Zaverečná písomka PV080 2012 11.12.
(symbolom „ * “ sú označené správne odpovede)

1.Pro zajištění prokazatelné zodpovědnosti (accountability)?

*Je na začátku práce v systému obvykle prováděna autentizace nebo identifikace.

Ja na začátku práce v systému obvykle prováděno dešifrování dat pro práci s účtem.

*Je prováděna archivace dat umožňujících propojení činnosti s konkrétní osobou tak, že daná osoba se nemůže zříci zodpovědnosti za svoji činnost.

Je prováděna archivace dat pro udržení schopnosti správy účtu.

2.Bezpečnostní politika zahrnuje

*Požadavky, pravidla a postupy určující způsob ochrany a zacházení s ochraňovanými hodnotami

Seznam konkrétních osob, které mají povoleno přistupovat k citlivým datům společnosti

Specifikaci technologických opatření kterými budou prosazovány bezpečnostní požadavky společnosti

3.Které z těchto tvrzení je správné, pokud mluvíme o platebních kartách?

*PIN platební karty lze získat i jinak než odpozorováním při zadávání.

*Embosované platební karty patří k těm nejsnadněji zneužitelným.

Nehledě na uživatelovo chování (a možnost odpozorování PINu) je platební karta s čipem absolutně bezpečná.

PayPal je rozšíření a vylepšení základních bezpečnostních mechanizmů platebních karet (schváleno jak MasterCard, tak VISA).

Dodatečným mechanizmem ochrany čipu je magnetický proužek (jedná se o tzv. vícefaktorovou autentizaci).

Embosované platební karty poskytují nejvyšší stupeň zabezpečení (proto jsou vyžadovány při transakcích s vyšším obnosem).

4. Zabezpečení provozu na úrovni IP dosáhnu pokud zvolím:

*IPv6

IPv4s

Stunnel

PGP

*IPsec

5.Které z následujících metod lze využít k analýze rizik?

Metoda ARO (Annualized Rate of Occurence)

Metoda RSA (Risk System Analysis)

*Metoda BPA (Business Process Analysis)

*Metoda ALE (Annual Loss Expentancy)

Metoda AES (Advanced Evaluation Standard)

6. Pokud existuje v systému zranitelnost a existuje útočník, který ji může využít, výsledný stav je nazýván:

riziko

zranitelnost

útok

*hrozba

7. Pod pojmem hybridní kryptosystémy rozumíme například

Data jsou před šifrováním algoritmem symetrické kryptografie hašována, šifrována je pouze výsledná haš

Data jsou před podpisem zašifrována algoritmem asymetrické kryptografie

*Data jsou šifrována náhodným symetrickým klíčem, ten je šifrován veřejným klíčem příjemce

8. Která z uvedených tvrzení jsou pravdivá?

*Symetrická kryptografie využívá jeden klíč sdílený mezi dvěma a více uživateli.

Pokud chceme využít asymetrickou kryptografii k šifrování, musí zůstat oba klíče utajeny.

Teoreticky lze použít asymetrickou kryptografii i k šifrování, ale v praxi se toho nevyužívá.

Symetrická kryptografie se využívá pouze pro šifrování, zatímco asymetrická pouze k podepisování.

9. Pro emailové zprávy posílané pomocí systému Mixminion platí

odpovědi jsou v systému doručovány odlišně od normálních emailů

*je možné na ně v určitém časovém rámci odpovědět

*uživatel specifikuje cestu po síti

jsou pseudonymní

*jsou anonymní

hlavičky mailů nejsou modifikovány

10. Mezi bezpečnostní požadavky podle standardu pro hodnocení kryptografických modulů FIPS 140-1/2 patří:

*Služby a autentizace

*Rozhraní modulu

Testování GUI modulu

Odolnost vůči lidskému faktoru

*Bezpečnost O/S

*Fyzická bezpečnost

11. Co zajišťuje certifikát veřejného klíče?

*Integritu veřejného klíče.

*Spojení veřejného klíče s označením entity.

Důvěryhodnost označené entity.

Důvěryhodnost vlastníka veřejného klíče.

Důvěrnost veřejného klíče.

12. Proč platební karty s čipem mají magnetický proužek?

Čip provádí kryptografické operace nad daty uloženými na magnetickém proužku.

Žádná z těchto odpovědí není správná.

*Kvůli zpětné kompatibilitě.

13. Cílem projektu Eternity server je

poskytnout trvalé úložiště dat s operacemi uložit, nalézt a smazat

*poskytnout trvalé úložiště dat

navrhnout službu, která je odolná vůči útoku typu Denial of Service

*vytvořit datové úložiště, které je odolné vůči výpadkům

14. Které dvě z těchto biometrických technik jsou nejpohodlnější pro uživatele?

vzor oční sítnice

EKG

*vzor oční duhovky

*srovnání tváře

15. Je lepší používat TOR nebo Mixminion?

Ani jedno, ani druhé.

*Záleží na tom, co chceme dělat.

Jednoznačně Mixminion.

Jednoznačně TOR.