually the Internet, to create a secure communication channel. A VPN connects two endpoints such as two remote offices over the Internet to form the connection.

- VPNs use IPsec. IPsec is a suite of protocols developed to achieve secure services over networks.
- IPsec services allow for authentication, integrity, access control, and confidentiality.
- With IPsec, remote sites can exchange encrypted and verified information.
- Data in use is a growing concern to many organizations. When in use, data no longer has any protection because the user needs to open and change the data.
- System memory holds data in use and it can contain sensitive data such as the encryption key.
- If criminals compromise data in use, they will have access to data at rest and data in motion.

4.2 Access Control

Cisco | Networking Academy®
Mind Wide Open™

Types of Access Control

Physical Access Controls - actual barriers deployed to prevent direct contact with systems. The goal is to prevent unauthorized users from gaining physical access to facilities, equipment, and other organizational assets. Physical access control determines who can enter (or exit), where they can enter (or exit), and when they can enter (or exit).

Logical Access Controls - hardware and software solutions used to manage access to resources and systems. These technology-based solutions include tools and protocols that computer systems use for identification, authentication, authorization, and accountability.

Administrative Access Controls - policies and procedures defined by organizations to implement and enforce all aspects of controlling unauthorized access. Administrative controls focus on personnel and business practices.

Access Control Strategies

Mandatory access control (MAC) - restricts the actions that a subject can perform on an object. A subject can be a user or a process. An object can be a file, a port, or an input/output device. An authorization rule enforces whether or not a subject can access the object.

Discretionary access control (DAC) - DAC grants or restricts object access determined by the object's owner. As the name implies, controls are discretionary because an object owner with certain access permissions can pass on those permissions to another subject.

Role-based access control (RBAC) - is based on the role of the subject. Roles are job functions within an organization. Specific roles require permissions to perform certain operations. Users acquire permissions through their role. RBAC can work in combination with DAC or MAC by enforcing the policies of either one.

Rule-based access control - uses access control lists (ACLs) to help determine whether to grant access. A series of rules is contained in the ACL, as shown in the figure. The determination of whether to grant access depends on these rules. An example of such a rule is one that states that no employee may have access to the payroll file after hours or on weekends.

Identification

Identification enforces the rules established by the authorization policy:

- A subject requests access to a system resource.
- Every time the subject requests access to a resource, the access controls determine whether to grant or deny access.
- Cybersecurity policies determine which identification controls should be used.
- The sensitivity of the information and information systems determine how stringent the controls.
- The increase in data breaches has forced many organizations to strengthen their identification controls.

Authentication Methods

What You Know - Passwords, passphrases, or PINs are all examples of something that the user knows. Passwords are the most popular method used for authentication.

What You Have - Smart cards and security key fobs are both examples of something that users have in their possession.

Who You Are - A unique physical characteristic, such as a fingerprint, retina, or voice, that identifies a specific user is called biometrics.

Multi-factor Authentication - Multi-factor authentication uses at least two methods of verification. A security key fob is a good example. The two factors are something you know, such as a password, and something you have, such as a security key fob.

Authorization

Authorization controls what a user can and cannot do on the network after successful authentication:

- After a user proves his or her identity, the system checks to see what network resources the user can access and what the users can do with the resources.
- Authorization uses a set of attributes that describes the user's access to the network.
- The system compares these attributes to the information contained within the authentication database, determines a set of restrictions for that user, and delivers it to the local router where the user is connected.
- Defining authorization rules is the first step in controlling access. An authorization policy establishes these rules.

Accountability

Accountability traces an action back to a person or process making the change to a system, collects this information, and reports the usage data:

- The organization can use this data for such purposes as auditing or billing.
- The collected data might include the log in time for a user, whether the user log in was a success or failure, or what network resources the user accessed.
- This allows an organization to trace actions, errors, and mistakes during an audit or investigation.
- Implementing accountability consists of technologies, policies, procedures, and education.
- Log files provide detailed information based on the parameters chosen.

Types of Security Controls

Preventative Controls - Prevent means to keep something from happening. Preventative access controls stop unwanted or unauthorized activity from happening.

Deterrent Controls - A deterrent is the opposite of a reward. A reward encourages individuals to do the right thing, while a deterrent discourages them from doing the wrong thing. Cybersecurity professionals and organizations use deterrents to limit or mitigate an action or behavior. Deterrents do not always stop these actions.

Detective Controls - Detection is the act or process of noticing or discovering something. Access control detections identify different types of unauthorized activity. Detection systems can be very simple, such as a motion detector or security guard. They can also be more complex, such as an intrusion detection system.

Types of Security Controls

Corrective Controls - Corrective counteracts something that is undesirable. Organizations put corrective access controls in place after a system experiences a threat. Corrective controls restore the system back to a state of confidentiality, integrity, and availability. They can also restore systems to normal after unauthorized activity occurs.

Recovery Controls - Recovery is a return to a normal state. Recovery access controls restore resources, functions, and capabilities after a violation of a security policy. Recovery controls can repair damage, in addition to stopping any further damage. These controls have more advanced capabilities over corrective access controls.

Compensative Controls - Compensate means to make up for something. Compensative access controls provide options to other controls to bolster enforcement in support of a security policy. A compensative control can also be a substitution used in place of a control that is not possible under the circumstances.

4.3 Obscuring Data

Cisco | Networking Academy®
Mind Wide Open™

Obscuring Data

Data Masking

Data Masking is a technology that secures data by replacing sensitive information with a non-sensitive version. The non-sensitive version looks and acts like the original. This means that a business process can use non-sensitive data and there is no need to change the supporting applications or data storage facilities.

In the most common use case, masking limits the propagation of sensitive data within IT systems by distributing surrogate data sets for testing and analysis.

There are data masking techniques that can ensure that data remains meaningful but changed enough to protect it:

- **Substitution** - replaces data with authentic looking values to apply anonymity to the data records.
- **Shuffling** - derives a substitution set from the same column of data that a user wants to mask. This technique works well for financial information in a test database, for example.

Steganography

Steganography conceals data (the message) in another file such as a graphic, audio, or other text file.

The advantage of steganography over cryptography is that the secret message does not attract any special attention. No one would ever know that a picture actually contained a secret message by viewing the file either electronically or in hardcopy.

There are several components involved in hiding data:

- There is the embedded data, which is the secret message.
- Cover-text (or cover-image or cover-audio) hides the embedded data producing the stego-text (or stego-image or stego-audio).
- A stego-key controls the hiding process.

Data Obfuscation

Data obfuscation - is the use and practice of data masking and steganography techniques in the cybersecurity and cyber intelligence profession:

- Obfuscation is the art of making the message confusing, ambiguous, or harder to understand.
- A system may purposely scramble messages to prevent unauthorized access to sensitive information.
- Software watermarking protects software from unauthorized access or modification.
- Software watermarking inserts a secret message into the program as proof of ownership.
- The secret message is the software watermark. If someone tries to remove the watermark, the result is nonfunctional code.

5.1 Types of Data Integrity Controls

Cisco | Networking Academy®
Mind Wide Open™

Hashing Algorithms

- Hashing is a tool that ensures data integrity by taking binary data (the message) and producing a fixed-length representation called the hash value or message digest.
- Hashing is a one-way mathematical function that is relatively easy to compute, but significantly harder to reverse. Grinding coffee beans is a good analogy of a one-way function. It is easy to grind coffee beans, but it is almost impossible to put all of the tiny pieces back together to rebuild the original beans.

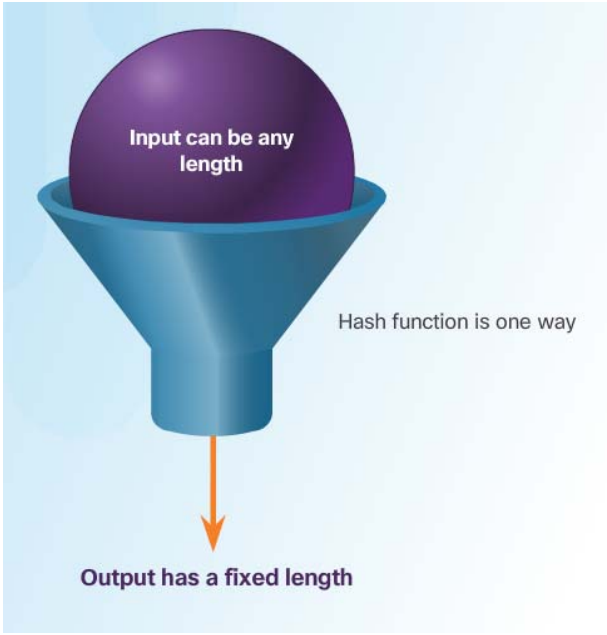
  A cryptographic hash function has the following properties:

  - The input can be any length.
  - The output has a fixed length.
  - The hash function is one way and is not reversible.
  - Two different input values will always result in different hash values.

Hashing Algorithms

There are many modern hashing algorithms widely used today. Two of the most popular are MD5 and SHA.

- **Message Digest 5 (MD5) Algorithm -** is a hash algorithm developed by Ron Rivest that produces a 128-bit hash value.
- **Secure Hash Algorithm (SHA) –** was developed by the U.S. National Institute of Standards and Technology (NIST) and can be implemented in different strengths:
- SHA-224 (224 bit)
- SHA-256 (256 bit)
- SHA-384 (384 bit)
- SHA-512 (512 bit)



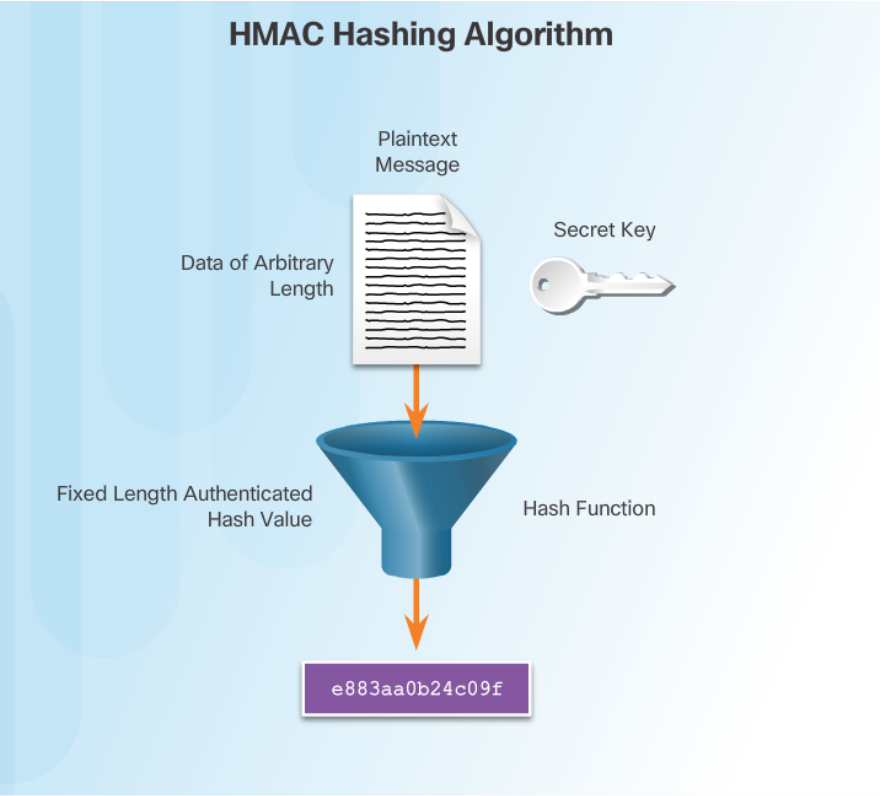
Salting

- Salting is used to make hashing more secure. If two users have the same password, they will also have the same password hashes. A salt, which is a random string of characters, is an additional input to the password before hashing.
- This creates a different hash result for the two passwords as shown in the figure. A database stores both the hash and the salt.

	Salt		Hash Value
Hash ("password" +	QxLUF1bIAdeQX)	=	b3bad1e5324f057753a4b8d7cef293e4
Hash ("password" +	R9PeIC7sxQXb8)	=	713c7beb54841a26a7c81eb06d6cf066

HMAC

- HMACs strengthens hashing algorithms by using an additional secret key as input to the hash function.
- The use of HMAC goes a step further than just integrity assurance by adding authentication.
- An HMAC uses a specific algorithm that combines a cryptographic hash function with a secret key, as shown in the figure.



The same procedure is used for generation and verification of secure fingerprints.

5.2 Digital Signatures

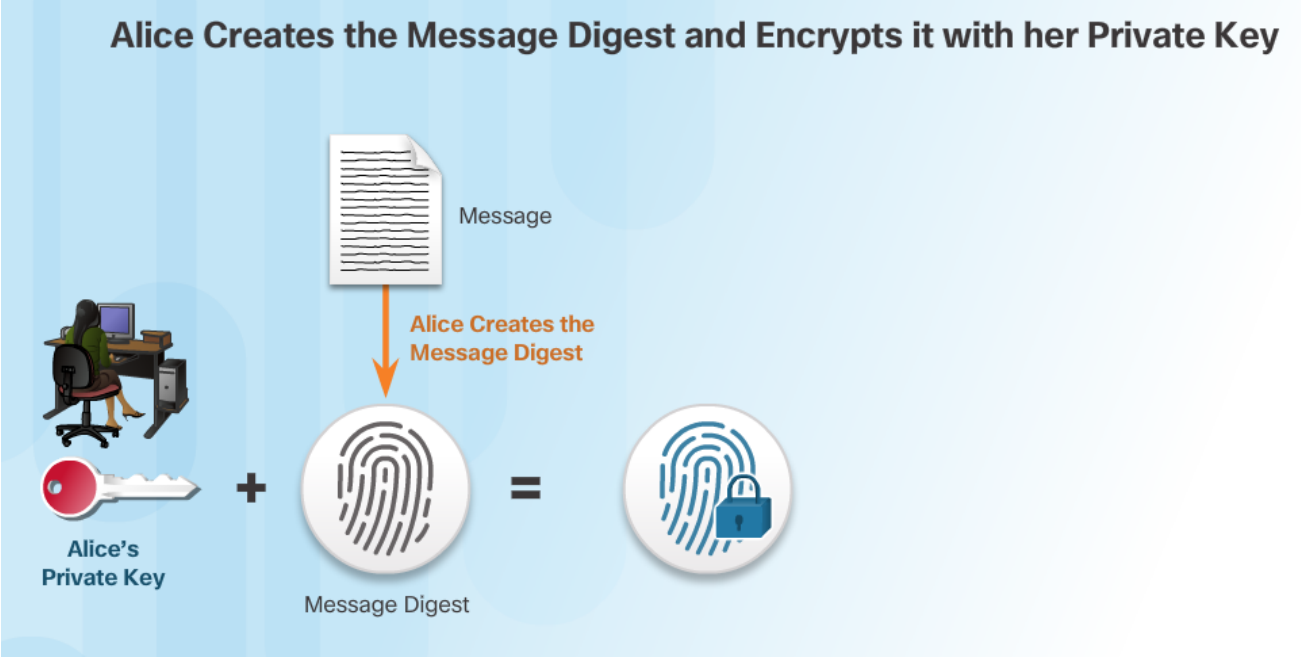
Cisco | Networking Academy®
Mind Wide Open™

Signatures and the Law

- Digital signatures provide the same functionality as handwritten signatures for electronic documents.
- A digital signature is used to determine if someone edits a document after the user signs it.
- A digital signature is a mathematical method used to check the authenticity and integrity of a message, digital document, or software.
- In many countries, digital signatures have the same legal importance as a manually signed document.
- Digital signatures also provide repudiation.

How Digital Signature Technology Works

Asymmetric cryptography is the basis for digital signatures. A public key algorithm like RSA generates two keys: one private and the other public. The keys are mathematically related.



5.3 Certificates

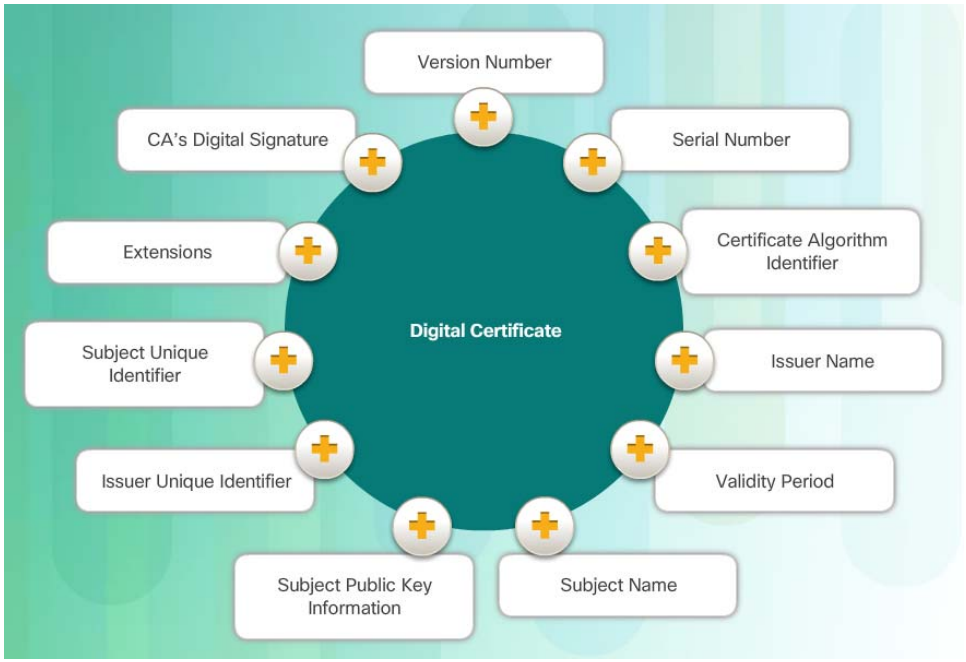
Cisco | Networking Academy®
Mind Wide Open™

The Basics of Digital Certicates

- A digital certificate is equivalent to an electronic passport.
- Digital certificates enable users, hosts, and organizations to exchange information securely over the Internet.
- A digital certificate authenticates and verifies that users sending a message are who they claim to be.
- Digital certificates can also provide confidentiality for the receiver with the means to encrypt a reply.

Constructing a Digital Certificate

- Digital certificate must follow a standard structure so that any entity can read and understand it regardless of the issuer.
- TheX.509 is the standard for construction of digital certificates and the public key infrastructure (PKI) used to manage digital certificates.
- PKI is the policies, roles, and procedures required to create, manage, distribute, use, store, and revoke digital certificates.



5.4 Database Integrity Enforcement

Cisco | Networking Academy®
Mind Wide Open™

Database Integrity

- Databases provide an efficient way to store, retrieve, and analyze data.
- As data collection increases and data becomes more sensitive, it is important for cybersecurity professionals to protect the growing number of databases.
- Data integrity refers to the accuracy, consistency, and reliability of data stored in a database.

ID	Company	First Name	Last Name
8	Company H	Elizabeth	Andersen
18	Company R	Catherine	Autier Miconi
3	Company C	Thomas	Axen
17	Company Q	Jean Philippe	Bagel
1	Company A	Anna	Bedecs
12	Company L	John	Edwards

Database Integrity (Cont.)

The four database integrity rules or constraints are as follows:

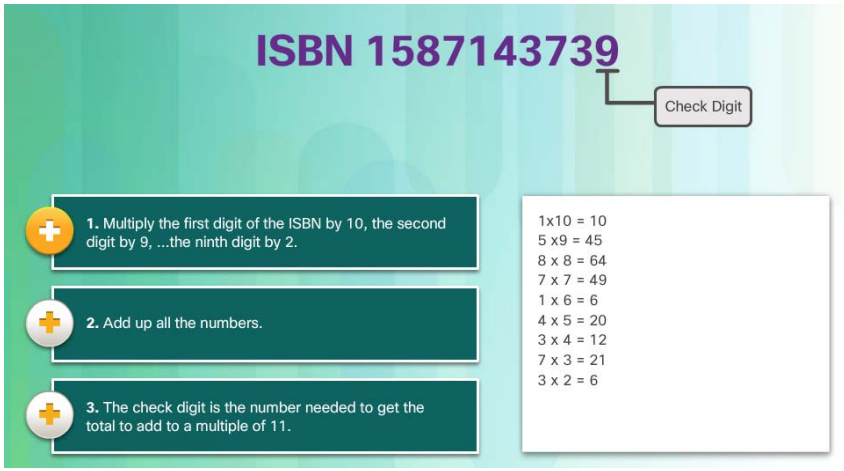
- **Entity Integrity**: All rows must have a unique identifier called a Primary Key.
- **Domain Integrity**: All data stored in a column must follow the same format and definition.
- **Referential Integrity**: Table relationships must remain consistent. Therefore, a user cannot delete a record which is related to another one.
- **User-defined Integrity**: A set of rules defined by a user which does not belong to one of the other categories. For example, a customer places a new order. The user first checks to see if this is a new customer. If it is, the user adds the new customer to the customers table.

ID	Company	First Name	Last Name
8	Company H	Elizabeth	Andersen
18	Company R	Catherine	Autier Miconi
3	Company C	Thomas	Axen
17	Company Q	Jean Philippe	Bagel
1	Company A	Anna	Bedecs
12	Company L	John	Edwards

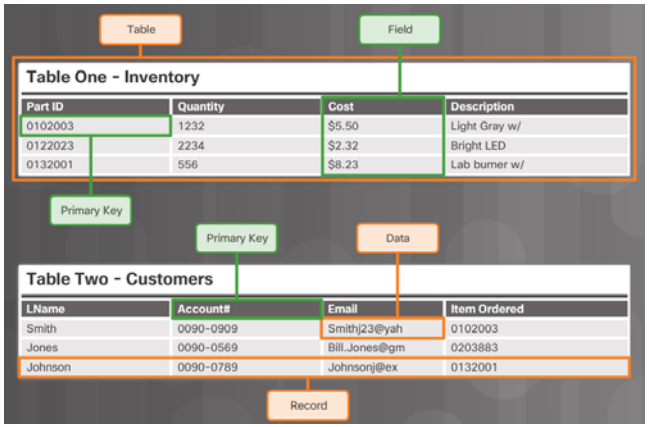
Database Validation

A validation rule checks that data falls within the parameters defined by the database designer. A validation rule helps to ensure the completeness, accuracy and consistency of data. The criteria used in a validation rule include the following:

- Size – checks the number of characters in a data item
- Format – checks that the data conforms to a specified format
- Consistency – checks for the consistency of codes in related data items
- Range – checks that data lies within a minimum and maximum value
- Check digit – provides for an extra calculation to generate a check digit for error detection.

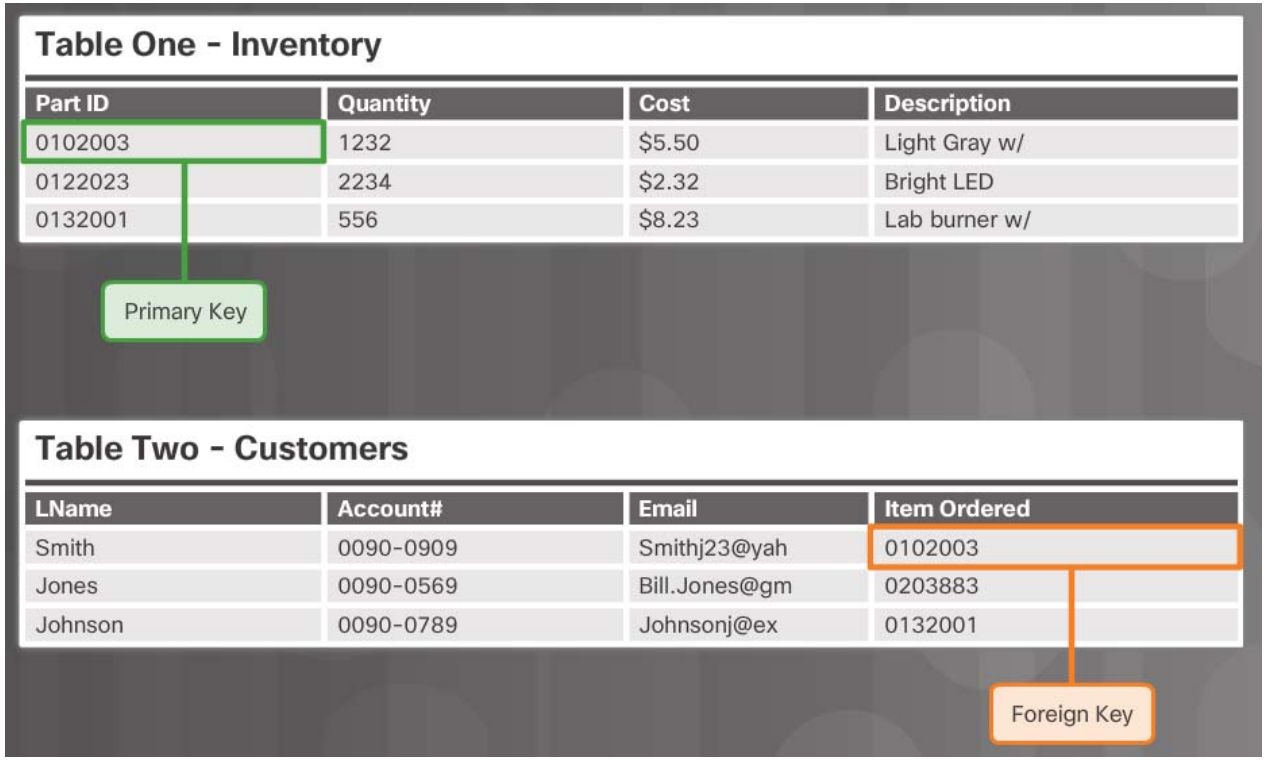


Database Integrity Requirements



- Maintaining proper filing is critical in maintaining the trustworthiness and usefulness of the data within the database.
- Tables, records, fields, and data within each field make up a database.
- In order to maintain the integrity of the database filing system, users must follow certain rules.
- Entity integrity is an integrity rule, which states that every table must have a primary key and that the column or columns chosen to be the primary key must be unique and not NULL.
- Null in a database signifies missing or unknown values. Entity integrity enables proper organization of data for that record.

Database Integrity Requirements (Cont.)



- Another important integrity check is referential integrity which deals with foreign keys. A foreign key in one table references a primary key in a second table. The primary key for a table uniquely identifies entities (rows) in the table. Referential integrity maintains the integrity of foreign keys.

Database Integrity Requirements (Cont.)

SSN 243-27-3361	• Must have nine integers • Format xxx-xx-xxxx • Entered or modified by customer only • Must be validated
Credit Card Number 4539 4769 0728 4479	• Must have sixteen integers • Format xxxx-xxxx-xxxx-xxxx • Entered or modified by customer only • Must be validated
Email Address tortor@odio.com	• Must have no more that 128 characters • Format xxxx@xxxx.xxx • Entered or modified by customer only • Validated by email response

- Domain integrity ensures that all the data items in a column fall within a defined set of valid values. Each column in a table has a defined set of values, such as the set of all numbers for credit card numbers, social security numbers, or email addresses. Limiting the value assigned to an instance of that column (an attribute) enforces domain integrity. Domain integrity enforcement can be as simple as choosing the correct data type, length and or format for a column.

The Five Nines

What is Five Nine?

- Five nines mean that systems and services are available 99.999% of the time. It also means that both planned and unplanned downtime is less than 5.26 minutes per year. High availability refers to a system or component that is continuously operational for a given length of time. To help ensure high availability:
- Eliminate single points of failure
- Design for reliability
- Detect failures as they occur

Availability	Downtime per Year
99%	87 hours 36 mins
99.5%	43 hours 48 mins
99.95%	4 hours 23 mins
99.99%	53 mins
99.999%	5 mins

The Five Nines (Cont.)

Environments That Require Five Nines

Although the cost of sustaining high availability may be too costly for some industries, several environments require five nines.

- The finance industry needs to main high availability for continuous trading, compliance, and customer trust.
- Healthcare facilities require high availability to provide around-the-clock care for patients.
- The public safety industry includes agencies that provide security and services to a community, state, or nation.
- The retail industry depends on efficient supply chains and the delivery of products to customers. Disruption can be devastating, especially during peak demand times such as holidays.

Finance Industry


Health Care Facilities


Public Safety

The Five Nines (Cont.)

Threats to Availability

There are many different types of threats to high availability, the threats can range from failure of a mission-critical application to severe storm such as a hurricane or tornado. Threats can also include catastrophic event such as a terrorist attack, building bombing, or building fires.

Designing a High Availability System

High availability incorporates three major principles to achieve the goal of uninterrupted access to data and services:

- Elimination or reduction of single-points of failure
- System Resiliency
- Fault Tolerance

Finance Industry


Health Care Facilities


Public Safety

Asset Management

An organization needs to know what hardware and software assets they have in order to protect them. Asset management includes a complete inventory of hardware and software. This means that the organization needs to know all of components that can be subject to security risks, including:

- Every hardware system
- Every operating system
- Every hardware network device
- Every network device operating system
- Every software application
- All firmware
- All language runtime environments
- All individual libraries

Many organizations may choose an automated solution to keep track of assets.

Asset Management (Cont.)

- **Asset classification -** assigns all resources of an organization into a group based on common characteristics. An organization should apply an asset classification system to documents, data records, data files, and disks.
- **Asset Standardization -** as part of an IT asset management system, an organization specifies the acceptable IT assets that meet its objectives
- **Threat Identification -** The United States Computer Emergency Readiness Team (US-CERT) and the U.S. Department of Homeland Security sponsor a dictionary of common vulnerabilities and exposure (CVE). The CVE identification contains a standard identifier number with a brief description, and references to related vulnerability reports and advisories.
- **Risk Analysis -** is the process of analyzing the dangers posed by natural and human-caused events to the assets of an organization. A user performs an asset identification to help determine which assets to protect.
- **Mitigation -** Mitigation involves reducing the severity of the loss or the likelihood of the loss from occurring. Many technical controls mitigate risk including authentication systems, file permissions, and firewalls.

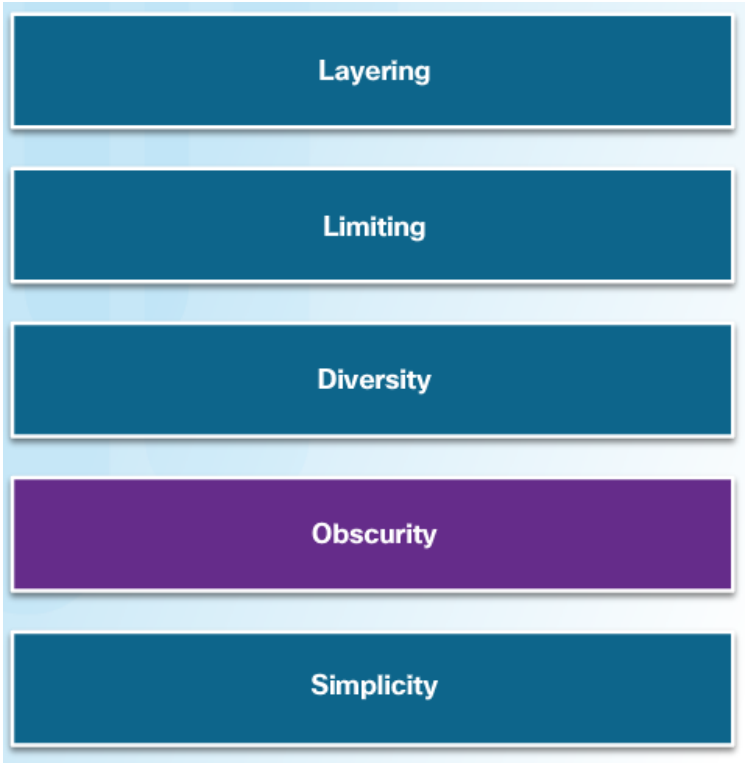
Defense in Depth

Defense in depth will not provide an impenetrable cyber shield, but it will help an organization minimize risk by keeping it one step ahead of cyber criminals. To make sure data and information remains available, an organization must create different layers of protection:

- A **layered** approach provides the most comprehensive protection. If cyber criminals penetrate one layer, they still have to contend with several more layers with each layer being more complicated than the previous one. Layering is creating a barrier of multiple defenses that coordinate together to prevent attacks.
- **Limiting** access to data and information reduces the possibility of a threat. An organization should restrict access so that users only have the level of access required to do their job.

Defense in Depth

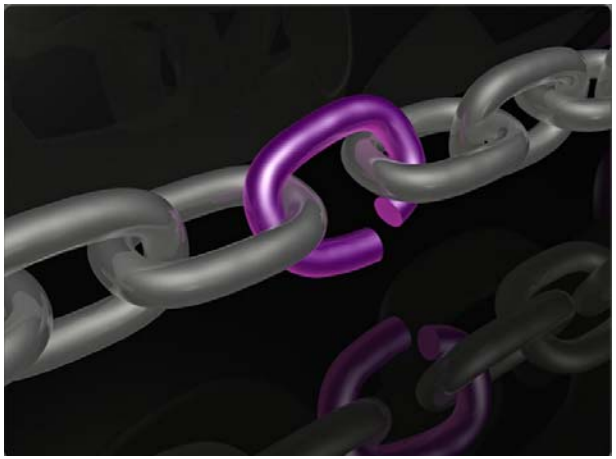
- **Diversity** refers to changing the controls and procedures at different layers. Breaching one layer of security does not compromise the whole system. An organization may use different encryption algorithms or authentication systems to protect data in different states.
- **Obscuring** information can also protect data and information. An organization should not reveal any information that cyber criminals can use to figure out what version of the operating system a server is running or the type of equipment it uses.
- Complexity does not necessarily guarantee security. If the process or technology are too complex, misconfigurations or failure to comply can result. **Simplicity** can actually improve availability.



Redundancy

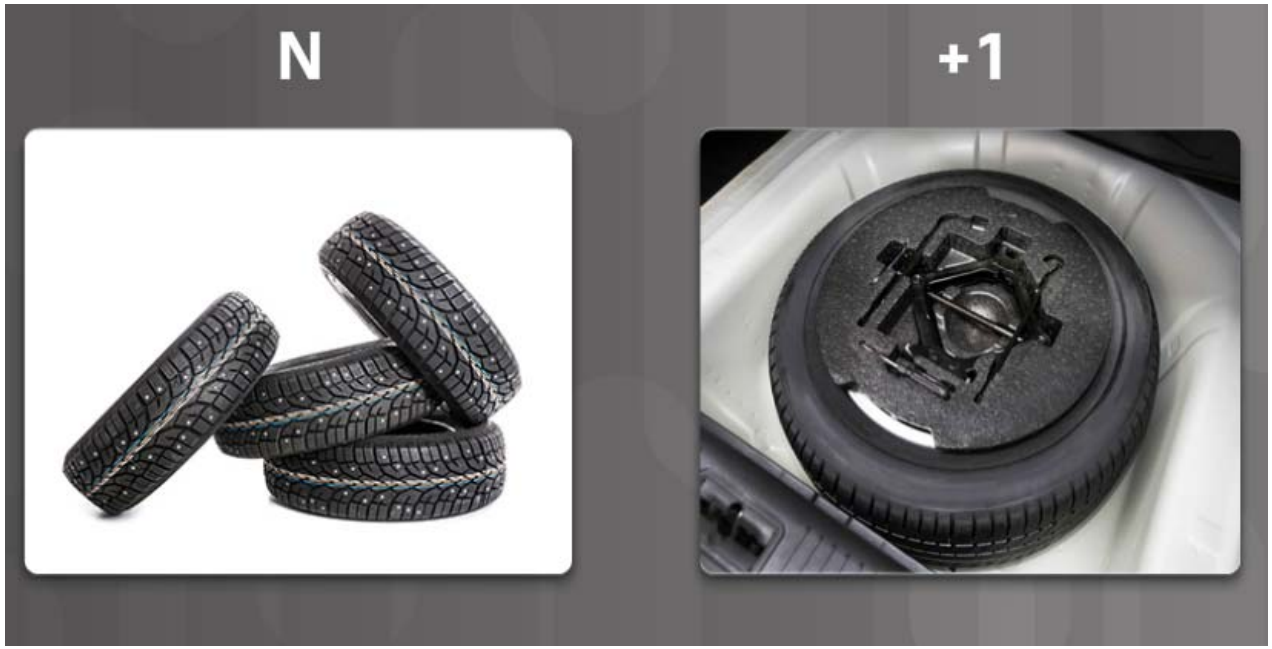
A **single point of failure** must be identified and addressed. A single point of failure can be a specific piece of hardware, a process, a specific piece of data, or even an essential utility.

- Single points of failure are the weak links in the chain that can cause disruption of the organization's operations.
- Generally, the solution to a single point of failure is to modify the critical operation so that it does not rely on a single element.
- The organization can also build redundant components into the critical operation to take over the process should one of these points fail.



Redundancy (Cont.)

- **N+1 redundancy** ensures system availability in the event of a component failure.
- Components (N) need to have at least one backup component (+1).
- For example, a car has four tires (N) and a spare tire in the trunk in case of a flat (+1).



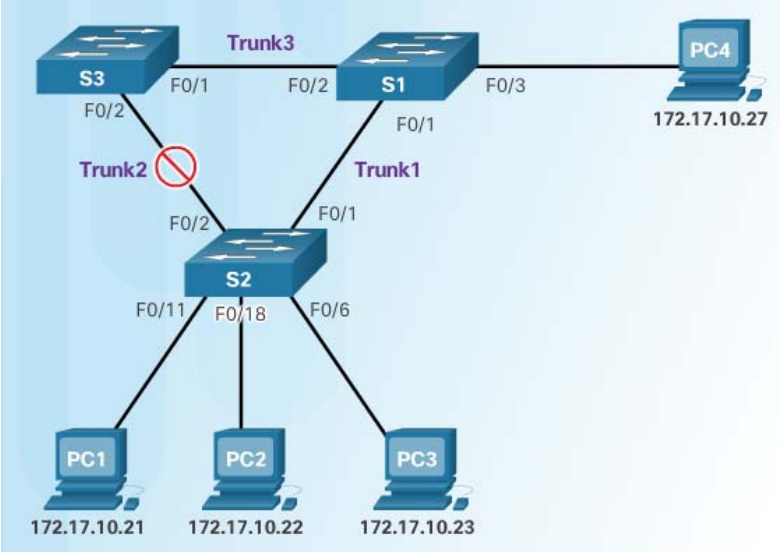
Redundancy (Cont.)

- A **redundant array of independent disks (RAID)** combines multiple physical hard drives into a single logical unit to provide data redundancy and improve performance.
- RAID takes data that is normally stored on a single disk and spreads it out among several drives. If any single disk is lost, the user can recover data from the other disks where the data also resides.
- RAID can also increase the speed of data recovery.
- Using multiple drives makes retrieving requested data faster, instead of relying on just one disk to do the work.
- A RAID solution can be either hardware-based or software-based. The following terms describe how RAID stores data on the various disks:
  - **Parity** - Detects data errors.
  - **Striping** - Writes data across multiple drives.
  - **Mirroring** - Stores duplicate data on a second drive.

Redundancy (Cont.)

Spanning Tree is a network protocol that provides for redundancy:

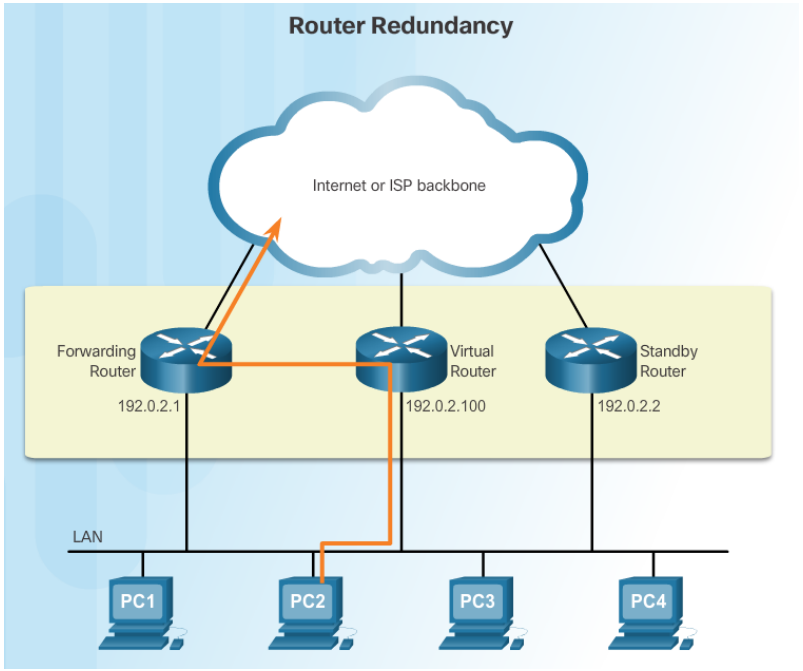
- The basic function of STP is to prevent loops on a network when switches interconnect via multiple paths.
- STP ensures that redundant physical links are loop-free. It ensures that there is only one logical path between all destinations on the network.
- STP intentionally blocks redundant paths that could cause a loop.



Redundancy (Cont.)

The default gateway is typically the router that provides devices access to the rest of the network or to the Internet. If there is only one router serving as the default gateway, it is a single point of failure. Router redundancy involves:

- Choosing to install an additional standby router.
- The ability of a network to dynamically recover from the failure of a router acting as a default gateway is known as first-hop redundancy.



Redundancy (Cont.)

Router Redundancy Options - options available for router redundancy include:

- **Hot Standby Router Protocol (HSRP)** - HSRP provides high network availability by providing first-hop routing redundancy.
- **Virtual Router Redundancy Protocol (VRRP)** - A VRRP router runs the VRRP protocol in conjunction with one or more other routers attached to a LAN. In a VRRP configuration, the elected router is the virtual router master, and the other routers act as backups, in case the virtual router master fails.
- **Gateway Load Balancing Protocol (GLBP)** - GLBP protects data traffic from a failed router or circuit, like HSRP and VRRP, while also allowing load balancing (also called load sharing) between a group of redundant routers.

Redundancy (Cont.)

Location Redundancy - An organization may need to consider location redundancy depending on its needs. The following outlines three forms of location redundancy:

- **Synchronous -** Synchronizes both locations in real time, requires high bandwidth and locations must be close together to reduce latency.
- **Asynchronous Replication -** Not synchronized in real time but close to it, requires less bandwidth and sites can be further apart because latency is less of an issue.
- **Point-in-time-Replicatio**n - Updates the backup data location periodically and is the most bandwidth conservative option because it does not require a constant connection.

System Resilience

Resiliency defines the methods and configurations used to make a system or network tolerant of failure. Routing protocols provide resiliency. Resilient design is more than just adding redundancy. Resiliency is critical to understand the business needs of the organization, and then incorporate redundancy to create a resilient network.

Incident Response Phases

Incident response defines the procedures that an organization follows after an event occurs outside the normal range. When an incident occurs, the organization must know how to respond. Organizations needs to develop an incident response plan and put together a Computer Security Incident Response Team (CSIRT) to manage the response. Incident response has consist of four phases:

1. **Preparation** – planning for potential incidents
2. **Detection and Analysis** - discovering the incident
3. **Containment and Eradication, and Recovery** - efforts to immediately contain or eradicate the threat and begin recovery efforts
4. **Post-Incident Follow-Up** – investigate the cause of the incident and ask questions to better understand the nature of the threat

Incident Response Technologies

There are many technologies that are used to implement an incident response:

- **Network Admission Control (NAC)** - allows network access for authorized users with compliant systems. A compliant system meets all of the policy requirements of the organization.
- **Intrusion Detection Systems (IDSs)** - monitor the traffic on a network. IDS systems are passive.
- **Intrusion Prevention Systems** - operates in inline mode. It can detect and immediately address a network problem.
- **NetFlow and IPFIX** - NetFlow is a Cisco IOS technology that provides statistics on packets flowing through a Cisco router or multilayer switch. The Internet Engineering Task Force (IETF) used Cisco's NetFlow Version 9 as the basis for IP Flow Information Export (IPFIX).
- **Advanced Threat Intelligence** - can help organizations detect attacks during one of the stages of the cyberattack (and sometimes before with the right information).

Disaster Recovery Planning

Types of Disasters - It is critical to keep an organization functioning when a disaster occurs. A disaster includes any natural or human-caused event that damages assets or property and impairs the ability for the organization to continue operating.

- **Natural Disasters -** geological disasters (earthquakes, landslides, volcanoes, and tsunamis), meteorological disasters (hurricanes, tornadoes, snow storms, lightning, and hail), health disasters (widespread illnesses, quarantines, and pandemics) and miscellaneous disasters (fires, floods, solar storms, and avalanches).
- **Human-caused Disasters -** Human-caused disasters - labor events (strikes, walkouts, and slowdowns), social-political events (vandalism, blockades, protests, sabotage, terrorism, and war), materials events (hazardous spills and fires) and utilities disruptions (power failures, communication outages, fuel shortages, and radioactive fallout)

Business Continuity Planning

Need for Business Continuity - Business continuity is one of the most important concepts in computer security. Even though companies do whatever they can to prevent disasters and loss of data, it is impossible to predict every scenario. It is important for companies to have plans in place that ensure business continuity regardless of what may occur.

Business Continuity Considerations - Business continuity controls are more than just backing up data and providing redundant hardware. Business Continuity Considerations should include:

- Documenting configurations
- Establishing alternate communications channels
- Providing power
- Identifying all dependencies for applications and processes
- Understanding how to carry out automated tasks manually

Business Continuity Planning

Business Continuity Best Practices

1. Write a policy that provides guidance to develop the business continuity plan and assigns roles to carry out the tasks.
2. Identify critical systems and processes, and prioritize them based on necessity.
3. Identify vulnerabilities, threats, and calculate risks.
4. Identify and implement controls and countermeasures to reduce risk.
5. Devise methods to bring back critical systems quickly.
6. Write procedures to keep the organization functioning when in a chaotic state.
7. Test the plan.
8. Update the plan regularly.

Host Hardening

Operating System Security - The operating system plays a critical role in the operation of a computer system and is the target of many attacks.

- An administrator hardens an operating system by modifying the default configuration to make it more secure to outside threats.
- This process includes the removal of unnecessary programs and services.
- Another critical requirement of hardening operating systems is the application of security patches and updates.

Antimalware - Malware includes viruses, worms, Trojan horses, keyloggers, spyware, and adware.

- They all invade privacy, steal information, damage the system, or delete and corrupt data.
- It is important to protect computers and mobile devices using reputable antimalware software.

Host Hardening (Cont.)

Patch Management - Patches are code updates that manufacturers provide to prevent a newly discovered virus or worm from making a successful attack. Manufacturers combine patches and upgrades into a comprehensive update application called a service pack.

Host-based Firewalls - A software firewall is a program that runs on a computer to allow or deny traffic between the computer and other connected computers. The software firewall applies a set of rules to data transmissions through inspection and filtering of data packets.

Host Intrusion Detection Systems - A host intrusion detection system (HIDS) is software that runs on a host computer that monitors suspicious activity.

Secure Communications (VPNs) - When connecting to the local network and sharing files, the communication between computers remains within that network. To communicate and share resources over a network that is not secure, users employ a Virtual Private Network (VPN). A VPN is a private network that connects remote sites or users together over a public network, like the Internet.

Hardening Wireless and Mobile Devices

Wired Equivalent Privacy (WEP) - One of the most important components of modern computing are mobile devices. The majority of devices found on today's networks are laptops, tablets, smart phones and other wireless devices. WEP is one of the first widely used Wi-Fi security standards. The WEP standard provides authentication and encryption protections.

WPA/WPA2 - The next major improvement to wireless security was the introduction of WPA and WPA2. Wi-Fi Protected Access (WPA) was the computer industry's response to the weakness of the WEP standard. The WPA standard provided several security improvements.

Mutual Authentication - The imposter can launch a man-in-the-middle attack which is very difficult to detect and can result in stolen login credentials and transmitted data. To prevent rogue access points, the computer industry developed mutual authentication. Mutual authentication, also called two-way authentication, is a process or technology in which both entities in a communications link authenticate to each other.

Host Data Protection

File Access Control – This consists of permissions that limit folder or file access for an individual or for a group of users.

File Encryption – File encryption is a tool used to protect data stored in the form of files. Encryption transforms data using a complicated algorithm to make it unreadable. Software programs can encrypt files, folders, and even entire drives.

System and Data Backups - A data backup stores a copy of the information from a computer to removable backup media. Backing up data is one of the most effective ways of protecting against data loss. If the computer hardware fails, the user can restore the data from the backup after the system is again functional.

Images and Content Control

Content Screening and Blocking

Content control software restricts the content that a user can access with a web browser over the Internet.

Content control software can block sites that contain certain types of material such as pornography or controversial religious or political content.

Disk Cloning and Deep Freeze

- Many third-party applications are available to restore a system back to a default state. This allows the administrator to protect the operating system and configuration files for a system.
- Disk cloning copies the contents of the computer's hard disk to an image file.
- Deep Freeze "freezes" the hard drive partition. When a user restarts the system, the system reverts to its frozen configuration. The system does not save any changes that the user makes, so any applications installed or files saved are lost when the system restarts.

Physical Protection and Workstations

Security Cables and Locks - There are several methods of physically protecting computer equipment:

- Use cable locks
- Keep telecommunication rooms locked.
- Use security cages around equipment.

Logout Timers - An employee gets up and leaves his computer to take a break. If the employee does not take any action to secure his workstation, any information on that system is vulnerable to an unauthorized user.

Idle Timeout and Screen Lock - Employees may or may not log out of their computer when they leave the workplace. Therefore, it is a security best practice to configure an idle timer that will automatically log the user out and lock the screen.

Login Times - In some situations, an organization may want employees to log in during specific hours, such as 7 a.m. to 6 p.m. The system blocks logins during the hours that fall outside of the allowed login hours.

Physical Protection and Workstations

GPS Tracking – uses satellites and computers to determine the location of a device. GPS technology is a standard feature on smartphones that provides real-time position tracking. GPS tracking can pinpoint a location within 100 meters.

Inventory and RFID Tags - Radio frequency identification (RFID) uses radio waves to identify and track objects. RFID inventory systems use tags attached to all items that an organization wants to track.

Secure Remote Access

Managing Remote Access - Remote access refers to any combination of hardware and software that enables users to access a local internal network remotely.

Telnet, SSH, and SCP - Secure Shell (SSH) is a protocol that provides a secure (encrypted) management connection to a remote device.

- **SSH** should replace Telnet for management connections.
- **Telnet** is an older protocol that uses unsecure plaintext transmission of both the login authentication (username and password) and the data transmitted between the communicating devices.
- **Secure copy (SCP)** securely transfers computer files between two remote systems. SCP uses SSH for data transfer (including the authentication element), so SCP ensures the authenticity and confidentiality of the data in transit.

Administrative Measures

Securing Ports and Services - Cyber criminals exploit the services running on a system because they know that most devices run more services or programs than they need. An administrator should look at every service to verify its necessity and evaluate its risk. Remove any unnecessary services.

Privileged Accounts - Cyber criminals exploit privileged accounts because they are the most powerful accounts in the organization. Privileged accounts have the credentials to gain access to systems and they provide elevated, unrestricted access. Administrators use these accounts to deploy and manage operating systems, applications, and network devices. These account should be secured or removed to mitigate these risks.

Group Policies - In most networks that use Windows computers, an administrator configures Active Directory with Domains on a Windows Server. An administrator configures user account policies such as password policies and lockout policies by adding users to groups and setting policy at a group level.

Enable Logs and Alerts - A log records events as they occur on a system. Log entries make up a log file, and a log entry contains all of the information related to a specific event. Logs that relate to computer security have grown in importance.

Physical Protection of Server

Power - A critical issue in protecting information systems is electrical power systems and power considerations. A continuous supply of electrical power is critical in today's massive server and data storage facilities.

Heating, Ventilation, and Air Conditioning (HVAC) - HVAC systems are critical to the safety of people and information systems in the organization's facilities. When designing modern IT facilities, these systems play a very important role in the overall security. HVAC systems control the ambient environment (temperature, humidity, airflow, and air filtering) and must be planned for and operated along with other data center components such as computing hardware, cabling, data storage, fire protection, physical security systems and power.

Hardware Monitoring - Hardware monitoring is often found in large server farms. A server farm is a facility that houses hundreds or thousands of servers for companies.

Securing Network Devices

Operation Centers - The Network Operation Center (NOC) is one or more locations containing the tools that provide administrators with a detailed status of the organization's network. The NOC is ground zero for network troubleshooting, performance monitoring, software distribution and updates, communications management, and device management.

Switches, Routers, and Network Appliances - Network devices ship with either no passwords or default passwords.

- **Network switches** are the heart of the modern data communication network. The main threat to network switches are theft, hacking and remote access, attacks against network protocols like ARP/STP or attacks against performance and availability.
- **VLANs -** provide a way to group devices within a LAN and on individual switches. VLANs use logical connections instead of physical connections.

Securing Network Devices (Cont.)

- **Firewalls -** are hardware or software solutions that enforce network security policies. A firewall filters unauthorized or potentially dangerous traffic from entering the network.
- **Routers -** Routers form the backbone of the Internet and communications between different networks. Routers communicate with one another to identify the best possible path to deliver traffic to different networks. Routers use routing protocols to make routing decision.
- **Wireless and Mobile Devices** - Wireless and mobile devices have become the predominant type of devices on most modern networks. They provide mobility and convenience but pose a host of vulnerabilities. These vulnerabilities include theft, hacking and unauthorized remote access, sniffing, man-in-the-middle attacks, and attacks against performance and availability.
- **Network and Routing Services** - Cyber criminals use vulnerable network services to attack a device or to use it as part of the attack. Securing network services ensures that only necessary ports are exposed and available. Network services include; DHCP, DNS, ICMP, Routing Services (RIP-OSPF-ISS), NTP and others.

Voice and Video Equipment

VoIP Equipment - uses networks such as the Internet to make and receive phone calls. The equipment required for VoIP includes an Internet connection plus a phone.

Cameras - An Internet camera sends and receives data over a LAN and/or the Internet. A user can remotely view live video using a web browser on a wide range of devices including computer systems, laptops, tablets, and smartphones. Cameras come in various forms including the traditional security camera.

Videoconferencing Equipment - allows two or more locations to communicate simultaneously using telecommunication technologies. These technologies take advantage of the new high definition video standards. Videoconferencing is now part of normal day-to-day operations in industries like the medical field.

Network and IoT Sensors - One of the fastest sectors of information technology is the use of intelligent devices and sensors. The computer industry brands this sector as the Internet of Things (IoT). Businesses and consumers use IoT devices to automate processes, monitor environmental conditions, and alert the user of adverse conditions.

Physical Access Control

Fencing and Barricades - Physical barriers are the first thing that comes to mind when thinking about physical security. This is the outermost layer of security, and these solutions are the most publicly visible. A perimeter security system typically consists of perimeter fence system, security gate system, bollards, vehicle entry barriers and guard shelters.

Biometrics - are the automated methods of recognizing an individual based on a physiological or behavioral characteristic. Biometric authentication systems include measurements of the face, fingerprint, hand geometry, iris, retina, signature, and voice. Biometric technologies can be the foundation of highly secure identification and personal verification solutions.

Badges and Access Logs – A badge allows an individual to gain access to an area with automated entry points. An entry point can be a door, a turnstile, a gate, or other barrier. Access badges use various technologies such as a magnetic stripe, barcode, or biometrics. The system logs the transaction for later retrieval. Reports reveal who entered what entry points at what time.

Surveillance

Guards and Escorts - All physical access controls including deterrent and detection systems ultimately rely on personnel to intervene and stop the actual attack or intrusion. In highly secure information system facilities, guards control access to the organization's sensitive areas.

Video and Electronic Surveillance – This type of surveillance can supplement or in some cases, replace security guards. The benefit of video and electronic surveillance is the ability to monitor areas even when no guards or personnel are present, the ability to record and log surveillance videos and data for long periods, and the ability to incorporate motion detection and notification.

RFID and Wireless Surveillance – These types of surveillance are used to manage and locate important information system assets.

User Domain

Common User Threats and Vulnerabilities

- The User Domain includes the users who access the organization's information system.
- Users can be employees, customers, business contractors and other individuals that need access to data.
- Users are often the weakest link in the information security systems and pose a significant threat to the confidentiality, integrity, and availability of the organization's data.

Managing User Threats

- Conduct security awareness training and user education.
- Enable and automate content filtering and antivirus scanning.
- Disable internal CD drives and USB ports.
- Minimize permissions, restrict access, track and monitor users and enable intrusion detection.

Device Domain

Common Threats to Devices

- Unattended workstations, user downloads, unpatched software
- Malware, use of unauthorized media, and violations of the acceptable use policy.

Device Domain Threats	Countermeasure to Manage Threat
Unattended workstations	Establish user account policies for passwords and threshold lockouts
User downloads	Establish access control policies, standards, procedures, and guidelines
Unpatched software	Update and apply security patches according to defined policies, standards, procedures, and guidelines
Malware	Enable an automated antivirus solution to scan systems and update antivirus software
Unauthorized media	Disable internal CD drives and USB ports
Acceptable Use Policy Violation	• Use content filtering • Use antivirus scanning for downloaded files • Disable internal CD drives and USB port

Local Area Network Domain

Common Threats to the LAN

- Unauthorized LAN access, unauthorized access to systems, applications, wireless networks and data
- Network operating system software vulnerabilities, misconfigurations and failure to perform updates
- Unauthorized network probing and port scanning

LAN Domain Threats	Countermeasure to Manage Threat
Unauthorized LAN access	• Secure wiring closets, data centers, computer rooms • Define strict access control policies, procedures, and guidelines
Unauthorized access to systems, applications, and data	• Define strict access control policies, procedures, and guidelines • Restrict access privileges for folders and files based on need
Network operating system software vulnerablitities	• Implement policy to patch and update operating systems
Network operating system unpatched	• Implement policy to patch and update operating systems
Unauthorized access by rogue users	• Require passphrases or authentication for wireless networks
Exploits of data in-transit	• Implement encryption between devices and wireless networks
LAN servers with different hardware or operating systems	• Implement LAN server configuration standards
Unauthorized network probing and port scanning	• Conduct post-configuration penetration tests
Firewall misconfiguration	• Conduct post-configuration penetration tests

Private Cloud (WAN) Domain

Common Threats to the Private Cloud:

- Unauthorized network probing, port scanning and access to resources.
- Router, firewall, or network device operating system software vulnerability and misconfiguration.
- Remote users accessing the organization's infrastructure and downloading sensitive data.

Private Cloud Domain Threats	Countermeasure to Manage Threat
Unauthorized network probing and port scanning	• Disable ping, probing, and port scanning
Unauthorized access to resources	• Implement intrusion detection and prevention systems
Router, firewall, or network device operating system software vulnerability	• Update devices with security fixes and patches
Router, firewall, or network device configuration error	• Conduct penetration tests post configuration • Test inbound and outbound traffic
Remote users download sensitive data	• Implement data classification standard • Implement file transfer monitoring and scanning

Public Cloud Domain

Common Threats to the Public Cloud:

- Data breaches, loss or theft of intellectual property and compromised credentials.
- Federated identity repositories are a high-value target.
- Account hijacking, social engineering attacks and lack of understanding on the part of the organization.

Public Cloud Domain Threats	Countermeasure to Manage Threat
Data breaches	• Multifactor authentication • Use of encryption • One-time passwords, phone-based authentication, and smartcards
Loss or theft of intellectual property	• Due diligence • Use of encryption • Data backup
Compromised credentials	• Multifactor authentication • Use of encryption • One-time passwords, phone-based authentication, and smartcards
Use of federated identity repositories	• Multifactor authentication • Implement one-time passwords, phone-based authentication, and smartcards
Account hijacking	• Multifactor authentication • Implement one-time passwords, phone-based authentication, and smartcards
Lack of understanding on the part of organization	• Due diligence on agreement responsibilities
Social engoneering attacks that lure the victim	• Security awareness programs
Compliance violations	• Due diligence • Policies

Physical Facilities Domain

Common Threats to Physical Facilities:

- Natural threats including weather problems, geological hazards, and power interruptions
- Unauthorized access to the facilities, open lobbies, theft, unlocked data center, lack of surveillance
- Social engineering, breach of electronic perimeter defenses

Physical Facilities Domain Threats	Countermeasure to Manage Threat
Natural threats including weather and geological problems	• Develop a disaster recovery plan • Develop a business continuity plan
Unauthorized access to facilities	• Implement badge encryption for entry access
Power interruptions	• Develop a disaster recovery plan
Social engineering	• Implement badge encryption for entry access • Conduct security awareness training regularly
Breach of electronic perimeter defenses	• Test building security using both cyber and physical means to covertly gain access
Theft	• Implement an asset tagging system • Establish policies and procedures for visitors
An open lobby	• Implement badge encryption for entry access
Lack of surveillance	• Implement CCTV coverage of all entrances • Test building security using both cyber and physical means to covertly gain access
An unlocked data center	• Implement badge encryption for entry access

Application Domain

Common Threats to Applications:

- Unauthorized access to data centers, computer rooms, and wiring closets
- Server downtime for maintenance, IT systems down for extended periods
- Network operating system software vulnerability
- Unauthorized access to systems
- Data loss

Application Domain Threats	Countermeasure to Manage Threat
Unauthorized access to data centers, computer rooms, and wiring closets	• Policies, standards, and procedures for staff and visitors
Server downtime for maintenance	• Disaster recovery plan • Business continuity plan
Network operating system software vulnerability	• Patches and updates completed regularly
Unauthorized access to systems	• Multi-factor authentication • Monitor log files
Data loss	• Data classification standards • Backup procedures
Downtime of IT systems for an extended period	• Disaster recovery plan • Business continuity plan
Software development vulnerabilities	• Conduct software testing prior to launch

Cybersecurity Information Websites

National Vulnerability Database (NVD) - is a U.S. government repository of standards-based vulnerability management data that uses the Security Content Automation Protocol (SCAP).

CERT - The Software Engineering Institute (SEI) at Carnegie Mellon University helps government and industry organizations to develop, operate, and maintain software systems that are innovative, affordable, and trustworthy. It is a Federally Funded Research and Development Center sponsored by the U.S. Department of Defense.

Internet Storm Center - provides a free analysis and warning service to Internet users and organizations. It also works with Internet Service Providers to combat malicious cyber criminals. The Internet Storm Center gathers millions of log entries from intrusion detection systems every day using sensors covering 500,000 IP addresses in over 50 countries.

The Advanced Cyber Security Center (ACSC) - is a non-profit organization that brings together industry, academia, and government to address advanced cyber threats. The organization shares information on cyber threats, engages in cybersecurity research and development, and creates education programs to promote the cybersecurity profession.

Cybersecurity Weapons

Vulnerability Scanners - assess computers, computer systems, networks, or applications for weaknesses. Vulnerability scanners help to automate security auditing by scanning the network for security risks and producing a prioritized list to address weaknesses.

Penetrating Testing (or pen testing) - is a method of testing the areas of weaknesses in systems by using various malicious techniques. Pen testing is not the same as vulnerability testing. Vulnerability testing just identifies potential problems. Pen testing involves a cybersecurity specialist who hacks a website, network, or server with the organization's permission to try to gain access to resources without the knowledge of usernames, passwords, or other normal means.

Packet Analyzers (or packet sniffers) - intercept and log network traffic. The packet analyzer captures each packet, shows the values of various fields in the packet, and analyzes its content. A sniffer can capture network traffic on both wired and wireless networks.

Security Tools - There is no one size fits all when it comes to the best security tools. Much depends on the situation, circumstance, and personal preference. A cybersecurity specialist must know where to go to get sound information.