1 Pro urychlení počítačových systémů využívajících digitální podpis
- [ ] se často používá podchlazování ochranných komponent čipových karet
- [x] ✔ *obvykle využíváme hašovací funkce pro reprezentaci podepisovaných dat
- [ ] používají obě strany identický privátní klíč
- [ ] lze využít prokazatelnou odpovědnost metodou Monte Carlo
- [x] ✔ *u čipových karet bývají použity kryptografické koprocesory

body = 2 = 2

2 Zjistitelností narušení se u čipových karet myslí:
- [ ] Vlastnost části systému umožňující reagovat na fyzický útok.
- [ ] Odolnost proti pokusům o zjištění robustnosti vůči fyzickým útokům.
- [ ] Při zjištění narušení je automaticky provedena chráněnou částí obranná akce.
- [x] ✔ *Po narušení jsou stopy narušení obtížně odstranitelné.

body = 4 = 4

3. Pro autentizaci v sítích GSM se používá:
- [ ] asymetrická kryptografie s protokolem RAND
- [ ] *dvoufaktorová autentizace - SIM a (nepovinný) PIN
- [x] ✔ *jedno nebo dvoufaktorová autentizace podle nastavení PINu
- [ ] Shamirův bezklíčový protokol
- [ ] zero-knowledge protokol Fiat-Feige se čtyřmi faktory

body = 2 = 2

4 Integrita dat znamená
- [ ] Data nebyla autorizovaně předána
- [ ] Data v původní podobě lze obnovit i přesto, že byla modifikována
- [x] ✔ *Data nebyla neautorizovaně změněna
- [ ] Data nebyla neautorizovaně změněna pouze v průběhu přenosu nezabezpečeným kanálem

body = 4 = 4

5 Proti jakým útokům brání protokol ssh?
- [ ] Odposlech hesla a pozdější přehrání (na uživatelově PC)
- [x] ✔ *Odposlech hesla a pozdější přehrání (na síťové vrstvě)
- [x] ✔ *DNS/IP/Routing spoofing
- [ ] Analýza šifrovaného provozu na síťové vrstvě

body = 4 = 4

6. Offline verifikace karetní transakce:
- [ ] *je zakalkulovaná v systému řízení rizik a provádí se pro snížení transakčních nákladů
- [ ] *se dnes již v bankomatech neprovádí
- [ ] *se za určitých podmínek provádí v PINpadu
- [ ] vyžaduje přiblížení pasu s čipem podporujícím DDA k PINpadu
- [ ] se používá jen v zemích Eurozóny (země platící eurem)
- [ ] je povolena jen při biometrické autentizaci uživatele

body = null = 0

7 Jaké jsou typické velikosti pamětí u současných čipových karet?
- [ ] < 100KB RAM, < 100KB ROM, > 1MB EEPROM
- [ ] > 256KB RAM, ~100KB ROM, < 100KB EEPROM
- [x] ✔ *< 10KB RAM, ~100KB ROM, < 100KB EEPROM
- [ ] ~128KB RAM, ~512KB ROM, ~512KB EEPROM

body = 2 = 2

8 Které z výroků o autentizaci na základě rozpoznání obličeje nejsou pravdivé?
- [x] ✔ *Přesnost se v posledních 9 letech příliš nezlepšila.
- [ ] Autentizaci komplikuje osvětlení a pozadí.
- [ ] Autentizaci komplikuje změna účesu, náušnice a brýle.
- [ ] Jedná se o výpočetně náročnou metodu autentizace.

body = 2 = 2

9 Které z uvedených režimů nepodporuje IPsec:
- [x] ✔ *Překladový režim.
- [x] ✔ *Dynamický virtuální režim.
- [ ] Transportní režim.
- [ ] Tunelovací režim.

P. Hurychová, učo 422403, 18. 5. 2015 14:47.02

body = 2 = 2

10 Čím je dáno, že komunikace s RFID tagem musí probíhat pouze na přímou viditelnost?
- [ ] Použitými kryptografickými mechanizmy
- [x] ✔ *Použitou vlnovou délkou
- [ ] Množstvím přenášených dat
- [x] ✔ *Použitým frekvenčním pásmem

P. Hurychová, učo 422403, 18. 5. 2015 14:47.02

body = 2 = 2

11 Při hašování hesel pro autentizaci uživatelů pomocí hesel:
- [ ] Ukládáme pouze haš hesla s možností rekonstrukce hesla v otevřené podobě
- [x] ✔ *Ukládáme pouze haš hesla a rekonstrukce otevřené podoby není možná
- [x] ✔ *Při ukládání můžeme využít techniky "solení"

body = 4 = 4

12 Markanta v oblasti biometrik znamená:
- [ ] Biometrická technologie s významně vysokou hodnotou EER.
- [x] ✔ *Významný bod v otisku prstu.
- [ ] Zpracovaný obraz oční duhovky se zvýrazněnými přechody.
- [ ] Výrazné poškození dané biometriky u konkrétního uživatele.

body = 4 = 4

13 Které z následujících dělení modelů řízení přístupu není používáno:
- [x] ✘ centralizované / decentralizované
- [x] ✔ *synchronní / asynchronní
- [ ] seznam přístupových oprávnění (capabilities) / seznam přístupových práv (ACL)
- [ ] *řízené pravidly / náhodné
- [ ] volitelné / povinné
- [x] ✔ *symetrické / asymetrické

body = 2 = 2

14 Zaručený elektronický podpis
- [x] ✔ *Je jednoznačně spojen s podepisující osobou
- [x] ✔ *Umožňuje detekci změn ve zprávě, ke které je připojen
- [ ] Autorizuje podepisující osobu ve vztahu k datové zprávě
- [x] ✔ *Umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě
- [ ] Je spojen s dostatečnou finanční zárukou
- [x] ✔ *Je jednoznačně ověřitelný

body = 6 = 6

15 Řízení přístupu, při němž vlastník rozhoduje o přístupech ke svým souborům, se nazývá:
- [ ] Princip maximálních privilegií.
- [x] ✔ *Volitelné řízení přístupu.
- [ ] Povinné řízení přístupu.
- [ ] Flexibilní řízení přístupu.

body = 2 = 2

Celkem bodů: 42 (z maximálních 52) (celkem otázek: 15, z toho špatně 0, nezodpovězených 3)

Otevřené otázky:

1. Napište 2 výhody a 2 nevýhody autentizace biometrikou oproti jiné metodě.

2. Popište, jak probíhá man in the middle útok na Diffie-Hellman protokol.

3. Co jsou a jak fungují tokeny založené na hodinách? Jaké jsou jejich bezpečnostní nedostatky?

4. model Bell-LaPadula (nepamatuji si přesně)

odpovědníková část – max. 52 b.

otevřené otázky – max. 20 b.

vnitrosemestrální – max. 28 b.

<100,90> … A

(90, 80> … B

(80, 70> … C

(70, 60> … D

(60, 50> … E

(50, 0> … F
