Otázka1. - Vlastnosti bezpečnosti

1.Utajenosť – Mechanizmus na zabránenie prístupu k informáciám neautorizovaným osobám ktorí nemajú na to dostatočne pravá. Nástroje pre zabezpečenie utajenia sú: a) Šifrovanie – Je to transformácia informácie s použitím privátneho šifrovacieho kľúča do podoby, ktorá nemá žiadnu informačnú hodnotu. Takáto zašifrovaná správa môže byť prečítaná len príjemcom, ktorí vlastnia de-šifrovací kľuč. b) Kontrola prístupu – Mechanizmus, ako rozlišovať medzi požívateľmi to, že kto má alebo nemá prístup k určitým informáciám. Nástroje pre kontrolu prístupu sú: c) Autentifikácia – Je to overenie pravosti identity alebo roly používateľa v systéme. Overenie prebieha tak, že užívateľ spojí svoju identitu s tajnou informáciou, napríklad heslom, otlačkom prsta a pod. d) Autorizácia – Je to stanovenie, či má osoba alebo systém prístup k určitej operácií. Táto kontrola prístupu je väčšinou zadefinovaná v tzv. white list, v ktorom sa definuje kto a akú operáciu smie vykonávať. e) Fyzická kontrola prístupu – Zavedenie fyzických bariér k obmedzeniu prístupu k chráneným výpočtovým zdrojom. Napr. zámky na dverách, alebo budovy, kde elektromagnetické signály nemôžu uniknúť dnu ani von z budovy.
2.Integrita – Mechanizmus na to, aby v komunikácií nedošlo k nejakej modifikácií informácií, či už nejakými útočníkmi alebo nejakým iným spôsobom (napr. zlý prenosový kanál, rušenie wi-fi siete a pod.) Nástroje pre zabezpečenie integrity sú: a) Zálohovanie – Periodická záloha dát. b) Kontrolné sumy – funkcia ktorá vypočíta číselnú hodnotu (kontrolnú sumu) zo súboru. Tzn. Že ak bol súbor čo i len trochu upravený bude kontrolná suma odlišná.
3.Dostupnosť – Pokiaľ má používateľ prístup k určitej službe alebo zdrojom, tak mal by mať k tmu prístup vždy keď o to požiada. Nástroje pre zabezpečenie dostupnosti sú: a) Fyzická ochrana – zabezpečenie zariadenia, budovy, tak aby nemohli byť narušené treťou osobou. b) Výpočtové redundancie – automatické nahrádzanie zdrojov, pokiaľ jeden z nich vypadne.
4.Istota (Dôvernosť) – Existuje tu tzv. manažment dôveryhodnosti (dôvernosť medzi systémom a používateľom) je na takom stupni, že systém a používateľ si dôverujú navzájom. Nástroje pre zabezpečenie dôvernosti sú: a) Bezpečnostná politika – špecifikuje správanie ľudí alebo systémov v rámci ostatných (povinná alebo diskrétna kontrola prístupu). b) Bezpečnostné práva – opisujú správanie, že čo používateľ môže vykonať a čo nemôže. c) Bezpečnostná ochrana – opisuje mechanizmy na zaistenie práv a politiky na základe identity používateľa.
5.Autentickosť – Je to stanovenie, že údaje, postupy a práva vydané osobami alebo systémom sú pravé. Hlavným nástrojom na zaistenie autentickosti je digitálny podpis.
6.Anonymita – Je to vlastnosť, že určité záznamy alebo transakcie nepripadnú ku žiadnemu jednotlivcovi. Nástroje pre zabezpečenie anonymity sú: a) Agregácia – kombinácia dát od viacerých používateľov. b) Mixácia – agregovanie informácií z viacerých strán a spájanie ich do zložiek, ktoré sa nedajú rozložiť. c) Proxy – dôveryhodní agenti, ktorí nahrádzajú skutočnú identitu používateľa.
d) Pseudonym – fiktívna identita používateľa, ktorý predstiera identitu.

Otázka2. – Modelovanie hrozieb

Metodológia na identifikovanie, ohodnotenie a zdokumentovanie hrozieb, útokov a zraniteľnosti. Aplikuje sa na rôzne časti systému. Cieľom je minimalizovať bezpečnostné riziká počas návrhu, implementácie a údržby.

Fázy:
a) Identifikácia assets – identifikácia zdrojov, s ktorými aplikácia pracuje.
b) Definícia cieľov bezpečnosti – stupeň požadovaného utajenia, integrity a dostupnosti.
c) Návrh architektúry aplikácie – moduly, funkčnosti, aplikácie.

d) Bezpečnostný profil – dátové toky, vstupne a výstupne body.
e) Identifikácia hrozieb a rizík – STRIDE
f) Dokumentácia hrozieb a rizík
g) Ohodnotenie hrozieb – vážnosť zraniteľnosti.

STRIDE – systém na kategorizovanie hrozieb do skupín:
a) Spoofing – maskovanie totožnosti a vydávanie sa za inú osobu.
b) Tempering – zmena údajov
c) Repudation – ak aplikácia alebo systém nemá nástroje na správne sledovanie a zaznamenávanie akcii používateľov. Umožňuje tak škodlivé manipulácie alebo vytváranie akcii
d) Information disclosure – uník informácii, útočník môže získať cestu k súborom, získať súkromne informácie
e) Denial of service – DOS – zahltenie cieľa nepotrebnými požiadavkami natoľko, že nestíha obsluhovať bežných používateľov. Napr. Spam.
e) Evelation of privilage – je zneužitie chyby v programe tak, že útočník získa (napr. v operačnom systéme) vyššie oprávnenie ako mu bola pôvodne správcom počítača udelené.

Otázka3. – Digitálny podpis

Je analogicky ručnému podpisu, ktorý slúži ako dôkaz autorstva, resp. súhlasu s obsahom dokumentu. Je to určitá dátová štruktúra, ktorá je závislá na dokumente, vzniká hashovaním toho dokumentu a tento kód je zašifrovaný súkromným kľúčom, ktorý je jednoznačným vlastníctvom vlastníka dokumentu.
Verifikácia DP – správa sa dešifruje verejným kľúčom (t. j., že správa bola zašifrovaná súkromným kľúčom a jej jednoznačným vlastníkom je odosielateľ - autentizácia), dostaneme hashovací kód. Ak má odosielateľ a príjemca rovnaký hashovací kód, tak máme istotu, že správa nebola zmenená. Ak bla zmenená, tak nedostaneme rovnaký hashovací kód – integrita.
Vlastnosti DP – forma skupiny bitov, ktorých hodnoty sú závislé na podpísanej správe. DP využíva určitú jedinečnú informáciu (súkromný kľúč), ktorá je vlastníctvom držiteľa podpisu a zabezpečuje ochranu pred falšovaním a odmietnutím. Realizácia a implementácia DP by mala byť relatívne ľahká. Falšovanie DP by malo byť výpočtovo obťažné. Uloženie DP v pamäti by malo byť jednoduché.

Otázka4. – XSS (cross site scripting)

Útočník vloží kód do stránky vygenerovanej web aplikáciou. Tento skript môže byť škodlivý kód. Je reprezentovaný pomocou JavaScript (Ajax), VBScript, ActiveX, HTML alebo Flash.
Hrozby:
a) phishing – je činnosť, pri ktorej sa snaží podvodník od používateľov vylákať rôzne heslá.
b) hijacking - je odcudzenie autentizačných dát prostredníctvom HTML cookie a získanie neoprávneného prístupu k nejakému webu, účtu, online službám a pod.
c) zmena používateľských nastavení
d) odcudzenie cookies
e) klamlivá reklama
f) vykonávanie kódu u klienta

Klientska ochrana proti XSS:
a) Proxy – sledovanie trafficu http medzi prehliadačom a web serverom. Hľadanie špeciálnych HTML znakov. Enkodovať všetky znaky pred tým ako je stránka vy-renderovaná (napr. Firefox plugin NoScript).
b) Aplikačný firewall - Analýza HTML stránok za účelom nájsť hyperlinky, ktoré môžu viesť k úniku citlivých informácií. Zastavenie zlých requestov s použitím sady pravidiel.
c) Auditovací systém - Sledovanie spustenia javascriptového kódu a porovnanie operácií oproti vysoko prioritným podmienkam pre detekovanie škodlivého kódu.

Otázka5. – Pretečenie zásobníka (Buffer Overflow Attack)

Ide o útok napadnutia programu alebo operačného systému, ktorý využíva pretečenie zásobníka k vykonaniu požadovaného príkazu. Je to najbežnejšia chyba v operačnom systéme.

Vznik pretečenia zásobníka:

- Developer nespraví kontrolu, či vstup sa zmestí do zásobníka
- Vstup v spustenom procese presahuje dĺžku zásobníka
- Vstup prepíše cash pamäte procesu
- Spôsobí, že sa aplikácia začne správať nesprávne a neočakávane
- Je často problémom jazyka C

Princíp pretečenia zásobníka:

- Proces môže pracovať so škodlivými dátami alebo môže spúšťať škodlivý kód vložený do vstupu útočníka
- Ak proces je spustený ako root, škodlivý kód bude spustený s root právami

Riešenie problému:

- Zabrániť vieme tomu tak, že zásobník budeme alokovať dynamicky
- Uprednostniť jazyk ktorý sám manažuje prácu s pamäťou, ak je to možné
- Budeme používať bezpečné funkcie v kóde, ktoré vyžadujú definovanie veľkosti strcpy(), strncpy()
- Náš program nebude bežať pod root právami
- Kontrola zadaného vstupu

Otázka6. – IDS Systémy (Intrusion Detection System)

Je to obranný systém, ktorý monitoruje sieťový chod a snaží sa odhaliť podozrivé aktivity. Okrem samotného útoku detekuje aj predprípravu na útok, skenovanie portov, zbieranie informácií. Hlavnými činnosťami IDS systému je detekcia automatizovaných útokov a hrozieb vrátane:
a) Port scan – zhromažďovanie informácií za účelom určenia, ktoré porty sú otvorené pre TCP spojenie.
b) Denial of service attack – sieťový útok chce premôcť hostiteľa a vypnúť legitímny prístup.
c) Malware attack – útok malware vírusom
d) ARP Spoofing – pokus o presmerovanie IP v lokálnej sieti.
e) DNS cache poisoning

Typy IDS:
a) uzlovo orientované IDS – softvér, ktorý kontroluje systémové volania, prácu so systémovými súbormi, činnosť aplikácie a pod.
b) sieťovo orientované IDS – platforma, ktorá monitoruje sieťovú komunikáciu (kontroluje všetky pakety).
c) pasívne IDS – proti útoku nezasahuje, len vygeneruje Alert, log a kontaktuje správcu
d) aktívne IDS – zasahuje proti útoku

Otázka7. – DNSsec

Umožňujú zabezpečiť informácie poskytované DNS systémom v IP sieťach (t. j. na Internete) proti odcudzeniu (tzv. spoofing) a úmyselnej manipulácii. DNSsec používa asymetrické šifrovanie.

- Držiteľ domény vygeneruje verejný a súkromný kľúč
- Súkromným kľúčom podpíše údaje o svojej DNS
- Verejný kľúč potom odošle všetkým nadriadeným autoritám jeho domény
- Týmto sa zabezpečí neprijímanie podvrhnutých záznamov ako odpovedi

Otázka8. – Symetrické šifrovanie

Princíp symetrického šifrovania spočíva v tom, zem na dešifrovanie správy sa používa ten istý kľuč, pomocou ktorého bola sprava zašifrovaná. Tento kľuč poznajú len tie osoby, ktoré pomocou tejto šifry navzájom komunikujú.

Medzi najjednoduchšie symetrické šifrovanie patri napríklad šifrovanie zámenou písmena. Každému písmenu v abecede je priradene iné písmeno abecedy.

Ďalšou známou možnosťou sú posuny v abecede. Pri tomto spôsobe šifrovania sa zamieňajú znaky v správe za znaky, ktoré stoja v abecede o niekoľko miest doprava (resp. doľava).

Uvedene šifry majú niekoľko vážnych nedostatkov. Ak poznáme šifrovanú správu a zároveň poznáme originál správy, môžeme si veľmi jednoducho zistiť šifru, ktorou je sprava zašifrovaná. Takisto je problémom oboznámiť adresáta šifrovanej správy so šifrovacím kľúčom tak, aby sa o ňom nikto iný nedozvedel.

Otázka9. – Hash funkcia

Hashovacia funkcia slúži na kontrolu integrity dát. Hashovacia funkcia je funkcia, ktorá transformuje správu s ľubovoľnou dĺžkou na vstupnú hodnotu vyjadrenú fixným počtom bitov bez použitia kľúča. Vstupná hodnota označovaná ako hashovací kód slúži ako identifikátor. Výstupný hashovací kód sa označuje: h = H(M), kde h má pevnú dĺžku desiatky až stovky bitov.
Hashovacia funkcia musí obsahovať dve základne požiadavky:
a) Jedno čestnosť - Hashovacia hodnota sa počíta ľahko. Na základe hashovacej hodnoty je ťažké nájsť dokument s tou istou hodnotou.
b) Odolnosť voči kolízií – Je veľmi ťažké nájsť dva rozličné dokumenty s rovnakou hashovacou hodnotou.

Otázka10. – ARP Spoofing

ARP protokol:

- Využíva sa na získavanie MAC adresy počítača z jeho IP adresy
- Dôvodom je poznať fyzickú MAC adresu počítača v rovnakej LAN siete
- Takéto zisťovanie adries sa zapisuje do ARP cache
- ARP protokol používa IPv4

ARP Spoofing:

- Vydávanie sa za iný počítač
- Útočník neustále posiela svoju MAC adresu na všetky requesty IP adries
- Ochranou je použitie statickej ARP tabuľky (vopred danej)

Otázka11. – Certifikáty s využitím asymetrického šifrovania

SSH ...

Otázka12. – Protokol HTTPS

- využíva asymetrické šifrovanie SSL alebo TLS
- obe strany si pred zahájením komunikácie vygenerujú dvojicu kľúčov
- -obe strany si vymenia verejne kľúče
- skontroluje sa digitálny podpis nejakej certifikačnej autority ktorej verejný kľuč mame uložený
- ak je všetko OK môžeme nadviazať komunikáciu

Otázka13. – Cookies

Sú informácie uložené v počítači spojené s niektorým špecifickým serverom.

- Ak navštívime špecifickú web stránku, tak server môže uložiť nejakú informáciu v počítači ako cookies.
- Vždy, keď navštívime danú web stránku, cookies je znovu odoslaná na daný server.
- Efektívne sa používa na udržanie stavovej informácie nad sessions.
- Môžu obsahovať hocijakú informáciu.
- Môže obsahovať citlivé informácie ako heslá, informácie o kreditnej karte a pod.
- Skoro každá web stránka používa cookies.
- Veľa stránok vyžaduje povolenie cookies na používanie.
- Ich uloženie v počítači sa prirodzene hodí exploitom (napr. ActiveX môžu zneužiť cookies).
- Používateľ môže resp. by mal vymazať cookies z počítača.
- Webové prehliadače podporujú vypnutie cookies a ich povolenie len pre konkrétne vymenované webové stránky.

Expirácia cookies:

- Expirácia je defaultne nastavená prostredníctvom sessions zo stránok servera
- To znamená, že cookies budú aktívne nejakú dobu

Manažovanie cookies:

- Vymazanie konkrétnej cookies

- Vymazanie všetkých cookies
- Zobrazenie informácií o konkrétnych cookies

Otázka14. – DNS (Domain name system)

DNS je protokol aplikačnej vrstvy, ktorý prekladá doménové mená (hostname) do IP adries. DNS zabezpečuje distribuovanú databázu nad internetom, ktorá ukladá rôzne záznamy vrátane:
a) Address (A) – IP adresy spojené s názvom hostiteľského zariadenia
b) Mail Exchange (MX) – mail server v doméne
c) Name Server (NS) – autoritatívny server pre doménu

Otázka15. – Asymetrické šifrovanie

Dva kľúče, privátny a verejný. Odosielateľ zašifruje správu verejným kľúčom prijímateľa. Prijímateľ dešifruje správu svojím privátnym kľúčom. Veľkou výhodou asymetrického šifrovania je, že vieme v ňom využiť digitálny podpis na zabezpečenie autencity správy.