Bezpečnost

Úvod do problematiky bezpečnosti

INS_2020_12. přednáška

Zranitelnost informačního systému

- Fyzická – technické závady, zcizení, …
- Přírodní – IS nemá schopnost vyrovnat se s objektivními faktory – blesk, záplava, požár, …
- Technologická - IS/ICT svými konstrukčními charakteristikami neumožňuje zajistit např. požadovaný trvalý plynulý provoz
- Fyzikální – IS/ICT pracuje na takových fyzikálních principech, které umožňují jejich zneužití (např. odposlech)
- Lidská – působení lidí – úmyslné /neznalost, omyl
- Programátorská – možnost algoritmického prolomení zabezpečovacích algoritmů

Fyzické a přírodní ohrožení

– Technické závady
– Přírodní katastrofy
– Výpadky dodávky elektrické energie

Typy programových ohrožení

- Počítačové viry - program, který se šíří bez vědomí uživatele
- Trojské koně - skrytá část programu nebo aplikace provádějící funkce, se kterou uživatel nesouhlasí
- Back-doors – vstup do systému bez hesla
- Zapomenuté funkce z doby vývoje
- Phishing - podvodný email snažící se vylákat důvěrné informace-hesla atd.
- Hoax – poplašná zpráva
- Spyware – sw sleduje uživatele nebo informace o jeho počítači a data odesílá
- Rootkit – program k zamaskování určitých aktivit na počítači

Zabezpečení sítí

Příklady hrozeb:

- Virová nákaza
- Útoky typu DoS (Denial of Services)
- Odposlech provozu (bezdrátové sítě, vyzařování CRT monitorů…)
- Přístup k nezabezpečeným kanálům

Cíle útočníků

- Krádež dat a informací
- Zničení dat
- Destabilizace systému
- Blokování místa nebo určitých zdrojů

Typy útočníků

- Hacker
  - Začátečník -> uznání, seberealizace
  - Profesionál -> překonání intelektuálních výzev, ideál o svobodném přístupu informací...
- Virový tvůrce – „zrazení idealisté“, „nedocenění odborníci“,…
- Vnitřní nepřítel („Insider thread“) – odplata vůči zaměstnavateli, pocit křivdy, …
- Informační válečník – vlastenecké motivy – destabilizace nepřátelských zdrojů
- Zloděj – snaha o zisk financí, př. Phishing
- Politický aktivista – fanatik, idealista…

Chyby, které využívají útočníci

- **Programátorské chyby**
- **Návrhové chyby**
- **Konfigurační chyby**
- **Fyzické narušení**
- **Chyby obsluhy**

Obranné mechanismy

Ochranné mechanismy

Fyzické a přírodní ohrožení:

- **Zálohování** – úplná/inkrementální
- **Zabezpečení** – UPS, přepěťové ochrany

Ochranné mechanismy

Softwarové ohrožení:

- Firewall, antivirové programy, …
- Sítě – VPN (Virtual Private Network) –
- Autentizace a řízení přístupových práv
- Bezpečnostní politika, plán obnovy činnosti, havarijní plán

Firewall

Firewall, tzv.„bezpečnostní brána“, je zařízení či software oddělující provoz mezi dvěma sítěmi (např. interní podniková a veřejný internet), přičemž propouští jedním nebo druhým směrem data podle určitých předem definovaných pravidel.

Brání tak zejména před neoprávněnými průniky do sítě a odesílání dat ze sítě bez vědomí a souhlasu uživatele.

Autentizace a Autorizace

Autentizace = ověření uživatele

Autorizace = ověření práv

Autentizace

- **Přístup přes uživatelská jména a hesla nebo PIN**
  - Expirační doba hesel
  - Omezený počet pokusů přihlášení (heslo, PIN)
  - „Strong“ password – minimální počet znaků, povinné kombinace čísel a písmen, zákaz používání smysluplných slov
  - Zákaz „prázdného“ hesla
- **Ověření uživatele**
  - Vlastnictví určitého předmětu – karta, čárový kód, token
  - Ověření fyziologických charakteristik – biometrie
- **Využití časových intervalů** (automatické odhlášení při delší nečinnosti)

Biometrie

- Moderní definice biometrie se od původního chápaní liší zejména tím, že do procesu vstupuje automatizace: Biometrie je obecný termín popisující charakteristiku nebo proces.
- Biometrie jako charakteristika:
  - Měřitelná biologická (anatomická a fyziologická) a behaviorální charakteristika, kterou můžeme použít pro automatizované rozpoznávání.
- Biometrie jako proces:
- Automatizované metody rozpoznávání jednotlivce založené na měřitelných biologických (anatomických a fyziologických) a behaviorálních charakteristikách.

15

Autentizace

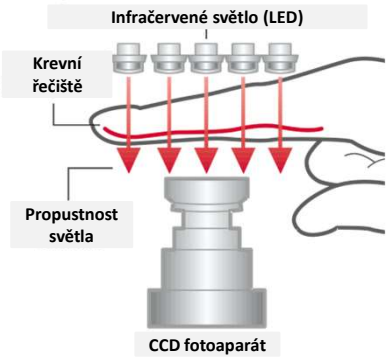
Biometrie:

- Otisky prstů
- Snímek oční sítnice a duhovky
- Rozpoznání obličeje, dlaně
- Rozpoznání hlasu
- Dynamika podpisu, psaní na klávesnici

Autentizace - biometrie

- Problémy biometrických metod
  - Obtížnost měření biometrických informací
  - Závislost měření na prostředí a fyzické kondici uživatele
- Chyby biometrických systémů
  - Oprávněnému uživateli je odmítnut přístup do systému (False Rejection Error)
  - Neoprávněný uživatel je biometrickým zařízením označen jako oprávněný (False Acceptance Error)

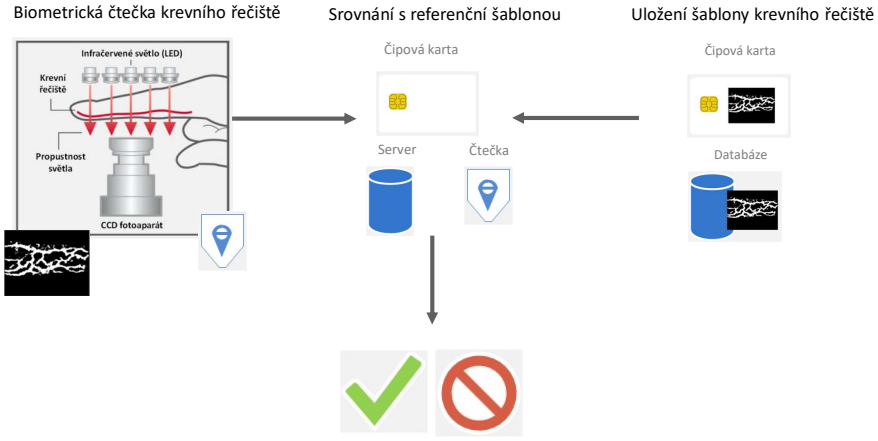
Biometrie krevního řečiště



- Založená na snímání vzorků krevního řečiště v prstu
- Každý vzorek je jedinečný i pro dvojčata, stárnutí nemá vliv na krevní řečiště
- Biometrická šablona je vytvořena na základě matematické analýzy struktury krevního řečiště a uložena v šifrované podobě
- Použité infračervené osvětlení je zcela bezpečné pro lidi i zvířata

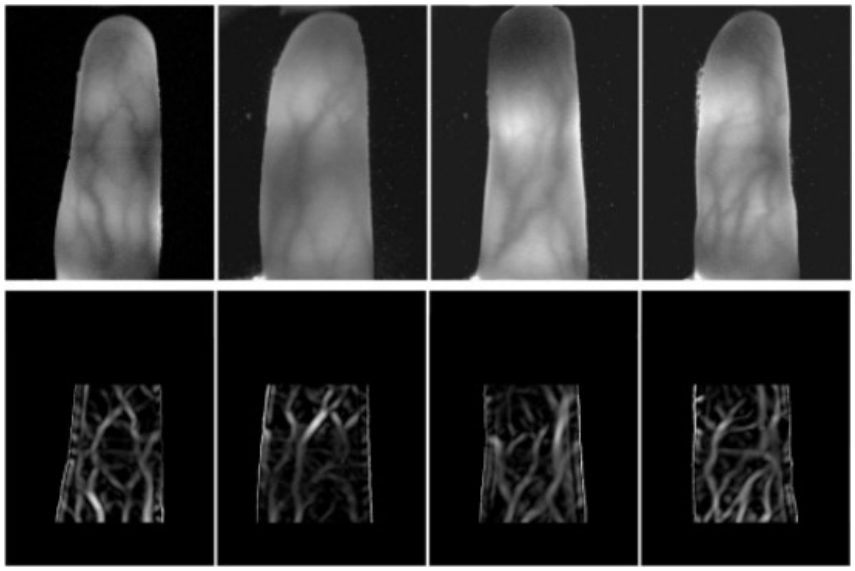
18

Použití biometrie krevního řečiště

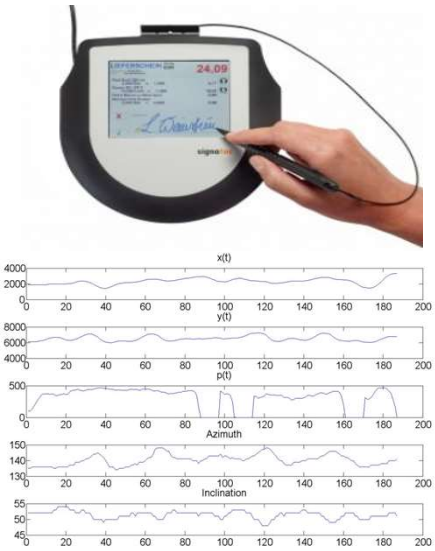


19

Snímky krevního řečiště



Biometrie dynamického podpisu



- Dynamické systémy produkují jedinečné podpisy
- Nenáročné na použití a akceptaci u uživatelů
- Společensky velmi přívětivé vzhledem ke zvyku podepisování na papír
- Vyjadřuje souhlas stejně jako identitu osoby
- Obtížné zajistit stoprocentní strojové ověření mezi různými podpisy uživatele – pravost je ověřitelná písmo znalcem

21

Legislativa

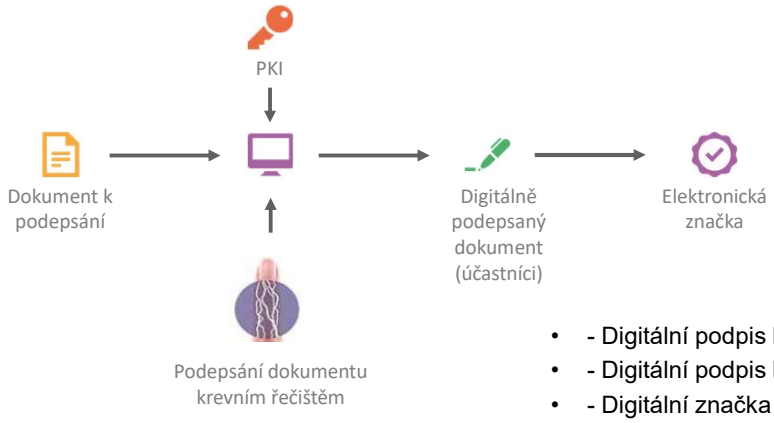
- Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických údajů v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů
- Zákon 101 ze dne 4. dubna 2000 o ochraně osobních údajů a o změně některých zákonů
- GDPR

ÚOOÚ:

- Stanovisko č. 3/2012 k vývoji biometrických technologií
- Stanovisko č. 2/2014 – Dynamický biometrický podpis z pohledu zákona o ochraně osobních údajů
- Zpracování citlivých osobních údajů

22

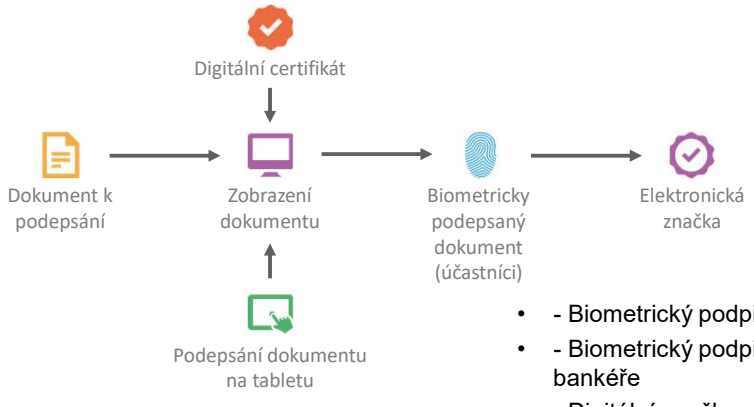
Podepisování biometrií krevního řečiště



- - Digitální podpis klienta
- - Digitální podpis bankéře
- - Digitální značka společnosti
- - Digitální časové razítko

23

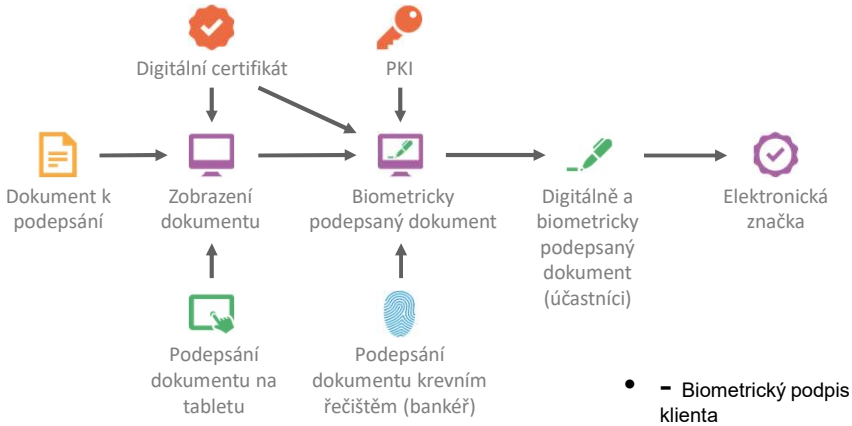
Podepisování dynamickým biometrickým podpisem



- - Biometrický podpis klienta
- - Biometrický podpis bankéře
- - Digitální značka společnosti
- - Digitální časové razítko

24

Podepisování Bio PKI + DBP



- - Biometrický podpis klienta
- - Digitální podpis bankéře
- - Digitální značka společnosti
- - Digitální časové razítko

25

Porovnání BioPKI A DBP

BioPKI	Dynamický biometrický podpis
Využití certifikátů s privátním klíčem pro digitální podepisování dokumentů	Okamžité použití bez nutnosti registrace uživatelů
Legislativní podpora uznávaných elektronických podpisů na dálku	Sociálně velmi přívětivé vyjádření souhlasu
Instantní ověření dokumentů dle principu PKI	Možnost využití tabletu pro zobrazení a podepsání dokumentů
Automatizovaná správa certifikátů a privátních klíčů	Ověření biometrického podpisu závisí na dostupnosti privátního klíče a písmo znalce
Nutná registrace biometrie uživatelů	Biometrický podpis přímo vložen do dokumentu jako citlivý osobní údaj
Použití ve všech oblastech banky	Legislativně nedosažitelný uznávaný podpis
	Jednoúčelové řešení jen pro podepisování

26

Bio PKI – možnosti využití

27

Problémy autentizace

- Příliš mnoho hesel do různých systémů
- Nejednoznačnost identity (v jiném systému pod stejným uživatelským jménem vystupuje někdo jiný)

Bezpečnostní politika obsahuje:

- Popis informačního systému
- Cíle bezpečnostní politiky
- Definice citlivosti informací
- Definice možných hrozeb
- Zásady personální politiky
- Stanovení politiky zálohování
- Plán obnovy pro havárii
- Metodiku řešení krizových stavů

Nejsou věci „bezpečné“ a „nebezpečné“, jsou jen různé míry rizika.

Různí lidé akceptují v různých situacích různou míru rizika.

Standardní kroky řešení bezpečnosti

- studie informační bezpečnosti – aktuální stav,
- riziková analýza,
- tvorba bezpečnostní politiky - vytýčení cílů,
- bezpečnostní standardy – pro naplnění cílů bezpečnostní politiky,
- bezpečnostní projekt – technická opatření,
- implementace bezpečnosti – nasazení výše uvedeného,
- monitoring a audit – prověřování, zda vytvořené bezpečnostní mechanismy odpovídají dané situaci.

Analýza rizik

- Co se stane, když informace nebudou chráněny?
- Jak může být porušena bezpečnost informací?
- S jakou pravděpodobností se to stane?

Identifikace a kvantifikace hrozeb

- **Úmyslné škody**
- **Neúmyslné škody**
- **Technické selhání**
- **Přírodní hrozby**

Stupeň	Zkratka	Úroveň hrozby	Popis hrozby	Od	Do
1	N	nízká	nepravděpodobná	0%	25%
2	S	střední	pravděpodobná	25%	50%
3	V	vysoká	vysoce pravděpodobná	50%	75%
4	K	jistá	jistá	75%	100%

Identifikace a kvantifikace zranitelností

Stupeň	Zkratka	Zranitelnosti	Opatření	Od	Do
1	N	nízká	Opatření jsou zavedena, dokumentována, kontrolována a zlepšována.	0%	25%
2	S	střední	Opatření jsou zavedena, dokumentována a kontrolována.	25%	50%
3	V	vysoká	Opatření jsou zavedena a dokumentována.	50%	75%
4	K	kritická	Žádná opatření nejsou zavedena, dokumentována, kontrolována a zlepšována.	75%	100%

Stupeň	Zkratka	Zranitelnost	Bezpečnostní incidenty	Od	Do
1	N	nízká	Neexistují důkazy o žádných závadách či selhání bezpečnostních opatření.	0%	25%
2	S	střední	Existují důkazy o malém počtu závad či selhání bezpečnostních opatření.	25%	50%
3	V	vysoká	Existují důkazy o větším počtu závad či selhání bezpečnostních opatření.	50%	75%
4	K	kritická	Existují důkazy o rozsáhlých závadách či selhání bezpečnostních opatření.	75%	100%

Stupeň	Zkratka	Zranitelnost	Havarijní plány	Od	Do
1	N	nízká	Pro všechna potenciální narušení businessu jsou připraveny havarijní plány a jsou pravidelně testovány a optimalizovány.	0%	25%
2	S	střední	Havarijní plány spíše neselžou.	25%	50%
3	V	vysoká	Havarijní plány spíše selžou.	50%	75%
4	K	kritická	Pro žádná potenciální narušení businessu nejsou připraveny žádné havarijní plány.	75%	100%

Zákon o kybernetické bezpečnosti a jeho aktuální novelizace

- Právní úprava, která se týká kybernetické bezpečnosti v České republice, je převážně obsažena v zákoně č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).
- Novela č. 205/2017 Sb. je harmonizace s evropským právem, konkrétně transpozice směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (směrnice NIS).[4] Novela nabyla účinnosti ke dni 1. 8. 2017.

Zákon o kybernetické bezpečnosti a jeho aktuální novelizace

- Právní předpisy zavádějí povinnost k zajištění kybernetické bezpečnosti pouze u poměrně malé množiny subjektů, jejichž bezpečnost v této oblasti je považována za nejvýznamnější, neboť přímo souvisí se zajištěním bezpečnosti státu a jeho funkcí. Jedná se především o významné subjekty v odvětví energetiky, telekomunikací, bankovnictví atd.
- ALE - i pro subjekty, které nejsou povinnými osobami podle zákona o kybernetické bezpečnosti, platí povinnost zajištění určité míry kybernetické bezpečnosti.

Zákon o kybernetické bezpečnosti a jeho aktuální novelizace

- Povinnosti jsou stanoveny jak obecnými předpisy, tak i předpisy sektorovými, především nařízením GDPR.
- Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů („nařízení GDPR“) - k zabezpečení zpracování osobních údajů stanoví čl. 32 nařízení GDPR povinnost správce, ale i zpracovatele osobních údajů, přijmout vhodná technická a organizační opatření k zajištění úrovně zabezpečení odpovídající danému riziku.
- Výčet právních předpisů, které povinnosti v oblasti kybernetické bezpečnosti stanovují, je samozřejmě širší, nedopadají však již na tak velkou množinu subjektů.

Rozšíření osobní působnosti

- V návaznosti na uvedenou směrnici Evropského parlamentu a Rady novela zákona doplňuje seznam povinných osob, když v nově vymezeném ust. § 3 jsou pod následujícími písmeny doplněny tyto osoby:

  f) správce a provozovatel informačního systému základní služby, pokud nejsou správcem podle písmene c) nebo d),
  g) provozovatel základní služby, pokud není správcem nebo provozovatelem podle písmene f), a
  h) poskytovatel digitální služby.

Digitální služba

- Digitální službou se dle ust. § 2 písm. l) zákona o kybernetické společnosti rozumí služba informační společnosti podle zákona č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů, ve znění pozdějších předpisů, která spočívá v provozování:
- **on-line tržiště** (marketplace) - které spotřebiteli nebo prodávajícímu umožňuje on-line uzavírat s prodávajícím podnikatelem kupní smlouvu nebo smlouvu o poskytnutí služeb, a to prostřednictvím internetové stránky on-line tržiště nebo prostřednictvím internetové stránky prodávajícího, který využívá službu poskytovanou on-line tržištěm,

Digitální služba

- **Internetového vyhledávače -** který umožňuje provádět vyhledávání v zásadě na všech internetových stránkách, a to na základě dotazu uživatele na jakékoliv téma v podobě klíčového slova, sousloví nebo jiného zadání, přičemž služba poskytuje odkazy, na nichž lze nalézt informace související s požadovaným obsahem (nejedná se tedy o funkcionalitu vyhledávání v rámci jedné konkrétní internetové stránky),

Digitální služba

- **Cloud computing-** na základě žádosti bez zbytečného odkladu budou poskytnuty informace a data, která poskytovatel služeb cloud computingu uchovává, a bez zbytečného odkladu je umožněna jejich kontrola.
- Dle přechodných ustanovení platí obecná lhůta 1 roku ode dne nabytí účinnosti novely zákona k tomu, aby orgány a osoby uvedené v § 3 písm. c) až f) zákona uvedly smluvní vztah do souladu se všemi požadavky, pokud podmínky jejich smluvního vztahu uzavřeného s dodavatelem pro jejich informační nebo komunikační systém neodpovídají v plném rozsahu zákonným požadavkům.

Nový institucionální model -

Novela v podobě zákona č. 104/2017 Sb.

Novela zákona o kybernetické bezpečnosti provedla institucionální změny, konkrétně zřízení nového správního úřadu pro oblast kybernetické bezpečnosti, tj. Národního úřadu pro kybernetickou a informační bezpečnost, který převzal dosavadní kompetence od Národního bezpečnostního úřadu (blíže viz § 21a zákona o kybernetické bezpečnosti ve znění novely).

Dříve schválená novela zákona o kybernetické bezpečnosti, tj. zákon č. 104/2017 Sb., kterým se mění zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, zákon o kybernetické bezpečnosti a některé další zákony nabyla účinnosti dne 1. 7. 2017.