Aplikace bezpečnostních standardů v prostředí ochrany dat

Bc. Gabriel Bílý

Diplomová práce
2020

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav elektroniky a měření

Akademický rok: 2019/2020

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Gabriel Bílý**
Osobní číslo:	**A17673**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**Kombinovaná**
Téma práce:	**Aplikace bezpečnostních standardů v prostředí ochrany dat**
Téma práce anglicky:	**Application of Security Standards in a Data Protection Environment**

Zásady pro vypracování

1. Analyzujte literární zdroje tématu současných bezpečnostních standardů v oblasti ochrany dat v kyberprostoru
2. Popište současné prostředí bezpečnosti mobilních elektronických platebních nástrojů
3. Stanovte požadavky na bezpečnost digitálních dvojčat na platformách iOS a Android
4. Navrhněte bezpečnostní rámec pro návrh mobilních platebních nástrojů
5. Vyhodnoťte přínosy vašeho návrhu

Rozsah diplomové práce:
Rozsah příloh:
Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. *GDPR* [online]. Praha: nakl. Mgr. Eva Škvorničková, 2018 [cit. 2019-11-20]. Dostupné z: https://www.gdpr.cz/
2. JAŠEK, Roman a David MALANÍK. *Bezpečnost informačních systémů*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013, 1 online zdroj. ISBN 9788074543128. Dostupné také z: http://hdl.handle.net/10563/25821
3. KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. Edice CZ.NIC. ISBN 978-80-88168-18-8. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf
4. KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7.
5. STALLINGS, William, Lawrie BROWN, Michael D BAUER a Michael HOWARD. *Computer security: principles and practice*. 2nd ed. Boston: Pearson, c2012, xxii, 788 s. ISBN 9780132775069.

Vedoucí diplomové práce: **prof. Mgr. Roman Jašek, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **9. prosince 2019**
Termín odevzdání diplomové práce: **29. května 2020**

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Milan Navrátil, Ph.D.
ředitel ústavu

Ve Zlíně dne 9. prosince 2019

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 12.8.2020

GABRIEL BÍLÝ, v.r.

podpis diplomanta

ABSTRAKT

Tato diplomová práce se zabývá aplikací současných bezpečnostních standardů v oblasti ochrany dat a platebních nástrojů. V teoretické části jsou na základě zdrojů definovány a formulovány pojmy se samotným tématem kyberprostoru a kybernetické bezpečnosti. Dále jsou popsány legislativní nařízení a směrnice EU, které je nutné dodržovat, a bezpečnostních standardy, které musí být nedílnou součástí vývoje platebních nástrojů. Na závěr teoretické části je popsáno současné prostředí bezpečnosti mobilních elektronických platebních nástrojů. Jsou zde uvedeny typy mobilních plateb a následně jsou popsány technologie, které se při mobilních platbách využívají – NFC a tokenizace. V praktické části této práce je nejdříve analyzován platební proces a bezpečnostní prvky platebních nástrojů Apple Pay a Google Pay. V druhé části je zpracován bezpečnostní rámec pro firmu vyvíjející platební nástroje. Do tohoto rámce patří vývojová metodika OWASP, používání dvoufaktorové autentizace a využití RASP softwaru Talnec. Poslední kapitolou je vyhodnocení přínosu tohoto návrhu.

Klíčová slova: Kyberbezpečnost, legislativa EU, bezpečnostní standardy, mobilní platby, rámec, Android, iOS, Google Pay, Apple Pay, NFC, OWASP, 2FA, RASP.

ABSTRACT

This master thesis deals with the application of current security standards in the field of data protection and payment instruments. In the theoretical part, concepts with the very topic of cyberspace and cyber security are defined and formulated on the basis of sources. The work also describes the legislative regulations and EU directives that must be observed as well as security standards, which must be an integral part of the development of payment instruments. The current security environment for mobile electronic payment instruments is described at the end of the theoretical part. The types of mobile payments are listed here, followed by a description of the technologies used in mobile payments - NFC and tokenization. The payment process and security elements of payment instruments Apple Pay and Google Pay are analyzed in the introduction of the practical part of the thesis. The second part elaborates a security framework for a company developing payment instruments. This framework includes the OWASP development methodology, the use of two-factor authentication and the use of RASP Talnec software. The evaluation of the benefits of concrete proposal is included in the last chapter of the thesis.

Keywords: Cybersecurity, security standards, EU legislation, mobile payments, framework, Android, iOS, Google Pay, Apple Pay, NFC, OWASP, 2FA, RASP.

Rád bych poděkoval vedoucímu mé diplomové práce prof. Mgr. Romanu Jaškovi, Ph.D. za cenné rady, odborné vedení a připomínky při zpracování práce.

Dále bych chtěl poděkovat svým přátelům a celé rodině za podporu a trpělivost.

V neposlední řadě mé velké poděkování patří mým kolegům v práci za vstřícnost a obohacující rady při zpracování této diplomové práce. Děkuji.

OBSAH

ÚVOD

Diplomová práce je zaměřena na aplikaci bezpečnostních standardů v prostředí ochrany dat.

V úvodu práce budou rozebrány pojmy kyberprostoru a kybernetické bezpečnosti. Kybernetická bezpečnost je praxe ochrany systémů, sítí a programů před digitálními útoky. Tyto počítačové útoky jsou obvykle zaměřeny na přístup, změnu nebo zničení citlivých informací; vydírání peněz od uživatelů; nebo přerušení běžných obchodních procesů.

Provádění účinných opatření v oblasti kybernetické bezpečnosti je dnes zvláště náročné, protože existuje více zařízení než lidí a útočníci jsou stále více inovativní. Z toho důvodu vznikají stále nové legislativní nařízení a bezpečnostní standardy pro zamezení těchto útoků, úniku dat a ochrany uživatelů.

V posledních letech EU zavedla řadu nařízení a směrnic pro stanovení digitálního evropského hospodářského prostoru se zaměřením na identitu a osobní údaje. Nakládání s identifikačními údaji a osobními údaji podléhá státní regulaci. V posledních letech bylo v Evropě zahájeno několik legislativních iniciativ, každá s jiným zaměřením, které mají za úkol stanovit rámec pro služby digitální identity. V teoretické části této práce budou nejdříve zmíněny regulace a směrnice GDPR, eIDAS a PSD2. Dále budou popsány standardy, které musejí dodržovat instituce účastnící se platebních systémů. Tyto instituce by měly vyvinout procesy, které zajistí soulad s PCI DSS, PA-DSS a Dodatkem E: MFS od FFIEC.

Spolu s daleko častějším využitím mobilních zařízení pro kritické účely, jako jsou platební operace a elektronické mobilní bankovnictví, které mobilní telefony poskytují, vedlo k nárůstu malwaru a kyber-útočníků.

Bezpečnost je prioritou jak pro tvůrce platforem, tak i pro společnosti vyvíjející mobilní aplikace. Tyto subjekty se snaží chránit své klienty i své duševní vlastnictví. Vývojáři jsou často nuceni integrovat do aplikací dodatečné bezpečnostní mechanismy posunující ochranu aplikace na další úroveň.

Tyto získané znalosti budou použity pro vytvoření vlastního bezpečnostního rámce pro společnost vyvíjející platební nástroje. Popsána zde bude vývojová metodika dle OWASP a největší rizika dle OWASP Mobile 10. Důležitým sekundárním krokem k ochraně dat a uživatele je používání dvou či vícefaktorové autentizace. Vypsány budou možné metody této autentizace. Jako poslední krok bezpečnostního rámce bude implementace vhodného RASP.

I. TEORETICKÁ ČÁST

1 BEZPEČNOSTNÍ STANDARDY V OBLASTI OCHRANY DAT

Tato část má za úkol popsat současné bezpečnostní standardy v oblasti ochrany dat v kyberprostoru. Nejdříve je však nutné vysvětlit podstatu problematiky v oblasti bezpečnosti v kyberprostoru a potřebu ochranu dat.

Zabezpečení informací znamená chránit důvěrnost, integritu a dostupnost jakýchkoli dat, která mají obchodní hodnotu. Požadavky na bezpečnost informací mohou být právní a regulační povahy, smluvní, etické nebo související s jinými obchodními riziky.

Jak se všechny informace postupně mění v digitální data, tradiční zabezpečení informací se mění v kybernetickou bezpečnost. Moderní vedení by mělo vnímat kybernetickou bezpečnost zakořeněnou v organizační kultuře, nejen jako technické pojištění poskytované specializovaným bezpečnostním týmem. [1]

1.1 Kyberprostor a kybernetická bezpečnost

Tato kapitola vysvětluje, co je kyberprostor a co je myšleno kybernetickou bezpečností. Kybernetická bezpečnost se v podstatě zabývá počítačovými aktivy, která jsou vystavena různým hrozbám a pro která jsou přijímána různá opatření k ochraně těchto aktiv. V další části této kapitoly je proto uveden stručný přehled kategorií aktiv souvisejících s počítačem, které si uživatelé či firmy chtějí zachovat a chránit, a přehled různých hrozeb a útoků, které lze na tato aktiva provést. Poté zkoumáme opatření, která mohou být přijata k řešení těchto hrozeb a útoků. [50] Tato kapitola, se zaměřuje na tři základní otázky:

1. Jaká aktiva musíme chránit?
2. Jak jsou tato aktiva ohrožena?
3. Co můžeme udělat, abychom těmto hrozbám čelili?

Pro pochopení problematiky kybernetické bezpečnosti je důležité objasnění některých základních pojmů uvedených dále v diplomové práci.

1.1.1 Kyberprostor

Pojem kyberprostor se dostává do obecného povědomí až po vydání deklarace Johna Barlowa: „A Declaration of the Independence of Cyberspace.“ [2]

Oxford Dictionary k definici termínu cyberspace uvádí, že jde o fiktivní prostředí, ve kterém dochází ke komunikaci skrze počítačové sítě. [3]

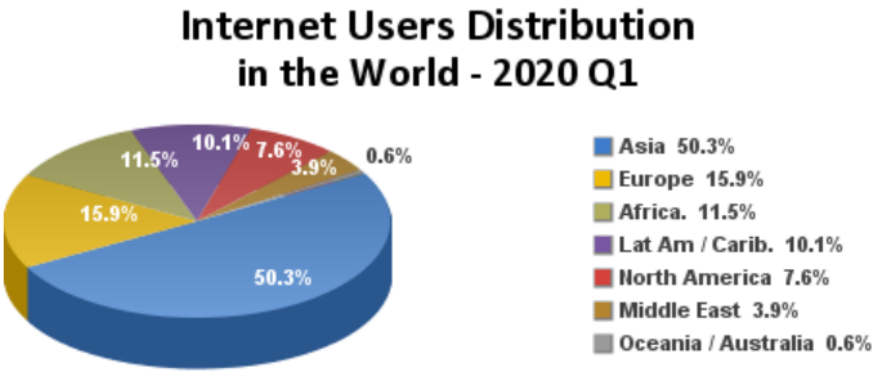
Lze vyjádřit, že kyberprostor je virtuální realitou nemající konec ani začátek a je prakticky neomezený. Avšak je zcela závislá na materiální podstatě, a to jsou technologie nacházející se v reálném světě.

Z těchto faktů je možné kyberprostor definovat jako prostor kybernetických aktivit či prostor vytvořený informačními a komunikačními technologiemi, který vytváří svět (či prostor) virtuální jako paralelu k reálnému prostoru. [4]

V legislativě najdeme definici kyberprostoru v zákoně č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) v § 2 písm. a),

kde je uvedeno, že *„kybernetickým prostorem je digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.“* [5]

Ze statistik Internet World Stats vyplývá, že do kyberprostoru se propojila značná část společnosti. Z celkové populace 7,7 miliard obyvatel je celkem 4,5 miliard uživatelů internetu (což je 58,7%, viz tab. 1). Na výsečovém grafu níže (obr. 1) lze vidět rozdělení uživatelů internetu na světě. [6]



Obr. 1: Rozdělení uživatelů internetu na světě [6]

Tab. 1: Poměr uživatelů internetu k celkové populaci k 31.12.2019 [6]

Světový region	Populace (odhadovaná 2020)	Poměr populace k celosvětové (%)	Uživatelé internetu (k 31.12.2019)	Poměr uživatelů internetu k populaci (%)
Afrika	1,340,598,447	17,2	526,374,930	39,3
Asie	4,294,516,659	55,1	2,300,469,859	53,6
Evropa	834,995,197	10,7	727,814,272	87,2

Latinská Amerika / Karibik	658,345,826	8,5	453,702,292	68,9
Střední východ	260,991,690	3,9	180,498,292	69,2
Severní Amerika	368,869,647	4,7	348,908,868	94,6
Oceánie / Austrálie	42,690,838	0,5	28,775,373	67,4
Svět celkem	7,796,615,710	100,0	4,574,150,134	58,7

Mezi symboly kyberprostoru lze jmenovat jeho globálnost, decentralizaci, otevřenost, bohatost na informace, interaktivnost a schopnost ovlivňování dopadů ve světě reálném. Primární roli v něm zaujímají technologie a na ně navázané služby.

Dostupnost a rychlost přenášených informací se stává klíčovým prvkem naší doby. Uživatelé nemají potřebu a většinou ani nechtějí vědět, jakým způsobem dochází k přenosu dat, které do informační sítí vložili. Mnohdy odesílatele nezajímá, kde se adresát přenášených informací nachází, či kde se data uchovávají, a tím dochází k odhmotnění obsahu od fyzické podstaty infomačních sítí. [4]

Z jedné strany lze sledovat situaci, kdy jsou společenské vztahy v kyberprostoru delokalizovány, což vede k problémům z hlediska aplikace práva, avšak na druhou stranu delokalizace umožňuje volně a svobodně komunikovat, zasílat, měnit a uchovávat data. [7]

1.1.2 Kybernetická bezpečnost

Pojem kybernetická bezpečnost (dále jen KB) nemá pouze jednu ustálenou definici, takže budou uvedeny takové, jenž jsou tématu této práce nejbližší.

1) Dle Oxford Dictionary představuje KB jako stav, kdy dochází k ochraně před kriminálním či neautorizovaným užitím elektronických dat. Je zde také potřeba zahrnout opatření, která je nutno přijmout k dosažení tohoto stavu. [8]
2) V Národní strategii kybernetické bezpečnosti České republiky za období let 2015 až 2020 je pak KB definována takto: *„KB představuje souhrn organizačních, politických, právních, technických a vzdělávacích opatření a nástrojů směřujících k zajištění zabezpečeného, chráněného a odolného kyberprostoru v České republice, a to jak pro subjekty veřejného a soukromého sektoru, tak pro širokou českou veřejnost.“* [9]

3) Jan Kolouch a Pavel Bašta v knize Cyber Security přicházejí s definicí založenou na základě jejich analýzy a vlastních zkušeností a vymezují KB následovně:
    - *„souhrn právních, organizačních, technických a vzdělávacích prostředků, které směřují k zajištění ochrany počítačových systémů a dalších prvků ICT, aplikací, dat a uživatelů,*
    - *schopnost počítačových systémů a využívaných služeb reagovat na kybernetické hrozby či útoky a jejich následky, jakož i plánování obnovy funkčnosti počítačových systémů a služeb s nimi spojených.“* [10]

KB pro mnoho lidí představuje pouze oblast, kterou se zabývají ve skutečnosti jen oddělení informačních a komunikačních technologií (dále ICT).

Avšak tento předpoklad je mylný, neboť problematika KB ovlivňuje každého člověka, který využívá jakékoliv prvky ICT ve svém běžném životě. To znamená, že by si každý jedinec měl uvědomovat, že je součástí kyberprostoru a v mnoha případech stěžejním prvkem KB. Právě člověk tak svou nevědomostí často zvyšuje pravděpodobnost úspěchu kybernetických útoků.

KB je oblast, která by měla být pro řadu organizací i jedinců samotných klíčová a v současné době ji nelze podceňovat. Měla by tedy být řešená systematicky a dlouhodobě. [10]

1.1.3 Principy KB

Při užití KB dochází k využití několika principů, které jsou nazývány triády kybernetické bezpečnosti. [11]

Jedná se o následující tři triády:

1) **CIA** [C-Confidentiality (důvěrnost); I-Integrity (celistvost); A-Availability (dostupnost)].
2) **Prvky kybernetické bezpečnosti** (Lidé, Technologie, Procesy).
3) **Životní cyklus kybernetické bezpečnosti** (Prevence, Detekce, Reakce).

Triáda CIA je nejpoužívanější a nejznámější triádou KB, avšak k udržení adekvátní úrovně KB je zapotřebí také implementace dalších principů.

KB má za úkol zajistit jak bezpečnost ICT, tak především bezpečnost dat a informací, které jsou pomocí těchto prvků zpracovány, přenášeny a uchovávány. K informační bezpečnosti

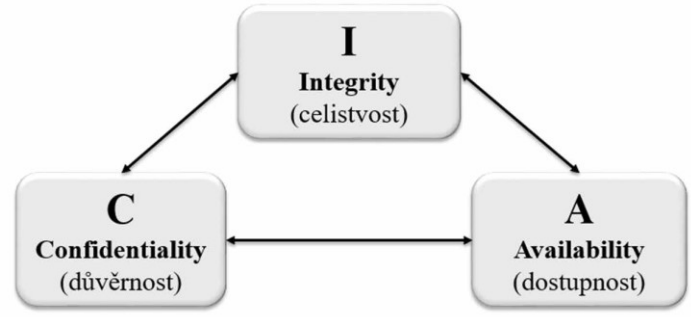
je právě vztahována triáda CIA. Informační bezpečnost je definována také řadou norem ISO 27000. [10]

Je třeba vždy zvážit, jak vysoký stupeň ochrany si daná informace zaslouží a která opatření je potřeba přijmout. Každé opatření totiž stojí jak vynaložené finanční prostředky, tak i určitá omezení při práci s informacemi. Odpovídající úroveň ochrany je možné stanovit pouze na základě detailní analýzy rizik. Cílem takové analýzy je identifikace informací, které se zpracovávají a určení hrozeb, které by mohly ohrozit důvěrnost, integritu a dostupnost těchto informací. [12]

Jak již bylo zmíněno výše, tato triáda je postavena na třech základních atributech, kterými jsou:

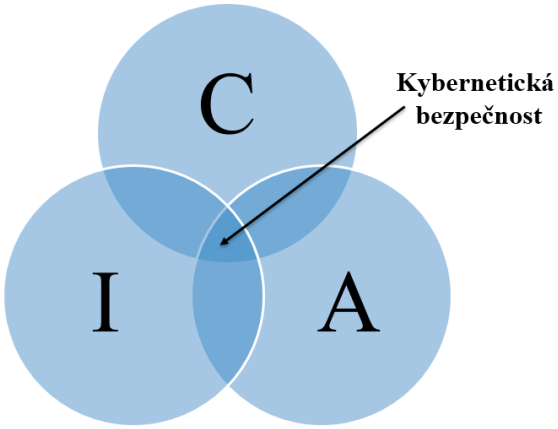
- **Důvěrnost** (confidentiality), která spočívá v zachování skutečnosti, že k datům, informacím, či ICT mají přístup subjekty, které jsou k této činnosti oprávněné a má zabránit přístupu neautorizovaným osobám.
- **Integrita** (integrity), jenž představuje zabránění zásahu do dat, informací, IT systémů a jejich nastavení (či modifikaci) jinou osobou, než tou, která je k tomuto úkonu oprávněna.
- **Dostupnost** (availability) je vlastnost přístupnosti a použitelnosti služeb či systému na žádost oprávněné entity. Sebedokonalejší systém zajišťující pouze integritu a přístup k samotnému systému či datům je bez zajišťování spolehlivého přístupu dle potřeby nevyužitelný.

Tato triáda bývá znázorňována graficky (obr. 2 níže) pro pochopení jejich vztahů a jednotlivých atributů. [10]



Obr. 2: Triáda CIA [10]

V rámci implementace triády CIA bývá vymezen prostor kybernetické bezpečnosti jako průnik jednotlivých principů této triády (viz obr. 3).



Obr. 3: Triáda CIA a kybernetická bezpečnost [10]

V některých zdrojích bývá uvedeno, že CIA triáda je nedostačující a měla by být kromě výše zmíněných atribut doplněna ještě o další tři, a to konkrétně:

- **Držení či kontrola** (possession/control) by měla zabránit neoprávněné osobě získat kontrolu nad systémy či informacemi, ke kterým by přístup mít neměla. Pokud by k takové situaci došlo, pak se jedná o ztrátu kontroly nebo vlastnictví a jde o krádež citlivé informace.
- **Užitečnost** (utility) nastává v situaci, kdyby např. došlo ke ztrátě klíče k zašifrovaným datům, která sice dostupná jsou, ale nejdou použít. Pak se jedná o ztrátu užitečnosti.
- **Autentičnost** (authenticity) může být narušena v okamžiku, kdy dojde k padělání elektronického podpisu útočníkem, ale zároveň nebyla narušena ani důvěrnost, integrita a dostupnost.

Kdyby se rozšířily základní atributy CIA o tyto další tři, pak nám vznikne situace znázorněná prostřednictvím následujícího obr. 4, kterému se také říká „Parkenian hexad“. [13]

Obr. 4: Zobrazení Parkenian hexad [10]

1.1.4 Prvky kybernetické bezpečnosti

Prvky kybernetické bezpečnosti jsou prvky, jejichž vzájemná interakce umožňuje do jisté míry vytvořit nebo zavést kybernetickou bezpečnost. Prvky kybernetické bezpečnosti jsou tedy tyto tři následující:

- lidé,
- technologie,
- procesy.

V tomto případě platí věta, že jakýkoliv systém je bezpečný tak, jak je bezpečný jeho nejslabší článek (čili prvek). [10]

U prvního prvku, tedy lidí, je vhodné použít citát Bruce Schneiera: *„Lidé často představují nejslabší článek v bezpečnostním řetězci a jsou chronicky zodpovědní za selhání bezpečnostních systémů.“* [14] Typicky právě lidé jsou oním nejslabším článkem, a tím také nejčastějším cílem útočníků.

To je zapříčiněno tím, že doba, po kterou jsou využívány počítačové systémy, je relativně krátká. Lidé začali využívat některý z počítačových systémů až po roce 1990, k Internetu se masově začali připojovat kolem roku 1995 a chytré mobilní telefony jsou používány zhruba od roku 2007. Sociální sítě, které momentálně považuje většina lidí za nezbytnou součást svých životů, se využívají ne více než 10 let.

Dalším důvodem je obrovská dynamika vývoje hardwaru i softwaru, který se neodmyslitelně pojí s naší interakcí v digitální světě. Tato dynamika vývoje softwaru neumožňuje spoustě uživatelů, aby se při jeho využívání podrobněji zabývali otázkami bezpečnosti a na tyto systémy se dostatečně adaptovali.

V neposlední řadě zůstává důvod, kdy si mnozí lidé současné společnosti život bez ICT jednoduše nedokáží představit. Digitální svět vytváří avatary nás samotných, ale s mnohem větším množstvím informací a dat, než jsme si jako fyzické osoby schopné uchovat a zapamatovat. Toho jsou si velmi dobře vědomi i útočníci, a právě proto cíleně útočí na lidi v kyberprostoru. [10] Tento fakt podporuje rovněž citát Bruce Schneiera: *„Amatéři hackují systémy, profesionálové hackují lidi.“* [15]

Lidé, kteří využívají ICT a nějakým způsobem interagují v kyberprostoru, by měli nezbytně dodržovat tyto základní zásady:

- pochopit minimálně základní principy a pravidla vztahující se ke kybernetické bezpečnosti,
- porozumět alespoň základním funkcím moderních technologií (jako PC, notebook, smart TV, mobil, atd.), které k interakci používají,
- být schopni porozumět aplikacím, které k interakcí používají, a pokud jim činnost či smluvní podmínky těchto aplikací nevyhovují, je nevyužívat,
- vzdělávat se v oblasti kybernetické bezpečnosti.

Na osoby v interakci s kybernetickou bezpečností lze nahlížet jako na:

- tvůrce této bezpečnosti – typicky osoby snažící se implementovat a prosadit jednotlivé prvky kybernetické bezpečnosti,
- příjemce pravidel kybernetické bezpečnosti – osoby, jenž se rozhodly (či jsou nuceni) implementovat již existující pravidla kybernetické bezpečnosti,
- subjekty, které je třeba před kybernetickými útoky chránit,
- subjekty, které je třeba proškolit a informovat o pravidlech a principech kybernetické bezpečnosti,
- hrozbu či riziko v rámci vytváření a udržování kybernetické bezpečnosti. [10]

Dalším prvkem kybernetické bezpečnosti jsou technologie. Pro uvedení do problematiky je vhodný citát Bruce Schneiera: *„Pokud se domníváte, že technologie dokáže vyřešit vaše bezpečnostní problémy, nerozumíte problémům a nerozumíte technologii.“* [16]

Technologie většinou představují prostředek umožňující připojit se k Internetu, sociálním sítím či dalším aplikacím. Standardní uživatel běžně vnímá a interaguje pouze s koncovými technologiemi, které sám používá, jako je PC, tablet, mobilní telefon, které sám používá, ale o další technologické vrstvy, které jsou pro jeho činnost v kyberprostoru nezbytné, se již povětšinou nezajímá.

V organizacích technologie představují širokou škálu zařízení a technologií, jako např.:

- zařízení pro uživatele (desktop, notebook, mobilní zařízení, atd.),
- kompletní infrastrukturu sítě (LAN, aktivní prvky, Wi-Fi prvky, aj.) a služeb (aplikace, servery)
- prvky sloužící k zajištění zabezpečení perimetru (firewall, IDS/IPS, honeypot) a infrastruktury (prvky k autentizaci a autorizaci, analýze, monitoringu). [10]

Pro udržování a budování kybernetické bezpečnosti se provádí analýza stávajících aktiv a na jejím základě se poté doplňují či modifikují existující systémy. S ohledem na specifika organizace by měly být nedílnou součástí ICT organizace tyto prvky:

- detekční systémy – IDS (Intrusion Detection System), IPS (Intrusion Prevention System),
- centralizovaná správa klasifikace informací,
- centrální správa uživatelů a rolí,
- ochrana před škodlivým kódem (antivirové, antispamové nebo jiné řešení, aplikační firewall),
- správa síťové bezpečnosti (DMZ, VLAN, firewall),
- technologie pro zaznamenávání činností jednotlivých prvků ICT, uživatelů a administrátorů (log system),
- zálohy virtuálních serverů, aplikací a databází (recovery system), aktivní a offline zálohovací systémy. [10]

Technologie jsou součást kybernetické bezpečnosti, na které organizace ani jedinci zpravidla nešetří. Aby tato bezpečnost byla zajištěna, je potřeba udržovat technologie ve stavu, aby byly schopny reagovat na vývoj ICT. Hardware i software by měl být neustále udržován aktualizovaný a zabezpečený. Mnohé zdroje tvrdí, že byť jsou technologie významnou součástí procesu tvorby a udržování kybernetické bezpečnosti, daleko důležitější jsou správně nastavené procesy a lidé, kteří umějí tyto procesy aplikovat a dodržovat stanovená pravidla. [10]

Tím se dostáváme k poslednímu prvku kybernetické bezpečnosti, kterým jsou procesy. Bruce Schneiera k procesům uvádí: *„Mantrou dobrého bezpečnostního inženýra je: ‚Bezpečnost není produkt, ale proces.' Je to víc než navrhnout silnou kryptografii do systému; je to o tom navrhnout celý systém tak, aby všechna bezpečnostní opatření, včetně kryptografie, spolupracovala.“* [17]

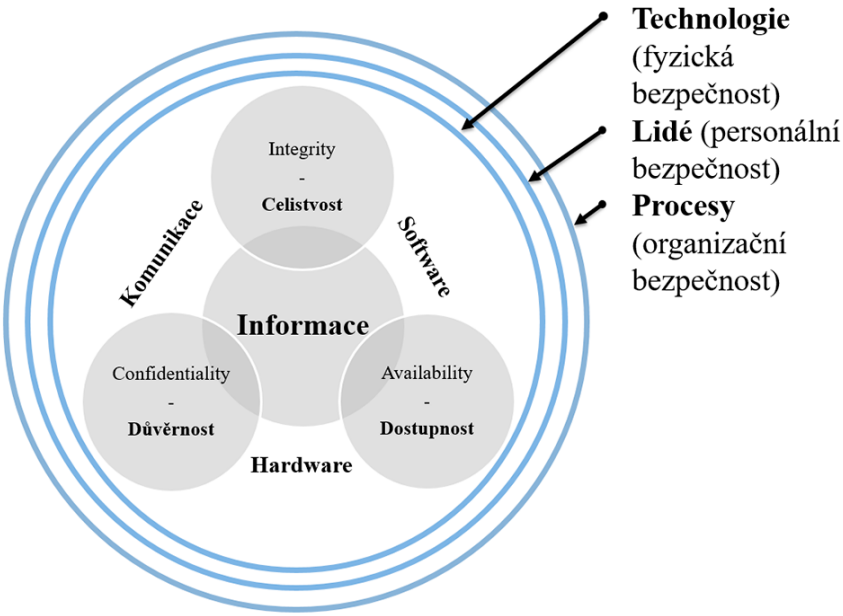
Je to činnost, kterou je nutno vynaložit, aby byli lidé schopni používat technologie a služby s nimi spojené. Procesy z hlediska plynutí času jsou:

- řízení aktiv a rizik,
    - definování a kategorizace aktiv,
    - analýza a kategorizace rizik,
- implementace ICT a aplikací,
- správa uživatelů a rolí,
- autentizace a autorizace,
- testování zabezpečení jednotlivých systémů a služeb,
- aktualizace a údržba systémů a služeb,
- analýza nápravných opatření,
- realizace nápravných opatření,
- audit kybernetické bezpečnosti,
- detekce kybernetických útoků nebo anomálií,
- reakce na kybernetické útoky nebo jiné incidenty,
- proces k zajištění kontinuity,
- cvičení a školení.

Tento výčet procesů není rozhodně zcela kompletní, ale platí pravidlo, že jednotlivé procesy jsou realizovány v rámci celého životního cyklu ICT, dat, informací a ve vztahu k uživatelům.

Správné nastavení procesů a jejich neustálá údržba často představuje nejnáročnější část budování kybernetické bezpečnosti. Mnohdy je vhodné v organizaci simulovat typické kybernetické útoky (phishing, kompromitovat e-mail, apod.) z důvodu reálné demonstrace těchto útoků a případných dopadů. Penetrační testování také dovoluje nalézt chyby v již stanovených procesech. [10]

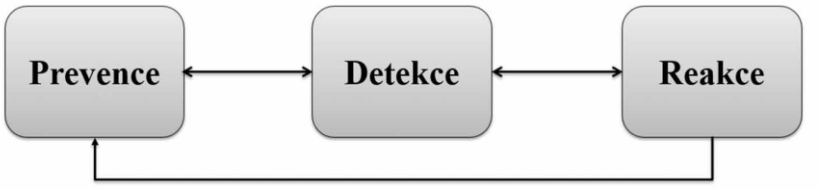
Ke shrnutí těchto třech prvků zmíněných výše slouží následující schéma (obr. 5), na kterém je triáda CIA doplněna o technologie, lidi a procesy.



Obr. 5: Triáda CIA doplněná o prvky kybernetické bezpečnosti [10]

1.1.5 Životní cyklus kybernetické bezpečnosti

Jak již bylo zmíněno, při realizaci kybernetické bezpečnost je nutné uplatňovat triádu CIA i dílčí prvky kybernetické bezpečnosti v průběhu jejich celého životního cyklu. Jedná se o prevenci, detekci a reakci na útok. Tento životní cyklus je zjednodušeně znázorněn níže na obr. 6. [10]

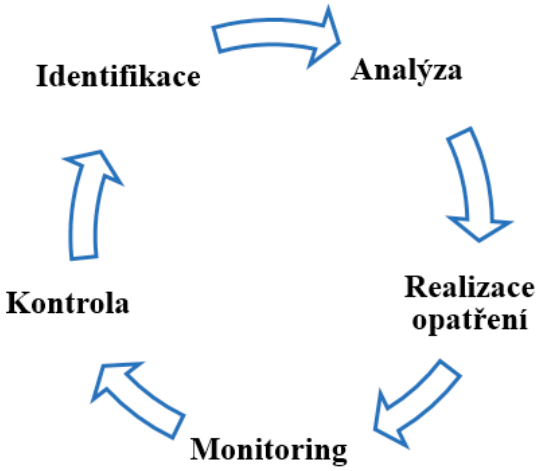


Obr. 6: Zobrazení životního cyklu kybernetické bezpečnosti [10]

Dle kybez.cz je pak životní cyklus kybernetické bezpečnosti znázorněn na obr. 7 níže.

Obr. 7: Životní cyklus kybernetické bezpečnosti dle kybez.cz [18]

U řešení kybernetické bezpečnosti nelze říci s úplným přesvědčením, že je společnost „kyberneticky bezpečná“ a nemá žádný záchytný bod. Budování a udržování kybernetické bezpečnosti je jakási nekončící analýza rizik, kterou je potřeba doplnit o další podpůrné procesy, které pomáhají ke zvýšení kybernetické bezpečnosti v organizaci. Tato analýza rizik je zobrazena na obr. 8. [10]



Obr. 8: Analýza rizik [10]

Každý proces životního cyklu kybernetické bezpečnosti je dále stručně rozšířen.

1) Analýza
   - standardní analýza činnosti systémů a služeb
   - forenzní analýza, aj.
2) Realizace a opatření

   - pro obnovení systémů a služeb
   - doporučení na základě analýzy incidentu
   - best practices
   - školení a další vzdělaní, aj.
3) Monitoring a podpora
   - činnosti systémů a služeb
   - poskytování podpory koncovým uživatelům
   - CSIRT/CERT, aj.
4) Kontrola
   - audit
   - realizace opatření, aj.
5) Identifikace a detekce
   - hrozeb
   - incidentů a útoků
   - systémových událostí, aj. [10]

Pro shrnutí této subkapitoly slouží statistika z Verizon Data Breach Investigations Report (DBIR), která se zabývá narušením bezpečnosti vedoucím ke kompromitaci dat. DBIR 2019 je postaven na reálných datech ze 41686 bezpečnostních incidentů a 2013 případů narušení dat poskytovaných 73 zdroji dat, veřejnými i soukromými subjekty, které pokrývají 86 zemí po celém světě. Za rok 2018 tedy vyplynula následující fakta:

- za útokem stála:
  - **osoba mimo organizaci – 69 %**
  - osoba v rámci organizace – 34 %
  - organizovaná zločinecká skupina – 39 %
- k útoku bylo využito taktiky:
  - **hacking – 52 %**
  - sociální útoky – 33 %
  - malware 28 %
- oběťmi útoků jsou:
  - **malé podniky – 43 %**
  - subjekty veřejného sektoru – 16 %
  - zdravotnické organizace – 15 %
  - finanční odvětví – 10 %

- motiv útoku je:
    - **obohacení se - 71 %**
    - zisk strategické výhody (špionáž) – 25 %

Až 56 % útoků bylo odhaleno po několika měsících nebo po delší době. [19]

1.2 Legislativa a bezpečnostní standardy

Je několik zákonů a vyhlášek, které se nějakým způsobem dotýkají problematiky ochrany informací v Evropské unii. Mohou se lišit oblastí své působnosti, svými cíli, aspekty bezpečnosti beroucí do úvahy a také se odlišují v tom, jak podrobně a zda vůbec se zabývají otázkami řešení. S těmito zákony, vyhláškami, standardy včetně jejich komentářů je možné se seznámit například na odpovídajících internetových stránkách. [49] Tato kapitola bezpečnostních standardů je rozdělena do dvou částí, a sice:

- Legislativa EU a
- Bezpečnostní standardy.

1.2.1 Legislativa EU

V posledních letech EU zavedla řadu nařízení a směrnic, které mají spolupracovat a vzájemně interagovat, aby stanovily rámec pro Digitální evropský hospodářský prostor se zaměřením na identitu a osobní údaje. V podčásti věnující se legislativě EU budou vysvětlena především nařízení GDPR, eIDAS a PSD2.

1.2.1.1 GDPR

GDPR (z angličtiny General Data Protection Regulation) je obecné nařízení o ochraně osobních údajů (známé také jako informační soukromí a ochrana osobních údajů), které je jednotně účinné v celé EU od 25. května 2018. Tvoří legislativu EU a nový právní rámec ochrany osobních údajů v evropském prostoru s cílem chránit práva občanů EU proti neoprávněnému jednání s jejich daty včetně osobních údajů. Účelem je definovat, kdy a za jakých podmínek mohou být osobní údaje zpracovávány. Všechny údaje vztahující se k identifikované nebo identifikovatelné fyzické osobě (subjektu údajů) jsou osobní údaje. [1] [20]

GDPR se dotýká všech, kdo shromažďují nebo zpracovávají osobní údaje evropských občanů, a to také včetně společností a institucí mimo území EU, které na evropském trhu působí. GDPR je nařízení zaměřující se na firmy, instituce a jednotlivce zacházející s osobními

údaji, např. o zaměstnancích, zákaznících, klientech či dodavatelích napříč segmenty a odvětvími. Zasahuje také do analyzování chování uživatelů na webu, při používání aplikací nebo moderních technologií. S GDPR dochází k rozšíření definice osobních údajů, kdy sem spadají nově také data jako e-mail, IP adresa či cookie v zařízení uživatele. Odvětví jako bankovní instituce, veřejná správa, zdravotnictví, či e-shopy se musejí potýkat s nutností změnit způsob zpracování osobních údajů. GDPR také nařizuje některým zpracovatelům osobních údajů či správcům zřídit nezávislou kontrolní funkci DPO (Pověřenec pro ochranu osobních údajů, z anglického Data Protection Officer). Správce je osoba, společnost, úřad nebo komunita, která definuje účely a metody zpracování osobních údajů, zatímco zpracovatel je třetí strana zpracovávající osobní údaje jménem správce. [1] [20]

Nařízení o ochraně údajů existují poměrně dlouhou dobu (např. Směrnice EU 95/46 / ES z října 1995) a větší pozornost byla věnována novému nařízení EU (2016/679, známému také jako EU GDPR nebo obecné nařízení EU o ochraně údajů), která se stala závaznou ve všech členských státech EU dne 25. května 2018. Hlavní dokument GDPR EU nařízení je dlouhý (99 článků) a v závislosti na povaze podniku a míře, v jaké souvisí se zpracováním osobních údajů, existuje potenciální potřeba vedení a interpretace, aby bylo plně v souladu s ním. [1]

Hlavním důvodem, proč nařízení EU získalo tolik pozornosti, je prosazování, které umožňuje orgánům na ochranu údajů ukládat pokuty podnikům až do výše 20 milionů EUR nebo 4% celosvětového obratu společnosti. V praxi je maximální pokuta na úrovni, která jednak představuje obrovské riziko pro celé podnikání, a jednak odůvodňuje jakoukoli investici potřebnou k dosažení souladu s nařízením. [1]

V rámci povinností zpracování GDPR je sestaveno desatero pro správce jako základní jednoduchý návod, jak nakládat s osobními údaji. Do tohoto desatera patří:

1. Zpracování údajů musí být legitimní a nesmí být v rozporu s právními předpisy či morálkou.
2. Každé zpracování osobních údajů musí být založeno na nějakém základním důvodu (právním titulu pro zpracování).
3. Musí být jasně vymezen účel zpracování údajů.
4. Forma, způsob, rozsah zpracování a doba uchování těchto údajů musí být přiměřené účelu zpracování.
5. Zpracování ve veřejném sektoru musí mít jasný zákonný podklad.

6. Osobní údaje musí být patřičně zabezpečeny, chráněny technickými a organizačními opatřeními.
7. Zpracování by mělo být prováděno férově, transparentně a korektně. Informace o zpracování musí být zřetelné, srozumitelné a jednoznačné, v rozsahu odpovídající dané situaci.
8. Zpracování osobních údajů nesmí nadměrně zasahovat do soukromí.
9. Po naplnění účelu zpracování je povinnost tyto osobní údaje zlikvidovat.
10. V každé členské zemi EU je zaručena shodná ochrana osobních údajů, která je stanovena nařízení GDPR. Předávat osobní údaje mimo EU lze jen za určitých okolnosti (např. plnění smlouvy se subjektem údajů), nebo za splnění dodatečných pravidel. [21]

V případech, kdy zpracování osobních údajů má za následek vznik vysokého rizika pro práva a svobody fyzických osob s přihlédnutím k povaze, rozsahu, kontextu, účelům zpracování a využitím nových technologií, se předpokládá vypracování posouzení vlivu na ochranu osobních údajů. Doporučený postup správce pro zpracování posouzení vlivu na ochranu osobních údajů lze rozdělit do čtyř kroků:

- shromáždění informací o zpracování osobních údajů,
- analýza, zda je povinné zpracovávat posouzení vlivu,
- zpracování posouzení vlivu,
- monitorování dodržování opatření a pravidelné revize posouzení vlivu. [22]

Následně je vypsán seznam druhů operací zpracování osobních údajů, která podléhají posouzení vlivu na ochranu osobních údajů, a to je:

1. Zpracování zahrnující monitorování subjektů údajů
2. Zpracování kritických údajů, údajů umožňujících přímou identifikaci a/nebo údajů vysoce osobní povahy subjektů údajů
3. Zpracování osobních údajů, které mohou vystavit subjekty údajů ohrožení z okolního prostředí
4. Zpracování osobních údajů velkého rozsahu
5. Zpracování zahrnující snímání veřejně přístupných prostor
6. Zpracování osobních údajů so mezeným ovlivněním subjekty údajů
7. Zpracování osobních údajů veřejně přístupných

8. Zpracování osobních údajů v technologicky složitých nebo pokročilých infrastrukturách nebo platformách
9. Zpracování osobních údajů s vazbou na jiné správce nebo zpracovatele
10. Zpracování osobních údajů s využitím nových technologických nebo organizačních řešení.

U každého kritéria se hodnotí úroveň rizikovosti a na základě ní pak následně vzniká povinnost k vypracování Posouzení vlivu na ochranu osobních údajů. [22]

1.2.1.2 eIDAS

eIDAS je nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním evropském trhu. Toto nařízení ruší předchozí směrnici EU 1999/93/EC. eIDAS je základem legálních elektronických podpisů v Evropě. Toto nařízení zjednodušuje a standardizuje digitální ID a podpisy v celé Evropě s cílem dosáhnout „jednotný digitální trh“. Provádět zabezpečené digitální transakce v tuzemské zemi a ve všech členských státech Evropské unie by mělo být jednodušší jak pro zákazníky, tak i firmy. [23]

Cílem je poskytnout společnostem, občanům a státním orgánům členských států společný právní základ pro bezpečnou elektronickou komunikaci. eIDAS dohlíží na elektronickou identifikaci a důvěryhodné služby pro elektronické transakce EU. Upravuje elektronické transakce, elektronické podpisy, definuje zúčastněné subjekty a procesy, aby zajistila bezpečnost např. při elektronickém převodu finančních prostředků či při komunikaci s veřejnými službami. Umožňuje pohodlně a bezpečně provádět přeshraniční transakce bez užití papírových metod. Byly vytvořeny standardy pro elektronické podpisy, kvalifikované digitální certifikáty, elektronická časová razítka, elektronické pečeti a další způsoby ověření autentizačních mechanismů. [24]

Ke stanovení minimální technické specifikace a postupů pro úrovně záruky prostředků pro elektronickou identifikaci slouží Prováděcí nařízení Komise (EU) 2015/1502. Toto nařízení ustanovuje technické a provozní požadavky nad rámec interoperability tak, aby byla zajištěna schopnost spolupráce systému elektronické identifikace, které státy EU oznamují Komisi.

Součástí interoperability elektronické identifikace jsou uzly, které slouží k vzájemnému propojení avizovaných systémů elektronické identifikace. Právě tohle nařízení upravuje různé

aspekty provozu a správy těchto uzlů. Je to především důvěrnost, integrita a pravost dat vyměňovaných mezi uzly. Dalším aspektem je uchování údajů, které budou sloužit ke zjištění místa a povahy incidentu v případě vzniku incidentu. [25]

Důležitým spisem je rovněž Dokument konkretizující minimální požadavky na kvalifikované systémy elektronické identifikace a na prostředky pro elektronickou identifikaci v rámci nich vydávané a používané (zkráceně DKP IDP). Je to český konkretizující dokument vydaný Ministerstvem vnitra pro účely vysvětlení a bližší konkretizace požadavků CIR 2015/15021, na které odkazuje zákon č. 250/2017 Sb., o elektronické identifikaci a na prostředky pro elektronickou identifikaci.

Dokument je primárně určen pro žadatele o získání akreditace pro správu kvalifikované systému, pro kvalifikované správce a pro pověřené osoby posuzující splnění požadavků daných zákony zmíněných výše. Zde jsou přesně definovaná východiska a jejich důsledky v tomto znění: [26]

- *„Přístup k elektronickým službám ČR je umožněn osobám, které vlastní prostředek pro elektronickou identifikaci vydaný správcem kvalifikovaného systému v rámci kvalifikovaného systému (dle §3 zákona o elektronické identifikaci) nebo prostředek vydaný oznámeným systémem v rámci nařízení eIDAS. Pro úplnost je vhodné uvést, že pro obstarání výstupů z informačních systémů veřejné správy je možné využít prostředek pro elektronickou identifikaci umožňující přístup se zaručenou identitou ve smyslu §2 písm. x) zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů.*
- *Občanský průkaz s identifikačním certifikátem občanského průkazu vydaný Českou republikou je prostředek elektronické identifikace s vysokou úrovní záruky, jehož životní cyklus je řízen zákonem č. 328/1999 Sb., o občanských průkazech, ve znění pozdějších předpisů.“* [26]

Ke shrnutí prostředků pro elektronickou identifikaci slouží níže zpracovaná tab. 2.

Tab. 2: Prostředky pro elektronickou identifikaci [27]

Bezpečnostní funkce	Údaje	Předměty
Identifikace Jednoznačné rozlišení osoby (uživatele systému)	• Jedinečný identifikátor • Údaje specifikující osobu o jméno, datum narození	Předmět pro zjištění identity • Průkazy vydávané státem

	○ název firmy, DIČ	• ID karty s fotografií
Autentizace Ověření identity osoby pro přihlášení k systému	Tajný údaj pro ověření identity v systému • Heslo • PIN	Předmět pro ověření identity v systému • OTP – jednorázové kódy • Kryptografický token
Autorizace Udělení práva osoby použít funkci systému	Data pověření k funkcím systému • Registr práv uživatelů • Typy uživatelů a akcí	Prokázání odpovědnosti a vůle k provedení akce • SMS – zasílání OTP • Elektronický podpis

1.2.1.3 PSD2

PSD2 je směrnice Evropského parlamentu a Rady (EU) 2015/2366 o platebních službách na vnitřním trhu, která byla přijata dne 25. listopadu 2015. PSD2 je druhá směrnice Evropské unie o platebních službách, která podstatně ovlivnila způsob provádění online plateb a poskytování informací v platebním styku. Nařizuje další bezpečnostní opatření pro banky a poskytovatele platebních služeb, včetně používání zvláštních kvalifikovaných digitálních certifikátů. [28] [29]

Účelem směrnice je:

- Přispívat k integrovanějšímu a efektivnějšímu evropskému trhu plateb.
- Vytvořit rovnocenné podmínky pro poskytovatele platebních služeb v celé EU.
- Zajistit bezpečnější elektronické platby.
- Zajistit důslednější ochranu spotřebitele.

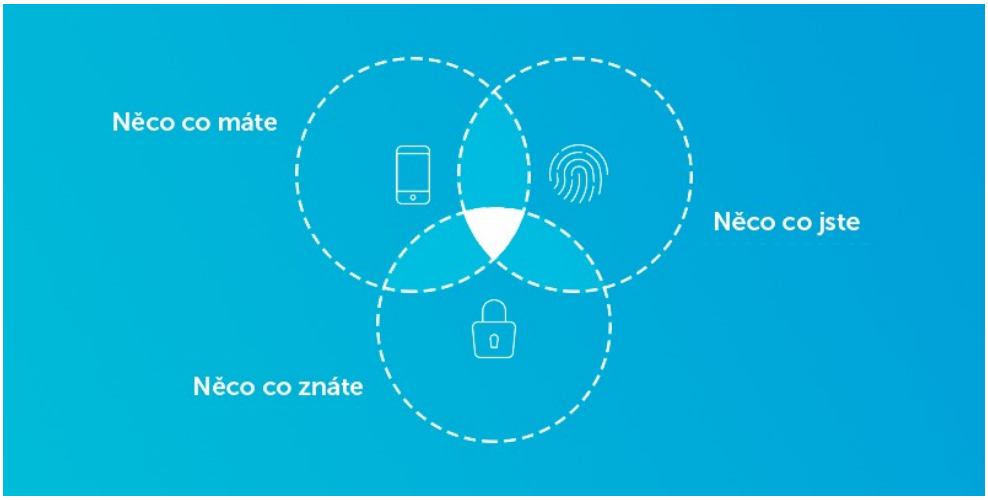
PSD2 pokrývá mnoho aspektů trhu s elektronickými platbami, ale zejména zavádí posílená opatření v oblasti ochrany soukromí a online zabezpečení, která musí banky a poskytovatelé platebních služeb podnikající v EU provádět. [29]

SCA (Strong Customer Authentication) vstoupila v platnost 14. září 2019. Silné ověření zákazníka je bezpečnostní mechanismus, který má za cíl snížit riziko vzniku podvodů v důsledku kompromitovaného hesla. Spočívá v použití kombinace dvou ze tří bezpečnostních prvků, díky kterým se ověří platba na internetu. Tomuto ověření se říká dvoufaktorová autentizace (2FA). Při zadávání 2FA se kombinují tyto bezpečnostní faktory:

- Znalost – to, co uživatel zná (např. heslo, PIN, CVV ze zadní strany platební karty).

- Vlastnictví – to, co uživatel vlastní (např. telefon, chytré hodinky).
- Jedinečnost – to, čím uživatel je (biologické prvky, jako je např. otisk prstu, fotka obličeje, sken duhovky, atd.). [30]

Tyto bezpečnostní faktory jsou znázorněny na obr. 9.



Obr. 9: Bezpečnostní faktory pro ověření 2FA [30]

Dalším důležitým standardem rozšiřujícím směrnici 2015/2366 je nařízení (EU) č. 2018/389, pokud jde o regulační technické normy týkající se silného ověření klienta a společných a bezpečných otevřených standardů komunikace (Regulatory Technical Standards on Strong Customer Authentication, dále jen „Nařízení RTS SCA“). Nařízení vstoupilo s účinností od 14. září 2019 stejně jako SCA. [31]

RTS SCA zavádí ve všech státech Evropského hospodářského prostoru řadu nových pravidel v oblasti zprostředkování internetových platebních služeb, např. při zpracovávání online plateb, což významně zasáhne jak větší bankovní a platební instituce, tak také poskytovatele platebních služeb či vydavatelů elektronických peněz malého rozsahu a jejich zákazníků. Týká se to tedy zprostředkovatelů platebních služeb, kteří uživatelům vedou online platební účet. Přitom se nerozlišuje, zda se jedná o plnohodnotné internetové bankovnictví. Pro tyto účely Soudní dvůr v Rakousku dospěl k závěru, že „základním znakem pojmu platební účet je možnost provádět z účtu platební transakce ve prospěch třetí strany nebo být příjemcem takových transakcí od třetí strany.“ [32]

Poskytovatelé platebních služeb za účelem provádění bezpečnostních opatření musí splňovat tyto požadavky:

- uplatňovat postup silného ověření klienta,

- na základě míry rizika, částce a opakování platební transakce a způsobu použitém k jejímu provedení použít výjimky ze zásady silného ověření klienta,
- chránit důvěrnost a integritu osobních bezpečnostních údajů uživatelů platebních služeb,
- určit společné a bezpečné otevřené standardy komunikace spolu s poskytováním a používáním platebních služeb, a to mezi:
    - poskytovateli platebních služeb, kteří vedou učet,
    - poskytovateli služeb iniciování platby,
    - poskytovateli služeb informování o účtu, plátci, příjemci a dalšími poskytovateli platebních služeb. [32]

Dále mezi nově zavedené povinnosti pro poskytovatele platebních služeb, kteří vedou účet a těm, kdo plátci platební účet nabízí, patří:

- umožnění přístupu pomocí rozhraní poskytovatelům služeb třetích stran (poskytovatelé služeb iniciování platby, poskytovatelé služeb informování o účtu a poskytovatelé platebních služeb vydávající karetní platební prostředky), které musí splňovat požadavky dle ustanovení čl. 30 a násl. Nařízení RTS SCA,
- v případě nefunkčnosti tohoto rozhraní musí být zaveden nouzový mechanismus,
- rozšíření rozhraní pro zadávání platebních příkazů a dalších typů operací, jako jsou trvalé platby, hromadné platby a inkasa,
- povinnost monitoringu a auditu, kdy uplatňování bezpečnostního opatření musí být pravidelně testováno, vyhodnocováno a kontrolováno auditory, kteří mají odborné znalosti v oblasti bezpečnosti informačních technologií a plateb a kteří jsou funkčně nezávislí na poskytovateli platebních služeb. [32]

1.2.2 Bezpečnostní standardy

Mobilní platby jsou relativně novým aspektem platebního ekosystému, ale rostou neuvěřitelně rychle. Společnosti, které chtějí vyvinout řešení pro mobilní platby, musí věnovat velkou pozornost pravidlům a směrnicím, které se budou vztahovat na jejich produkt. Ty nejdůležitější, které budou pro potřeby této práce uvedeny, jsou PCI DSS, PA-DSS a Dodatek E: MFS od FFIEC.

Mobilní aplikace NFC se řídí celou řadou standardů a specifikací, z nichž některé upravují základní technologii a funkčnost mobilních zařízení NFC a jiné, které jsou specifické pro aplikace.

1.2.2.1 PCI DSS

Jde o mezinárodní bezpečnostní standard (Payment Card Industry Data Security Standard), který má za cíl zamezit krádežím, únikům a následnému zneužití dat o držitelích platebních karet. Povinností firem (jichž se karetní platby a práce s klientskými daty týká) je požadavky tohoto standardu (kterých je 12) dodržovat, aby se vyvarovaly těm nejzákladnější a nejčastějším rizikům. PCI DSS poskytuje základní technické a provozní požadavky určené k ochraně dat účtu. PCI DSS se vztahuje na všechny subjekty zapojené do zpracování platebních karet - včetně obchodníků, zpracovatelů, acquirerů (akceptátor platebních karet), vydavatelů karet a poskytovatelů služeb. Dále platí také pro všechny ostatní entity, které ukládají, zpracovávají nebo přenášejí data držitelů karet nebo citlivá autentizační data. Níže v tab. 3 je uveden podrobný přehled 12 požadavků PCI DSS. [33]

Tab. 3: Přehled požadavků PCI DSS [33]

Požadavek	Krok
Vytvoření a údržba zabezpečené sítě a systémů	1. Nainstalujte a udržujte konfiguraci brány firewall pro ochranu dat držitelů karet. 2. Nepoužívejte výchozí nastavení dodaná dodavatelem pro systémová hesla a další bezpečnostní parametry.
Chránit data držitelů karet	3. Chraňte uložená data držitele karty. 4. Šifrování přenosu dat držitelů karet přes otevřené veřejné sítě.
Udržovat program pro řízení zranitelností	5. Chraňte všechny systémy před malwarem a pravidelně aktualizujte antivirový software nebo programy. 6. Vývoj a údržba zabezpečených systémů a aplikací.
Implementovat přísná opatření pro kontrolu přístupu	7. Omezte přístup k datům držitelů karet podle obchodních potřeb. 8. Identifikujte a ověřte přístup k systémovým komponentům. 9. Omezte fyzický přístup k datům držitelů karet.

Pravidelně monitorovat a testovat sítě	10. Sledujte a monitorujte veškerý přístup k síťovým prostředkům a datům držitelů karet. 11. Pravidelně testujte bezpečnostní systémy a procesy.
Dodržovat zásady zabezpečení informací	12. Udržujte pravidla zaměřená na bezpečnost informací pro všechny pracovníky.

Dodržování PCI DSS se věnují karetní asociace jako VISA nebo MasterCard, které byly také u vzniku PCI Security Standards Councilu. To je organizace sdružující auditory, kteří mají za úkol posuzovat, zda a jak dobře společnosti aplikují své povinnosti vyplývající z PCI standardů v praxi. [34]

1.2.2.2 PA-DSS

Payment Application Data Security Standard, tedy standard zabezpečení dat platebních aplikací, je mezinárodní standard vytvořený opět PCI SSC (Payment Card Industry Security Standards Council). Byl implementován ve snaze poskytnout datový standard pro dodavatele softwaru, kteří vyvíjejí platební aplikace. Cílem je zabránit vyvinutým platebním aplikacím pro třetí strany v ukládání zakázaných zabezpečených dat včetně magnetického proužku, CVV2 nebo PIN. Tento standard také rovněž stanovuje, že dodavatelé vyvíjející platební aplikace, musí být v souladu s PCI DSS.

Aby byla platební aplikace považována za kompatibilní s PA-DSS, musí dodavatelé softwaru zajistit, aby jejich software obsahoval následujících čtrnáct ochranných opatření:

1. Nezachovávat úplné údaje o trasovacích datech (track data), ověřovací kód nebo hodnotu karty (CAV2, CID, CVC2, CVV2) ani data PIN bloků.
2. Chránit uložená data držitele karty.
3. Poskytovat bezpečné funkce pro ověření uživatele.
4. Log aktivity aplikace plateb.
5. Vývoj bezpečných platebních aplikací.
6. Ochrana bezdrátových přenosů.
7. Testovat platební aplikace pro zjištění zranitelnosti a udržovat aktualizace platebních aplikací.
8. Usnadnit implementaci zabezpečené sítě.
9. Data držitele karty nesmí být nikdy uložena na serveru připojeném k internetu.

10. Usnadnit bezpečný vzdálený přístup k platební aplikaci.
11. Šifrování citlivého provozu ve veřejných sítích.
12. Zabezpečit veškerý administrativní přístup bez konzoly.
13. Udržovat průvodce implementací PA-DSS pro zákazníky, distributory a integrátory.
14. Přiřadit odpovědnosti za zaměstnance PA-DSS a udržovat vzdělávací programy pro zaměstnance, zákazníky, prodejce a integrátory. [35]

1.2.2.3 FFIEC MFS

Jako reakci na nárůst hackingu bankovní regulátoři zdůraznili potřebu finančních institucí zajistit bezpečnost aktiv, která chrání. Na základě toho vznikla podrobná Příloha E: Mobilní finanční služby (Appendix E: Mobile Financial Services, dále MFS) vydaná americkou FFIEC (The Federal Financial Institutions Examination Council). FFIEC zdůrazňuje složitost infrastruktury mobilní technologie a identifikuje konkrétní zranitelnosti, které existují v mobilním ekosystému.

Tento dodatek E se zaměřuje na rizika spojená s činnostmi a zařízeními pro mobilní finanční služby. Dodatek zdůrazňuje celofiremní přístup k řízení rizik pro efektivní řízení a zmírnění stávajících a vyvíjejících se rizik. Příloha E: MFS pojednává o různých typech mobilních finančních služeb, které instituce v současné době zavádějí, a poskytuje aktualizovaný pracovní program, který pomůže přezkoumat a poskytnout doporučení týkající se MFS. [36]

Dodatek E: MFS identifikuje čtyři současné technologie MFS používané finančními institucemi:

4. Mobilní bankovnictví SMS (textové bankovnictví).
5. Webové stránky a prohlížeče podporující mobilní zařízení.
6. Mobilní aplikace.
7. Bezdrátové (mobilní) platební technologie.

Mobilní bankovnictví SMS využívá textové zprávy, které zákazníkovi umožňují poskytovat finanční transakci své finanční instituci. Mezi typické transakce mobilního bankovnictví SMS patří shromažďování informací (kontrola zůstatku), převod prostředků mezi účty, upozornění nebo aktualizace účtů nebo jednorázová hesla pro ověření webových stránek.

Webové stránky a prohlížeče podporující mobilní zařízení umožňují zákazníkovi přístup ke stejným produktům a službám internetového bankovnictví jako uživateli stolního počítače, pouze web nebo prohlížeč je optimalizován pro mobilní zařízení (tablet, notebook nebo smartphone).

Mobilní aplikace jsou softwarové aplikace ke stažení vyvinuté speciálně pro použití na mobilních zařízeních. Aplikace mobilního bankovnictví jsou obvykle přizpůsobeny konkrétní finanční instituci (branding, produkty, služby) a umožňují zákazníkovi provádět stejné služby (shromažďování informací, iniciovat převody, platit účty atd.), jaké nabízí tradiční internetové bankovnictví. Mobilní aplikace nabízejí rychlejší a uživatelsky přívětivější rozhraní.

Technologie bezdrátových plateb (mobilní platby) přicházejí v různých aplikacích, včetně bezdrátových plateb na terminálech Point-of-Sale (POS) (Apple Pay, Android Pay nebo Samsung Pay), plateb typu Peer-to-Peer (Fiserv Popmoney, PayPal , Venmo) nebo jiné typy bezdrátových plateb (mobilní peněženky). Většina mobilních platebních technologií umožňuje uživateli provést transakci bez nutnosti fyzické karty během transakce. [36]

V příloze E jsou uvedeny čtyři různé typy technologií pro mobilní platby:

- NFC (Near field communication) - je bezdrátový protokol, který umožňuje výměnu platebních údajů (nebo jiných informací) uložených v mobilním zařízení pouze tehdy, když jsou platební terminál a zařízení v bezprostřední blízkosti sebe („klepnutí“ na zařízení na terminálu NFC je často slouží k zahájení transakce).
- Na základě obrazu - kódované obrázky podobné čárovým kódům (nazývané kódy rychlé reakce nebo „QR“) používané k iniciaci plateb. Pověření může být zakódováno v obraze QR kódu nebo uloženo v cloudu. Například konkrétní prodejci mohou používat kódy QR k identifikaci zákazníků v mobilním uzavřeném platebním systému.
- Na nosiči - transakce založené na operátoru jsou fakturovány přímo na fakturu mobilního operátora zákazníka. Obchodníci jsou placeni přímo mobilním operátorem a obchází tradiční platební sítě. Například k platbě na základě operátora může dojít, když mobilní uživatelé věnují peníze na charitu prostřednictvím SMS zpráv nebo si zakoupí „add-on“ v mobilní herní aplikaci.
- Mobilní P2P - platby typu Peer-to-Peer (P2P) jsou nejčastěji iniciovány na mobilním zařízení pomocí čísla mobilního telefonu příjemce, e-mailové adresy nebo jiného

identifikátoru. Platba probíhá prostřednictvím zavedených maloobchodních platebních technologií. Platby P2P lze provádět prostřednictvím textových zpráv (SMS) nebo mobilní aplikace (Fiserv Popmoney). P2P umožňuje zákazníkovi posílat peníze prostřednictvím svého mobilního zařízení dalším uživatelům zapsaným v systému instituce. [36]

Proces řízení rizik instituce by měl zahrnovat riziko používání mobilních finančních služeb. Riziko používání MFS také závisí na typech funkcí nabízených institucí, na typu informací, které jsou uloženy, přenášeny a zpracovávány prostřednictvím MFS, a na míře přijetí. Dodatek E: MFS identifikuje čtyři typy rizik:

- Strategické riziko: instituce musí určit, zda je využití MFS v souladu se stávající strategickou vizí a cíli. Pokud implementace MFS není v souladu s těmito položkami strategického plánování, zvyšuje se strategické riziko.
- Operační riziko: provozní rizika MFS zahrnují rizika spojená se zahájením transakce, autentizací a autorizací a samotným hardwarem a softwarem MFS.
- Riziko dodržování předpisů: Mezi rizika dodržování předpisů pro instituce patří nesoulad s právními předpisy, předpisy a pokyny pro dohled nad spotřebiteli, jakož i neprovedení řádné hloubkové kontroly a průběžné řízení prodejců MFS.
- Reputační riziko: riziko poškození pověsti finanční instituce v důsledku toho, že informace, které jsou uloženy, přenášeny a zpracovávány prostřednictvím MFS, budou po určitou dobu ohroženy nebo přerušeny. [36]

2 SOUČASNÉ PROSTŘEDÍ BEZPEČNOSTI MOBILNÍCH ELEKTRONICKÝCH PLATEBNÍCH NÁSTROJŮ

Peníze se v lidské historii několikrát vyvinuly od dob výměnného obchodu, od mincí k papíru, poté plastu a nyní telefonům. Asi před 15 lety byl mobilní telefon používán k telefonování, hraní jednoduchých her a posílání SMS zpráv. Dnes lze mobilní telefony použít k přístupu k internetu, videohovorům, fotografování, nalezení vaší polohy na mapě, nákupu přepravních dokladů a dokonce i pro bankovnictví, mezi mnoha dalšími aplikacemi. Díky pokrokům v mobilní technologii a komunikacích v blízkém poli (NFC) mění inovace v oblasti finančních služeb způsob, jakým platíme za zboží nebo služby nebo posíláme peníze do zahraničí, a nahrazují peněženku chytrým telefonem.

2.1 Typy mobilních plateb

V následujících podčástech této kapitoly budou představeny různé typy mobilních plateb s jejich odpovídajícími způsoby využití a výhodami. Níže bude uvedeno následujících sedm typů mobilních plateb.

2.1.1 Prémiové transakční platby založené na SMS

SMS platba znamená použití textových zpráv k platbě za produkty nebo služby.

K zaplacení může zákazník jednoduše odeslat zprávu SMS. Na oplátku je mu zaslán kód nebo heslo, které umožňuje přístup k prémiovému obsahu. Mobilní operátor poté přidá náklady do běžné měsíční faktury uživatele nebo ji odečte z předplaceného zůstatku.

SMS platby jsou snadný a pohodlný způsob zpracování mikroplatby. Nabízejí mnoho výhod pro poskytovatele obsahu a služeb, jako jsou vlastníci webových stránek nebo vývojáři aplikací.

Výhody:

- Okamžitý přístup k miliardám uživatelů mobilních telefonů po celém světě.
- Není třeba uzavírat samostatné smlouvy ani ověřovat totožnost zákazníků.
- Zákazníci nepotřebují kreditní karty ani bankovní účty.
- Fakturaci zajišťuje mobilní operátor.

Se snadností systému přichází bohužel některé **nevýhody** jako:

- Nízké výplaty - operátoři také vidí vysoké náklady na provoz a podporu transakčních plateb, což má za následek, že výplaty obchodníkovi jsou nízké až 30%. Obvykle kolem 50%.
- Ceny nemohou být stanoveny volně, ale vývojáři si musí vybrat z tzv. cenových bodů, které nabízí poskytovatel plateb SMS.
- Špatná spolehlivost - transakční prémiové platby SMS mohou snadno selhat, protože se zprávy ztratí.
- Pomalá rychlost - odesílání zpráv může být pomalé a obchodník může obdržet potvrzení o platbě i po pár hodinách. Spotřebitelé nechtějí čekat déle než několik sekund.
- Zabezpečení - šifrování SMS / USSD končí v rádiovém rozhraní, pak je zpráva prostým textem.
- Vysoké náklady - s nastavením tohoto způsobu platby je spojeno mnoho vysokých nákladů. [37]

2.1.2 Přímé mobilní fakturace

Spotřebitel používá při placení na webu elektronického obchodu možnost fakturace pomocí mobilního telefonu. Po dvoufaktorové autentizaci zahrnující PIN a jednorázové heslo je nákup účtován z mobilního účtu zákazníka.

Výhody:

- Zabezpečení - dvoufaktorové ověřování a modul řízení rizik zabraňuje podvodům.
- Pohodlí - není vyžadována žádná předběžná registrace a žádný nový mobilní software.
- Snadné - během procesu platby je to jen další možnost.
- Rychlý - většina transakcí je dokončena za méně než 10 sekund.
- Osvědčené - 70% veškerého digitálního obsahu zakoupeného online v některých částech Asie používá metodu přímého mobilního účtování.

Nevýhoda:

- Nejvýznamnějším omezením je druh a hodnota zboží, které lze zakoupit. [37]

2.1.3 Mobilní platby na webu (WAP)

Spotřebitel používá k provedení platby zobrazené webové stránky nebo další aplikace stažené a nainstalované do mobilního telefonu. Jako základní technologii používá protokol WAP (Wireless Application Protocol) a dědí všechny výhody a nevýhody protokolu WAP.

Výhody:

- Následný prodej, kdy platba na mobilním webu může přesměrovat zpět do obchodu nebo k jinému zboží, které si spotřebitel může přát. Tyto stránky mají adresu URL a lze je uložit do záložek, takže je snadné je znovu navštívit nebo sdílet.
- Vysoká spokojenost zákazníků díky rychlým a předvídatelným platbám.
- Snadné použití ze známé sady online platebních stránek.

Nevýhoda:

- Pokud není mobilní účet účtován přímo prostřednictvím operátora mobilní sítě, je vyžadováno používání kreditní nebo debetní karty nebo předběžná registrace v online platebním řešení, jako je PayPal. [37]

2.1.3.1 Přímá fakturace operátora

Přímá fakturace operátora, známá také jako fakturace mobilního obsahu, fakturace WAP a fakturace operátora, která vyžaduje integraci s operátorem mobilní sítě.

Výhody:

- Provozovatelé mobilních sítí již mají fakturační vztahy se zákazníky, platba bude připočtena k jejich fakturaci.
- Poskytuje okamžitou platbu.
- Chrání platební údaje a identitu zákazníka.
- Výhodněji přepočítaný koeficient.
- Snížené náklady na podporu zákazníků pro obchodníky.
- Alternativní možnost zpeněžení v zemích, kde je nízké využití kreditní karty.

Nevýhoda:

- Jednou z nevýhod je, že sazba vyplacení bude často mnohem nižší než u jiných platebních možností pro mobilní platby. Například výplata u Paypal je kolem 92%, 84% u kreditní karty a okolo 60% u fakturace operátora. [37]

2.1.3.2 Online peněženky

Online společnosti jako PayPal, Amazon Payments a Google Pay mají také mobilní možnosti. Obvykle jde o registraci, zadání telefonního čísla, přijetí kódu PIN prostřednictvím SMS, zadání kódu PIN, zadání informací o kreditní kartě nebo jiného typu platby k ověření platby. Při následné platbě je třeba zadat pouze číslo PIN.

Výhody

- Nižší náklady - používáním online peněženek se odstraní potřeba zprostředkovatelů.
- Konkurenční výhoda – pohodlnější způsob zpracování transakcí pro zákazníky, která dává podnikům, které tuto technologii využívají, konkurenční výhodu na trhu.
- Moderní - tradiční hotovostní podniky, jako jsou řemeslné veletrhy a bleší trhy, nyní mohou přijímat debetní a kreditní karty. To otevírá zcela nový aspekt platebních metod na velkých trzích, přináší mnoho obchodních příležitostí a vyšší potenciální příjem.
- Pohodlí - uživatelé jsou schopni provést nákup za pouhé sekundy pouhým klepnutím nebo naskenováním svého mobilního zařízení. Nákup zboží se stává rychlejší a snadnější.

Nevýhody:

- Investice - počáteční peněžní investice na vybudování funkční aplikace digitální peněženky je poměrně významná.
- Podpůrná technologie - v současné době existuje jen málo podpůrných technologií, z nichž nejčastější jsou terminály NFC a čtečky telefonů.
- Systémové výpadky - informace o digitálních peněženkách jsou uloženy v cloudu obchodních serverů; proto vždy existuje riziko selhání nebo vypnutí systému. To může mít za následek, že podniky nebudou schopny zpracovat platby nebo budou stále pomalejší kvůli vysokému provozu na serverech.
- Zabezpečení - společnosti musí zajistit, aby informace jejich zákazníků byly šifrovány a dobře chráněny. [37]

2.1.3.3 Kreditní karta

Jednoduchý mobilní platební systém na webu může také zahrnovat tok plateb kreditní kartou, který spotřebiteli umožňuje zadat své údaje o kartě a provádět nákupy.

Výhoda:

- Pokud dodavatel platebních služeb dokáže automaticky a bezpečně identifikovat zákazníky, lze pro budoucí nákupy vyvolat podrobnosti o kartě, díky čemuž se platby kreditní kartou změní na jednoduché kliknutí s nákupem, což poskytuje vyšší míru konverze pro další nákupy.

Nevýhoda:

- Jakékoli zadávání podrobností na mobilním telefonu snižuje úspěšnost (konverzi) plateb. [37]

2.1.4 Platby QR kódem

QR kódy jsou čtvercové čárové kódy. Čárové kódy QR nebo „Quick Response“ byly navrženy tak, aby obsahovaly smysluplné informace přímo v čárovém kódu.

Kódy QR mohou být ze dvou hlavních kategorií: QR kód je uveden na mobilním zařízení osoby platící a naskenované prostřednictvím POS nebo jiného mobilního zařízení příjemce. Nebo QR kód je předložen příjemcem statickým nebo jednorázovým způsobem a je naskenován osobou provádějící platbu.

Výhody:

- Snadná implementace - implementace je relativně rychlá a levná.
- Jednoduchost - relativně snadné použití.
- Spolehlivost - údaje o platbě, název a částka jsou vyplněny automaticky - nedochází k chybám.
- Mobilní aplikace Security Bank nabízejí nejvyšší standardy zabezpečení a bezpečnosti.
- Adresovatelný trh - protože je v telefonu vyžadován čip NFC, je adresovatelný trh pro toto technologické rozhraní poměrně velký.

Nevýhoda:

- Zabezpečení - škodlivé kódy QR mohou obsahovat malware nebo trojské koně. [37]

2.1.5 Bezkontaktní NFC

Technologie NFC (Near Field Communication) se používá hlavně při placení nákupů uskutečněných ve fyzických obchodech nebo v dopravních službách. Zákazník, který používá

speciální mobilní telefon vybavený chytrou kartou, se přiblíží svým telefonem poblíž čtecího modulu. Většina transakcí nevyžaduje ověření, ale některé (zpravidla transakce nad určitou částkou) vyžadují ověření pomocí PIN, než může být transakce dokončena. Platba může být odečtena z předplaceného účtu nebo účtována přímo na mobilní nebo bankovní účet přímo.

Výhody:

- Pohodlí - mnoho spotřebitelů „zaplatí“ za pohodlí, protože pohodlí je v dnešní společnosti velmi důležité.
- Všestrannost - NFC lze dobře přizpůsobit pro všechny druhy situací, od bankovních karet po cestovní a filmové průkazy, systémy odměňování a dokonce i klíče.
- Bezpečnost - kreditní karty podporující NFC jsou mnohem bezpečnější než magnetický proužek kreditní karty. Vyžaduje PIN. Maloobchodníci již nemají fyzický přístup k informacím o zákazníkově kreditní kartě.

Nevýhody:

- Pokud společnosti nesouhlasí s integrací NFC do svého podnikání, spotřebitelé nebudou moci tuto technologii používat.
- Zabezpečení - dalším velkým rizikem pro NFC je počítačové hackerství nebo telefonní hackerství. [37]

2.1.6 Cloudově založena mobilní platba

Cloudový přístup umisťuje poskytovatele mobilních plateb do středu transakce, což zahrnuje dva samostatné kroky. Nejprve je vybrána metoda platby spojená s cloudem a platba je autorizována prostřednictvím NFC nebo alternativní metodou. Během tohoto kroku poskytovatel plateb automaticky pokryje náklady platby s prostředky emitenta. Za druhé, v rámci samostatné transakce poskytovatel plateb zpoplatňuje vybraný účet kupujícího vybraný v cloudovém prostředí, kde není karta, aby nahradil své ztráty za první transakci.

Výhody:

- Otevřené a flexibilní - mobilní platby založené na cloudu otevírají více příležitostí k nasazení služeb zákazníkům pomocí flexibilních obchodních modelů.
- Odemkne hodnotu značky emitenta - emitenti mají přímou kontrolu nad brandingem a uživatelskou zkušeností.

- Žádná závislost na ekosystému - mobilní platby v cloudu vyžadují méně zprostředkovatelů, zkracují čas uvedení na trh a poskytují emitentům větší kontrolu nad zahájením a projektem.
- Zabezpečení - spolehnutí se na schválené dodavatele, kteří poskytují zcela zabezpečená prostředí a pokročilé metody tokenizace, mohou vydavatelé dosáhnout vysoké úrovně zabezpečení dat karet.

- Schváleny Visa a MasterCard - obě hlavní karetní asociace schválily cloudové mobilní platby. Normy, požadavky a procesy schvalování programů jsou definovány, aby finanční instituce mohly bezpečně hostovat digitální karty v cloudu.

Nevýhody:

- Zabezpečení v paměti chytrého telefonu - aby mohly být transakce prováděny v obchodních pokladních systémech, a to i bez pokrytí sítě, musí vydávající banka poskytnout do paměti telefonu podrobnosti o digitální kartě. Podrobnosti, jako je jméno držitele karty a číslo účtu, musí být uloženy v nezabezpečené paměti telefonu.
- Zabezpečení a vyhovění – digitální distributor zpracovává stejně citlivá data jako poskytovatelé plastových karet.
- Řízení rizik a podvodů - použití mobilních zařízení a cloudu k provádění transakcí vytváří pro emitenty výzvy i příležitosti pro řízení rizik.
- Zkušenosti s aplikacemi a uživateli - spotřebitelé chtějí volbu, zda platit pomocí bankovní aplikace, obchodní aplikace nebo jiné oblíbené aplikace. Toto očekávání zákazníků vyžaduje, aby platforma pro správu obsahovala konfigurace a pravidla podnikání. [37]

2.1.7 Mobilní platby zvukovým signálem (NSDT)

Zvukový kanál mobilního telefonu je dalším bezdrátovým rozhraním, které se používá k provádění mobilních plateb. Několik společností vytvořilo technologii, která využívá akustické funkce mobilních telefonů k podpoře mobilních plateb a dalších aplikací, které nejsou založeny na čipech. Technologie NSDT (Near sound data transfer), Data Over Voice a NFC 2.0 vytvářejí zvukové podpisy, které může mikrofon mobilního telefonu přijmout a umožnit tak elektronické transakce.

Výhody:

- Zabezpečený - používá zvukový kanál telefonu k přenosu bezpečných informací.
- Efektivní - poskytuje vynikající úroveň účinnosti a spolehlivosti i v hlučném prostředí.
- Není třeba žádný další hardware jako v NFC, takže se stává levnějším.

Nevýhoda:

- Hlučné prostředí může způsobit problém v přenosu dat. [37]

2.2 NFC

Ze všech výše zmíněných typů mobilních plateb je nejrozšířenější a nejhojněji používanou platbou platba za pomocí NFC technologie. Česká republika je v Evropě mezí předními státy ve využívání bezkontaktního placení a je zřejmé, že trend bude pokračovat i s využíváním technologie NFC. Princip je jednoduchý - vzít do ruky telefon, přiložit jej k terminálu stejně jako bezkontaktní kartu, zadat PIN a je zaplaceno. Nejpromyšlenějšími komplexními řešení jsou Google Pay a Apple Pay, které jsou podrobnější rozebrány v kapitole 3. [38]

Near Field Communication (zkráceně NFC) byl zaveden v roce 2002 pro bezkontaktní platby na krátký dosah a „poloduplexní komunikaci“, což umožňuje přenos signálu v obou směrech, ale přitom již současně nezajišťuje komunikaci mezi různými zařízeními. Komunikace probíhá mezi dvěma vysílacími a přijímacími zařízeními v rozmezí několika centimetrů (asi 10 cm) a s pracovní frekvencí 13,56 MHz.

Typy zařízení NFC jsou klasifikovány jako „iniciátor“ k iniciaci a vedení výměny dat a „cíl“ k odpovědi na požadavek iniciátoru. Komunikace NFC také sestává ze dvou režimů: aktivní režim, ve kterém jak „iniciátor“, tak „cíl“ používají k přenosu dat vlastní energii, zatímco v pasivním režimu cílové zařízení využívá energii, která je generována iniciátorem.

Po přiblížení telefonu NFC ke čtečce se telefon NFC chová podobně jako u čipové karty a čtečka komunikuje se softwarem Secure Element (zkráceně SE), který provádí akce, které vyžadující vysokou bezpečnost. Secure Element je čip zabudovaný do telefonu, který poskytuje zabezpečení jako čipová karta. [39]

2.2.1 Zranitelnost NFC

Vzhledem k povaze NFC je zjevně jednou z hlavních výzev odposlouchávání. Útočník se bude moci pokusit extrahovat a dekódovat data po obdržení radiofrekvenčních signálů. V případě přenosu dat v aktivním režimu je možné odposlouchávat až 10 m, ale v případě

pasivního režimu bude vzdálenost snížena na 1 m. V případě odposlechu je také možné data poškodit a narušit komunikaci tak, aby příjemce nemohl detekovat zařízení odesílatele útočníka. Při útoku DoS může protivník provést poškození dat přenosem platných dat ve správný čas, který by se mohl vypočítat naučením typu „modulace“ a „kódování“. Útočník však nemůže změnit skutečná data. Telefon NFC však dokáže detekovat tento typ útoku díky ověření pole Radio Frequency v době přenosu dat. [40]

Pro výměnu dat mezi telefony NFC se používá „NFC Data Exchange Format“ (ve zkratce „NDEF“). Je možné vytvořit škodlivý plakát útočníkem s manipulovanými značkami NDEF úpravou komerčního plakátu, což povede ke sdílení škodlivého obsahu s útočníkem. Řešením je podepisování šifrovaných přístupů přizpůsobených značkám nebo použití protokolů pro autentizaci pomocí kryptografických značek. [39]

Další zranitelností NFC je vysokofrekvenční (RF) rozhraní. V souladu s některými studiemi tento typ útoku zahrnuje „odposlouchávání útoků MITM“, „korupce dat, modifikace a vkládání“, „útoky DOS“, „útoky relací“ a „phishing pomocí sociálního inženýrství“ (sociální proces, pomocí kterého se útočník učí informace od uživatele o cíleném útoku). Řešením je zřízení bezpečné komunikace mezi telefony NFC pomocí sdíleného tajemství pomocí „protokolu klíčové dohody“.

Další typy chyb zabezpečení NFC souvisí se zařízením NFC a zabezpečeným prvkem. To zahrnuje: spuštění aplikace bez informování uživatele, instalace malwaru na hostitelském zařízení, útok proti zařízení NFC, přidání „modifikovaného zabezpečeného prvku“ k mobilnímu zařízení NFC, klonovací tokenu a odposlech „přes vzduch“. [39]

Navrhovaná řešení pro tyto typy útoků zahrnují:

- mechanismy ověřování založené na certifikátu,
- zásady správy klíčů pro ověření opatření zabezpečených prvků,
- povinné podepisování kódu pro API NFC a
- kryptografické propojení aplikace s jedinečnými identifikátory. [41]

2.2.2 Očekávání od NFC

Do oblasti mobilních plateb NFC je zapojeno mnoho zúčastněných stran. Do transakce spadají tyto zúčastněné strany: zákazník (plátce) a obchodník, mobilní operátoři, instituce finančního sektoru (např. banky), platební sítě (např. Visa, MasterCard), důvěryhodný správce

služeb, výrobce mobilních zařízení a poskytovatelé softwaru a služeb (např. vývojáři peněženek). Tabulka 4 ukazuje očekávání různých zúčastněných stran.

Tab. 4: Očekávání zúčastněných stran NFC plateb

Zúčastněný subjekt	Očekávání
Obchodník	• Rychlejší doba transakce • Nízké nebo nulové nové investiční a provozní náklady • Vše v jednom otevřeném interoperabilním zařízení (např. POS) se zpětnou kompatibilitou • Integrace / zjednodušení stávajících platebních přístupů • Vysoká bezpečnost a důvěra ve službu • Možnost přizpůsobení služby (např. přidání věrnostních schémat) • Stav mobilních peněžních transakcí v reálném čase
Spotřebitel	• Minimální křivka učení • Lepší a personalizované služby • Důvěryhodná a bezpečná řešení (na technické a sociální úrovni) • Nová služba k dispozici všude • Nízké nebo nulové dodatečné náklady na používání • Interoperabilita v POS a schopnost převádět peníze mezi různými poskytovateli služeb a bankami • Přehled stavu transakcí v reálném čase • Možnost platit „kdekoli“, „kdykoli“ a v jakékoli měně • Transakce mezi osobami
Provozovatel mobilní sítě	• Potenciál pro přidání hodnoty ke stávajícím službám • Zvýšení loajality zákazníků • Nové příjmové kanály • Zvýšit průměrné příjmy na uživatele
Výrobce mobilního zařízení / Vývojář služeb	• Velké přijetí trhu nových vestavěných hardwarových/softwarových funkcí zařízení • Otevřené, interoperabilní, široce používané standardy

	• Nízké náklady na nové technologie/funkce, které mají být integrovány. • Nízká doba uvedení na trh. • Multi-aplikační schopnosti. • Nové vztahy s bankami / operátory mobilních sítí / platebními sítěmi.
Banka	• Branding a loajalita zákazníků. • Noví zákazníci. • Vlastnictví nebo spoluvlastnictví nové platební aplikace. • Zabezpečená a důvěryhodná platební služba. • Integrace/využití stávající infrastruktury a platebních metod.
Platební síť	• Bezpečná autentizace. • Integrace/využití stávající infrastruktury. • Bezpečné zpracování plateb.
Důvěryhodní servisní manažeři	• Zabezpečený platební kanál. • Poskytovat služby bankám a operátorům mobilních sítí.

2.2.3 Výhoda NFC plateb

Placení pomocí NFC za použití mobilu je nejen jednoduché, ale oproti platbě standardní bezkontaktní platební kartou má spoustu výhod, a to zejména po praktické a bezpečnostní stránce. Tou první je, že uživatel u sebe nemusí mít svou peněženku a stačí mu mobil, který u sebe nosí naprostá většina lidí. Navíc NFC platby nevyžadují aktivní data nebo připojení na WiFi a stačí pouze platební terminál.

Další přínosy s NFC platbami plynou ze škálovatelnosti platební aplikace. V platební aplikaci (Apple Pay či Google Pay) lze uložit více karet, např. kreditní, debetní, Visa, či MasterCard. Mezi nimi je možno libovolně přepínat dle toho, kterou kartou je třeba zrovna platit. Praktické je, že ať je platba provedena kteroukoli kartou, použit je PIN, jenž byl zvolen při aktivaci aplikace. Při placení tedy není potřeba znát kódy všech „kreditek“, které zákazník používá. [38]

Na vývoji NFC plateb mobilem či hodinkami se podílejí i karetní společnosti Visa a MasterCard.

Při placení mobilem se není třeba bát úniku citlivých dat, nebo dokonce odcizení peněz. Tento způsob platby neodesílá číslo platební karty při platbě a ani ho neukládá do telefonu. Při platbě se vytvoří virtuální kód (token), který se přiřadí k jednotlivé transakci. U nízkých částek stačí telefon „probudit“, při platbě nad 500 korun je třeba zadat PIN nebo odemknout obrazovku.

Velkou výhodou je, že při ztrátě mobilního zařízení je možné jej uzamknout na dálku novým heslem nebo vymazat celý obsah. Není potřeba řešit blokaci karty a vystavení nové, jako je tomu při její ztrátě. [38]

2.3 Tokenizace

Koncept tokenizace byl představen v roce 2013 třemi značkami kreditních karet (tj. MasterCard, Visa a American Express), aby se zvýšila důvěrnost a soukromí uživatele při online transakcích. Cílem je nahradit primární číslo účtu (PAN) digitální hodnotou pojmenovanou jako token, aby se zajistilo soukromí citlivých informací držitele karty. Další kroky k tradičním transakcím jsou vyžádání a poskytnutí tokenu a poté držitel karty použije tento token místo PAN během transakce. Na druhé straně obchodníci a provozovatelé digitálních peněženek již nemusí ukládat PAN jako citlivá data, což k online transakcím přidává další bezpečnostní vrstvu.

Navrhovaný koncept musí mít následující klíčové vlastnosti:

- Poskytování úplnějších informací o transakci pomocí nových datových polí pro zlepšení detekce podvodů a urychlení procesu povolování a autorizace.
- Spolehlivé přístupy k ověření držitele karty před nahrazením PAN tokenem.
- Navrhování standardu pro dosažení zjednodušení transakčního procesu pro obchodníky při jakýchkoli typech plateb, jako jsou bezkontaktní platby, online platby, atd.

Na druhé straně generace tokenů musí mít také některé vlastnosti:

- Zajištění přijatelnosti tokenu z velké části jako náhradní hodnoty tradičního primárního čísla účtu.
- Schopnost všech současných účastníků elektronických plateb provádět transakci pomocí tokenu.

- Zajištění proveditelnosti pro vývoj bezpečných inovativních produktů a aplikací pro elektronické platby pohodlně.
- Zvýšení bezpečnosti a důvěrnosti držitele karty při používání PAN v nespolehlivých prostředích. [39]

Zabezpečení tokenu a kryptogramu (jednorázový šifrovaný řetězec představující transakci a informace o obchodníkovi) jsou zásadní pro celkovou bezpečnost samotné mobilní platební transakce samotné. Klíčovými bezpečnostními aspekty jsou způsob, jakým mobilní aplikace zpracovává tokeny, například zabezpečení tokenu v úložišti a při přenosu, jakož i návrh mobilní aplikace. [43]

II. PRAKTICKÁ ČÁST

3 POŽADAVKY NA BEZPEČNOST DIGITÁLNÍCH DVOJČAT NA PLATFORMÁCH IOS A ANDROID

Používání mobilního telefonu k provádění plateb za zboží a služby představuje posun paradigmatu směrem k platbám pouze v digitální podobě a je poháněno zákazníky, kteří chtějí nakupovat v maloobchodních prodejnách nebo převádět finanční prostředky pomocí své mobilní „digitální peněženky“. Pro většinu zákazníků nabízí možnost placení pomocí mobilního telefonu větší pohodlí než přenášení tradiční peněženky s více kreditními a debetními kartami. Používání mobilní peněženky však není bez rizika.

Obrovské šíření virů a malwaru ovlivňující mobilní zařízení, spolu se skutečným nebezpečím ztracení nebo odcizení zařízení vyvolalo v mysli spotřebitele pocit nejistoty ohledně ztráty jejich cenných prostředků. Pokud k tomu přidáme možnost přístupu k penězům a riziko neoprávněných plateb v případě ztráty, odcizení nebo napadení mobilního zařízení malwarem, pak se naše mobilní zařízení mohou náhle stát ohroziteli naší finanční svobody. V důsledků ztráty našich mobilů, jejich náchylnost k hackování nebo jiným podobným způsobům jejich napadání výrazně stoupá.

V tomto odvětví je velmi důležité, aby byly vypracovány pokyny, které pomohou vývojářům mobilních plateb a poskytovatelům mobilních plateb k zajištění ochrany před kybernetickými hrozbami spotřebitelům, maloobchodníkům a finančním institucím.

V následující kapitole budou uvedeny nejoblíbenější aplikace pro mobilní platby/digitální peněženky, tj. Apple Pay a Google Pay. Cílem této analýzy je zdůraznit (ne porovnat) bezpečnostní prvky, které jsou součástí každé z těchto mobilních platebních aplikací.

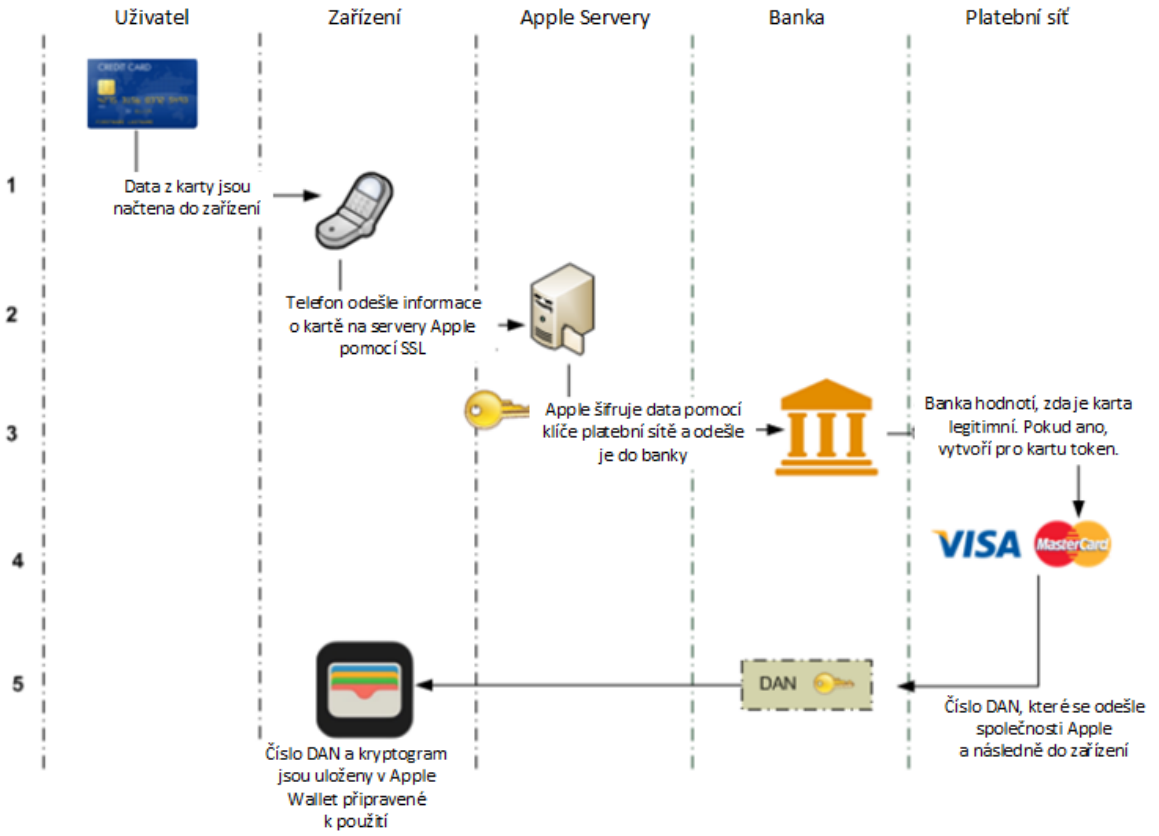
3.1 Apple Pay

Apple Pay je řešení společnosti Apple pro mobilní platby pomocí zařízení iOS včetně Apple Watch. Je navržen tak, aby chránil osobní údaje držitele karty a umožňuje uživateli provádět platby u obchodníků, kteří nasadili prodejní terminály podporující bezkontaktní platby Apple Pay.

Apple Pay kombinuje řadu existujících bezpečnostních technologií a bezpečnostních kontrol, které uživatelům umožňují iniciovat platby a autorizovat platební transakce mezi uživateli, obchodníky a vydavateli karet.

3.1.1 Registrace karty

První krok k používání Apple Pay zahrnuje proces přidání nové debetní nebo kreditní karty. Následující diagram (obr. 10) ukazuje postup založení karty.



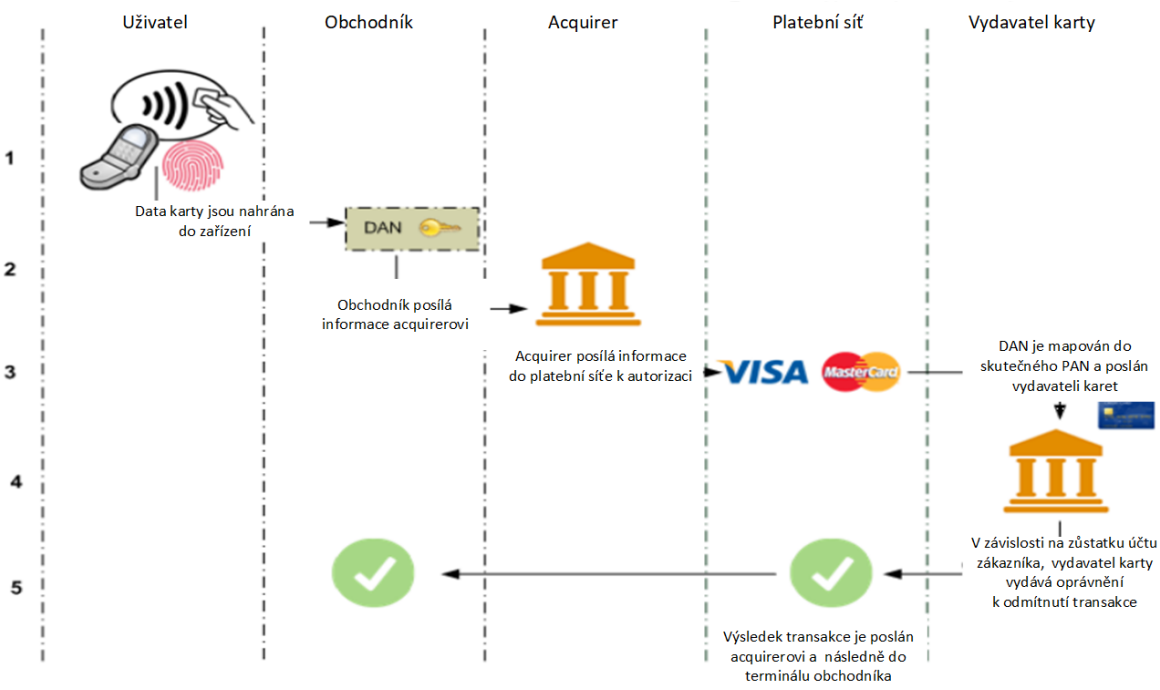
Obr. 10: Postup přidání karty v Apple Pay [43]

1. Uživatel přidá své stávající informace o kartě zadáním do aplikace nebo vyfotografováním kreditní nebo debetní karty pomocí svého telefonu.
2. Zařízení obdrží informace o kartě a odešle ji prostřednictvím zabezpečeného připojení k serverům Apple, spolu s dalšími daty uživatelů a zařízení, jako je aktivita iTunes/App Store, informace o zařízení (číslo mobilního telefonu, model, atd.) a umístění uživatele (pokud jsou povoleny služby určování polohy).
3. Banka obdrží informace a rozhodne, zda je karta platná nebo ne, obvykle v interakci s poskytovatelem platebních sítí. Přijaté informace (mobilní číslo, model, PAN atd.) budou použity v procesu řízení rizik k určení, zda je požadavek oprávněný a karta skutečně patří uživateli. To je zvláště důležité pro minimalizaci podvodů, protože stejná karta může být zapsána do několika zařízení.

4. Pokud je karta přijata, banka komunikuje s poskytovatelem platebních sítí a vytváří jedinečný token. Token je obvykle vytvářen spíše poskytovatelem TSP (Token Service Provider) než samotnou bankou.
5. TSP vygeneruje DAN (číslo účtu zařízení) specifické pro tuto kartu a zařízení. Poté bude odeslána zpět na servery Apple spolu s kryptogramem, který bude použit při generování bezpečnostních kódů během platby. Tato data budou předána do zařízení, které je uloží do Passbook/Apple Wallet pro budoucí použití.

3.1.2 Platební proces

Následující diagram (obr. 11) ukazuje platební proces Apple Pay.



Obr. 11: Platební proces Apple Pay [43]

1. Pro zahájení platebního procesu uživatel umístí své zařízení do blízkosti platebního terminálu NFC. Apple Pay spoléhá na identifikaci uživatele pomocí TouchID (nebo čísla PIN v případě Apple Watch). Jakmile je karta vybrána, její token (číslo DAN) se načte do SE (zabezpečený prvek). Apple podporuje EMV Contactless, a proto, pokud je podporován také terminálem, SE vygeneruje dynamický kryptogram.
2. Obchodník zašle informaci acquirerovi. Acquirerem je banka, která dostane zaplaceno za transakci kreditní kartou.

3. Acquirer obdrží číslo DAN, ale neví, zda se jedná o platný PAN nebo token. Ve skutečnosti acquirer jednoduše ověří BIN (identifikační číslo banky) a zašle jej příslušnému vydavateli karty prostřednictvím platební sítě, která funguje jako prostředník mezi acquirerem a vydavatel karty.
4. Platební síť zjistí, že je to skutečně DAN místo skutečného PAN, a proto předá číslo TSP (Token Service Provider), aby poslal skutečný PAN zpět vydavateli.
5. Vydavatel povolí nebo zamítne transakci a zašle oznámení acquirerovi, který ji zase pošle zpět obchodníkovi.

3.1.3 Ověření uživatele

Apple Pay vyžaduje, aby se uživatel k provedení platby autentizoval. Autentizace se provádí senzorem identifikace otisků prstů (TouchID) nebo číslem PIN v Apple Watch. Cílem této bezpečnostní kontroly je omezit to, co může útočník s ukradeným zařízením udělat. Použití identifikace nebo autentizace pomocí otisků prstů k zahájení platby je krokem vpřed v bezpečnosti ve srovnání s tradičními bezkontaktními platbami, kde lze odcizenou kartu použít bez jakékoli identifikace/autentizace uživatele, ale není to bez rizik (např. vícenásobné registrace, obcházení otisku prstu).

3.1.4 Ověření zařízení

Každá transakce Apple Pay vytváří jedinečnou hodnotu, která zajišťuje, že transakce pochází z autorizovaného zařízení. Tento jedinečný identifikátor spolu s tokenem a kryptogramem použitým k autorizaci transakce zajišťují, že i když je token odcizen, nemůže být použit z jiného zařízení, protože token musí pocházet ze zařízení, do kterého byl zaregistrován. Navíc je token počítán s částkou transakce, a proto i kdyby byl zachycen při přenosu, nemohl by jej použít útočník k provedení dalšího nákupu.

3.1.5 Ochrana dat

Apple Pay vyžaduje zabezpečení dat záměrně s následujícími ovládacími prvky:

1. Tokenizace: Během zápisu karty se vytvoří token, který se uloží do zařízení a použije se při platebních operacích. Během platby se nikdy nepoužívají skutečná čísla PAN a verifikační čísla karet (CVV). Tento prvek minimalizuje vystavení skutečných důvěrných dat a umožňuje uživateli rychle zablokovat kartu, pokud bylo zařízení odcizeno, přičemž karta zůstane funkční. Tento přístup také omezuje útoky nedůvěryhodných obchodníků, kteří nikdy nevidí skutečný PAN nebo CVV.

2. Využití zabezpečeného prvku: Zabezpečený prvek (SE) přítomný v zařízeních Apple je vysoce bezpečný čip, který je odolný proti neoprávněné manipulaci, např. pokud detekuje jakékoli pokusy o čtení jeho obsahu, automaticky nuluje paměť a zajišťuje, že nelze extrahovat žádné klíče.
3. Údaje o kreditní nebo debetní kartě se odesílají z platební sítě nebo vydavatele karty šifrované pomocí platebních appletů, které jsou umístěny v zabezpečeném prvku.
4. Během transakce terminál komunikuje přímo s SE prostřednictvím ovladače NFC přes vyhrazenou hardwarovou sběrnici.
5. Podrobnosti o autorizaci platby pro bezkontaktní transakce jsou lokalizovány do místního pole NFC a nikdy nejsou vystaveny procesoru aplikace.

3.2 Google Pay

Původní Google Wallet se spoléhal na zabezpečený prvek jako na důvěryhodné úložiště citlivých platebních informací. Google od té doby změnil směr pomocí emulace hostitelských karet (dále CHCE) po oznámení služby Google Pay v květnu 2015, což ve skutečnosti znamená, že platební údaje jsou uloženy v cloudu.

Kromě přechodu z SE na HCE změnil Google také proces ověřování, přidal věrnostní odměny a integroval se s dalšími aplikacemi.

Tyto změny přinesly významné architektonické změny v řešení, které zase měly dopad na plochu útoku.

3.2.1 Registrace karty

Uživatelé služby Google Pay musí nejprve zaregistrovat své debetní nebo kreditní karty pomocí služby Google Pay. Služba Google Pay zbavuje odpovědnost identifikace uživatele v bance zákazníka. Poskytuje tedy pouze několik identifikačních možností, které může vydavatel karty použít k rozhodnutí, zda je ověřena totožnost zákazníka. Jsou nabízeny následující způsoby ověření:

1. Ověření e-mailem nebo textem: Banka zákazníka zašle zákazníkovi e-mail/text s ověřovacím kódem.
2. Ověřování telefonicky: Zákazník může zavolat do banky a vyžádat si ověřovací kód.
3. Ověření prostřednictvím bankovní aplikace: Pokud má zákazník již na mobilním telefonu nainstalovanou bankovní aplikaci, je možné se do aplikace přihlásit a ověřit kartu.

4. Ověření pomocí „dočasného poplatku“: Tento proces ověření bude účtovat uživatelský účet velmi malým poplatkem, včetně šestimístného kódu. Uživatel by se musel přihlásit k elektronickému bankovnictví a poskytnout ověřovací kód.

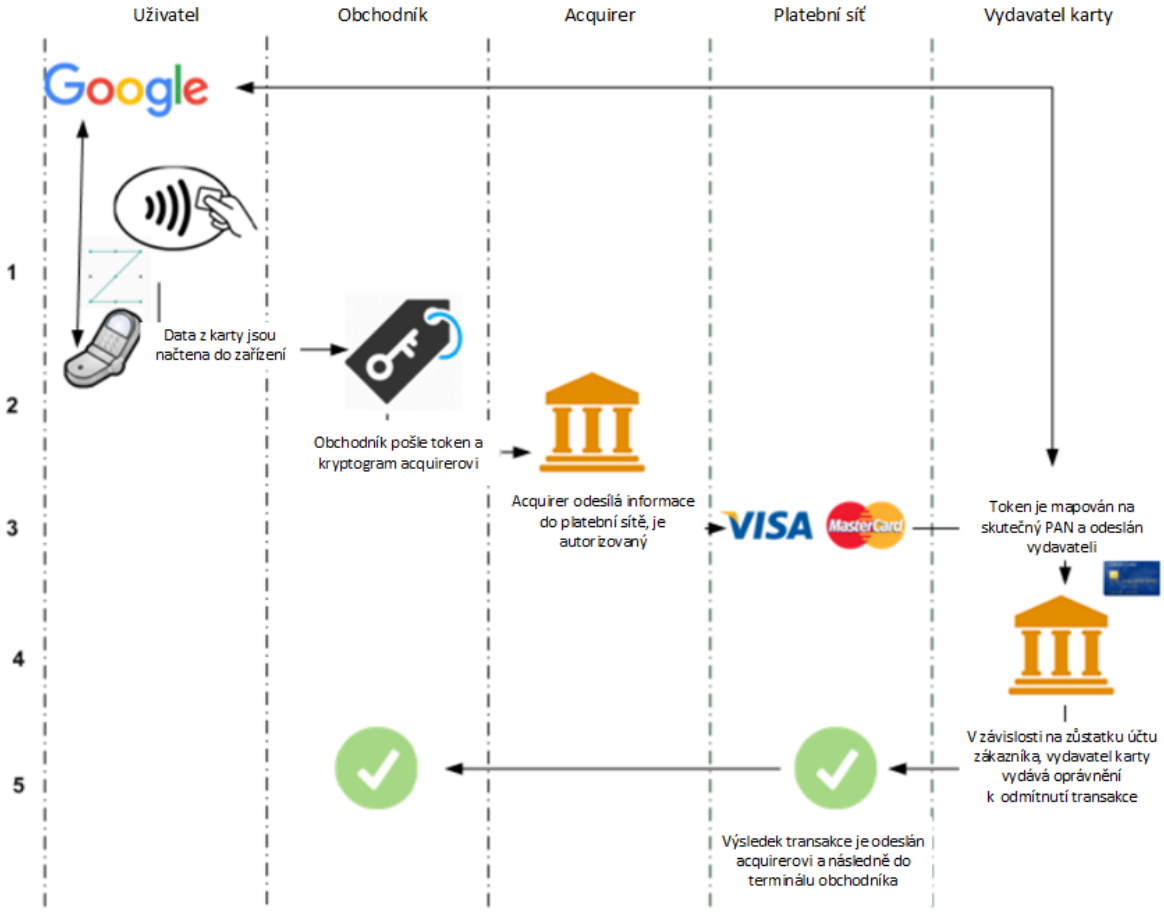
Uživatel, který přihlásí kartu do Google Pay, si musí být vědom, že číslo karty bude přeneseno a uloženo na cloudovém serveru Google.

3.2.2 Platební proces

Google Wallet byla původně implementována pomocí modelu založeného na zabezpečených prvcích pro bezpečné ukládání šifrovaných citlivých dat, jako jsou data držitelů karet a ověřovací kódy karet, ve formě tokenů na samotném zařízení samotném zařízení.

V roce 2014 bylo učiněno rozhodnutí považovat zařízení za nedůvěryhodné a ohrožené a místo toho přesunout SE do cloudu pomocí používáním HCE, to neznamená, že SE byla sama o sobě považována za kompromitovanou součást.

Následující diagram (obr. 12) představuje platební proces v Google Pay.



Obr. 12: Platební proces Google Pay [43]

1. Před zahájením platebního procesu se zařízení připojí k serverům Google a je mu poskytnuto množství platných platebních tokenů. Když uživatel umístí zařízení blízko k NFC POS (Point of Sale), povolí HCE ovladač NFC na zařízení, které bude řídit komunikaci mezi POS a peněženkou, a vyžádá si jeden z tokenů. Dynamický token a kryptogram jsou odeslány do POS.
2. Obchodník zašle informaci acquirerovi. Acquirerem je banka, která dostane zaplaceno za transakci kreditní kartou.
3. Acquirer obdrží token a kryptogram a pošle jej příslušnému vydavateli karty prostřednictvím platební sítě, která funguje jako prostředník mezi acquirer a vydavatelem.
4. Platební síť si vyžádá skutečný PAN od TSP (Token Service Provider) a zašle jej vydavateli ke schválení.
5. Vydavatel povolí nebo zamítne transakci a zašle oznámení acquirerovi, který ji zase pošle zpět obchodníkovi.

3.2.3 Ověření uživatele

Google Pay nabízí řadu možností k ověření uživatele před platbou. Služba Google Pay přijímá ověřování otisků prstů (ve výchozím nastavení není povoleno), kód PIN, heslo nebo vzor k ověření transakce.

Zatímco v tradičních platebních kartách má uživatel tendenci chránit číslo PIN (které uživatele ověřuje), mobilní vzory se běžně zobrazují na veřejnosti a mohou představovat významnou hrozbu pro bezpečnostní model Google Pay.

3.2.4 Ověření zařízení

Platební tokeny se do zařízení načítají předem, před platbou. Jakmile je k dispozici připojení, jsou tokeny pravidelně stahovány ze serverů Google.

Jako další opatření je služba Google Pay navržena tak, aby se nespouštěla na zařízeních, která mají povoleno administrativní (superuživatelské) řízení (známé také jako přístup root).

3.2.5 Ochrana dat

Protože HCE předpokládá, že jakákoli data uložená na přenosné částí jsou zranitelná (např. v případě odcizeného zařízení nebo ohroženého zařízení malwarem), ukládá citlivá data karty do databází hostovaných v bezpečném cloudovém prostředí.

Prevence neoprávněného přístupu k HCE závisí na čtyřech bezpečnostních pilířích:

- bezpečnostní klíče s omezeným použitím,
- tokenizace,
- otisky prstů zařízení a
- analýza transakčního rizika.

Klíče s omezeným použitím vyprší rychle a brání jejich zneužití. Tokeny snižují riziko nahrazením PAN daty s omezeným použitím, které plynule procházejí platebním systémem. Profily zařízení (otisky prstů) mohou telefon ověřit. Analýza dat poskytuje vyhodnocení transakcí v reálném čase pro identifikaci neobvyklé aktivity.

3.3 Přehled bank v ČR podporujících NFC platby

Banky v Česku podporujících NFC platby postupně přibývají a v nějaké formě tento způsob placení podporuje většina. Tady je však nutno poznamenat, že u některých bankovních domů je placení pomocí telefonu omezeno na vlastnictví platební karty konkrétního uživatele (nejčastěji MasterCard). K datu 18. 5. 2020 jsou to tedy následující finanční ústavy vypsány v tab. 5.

Tab. 5: Přehled bank v ČR podporujících NFC platby [38]

Banka	Apple Pay	Google Pay
Air Bank	✓	✓
CREDITAS	✓	✓
Česká spořitelna	✓	✓
ČSOB / Poštovní spořitelna	✓	✓
Equa Bank	✓	✓
Fio Banka	✓	✓
Komerční banka	✓	✓
mBank	✓	✓
MONETA Money Bank	✓	✓
Raiffeisenbank	✓	✓
Sberbank	✗	✗
UniCredit Bank	✓	✓

4 BEZPEČNOSTNÍ RÁMEC PRO NÁVRH MOBILNÍCH PLATEBNÍCH NÁSTROJŮ

V této kapitole bude zpracován bezpečnostní rámec pro firmu vyvíjející platební nástroje. Daná firma se specializuje na vývoj bezpečnostních technologií. Zaobírá se od vývoje kryptografických knihoven a autentizačních serveru až po implementaci webových frontendů a mobilních aplikací. Právě mobilní aplikace, které jsou cílené na koncového uživatele a jsou jim přímo využívány, jsou potenciálním terčem útoků.

Při vývoji těchto aplikací je důležité se zaměřit kromě stability a správnosti kódu i na prevenci a odolnost proti útokům. To znamená, že by aplikace měly být podrobeny penetračním testům a mělo by se zajistit nejen úspěšné projití těmito testy, ale také schopnost odolávat útokům z celého internetu.

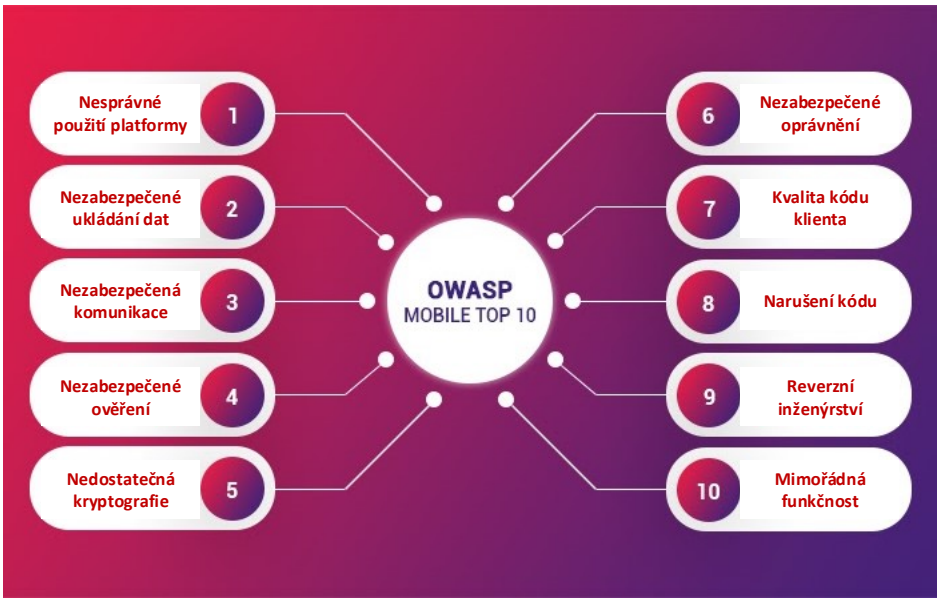
V dnešní době existuje plno pokročilých bezpečnostních funkcí pro platformy iOS a Android. Mezi ty nejprogresivnější, které budou využity, patří:

- Vývojová metodika OWASP.
- Dvoufaktorová autentizace (2FA).
- Ochrana aplikace RASP (Runtime Application Self-Proteciton).

4.1 Vývojová metodika OWASP

OWASP (Open Web Application Security Project) je komunitou vývojářů, která vytváří metodiky, dokumentaci, nástroje a technologie v oblasti zabezpečení webových a mobilních aplikací. Jedná se o aktualizované zdroje zaměřené na zvyšování povědomí o nových bezpečnostních hrozbách pro web a mobilní aplikace v komunitě vývojářů. Poskytuje seznam, který upozorňuje na bezpečnostní chyby a zranitelnosti, před kterými vývojáři potřebují chránit jejich aplikace. [44]

Níže jsou uvedena největší rizika dle OWASP Mobile 10, která jsou označena od M1 do M10 (viz obr. 13).



Obr. 13: OWASP Mobile 10 [45]

4.1.1 M1: Nesprávné použití platformy

Toto riziko se týká zneužití funkce operačního systému nebo nesprávného použití bezpečnostních ovládacích prvků platformy. To může zahrnovat intenty systému Android, oprávnění platformy, keychain nebo jiné ovládací prvky zabezpečení, které jsou součástí platformy. Tento výskyt je běžný, s průměrnou detekovatelností a může mít vážný dopad na postižené aplikace. [45]

Dále jsou uvedena rizika při nesprávném používání platformy. Ke každému riziku jsou popsány doporučené postupy, jak se jim vyhnout.

1. Únik dat využíváním intentu Android

Intent systému Android jsou objekty zpráv v operačním systému, které umožňují komunikaci mezi různými činnostmi. Tyto akce zahrnují komunikaci se službami na pozadí, přístup k datům uloženým v mobilním zařízení nebo serveru jiné aplikace, vysílání zpráv během změn událostí, spuštění nebo ukončení aktivity, jako je otevření prohlížeče nebo jiné aplikace, atd. Protože existuje nekonečné použití pro intenty, možnost úniku dat během těchto výměn zpráv se také zvyšuje.

Osvědčené postupy pro iOS, Android intent:

- Vydat se cestou povolení a omezit ty aplikace, které mají povoleno komunikovat s jejich aplikací, čímž se prakticky zablokují všechny pokusy trasy z mimo seznamu povolených. Další možností je nepovolit volbu exportu intentů pro jednu nebo

všechny činnosti, služby a přijímače vysílání s frameworkem Android tak, aby součásti systému Android, které nemají důvod komunikovat s aplikací, byly na začátku ponechány.

2. Android intent sniffing

Mnoho aplikací v ekosystému Android je primárně navrženo k tomu, aby ukradly informace z intentu. Tyto aplikace mohou studovat vzory adres URL nebo informace o uživateli, když jsou přenášeny mezi legitimní aplikací a dalšími komponenty systému Android.

Osvědčené postupy pro Android intent sniffing:

- Tento únik může být řízen definováním explicitních intentů, kde je objekt intentu jasně definován, čímž blokuje všechny ostatní komponenty pro přístup k informacím obsaženým v intentu. Před zveřejněním aplikace je třeba také pečlivě zkontrolovat oprávnění k souborům a ujistit se, že jsou požadovaná oprávnění na místě.

3. Riziko keychainu iOS

Keychain iOS je zabezpečený úložný prostor, který umožňuje uživateli mobilu vytvářet těžko zapamatovatelná hesla, která je obtížnější prolomit, a díky tomu jsou účty třetích stran (jako jsou bankovní a e-mailové účty) zpřístupněny na mobilních zařízeních zvlášť bezpečně. Systém iOS poskytuje šifrování keychainu, takže vývojář nemusí zavádět své vlastní metody šifrování. Pomocí seznamů řízení přístupu a přístupových skupin na keychainu se vývojář může rozhodnout, které aplikace a data vyžadují šifrování a které mohou zůstat otevřené. Pokud si uživatel nezvolí možnost Keychain, může si intuitivně zvolit snadno zapamatovatelná hesla, která mohou hackeři využít.

Osvědčené postupy pro iOS keychain:

- Nepovolovat šifrování keychainu po trase serveru a místo toho šifrované klíče uchovávat pouze v jednom zařízení, aby nemohlo být zneužito v jiných zařízeních nebo na serveru.
- Zabezpečit aplikaci pomocí keychainu k uložení tajemství aplikace, které by mělo mít vyhrazený seznam řízení přístupu. Zásadu autentizace uživatele v seznamu řízení přístupu může vynutit OS.6+.

4. Riziko iOS TouchID

Systém iOS umožňuje vývojářům používat technologii TouchID pro ověření jejich mobilních aplikací. Vynechání volby TouchID způsobuje, že proces autentizace je náchylný k pokusům o hackování.

4.1.2 M2: Nezabezpečené ukládání dat

OWASP označuje využitelnost M2 jako „snadnou“, prevalenci „běžnou“, detekovatelnost „průměrnou“ a dopad „závažnou“. Toto riziko v seznamu OWASP informuje komunitu vývojářů o snadných způsobech, jak může protivník získat přístup k nezabezpečeným datům v mobilním zařízení. Protivník může buď získat fyzický přístup k odcizenému zařízení, nebo do něj vstoupit pomocí malwaru nebo přebalené aplikace. [45]

V případě fyzického přístupu k zařízení lze přistupovat k souborovému systému zařízení po jeho připojení k počítači. Mnoho volně dostupného softwaru umožňuje protivníkovi přístup k adresářům aplikací třetích stran a k osobním identifikovatelným údajům v nich obsažených.

Dále jsou uvedena rizika nezabezpečeného ukládání dat. Pod těmito riziky jsou popsány doporučené postupy, jak se jim vyhnout.

1. Kompromitovaný systém souborů

I když zjevnou nevýhodou kompromitovaného systému souborů je ztráta osobních údajů uživatele, může vlastník aplikace také tyto data ztratit kvůli extrakci citlivých informací aplikace prostřednictvím mobilního malware, upravených aplikací nebo forenzních nástrojů. Z pohledu uživatele by tento druh datového kompromisu mohl vést ke krádeži identity, narušení soukromí a podvodům pro jednotlivého uživatele a poškození pověsti, narušení vnější politiky a materiální ztráty v případě firemních uživatelů.

Protivník vyhledává nezabezpečená data na několika místech v ohroženém zařízení. Zahrnují databáze SQL, soubory logu, úložiště dat XML, úložiště binárních dat, úložiště cookie, karty SD a data synchronizované s cloudem, jenž jsou převážně místem zranitelností a dějí se v důsledku operačního systému, frameworků, prostředí kompilátoru, nového hardwaru a rootnuté (jailbroken) zařízení.

2. Vykořisťování nechráněných dat

Vykořisťování nechráněných dat je možné díky nevědomosti vývojářů o tom, jak zařízení ukládá data mezipaměti, obrázky, stisknutí kláves a vyrovnávací paměti. Nedostatek řádné technické dokumentace těchto procesů na úrovni operačního systému a vývojového rámce

umožňuje vývojářům ignorovat tyto bezpečnostní procesy, a tak dát hackerům možnost manipulace s daty nebo procesů v zařízení.

Osvědčené postupy, jak zabránit nezabezpečenému ukládání dat:

Pro zařízení se systémem iOS se doporučuje používat cíleně zranitelné mobilní aplikace, jako je iGoat k modelování hrozeb jejich aplikací a vývojových rámců. Tento proces umožňuje vývojářům porozumět tomu, jak API pracují s informačními aktivy a procesy aplikací, jako je ukládání do mezipaměti URL, ukládání do mezipaměti stisknutí kláves, ukládání do mezipaměti, použití keychain, použití pozadí aplikace, logování, ukládání dat, správa souborů cookie prohlížeče, komunikace se serverem a přenos odesílaný k třetím stranám.

Vývojáři Androidu mohou pomocí shellu Android Debug Bridge (ADB) zkontrolovat oprávnění souborů cílové aplikace a systém správy databáze, například sqlite3 ke kontrole šifrování databáze. ADB také nabízí příkazy, jako je 'logcat', které vývojářům umožňují kontrolovat logy chyb obsažené v logách Android, kterými mohou pronikat citlivé uživatelské nebo bezpečnostní informace do malwaru. I když je všeobecně známo, že rozsáhlé logy chyb pomáhají vývojářům během vývojového procesu, pokud zůstanou bez povšimnutí, mohou tyto logy vést ke kompromitované aplikaci nebo datům. Vývojář systému Android by také měl používat nástroje, jako je Android Device Monitor a Memory Analysis Tool, aby se ujistil, že paměť zařízení nemá nechtěná data uložena po dobu neurčitou, kterou by mohl zneužít hacker nebo neoprávněná osoba, která může získat fyzický přístup k zařízení.

4.1.3 M3: Nezabezpečená komunikace

Přenos dat do a z mobilní aplikace se obvykle provádí prostřednictvím telekomunikačního operátora a/nebo přes internet. Hackeři zachycují data buď jako protivník sedící v místní síti uživatelů prostřednictvím kompromitované sítě Wi-Fi, „tapováním“ do sítě prostřednictvím routerů, celulárních věží, proxy serverů nebo využíváním napadené aplikace prostřednictvím malwaru. [45]

Rizika plynoucí z nezabezpečené komunikace:

1. Kradení informací

Sledování provozu prostřednictvím kompromitovaných nebo nezabezpečených sítí Wi-Fi je nejsnadnějším způsobem, jak protivník ukradne informace. Vývojáři by měli sledovat veškerý odchozí a příchozí přenos do mobilního zařízení včetně TCP/IP, Wi-Fi, Bluetooth/Bluetooth-LE, NFC, zvuku, infračerveného přenosu, GSM, 3G, SMS, atd.

2. Man in The Middle (MITM) útoky

Zatímco mobilní vývojáři obecně vědí, že pro ověřování používají SSL/TLS, neověřují tyto certifikáty správně a nechávají prostor síťovým útočníkům na útoky typu MITM (man-in-the-middle). Takové útoky umožňují protivníkovi prohlížet a upravovat provoz odesílaný mezi aplikací a jeho serverem a zachytávat ID relací. Protože jsou certifikáty zabezpečení specifické pro danou doménu, nejsou na testovacích serverech k dispozici. Vývojáři inklinují přijímat certifikáty s vlastním podpisem na produkčních serverech, když testují kódy. To ponechává mezeru pro útoky MITM, protože certifikát s vlastním podpisem je stejně dobrý jako nešifrované nebo prosté připojení. V případech, kdy vývojáři zakazují certifikáty podepsané uživatelem, mají útočníci tendenci využívat permisivní možnost ověření názvu hostitele, kterou vyvíjejí vývojáři. Pokud jsou povolena všechna jména hostitelů, mohou útočníci jednoduše použít jakýkoli platný certifikát vydaný certifikační autoritou a použít jej k získání kontroly nad přenosem na aplikačním serveru.

3. Kompromitování účtu správce

Skutečné nebezpečí útoku MITM není, když protivník ukradne uživatelská data, ale když nezabezpečená komunikace umožňuje krádež dat administrátorského účtu. To může vést k hackování celého webu a všech jeho citlivých dat. Takový útok může také ovlivnit nebo odcizit šifrovací klíče, hesla, soukromé informace o uživateli, podrobnosti o účtu, tokeny relací, dokumenty, metadata a binární soubory.

Vývojáři by měli zahrnout následující postupy k řešení nezabezpečené komunikace:

- Předpokládá se, že síťová vrstva není bezpečná a je náchylná k odposlouchávání.
- Dát si pozor na úniky přenášené mezi aplikací a serverem. Zkontrolovat také zařízení, které obsahuje aplikaci, a další místní zařízení nebo místní síť, včetně kabelových sítí.
- Aplikovat SSL/TLS pro přenos kanálů, které mobilní aplikace použije k přenosu citlivých informací, tokenů relací nebo jiných citlivých dat do koncového rozhraní API nebo webové služby.
- Účet pro externí subjekty, jako jsou analytické společnosti třetích stran, sociální sítě, atd. pomocí jejich verzí SSL, když aplikace spustí rutinu prostřednictvím prohlížeče/webkitu.
- Vyvarovat se smíšených relací SSL, protože mohou vystavit ID relace uživatele.
- Používat silné, průmyslově-standardní šifry s vhodnou délkou klíče.

- Používat certifikáty podepsané důvěryhodným poskytovatelem CA.
- Navázat zabezpečené připojení až po ověření identity serveru koncových bodů pomocí důvěryhodných certifikátů v řetězci klíčů.
- Upozornit uživatele prostřednictvím uživatelského rozhraní, pokud mobilní aplikace zjistí neplatný certifikát.
- Neposílat citlivá data přes alternativní kanály (např. SMS, MMS nebo oznámení).
- Pokud je to možné, aplikovat samostatnou vrstvu šifrování na všechna citlivá data před tím, než bude dána kanálu SSL. V případě, že budou v implementaci SSL objeveny budoucí chyby zabezpečení, zašifrovaná data poskytnou sekundární ochranu před porušením důvěrnosti.

4.1.4 M4: Nezabezpečené ověření

K tomuto problému dochází, když mobilní zařízení nedokáže správně rozpoznat uživatele a umožňuje protivníkovi přihlásit se do aplikace s výchozími přihlašovacími údaji. K tomu obvykle dochází, když útočník falšuje nebo obchází ověřovací protokoly, které buď chybí, nebo jsou špatně implementovány a interaguje přímo se serverem pomocí malwaru, který je umístěn v mobilním zařízení nebo botnetech, čímž nedochází k přímé komunikaci s aplikací. [45]

Rizika nezabezpečené autentizace:

1. Faktor vstupního formuláře

Nezabezpečené vstupní formuláře jsou běžným zdrojem manipulace v mobilních zařízeních, protože výrobci aplikací a mobilní platformy podporují snadno přístupná čtyř nebo šestimístná hesla pro snadný přístup. Kromě slabého vstupního faktoru, nespolehlivý přístup k internetu na mobilních zařízeních, nutí vývojáře, aby k ověřování relací přistupovali offline-online.

2. Nezabezpečené pověření uživatele

Technický dopad nezabezpečené autentizace spočívá v tom, že když aplikace nedokáže správně určit pověření uživatele, nemůže také správně zaznamenat aktivitu uživatele. Pokud takový uživatel využívá data nebo kód ze zařízení nebo přenosy do a ze zařízení, bezpečnostní tým nemůže správně zjistit zdroj a povahu útoku. Navíc, nezabezpečené ověřování také způsobuje zmatek s uživatelskými oprávněními v zařízení, protože operační systém nebude přesně vědět, jakou roli přiřadit uživateli, který nebyl řádně ověřen.

Doporučené postupy, jak se vyhnout nezabezpečené autentizaci:

Pečlivě prostudovat schéma autentizace aplikace a otestovat ji pomocí binárních útoků v režimu offline, aby se zjistilo, zda může být potenciálně zneužita. Bezpečnostní tým by měl zkontrolovat, zda aplikace umožňuje spuštění příkazu POST/GET k navázání spojení se serverem bez přístupového tokenu. Úspěšné připojení vytváří chyby v aplikaci. Vývojář by měl zajistit, aby hesla a bezpečnostní klíče nebyly místně uloženy v mobilním zařízení. Taková data jsou velmi náchylná k manipulaci.

Bezpečnostní tým by se měl pokusit implementovat následující metody k zabezpečení mobilní aplikace před nezabezpečeným ověřením:

- Bezpečnostní protokoly webové aplikace by se měly shodovat s protokoly mobilní aplikace, pokud jde o složitost a metody ověřování.
- Používat metody online ověřování stejně jako ve webovém prohlížeči. Pokud má snadný přístup v mobilním zařízení přednost, zkusit se chránit před binárními útoky, které jsou podrobně popsány v riziku M10.
- Nepovolit načítání dat aplikace, pokud server neověřil relaci uživatele. Lokální ukládání dat aplikace může vést k rychlejšímu načítání, ale může ohrozit zabezpečení uživatele.
- Vždy, když se místní úložiště dat stane eventualitou, ujistit se, že je šifrováno šifrovaným klíčem odvozeným z přihlašovacích údajů uživatele, a tím donutit aplikaci, aby ověřila data aplikace alespoň jednou.
- Trvalé požadavky na ověřování by měly být uloženy na serveru a ne lokálně. Vždy si pamatovat uživatele, když se rozhodnou pro možnost zapamatovat si.
- Bezpečnostní tým musí být opatrný při používání autorizačních tokenů zaměřených na zařízení v aplikaci, protože odcizená aplikace zařízení se stane zranitelnou. Autorizační token zaměřený na zařízení pro aplikaci zajišťuje, že k aplikaci nelze přistupovat, pokud nový vlastník zařízení změní přístupové heslo zařízení.
- Protože je běžný neoprávněný fyzický přístup k mobilním zařízením, bezpečnostní tým by měl vynucovat pravidelné ověřování uživatelských údajů a odhlášení ze strany serveru.
- Ujistit se, že je uživatel nucen zvolit pro hesla alfanumerické znaky. Jsou bezpečnější než jednoduché kombinace písmen. Kromě toho může vývojář nutit uživatele, aby

identifikoval obrázek nebo slovo, než povolí přístup k aplikaci. Metoda dvoufaktorové autentizace rychle získává na popularitě.

4.1.5 M5: Nedostatečná kryptografie

Data v mobilních aplikacích se stávají zranitelnými kvůli slabým procesům šifrování/dešifrování nebo slabostem v algoritmech, které spouštějí procesy šifrování/dešifrování. Hackeři mohou získat fyzický přístup k mobilnímu zařízení, špehovat síťový provoz nebo používat škodlivé aplikace v zařízení pro přístup k šifrovaným datům. Jejich cílem je pomocí chyb v šifrovacím procesu dešifrovat data do jejich původní podoby, aby je ukradli nebo zašifrovali pomocí opačného procesu, a stal se tak pro legitimního uživatele nepoužitelný. [45]

Rizika z nedostatečné kryptografie:

1. Krádež aplikací a uživatelských dat

Android i iOS vynucují šifrování kódů aplikací pomocí certifikátů vydaných důvěryhodnými zdroji, které dešifrují v paměti zařízení po ověření šifrovacího podpisu, když uživatel volá aplikaci. Mnoho běžně dostupných nástrojů však umožňuje obejít tuto metodu. Tyto nástroje lze použít ke stažení aplikace v jailbroken zařízení, k jejímu dešifrování a ke zhotovení snímku dešifrované aplikace zpět do paměti původního zařízení před spuštěním aplikace uživatelem. Jakmile se aplikace spustí v tomto ohroženém stavu, může hacker dále analyzovat aplikaci, aby provedla binární útoky nebo ukradla data uživatelů a aplikací. Jakýkoli vývojář, který se spoléhá na výchozí šifrovací proces poskytovaný operačním systémem, riskuje manipulaci s kódem.

2. Přístup k šifrovaným souborům

Mnoho vývojářů manipuluje se šifrovacími klíči, což protivníkům umožňuje získat kontrolu nad šifrovanými soubory, i když byly zabezpečeny pomocí nejlepších možných algoritmů. Vývojáři mají také tendenci umisťovat šifrovací klíče do stejných adresářů jako šifrovaná data. To usnadňuje hackerům přístup ke klíčům a jejich použití pro dešifrování.

Doporučené postupy, jak zabránit nedostatečné kryptografii:

- Pro šifrování aplikací zvolit moderní šifrovací algoritmy. Výběr algoritmu tuto chybu zabezpečení do značné míry zajišťuje, protože šifrovací algoritmus z důvěryhodného zdroje je obecně testován bezpečnostní komunitou.

- Národní institut pro standardy a technologie vlády USA čas od času publikuje kryptografické standardy a doporučuje šifrovací algoritmy. Vývojář by měl sledovat tento dokument a dávat si pozor na nové hrozby.

4.1.6 M6: Nezabezpečené oprávnění

Mnoho lidí zaměňuje riziko M4 s rizikem M6, protože obě jsou o pověřeních uživatele. Vývojáři by měli pamatovat na to, že nezabezpečená autorizace zahrnuje protivníka využívajícího zranitelnosti v procesu autorizace k přihlášení jako legitimní uživatel, na rozdíl od nezabezpečené autentizace, ve které se protivník pokouší obejít autentizační proces přihlášením jako anonymní uživatel. [45]

Rizika nezabezpečené autorizace:

1. Neregulovaný přístup ke koncovým bodům správce

V případě rizika M6, jakmile útočník získá přístup k aplikaci jako legitimní uživatel, je pro něho dalším úkolem získat administrativní přístup vynuceným procházením do koncového bodu, kde může provádět příkazy správce. Útočníci obvykle využívají botnety nebo škodlivé programy v mobilním zařízení k zneužití zranitelností v autorizaci. Výsledkem tohoto bezpečnostního kompromisu je, že útočník může připojit binární útoky na zařízení v režimu offline.

2. Přístup IDOR

V některých případech autorizační schéma umožňuje protivníkovi spouštět nezabezpečené přímé odkazy na objekty, známé pod zkratkou IDOR, kde může získat přístup k objektu, jako jsou databáze nebo soubory, jednoduše poskytnutím uživatelsky zadaných vstupů. Takové úniky mohou destabilizovat celý operační systém nebo vést ke ztrátě dat a pověsti.

Doporučené postupy, jak se vyhnout nezabezpečené autorizaci:

- Průběžně testovat uživatelská oprávnění spuštěním tokenů relací s nízkými oprávněními pro citlivé příkazy, které jsou vyhrazeny pro uživatele s vysokými oprávněními. Pokud lze příkazy úspěšně spustit, okamžitě zkontrolovat autorizační schéma aplikace.

- Vývojáři by měli mít na paměti, že schéma autorizace uživatelů se obvykle v režimu offline pokazí. V některých případech však vývojáři umožňují odesílání uživatelských oprávnění a rolí na server, což může také způsobit zranitelnost v autorizačním schématu.
- Spouštět autorizační kontroly rolí a oprávnění autentizovaného uživatele na serveru, nikoli z mobilního zařízení. Šance, že ověření uživatelé využívají vysoce privilegované funkce, se v systémech pro správu uživatelů ověřených v backendu spíše snižují, než když jsou ověřeni v mobilním zařízení.

4.1.7 M7: Špatná kvalita kódu

Riziko M7 vyplývá ze špatných nebo nekonzistentních praktik kódování, kdy každý člen vývojového týmu dodržuje odlišný postup kódování a vytváří nesrovnalosti v konečném kódu nebo nevytváří dostatečnou dokumentaci, aby ji mohli následovat ostatní. Úspora pro vývojáře zde je, že i když je toto riziko běžné, jeho detekovatelnost je nízká. Hackeři nemohou snadno studovat vzorce špatného kódování a často vyžadují ruční analýzu, což není snadné. Automatické nástroje, které se používají k identifikaci úniků paměti nebo přetečení vyrovnávací paměti pomocí fuzz testování, mohou pomoci získat přístup k informacím, ale neumožňují snadno provedení cizího kódu v mobilním zařízení. [45]

Rizika nízké kvality kódu:

1. Bezpečný webový kód kompromitovaný v mobilních zařízeních

Mobilní kód může ohrozit jinak bezpečnou aplikaci, která funguje dobře ve webových prohlížečích, a to tak, že agentovi hrozeb umožní kdykoli vyvolat podmnožiny kódu v mobilním zařízení nedůvěryhodnými vstupy. Naopak, takový mobilní kód nemusí být škodlivý, ale povolením spuštění nedůvěryhodného kódu v zařízení může vážně ohrozit informace o uživateli. Mezi typické chyby zabezpečení v této kategorii patří úniky paměti a přetečení vyrovnávací paměti.

2. Mezery v knihovnách třetích stran

Vývojáři by měli být opatrní při integraci populárních knihoven do svých aplikací. I zavedení hráči neúmyslně nabízejí kompromitované knihovny, což pro majitele aplikací vytváří bezpečnostní problém. Vývojáři často nesledují novější verze knihoven třetích stran, kde vývojář knihoven mohl opravit špatný kód dřívějších verzí, a tak umožnil protivníkům využívat aplikaci, kterou lze snadno zabezpečit.

3. Nejistota vstupu klienta

V aplikacích vytvořených pro konkrétní klienty vývojáři píšou kód, který akceptuje veškerý vstup jako bezpečný. Tato praxe může vést k útokům poskytovatele obsahu, protože volání poskytovatele obsahu může obsahovat citlivé informace. Útočník může také zavolat poskytovateli obsahu a získat přístup k nezajištěným informacím.

Doporučené postupy, jak zabránit špatné kvalitě kódu:

- Kód pro mobilní zařízení - nejjednodušším řešením, jak tento problém vyřešit, je přepsat kód v mobilním zařízení a nehledat řešení problémů na straně serveru. Vývojáři by měli mít na paměti, že špatné kódování na úrovni serveru se liší od kódování na straně klienta. Problém s kódem na straně serveru se projeví i ve webovém zobrazení aplikace, ale špatné kódování na straně mobilu ovlivní pouze mobilního uživatele.
- Statická analýza - vývojář by měl neustále používat nástroje třetích stran pro statickou analýzu k identifikaci úniků paměti a přetečení vyrovnávací paměti. Vývojový tým by se měl pokusit odstranit nesoulad mezi délkou příchozích dat vyrovnávací paměti a cílovou vyrovnávací pamětí.
- Logika kódu - vývojář by se měl vyhnout jednoduché logice v kódech. Hackeři mohou změnit hodnotu v kódu pomocí jednoduché logiky a obejít celý bezpečnostní aparát. Tyto kódy mohou být napadeny na úrovni sestavení a runtime. Vývojář by mohl tento únik ovládat zastavením nedůvěryhodných relací ve vymáhání oprávnění na úrovni zařízení a místo toho je aktivovat na serveru. Doporučuje se také neudělit oprávnění, dokud nebude relace ověřena pomocí protokolu OTP, tajných otázek nebo výzev.
- Verze knihovny - vývojový tým by měl vytvořit seznam všech knihoven třetích stran používaných v aplikaci a pravidelně kontrolovat jejich novější verze, i když používal knihovny pouze z důvěryhodných zdrojů.
- Poskytovatel obsahu - vývojáři by měli považovat veškerý vstup klienta za nedůvěryhodný a ověřit jej bez ohledu na to, zda pochází z aplikace nebo uživatele. Měli by pečlivě nastavit příznaky oprávnění na vstupech poskytovatele obsahu, aby zastavili veškerý neoprávněný přístup.

4.1.8 M8: Narušení kódu

Hackeři dávají přednost neoprávněné manipulaci s aplikacemi před jinými formami manipulace, protože jim umožňují získat neomezený přístup k aplikaci, chování uživatelů nebo dokonce celého mobilního zařízení. Mají tendenci nutit uživatele ke stahování narušených verzí populárních aplikací z obchodů s aplikacemi třetích stran prostřednictvím phishingových útoků a zavádějících reklam. [45]

Rizika manipulace s kódem:

1. Infuze malwaru

Jakmile byl uživatel úspěšně vyzván ke stažení narušené aplikace, stáhl a nainstaloval aplikaci, jejíž základní binární kód byl změněn, nebo byl změněn balíček zdrojů. Poškozené aplikace umožňují hackerům změnit systémová API, a umožnit tak provádění škodlivého cizího kódu v mobilním zařízení. Hackeři pak inklinují k oddávání se binárním opravám, úpravám rezidentního kódu v zařízení, úpravám paměti a krádeži dat.

2. Krádež dat

V upravených aplikacích, které v původních aplikacích neexistují, jsou často nabízeny další funkce a pobízejí uživatele k jejich přijetí. Převaha narušených aplikací je tak běžná, že společnosti investují obrovské množství prostředků do odhalování a odstraňování duplicitních aplikací z obchodů s aplikacemi a na vzdělávání uživatelů o možných scénářích krádeží dat.

Jejich kód však musí být umístěn v prostředí, které je mimo jejich dohled. Hackeři mohou také využít mezery v operačním systému k ovlivnění kódu legitimní aplikace. Navíc pokud uživatelé umožňují „rootnuté“ nebo „jailbreaknuté“ zařízení, vědomě vytvářejí možnosti pro třetí strany manipulovat s rezidentním kódem v zařízení.

Vývojáři by proto neměli dospět k závěru, že veškerá manipulace je nežádoucí. Některé případy mohou být bezvýznamné, zatímco jiné mohou být úmyslné ze strany uživatelů. V případě finančních nebo herních aplikací však musí být vývojáři zvlášť opatrní.

Doporučené postupy, jak zabránit neoprávněnému zásahu do kódu:

- Detekce runtime - vývojář by měl zajistit, aby aplikace mohla za běhu detekovat změnu kódu. Pokud chce narušená aplikace běžet v rootnutém nebo jailbreaknutém zařízení a vývojář si nepřeje tento druh provádění povolit, je nejlepší nahlásit tento

kompromis serveru sám za běhu. RASP je jedna taková technologie, kterou mohou vývojáři použít k detekci a odrazení útočných vektorů v reálném čase.

- Změny kontrolního součtu - vývojář by měl použít kontrolní součty a vyhodnotit digitální podpisy, aby zjistil, zda došlo k manipulaci se soubory. Protože manipulace s kódem a souborem téměř vždy mění hodnotu kontrolního součtu, je to nejjednodušší způsob, jak určit rozpornou akci.
- Vymazání dat - po zjištění manipulace se ujistěte, že kód aplikace, klíče a data jsou vymazána. Takové ustanovení zničí samotné důvody manipulace a odrazí hackery od cílení na stejnou aplikaci znovu.

4.1.9 M9: Reverzní inženýrství

Reverzní inženýrství mobilního kódu je běžně využitelnou událostí. Hackeři obvykle používají externí, běžně dostupné nástroje binární kontroly, jako je IDA Pro, Hopper, otool, atd. ke studiu vzorových kódů původní aplikace a jejích vazeb na serverové procesy. [45]

Rizika reverzního inženýrství:

1. Dynamická kontrola za běhu

Některé jazyky - jako Java, .NET, Objective C, Swift - jsou náchylnější k reverznímu inženýrství než jiné, protože umožňují dynamickou kontrolu za běhu. Kromě jiného poškození může reverzní inženýrství ovlivnit bezpečnost serverů, dat obsažených v mobilních zařízeních a schopnost serveru detekovat jailbroken nebo rootnuté zařízení.

2. Ukradení kódu

Reverzní inženýrství mohou konkurenti aplikace použít k tomu, aby si ukázali funkčnost aplikace, a dokonce i některé funkce tajně kopírovali. Tímto způsobem se sníží náklady na vývoj nového kódu.

3. Prémiové funkce

Hackeři mohou tuto techniku použít k přístupu k prémiovým funkcím aplikace obcházením procesu autentizace. Herní podvodníci mohou touto metodou získat nespravedlivou výhodu nad svými konkurenčními kolegy.

Doporučené postupy, jak se vyhnout reverznímu inženýrství:

- Použít podobné nástroje - nejlepší způsob, jak zabezpečit aplikaci proti zpětnému inženýrství, je použít stejné nástroje, které hackeři používají k pokusu o zpětné inženýrství. Pokud tyto nástroje mohou snadno analyzovat tabulky řetězců aplikace, řídit tok cesty, interakce se servery, kryptografické konstanty a šifry, metadata, atd., je kód ohrožen. Vývojáři mohou také použít nástroj jako AppSealing k detekci pokusů o zpětné inženýrství v reálném čase.
- Zmatení kódu - proces zmatení by měl zahrnovat cílení na konkrétní segmenty zdrojového kódu, tabulky řetězců a metody, které mají nejmenší dopad na výkonnost kódu. Vývojář by měl zajistit, aby úroveň zmatenosti, kterou používají, neměla být snadno zvrácena pomocí nástrojů pro odstraňování nejasností, jako jsou IDA Pro a Hopper.
- Používat jazyky C - zvážit použití C a C++, což může v runtime manipulaci do značné míry pomoci. Mnoho knihoven těchto dvou jazyků se snadno integruje s Objective C. Podobným přístupem pro aplikace pro Android bude použití jeho nativního rozhraní Java. Účelem používání knihoven C a C ++ je chránit nástroje runtime nebo reverzní inženýrství, jako jsou class-dump, class-dump-z, Cycript, nebo Frida.

4.1.10 M10: Mimořádná funkčnost

Než bude aplikace připravena k produkci, vývojový tým v ní často ponechá kód, aby měl snadný přístup k backend serveru, vytvářel logy k analýze chyb nebo přenášel pracovní informace a testovací podrobnosti. Tento kód je pro fungování aplikace cizí, to znamená, že nemá žádné použití pro zamýšleného uživatele, jakmile je aplikace v produkci a je vyžadován pouze během vývojového cyklu. [45]

Rizika mimořádné funkčnosti:

Ve většině případů neškodný kód nenabízí žádnou další výhodu pro protivníka, který získá přístup. V některých případech však tento kód může nést informace týkající se databází, uživatelských údajů, uživatelských oprávnění, koncových bodů API, atd. nebo může deaktivovat funkce, jako je dvoufaktorové ověřování.

Doporučené postupy, jak se vyhnout mimořádné funkčnosti:

Vývojář by měl vědět, že automatizované nástroje nemohou vždy detekovat přítomnost rizika M10. Častěji to vyžaduje ruční zásah před vypuštěním aplikací do aplikačních obchodů. Vývojář by měl před vydáním aplikace provést následující kroky:

- Ujistit se, že v konečné verzi není přítomen žádný zkušební kód.
- Zajistit, aby v nastavení konfigurace nebyly přítomny žádné skryté přepínače.
- Logy by neměly obsahovat popis procesů backend serveru, oprávnění správce, atd.
- Obecně by logy neměly být vůbec popisné.
- Zajistit, aby výrobci OEM nebyli vystaveni úplným systémovým logům.
- Pomocí ProGuard nebo DexGuard zastavit interakci mezi voláními metod a třídami logu.
- Zajistit, aby protivník nemohl nastavit příznak ladění aplikace na hodnotu true.
- Koncové body API, ke kterým aplikace přistupuje, by měly být dobře zdokumentovány.

4.2 2FA

Dvoufaktorové ověření (2FA) je důležitým sekundárním krokem k ochraně dat, peněz a jakékoli další zneužití aplikace na straně uživatele. Dvoufaktorové nebo vícefaktorové ověřování je další přihlašovací/potvrzovací kód pro účet k ochraně citlivých informací.

V dnešní době a zvláště u aplikací, které rozhodují o finančních prostředcích uživatele, již jedno heslo pro přihlášení či potvrzení operace nestačí. Pokud je heslo uživatele uhodnuto, nebo hackeři ukradnou databázi s přihlašovacími informacemi ve formátu prostého textu, pak se z účtu stane snadný cíl. Ověřování pomocí dvou faktorů se snaží tuto chybu vyřešit tím, že před získáním přístupu k vašemu účtu vyžaduje sekundární kód nazývaný jednorázové heslo (OTP) - obvykle šest znaků a generované aplikací pro chytré telefony. Tímto způsobem, i když hacker má vaše heslo, bude stále muset prolomit sekundární kód, což je mnohem obtížnější.

Existuje také snadnější způsob, jak používat 2FA s názvem standard FIDO U2F. Při tomto druhu ověřování používáte fyzický bezpečnostní klíč a vložíte jej do svého počítače, dotknete se tlačítka klíče a jste „automaticky“ přihlášeni.

Ovšem ne každá varianta 2FA je spolehlivá. Při používání 2FA prostřednictvím SMS, hacker může potenciálně zachytit tyto kódy. Ověřování SMS je stále mnohem lepší než 2FA nepoužívat vůbec, ale není nejlepším řešením. [46]

Autentizace uživatele musí být zajištěna řádně a používají se k tomu následující metody k ověření uživatelů:

- Něco, co uživatel zná, například heslo nebo přístupová fráze.

- Něco, co uživatel má, například tokenové zařízení nebo čipová karta.
- Něco, co uživatel je, jako je biometrie.

Hesla/přístupová fráze musí splňovat následující podmínky:

- Vyžadovat minimální délku nejméně sedm znaků.
- Obsahovat číselné i abecední znaky.

Silná hesla/přístupová fráze jsou první linií obrany v aplikaci, protože škodlivý člověk se často nejprve pokusí najít účty se slabými nebo neexistujícími hesly. Pokud jsou hesla krátká nebo snadno uhádnutelná, je pro škodlivého jedince relativně snadné najít tyto slabé účty.

4.2.1 Softwarové možnosti

Aplikace musí podporovat standardní přístup OTP 2FA. Jednorázové heslo (anglicky One-Time Password) je heslo, které je platné pouze pro jedno přihlášení nebo pro provedení transakce. Výhodou tohoto hesla je možnost vyhnout se problémům spojených se standardními stálými hesly, jako je odposlechnutí hesla nebo znovupoužití. Pokud útočník odposlechne jednorázové heslo, jeho znovupoužití již není možné. Naopak nevýhodou je jejich téměř nemožné zapamatování, jelikož se heslo stále mění. Proto je ve většině případů, potřeba využít dalších nástrojů, jako je např. Google Authenticator. [46]

Ať už se jedná o transakce elektronického obchodování nebo kontroly přihlášení/registrace, ověření OTP (jednorázové heslo) by mělo být nedílnou součástí ověření uživatele. Je to rozšířenější a bezpečnější způsob, který je obtížné hacknout.

Nejčastěji využívané aplikace pro OTP jsou:

- Google Authenticator - je bezplatná aplikace pro smartphony od Googlu, která je k dispozici pro Android i iOS. Jeho použití je velmi jednoduché. V aplikaci povolíte dvoufaktorové ověření. Po aktivaci vás aplikace požádá, abyste pomocí telefonu pořídili snímek QR kódu. Po načtení kódu QR začne aplikace Authenticator generovat kódy.
- LastPass Authenticator - používá funkci nazývanou oznámení jedním klepnutím push, která vám umožní přihlásit se jediným kliknutím místo zadávání kódů.
- Microsoft Authenticator – bezplatná aplikace pro ověřování pro Android, iOS a Windows 10 Mobile.

- Authy - bezplatná služba společnosti Authy řeší problém v případě výměny nového smartphonu či ztráty telefonu. Ukládá všechny tokeny 2FA v cloudu na svých serverech. Tímto způsobem je možný přístup ke kódům z jakékoli aplikace Authy, ať už je to na smartphonu, tabletu nebo notebooku Windows nebo Mac. [46]

4.2.2 Hardwarové možnosti

Absolutně nejbezpečnějším způsobem, jak uzamknout své účty pomocí dvoufaktorové autentizace, je použít fyzický bezpečnostní klíč.

Nevýhodou použití bezpečnostního klíče je však to, že pokud ztratíte nebo zlomíte klíč, můžete být uzamčeni ze svých účtů a budete muset přepnout metodu ověřování pomocí druhého faktoru na nový klíč.

N9že jsou uvedeny dva nejčastější typy hardwarového klíče:

- Yubico Authenticator - jedná se o malé zařízení podobné kartě s jedním koncem, které se zasune do standardního portu USB-A. Ověřování proběhne stisknutím tlačítka namísto ručního zadání krátkého kódu. YubiKey je také velmi odolný a vodotěsný, což znesnadňuje likvidaci těchto zařízení. Tento přístup jedním klepnutím funguje pouze pro účty, které podporují výše uvedený standard FIDO U2F. V systému Android potřebujete YubiKey, který podporuje NFC a aplikaci Yubico Authenticator, což je v tomto případě YubiKey 5 NFC. Díky těmto klíčům stačí otevřít telefon Authenticator v telefonu, klepnout na tlačítko poblíž čipu NFC telefonu a kód se zobrazí v aplikaci. Umožňuje snadno přenášet autentizační kódy z jednoho zařízení na druhé.
- Titan Security Key – jde o hardwarový bezpečnostní klíč od Google. Je nabízen v balíčku se dvěma fyzickými zařízeními. Jeden je klíč s USB-A, podobný YubiKey. Druhým je bluetooth klíč, který se může připojit k telefonu bezdrátově. [46]

4.2.3 Biometrická 2FA

Při hledání nejbezpečnější metody dvoufaktorové autentizace (2FA) by biometrie měla přicházet do úvahy jako první. Tato data je velmi těžké replikovat. Je to metoda ověření identity uživatele pomocí části „kdo jsou“, jako je jejich otisk prstu, rysy obličeje, tvar ruky, struktura duhovky nebo hlas.

Tyto faktory obsahují velké množství jedinečných datových bodů, které vyžadují replikaci sofistikované technologie. Proto mnoho organizací považuje biometrickou autentizaci za jednu z nejsilnějších metod autentizace uživatelů. [47]

Klady biometrické 2FA:

- Unikátní data je obtížnější prolomit: používání biometrické autentizace dat má takové jemné variace od jedné osoby k druhé, že bez pokročilých nástrojů je téměř nemožné replikovat.
- Rychlé a pohodlné ověřování: biometrické ověřování umožňuje uživatelům okamžitý přístup k jejich prostředkům. Vše, co musí udělat, je předložit svůj biometrický faktor (obličej, otisk prstu, hlas, apod.). A za předpokladu, že odpovídá údajům uloženým v jejich ověřovateli, bude jim udělen přístup. To eliminuje potřebu přístupových klíčů, karet a dalších tradičních forem 2FA.

4.3 RASP

Anglicky runtime application self-protection; je způsob, jak detekovat útoky uvnitř aplikace a zabránit jim. RASP je relativně nové řešení pro běžné body bezpečnosti aplikací. Software RASP je umístěn v aplikaci nebo v její blízkosti, zatímco běží, aby sledoval a analyzoval provoz a chování aplikace. Pokud je zjištěn problém, řešení RASP může odesílat výstrahy a blokovat jednotlivé požadavky. Je schopen spíše sledovat celé kategorie útoků, než se spoléhat na rozpoznávání znaků konkrétních zranitelných míst.

RASP neurčuje jen to, co se aplikaci hodí, ale také ví, jak se aplikace chová. To snižuje falešné pozitivní výsledky a dělá RASP lepší než jiná bezpečnostní řešení při detekci věcí, jako jsou injekce SQL a útoky skriptování mezi servery (XSS). To také znamená méně manuální práce při procházení bezpečnostními výstrahami a určování, jak reagovat. [48]

4.3.1 Implementace RASP

RASP pracuje nasazením agentů, kteří sedí v blízkosti aplikace, aby sledovali a reagovali na chování aplikace. Každé řešení RASP funguje odlišně, ale tito agenti mohou být na vaší aplikaci, nebo na webových serverech, anebo mohou existovat v prohlížeči.

Nasazení RASP je obvykle celkem snadné, není třeba instalovat nové servery nebo zařízení, překonfigurovat DNS, přepínače nebo vyvažovače zatížení. Není nutné ani měnit kód ani

překompilovat aplikaci. Rychlá implementace dobrého nástroje RASP může ušetřit spoustu času.

4.3.2 Výhody RASP

IT organizace, které nasazují RASP, zaznamenaly řadu výhod pro zabezpečení, provoz a testování. Zde je několik hlavních výhod RASP:

- Viditelnost - díky hloubkové viditelnosti RASP odstraňuje spoustu dohadů z bezpečnosti aplikací. Podrobné zobrazení aplikace umožní zjistit, zda došlo k útoku a co přesně se během útoku děje. Jednoduše dokázat zúčastněným stranám, že aplikace je napadena, může být neocenitelné pro odůvodnění potřeby budoucích bezpečnostních opatření.
- Spolupráce a DevOps - RASP prospívá rozvoji stejně jako zabezpečení - a je to skvělý nástroj pro získání obou týmů na stejnou stranu. Vztah mezi odborníky v oblasti zabezpečení a mezi vývojáři je pro úspěch organizace zásadní, ale komunikační mezery jsou hojné. S průhledností, kterou RASP poskytuje v aplikacích, všichni pracují se stejnými informacemi. Pokud existují problémy, které je třeba opravit, může bezpečnostní tým zaslat vývojářům podrobnou zprávu, která jasně nastíní, o jaký problém jde a jaké opravy jsou nutné k jeho vyřešení. V dnešním rychle se měnícím prostředí jsou vývojáři pod tlakem, aby rychle vydali aplikace. Není čas na bezpečnostní procesy, které přidávají spoustu dalších kroků k životnímu cyklu vývoje softwaru. Neustálé monitorování a analýza dat RASP se dobře integrují s rychlým tempem vývoje.
- Penetrační testování - RASP dokáže podpořit penetrační testovací úsilí zvýšenou viditelností, kterou poskytuje. Pomocí RASP je možné zpočátku strukturovat svůj test a jeho cíle. Rovněž se lze vyhnout duplicitnímu testování tím, že je známo, jaké útoky se dějí, jaká část aplikace již byla testována a které útoky byly úspěšné.
- Reakce na incident – RASP pomáhá protokolovat zabezpečení a dodržování předpisů tím, že umožňuje podávat zprávy o přizpůsobených událostech, jako je například přístup k určité součásti aplikace. Toho je dosaženo bez nutnosti úpravy samotné aplikace.

4.3.3 Volba správného nástroje RASP

Žádný užitečný nástroj pro zabezpečení aplikací nebude bránit výkonu samotné aplikace. Software RASP by měl být lehký a měl by být navržen tak, aby byl při selhání dále zajištěn trvalý provoz aplikace.

Společnost vyvíjející mobilní aplikace pro vysoce specializované bezpečnostní funkce zajišťované vlastními autentizačními a transakčními systémy, ve které byla praktická část zpracována, vyvíjí vlastní RASP software, znám pod názvem Talsec. Tyto autentizační a platební aplikace zohledňují bezpečnostní i uživatelské faktory, využívají robustní back-end, specializované bezpečnostní SDK, pokročilý RASP shielding a kontinuální analýzu hrozeb.

Smartphone se stal nejdůležitějším a nejcennějším přístupovým nástrojem pro digitální služby. S tím roste jeho atraktivita pro všechny druhy útočníků i rozmanitost útoků.

Talsec je kompaktní a snadno použitelná bezpečnostní knihovna, která se vkládá do mobilní aplikace a zajišťuje ji před útoky hackerů. Aplikace je vybavena sadou funkcí s bezpečnostními kontrolami na nejvyšší úrovni pro detekci a obranu před útoky v rizikovém prostředí mobilního telefonu, mimo kontrolu vydavatele aplikace. [51]

Talsec chrání před:

- malwarem,
- man-in-the-middle útokem,
- cheat nástroji,
- překryvným (overlay) útokem,
- sociálním inženýrstvím,
- vložením kódu,
- keyloggerem,
- dešifrováním aplikace.

Talsec RASP udržuje mobilní zařízení a finanční data v bezpečí. Zajišťuje svým zákazníkům nezbytnou úroveň zabezpečení a ochrany. Talsec je implementován jako specializovaná knihovna přímo v aplikaci, monitoruje jeho fungování, okamžitě reaguje na hrozby a útoky.

Výhody Talsec:

- Rychlá a snadná integrace do mobilní aplikace.
- Úplné zmatení zdrojových kódů, včetně řetězců.

- Na požádání mohou být implementovány další přizpůsobitelné kontroly a funkce.
- Rámec založený na vlastní bezpečnostní knihovně a ke zmatení pro potenciální hackery.
- Bohatý kontrolní panel.
- Konfigurovatelné odpovědi (Kill, Info & kill, Info, Ignore) na jednotlivé hrozby.
- Pravidelné aktualizace pro ochranu před nejnovějšími hrozbami.
- Řešení splňuje požadavky definované v PSD2 / RTS.

Talsec pomáhá splnit bezpečnostní standardy pro mobilní aplikace. Talsec může bránit mobilní aplikace před bezpečnostními riziky zveřejněnými v OWASP „Mobile Top 10“: V8: Odolnost proti zpětnému inženýrství.

Dále Talsec poskytuje komplexní přístup k zabezpečení mobilních aplikací, který je popsán v tab. 6.

Tab. 6: Bezpečnostní prvky zabezpečení aplikace [51]

Odolnost proti zpětnému inženýrství	Ochrana uživatele	Nástroje ke zvýšení bezpečnosti
Pokročilé detekce root / jailbreak	Ochrana proti překrytí	Zabezpečené úložiště
Detekce režimu ladění	Správa přístupových služeb	Dynamické připínání certifikátů
Detekce emulátoru / simulátoru	Kontrola malwaru	Obfuscator řetězce
Detekce neoprávněné manipulace		
Přebalení ovládání		
Otisk zařízení		

5 VYHODNOCENÍ PŘÍNOSŮ NÁVRHU

S rostoucím používáním chytrých telefonů se navrhuje a vyvíjí celá řada bezpečnostních řešení. Mnoho bezpečnostních řešení se nedokáže vypořádat s pokročilými útoky a není správně navrženo pro platformy smartphonů. Proto je třeba vynaložit úsilí pro efektivní bezpečnostní rámec.

Rámec pro finanční služby musí zajišťovat pokročilé zabezpečení, aby se zabránilo podvodům, zpětnému inženýrství a neoprávněné manipulaci s aplikací. Cílem je chránit citlivá data zákazníku a image značky. Správnou implementací bezpečnostních postupů se docílí vysoce zabezpečeným transakcím a platbám.

V e-commerce je jedním z důležitých faktorů zajistit bezpečnost zákazníka tím, že se zamezí zneužití spotřebitelských dat, jako e-mailové adresy, telefonního čísla, kreditní karty, atd.). Záměrem je vybudování důvěry pomocí funkcí zabezpečení na nejvyšší úrovni.

Díky vývojové metodice OWASP bylo zajištěno několik základních bezpečnostních požadavků organizace na zabezpečení mobilní aplikace. Mezi tyto požadavky patří:

- modelování architektury, designu a hrozeb,
- ukládání dat a soukromí,
- kryptografie,
- ověřování a správa relací,
- síťová komunikace,
- integrace platformy,
- kvalita kódu a sestavení,
- odolnost.

Pro ověřování požadavků je následně nutné provést testování zabezpečení mobilní aplikace. K těmto účelům dále slouží příručka OWASP Mobile Security Testing Guide (MSTG).

Šetřením slabostí v mobilních aplikací bylo zjištěno, že:

- nejčastějším problémem je nezabezpečené ukládání dat (až 76 % mobilních aplikací),
- hackeři jen zřídka potřebují fyzický přístup k smartphonu, aby ukradli data (89 % zranitelností lze provést pomocí malwaru)
- většina případů je způsobena slabostí bezpečnostních mechanismů (74 % a 57 % v případě aplikací pro iOS a Android a 42 % v případě komponent na straně serveru),

- mnoho kybernetických útoků závisí na nepozornosti uživatele; eskalující privilegia nebo postranní software mohou připravit cestu pro škodlivý útok.

Zranitelnosti na straně klienta:

- 60 % zranitelností je na straně klienta,
- 89 % zranitelných míst lze zneužít bez fyzického přístupu,
- 56 % zranitelných míst lze zneužít bez administrátorských práv (jailbreak nebo root).

Aplikace pro Android mají tendenci obsahovat kritickou zranitelnost o něco častěji než zranitelnosti napsané pro iOS (43 % vs. 38 %). Tento rozdíl však není významný a celková úroveň zabezpečení mobilních aplikačních klientů pro Android a iOS je zhruba stejná. Asi třetina všech zranitelností na straně klienta pro obě platformy jsou vysoce riziková.

Právě tomuto problému z velké části zabraňuje dvou či multifaktorová autentizace aplikovaná v tomto bezpečnostním rámci.

Pro další fázi monitorování, testování a ochranu proti útokům slouží RASP aplikace Talsec. Ta v aplikaci slouží pro:

- možnosti detekce neoprávněné manipulace,
- přidává funkce ochrany do běhového prostředí aplikace,
- zvyšuje úroveň ochrany před škodlivými útoky.

Je nutné podotknout, že RASP ochrana slouží pouze jako dodatečný bezpečnostní mechanismus, který nenahrazuje bezpečnostní prvky sloužící k autentizaci. Jejich účelem je spíše odrazení nebo zpomalení útočníka. RASP je jen jedna část z celkové hloubky obrany.

Kombinací znalosti bezpečnostních standardů, dodržením legislativních pravidel a použitím navrženého bezpečnostního rámce vzniká vysoká míra zabezpečení mobilní platební aplikace.

ZÁVĚR

Cílem diplomové práce bylo seznámit čtenáře s legislativou a bezpečnostními standardy ve sféře vývoje platebních nástrojů, ochrany dat uživatelů a platebních procesech. V Evropě jsou eIDAS, PSD2 a GDPR hlavní hnací silou pro stanovení společných evropských rámců pro výměnu osobních údajů a údajů o totožnosti. Evropa tím vysílá jasný signál směrem k jednotným a spolehlivým právním předpisům pro všechny evropské země. Z bezpečnostních standardů byly popsány PCI DSS, PA-DSS a Dodatek E: MFS od FFIEC.

Dalším záměrem práce bylo popsat podrobněji současné typy mobilních plateb. Jak bylo ukázáno, zájem o mobilní peníze je zřejmý, standardizační úsilí stále pokračuje a stále probíhá hledání správných obchodních modelů a úspěšných přístupů.

S rychlým přijetím a růstem mobilních technologií se mobilní peněžní služby přijímají po celém světě, i když v rozvinutých a rozvíjejících se zemích různými způsoby. Mobilní peníze budou v budoucnu stále více využívány vedle standardních platebních způsobů jako je hotovost, šeky, kreditní karty a debetní karty.

Mobilní finanční služby zde nejen zůstanou, ale také se staly základem moderních bankovních praktik. Mobilní zpracování plateb musí být globální. Jediným způsobem, jak zajistit jednotné zpracování, je vývoj a přijetí globálních standardů.

Zpracování bezpečnostního rámce proběhlo pro firmu vyvíjející platební nástroje. Při vývoji platebních aplikací je důležité se zaměřit na stabilitu a správnost kódu, a mimo to i na prevenci a odolnost proti útokům. Bezpečnostní rámec je sestaven ze tři důležitých pilířů, kterými jsou dodržování vývojové metodiky OWASP, používání dvoufaktorové autentizace a implementace ochrany aplikace pomocí RASP.

„Souboj“ mezi vývojáři mobilních aplikací a útočníky je nekonečný a nelze jej definitivně vyhrát, takže obránci musí vybudovat nejdokonalejší ochranu, používat nejméně známé nástroje pro útočníka a postupně je vylepšovat. Pro tyto účely je používán proprietární nástroj Talsec.

SEZNAM POUŽITÉ LITERATURY

[1] Security and Data Protection. *BUSINESS TECHNOLOGY STANDARD* [online]. [cit. 2020-01-05]. Dostupné z: https://www.managebt.org/book/strategy-and-governance/security-and-data-protection/

[2] BARLOW, John. A Declaration of the Independence of Cyberspace. *Electronic Frontier Foundation* [online]. [cit. 2020-01-16]. Dostupné z: https://www.eff.org/cyberspace-independence

[3] Cyberspace. *LEXICO* [online]. [cit. 2020-01-16]. Dostupné z: https://www.lexico.com/definition/cyberspace

[4] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. [cit. 2020-01-18].

[5] Zákon č. 181/2014 Sb.: Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). *Zákony pro lidi* [online]. [cit. 2020-01-18]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

[6] World Internet Users and 2020 Population Stats. Internet World Stats [online]. [cit. 2020-01-19]. Dostupné z: https://www.internetworldstats.com/stats.htm

[7] Kolizní otázky internetových právních vztahů: Delokalizace právních vztahů na internetu. MUNI IS: Informační systém Masarykovy univerzity [online]. [cit. 2020-01-19]. Dostupné z: https://is.muni.cz/do/1499/el/estud/praf/js09/kolize/web/index.html

[8] Cybersecurity. *Merriam-Webster* [online]. [cit. 2020-01-19]. Dostupné z: https://www.merriam-webster.com/dictionary/cybersecurity

[9] *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020.* [online]. [cit. 2020-01-20]. Dostupné z: https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf s. 5

[10] KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7. [cit. 2020-01-25]

[11] HSU, D. Frank a Dorothy MARINUCCI. Advances in cyber security: technology, operations, and experiences. New York: Fordham University Press, 2013. ISBN 978-0-8232-4456-0. [cit. 2020-01-26]

[12] CIA: Důvěrnost-Integrita-Dostupnost. *Clever and Smart* [online]. [cit. 2020-02-03]. Dostupné z: https://www.cleverandsmart.cz/duvernost-integrita-dostupnost/

[13] CIA: Je důvěrnost, integrita a dostupnost dostačující? *Clever and Smart* [online]. [cit. 2020-02-18]. Dostupné z: https://www.cleverandsmart.cz/cia-je-duvernost-integrita-a-dostupnost-dostacujici/

[14] SCHNEIER, Bruce. *AZ Quotes* [online]. [cit. 2020-02-20]. Dostupné z: https://www.azquotes.com/quote/570039

[15] SCHNEIER, Bruce. *AZ Quotes* [online]. [cit. 2020-02-20]. Dostupné z: https://www.azquotes.com/quote/570035

[16] SCHNEIER, Bruce. *AZ Quotes* [online]. [cit. 2020-02-20]. Dostupné z: https://www.azquotes.com/quote/570040

[17] SCHNEIER, Bruce. *AZ Quotes* [online]. [cit. 2020-02-20]. Dostupné z: https://www.azquotes.com/quote/570047

[18] ZÁKLADNÍ POJMY. *KYBEZ* [online]. [cit. 2020-02-22]. Dostupné z: https://www.kybez.cz/bezpecnost/pojmoslovi

[19] 2019 Data Breach Investigations Report. *Verizon* [online]. [cit. 2020-02-25]. Dostupné z: https://enterprise.verizon.com/resources/reports/dbir/

[20] Co je GDPR a jak bude aplikováno v Česku. GDPR Obecné nařízení o ochraně osobních údajů prakticky prakticky [online]. [cit. 2020-03-02]. Dostupné z: https://www.gdpr.cz/gdpr/co-je-gdpr/

[21] Desatero zpracování pro správce. Úřad pro ochranu osobních údajů [online]. [cit. 2020-03-05]. Dostupné z: https://www.uoou.cz/desatero-zpracovani-pro-spravce/ds-4821/p1=4821

[22] Seznam druhů operací zpracování (ne)podléhajících požadavku na posouzení vlivu na ochranu osobních údajů. Úřad pro ochranu osobních údajů. [cit. 2020-03-08]

[23] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. EUR-lex: Acces to European Union law [online]. 2014, 28.8.214 [cit. 2020-03-10]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0910

[24] Is the EU ready for eIDAS? SECURE IDENTITY ALLIANCE [online]. 2015 [cit. 2020-03-10]. Dostupné z: https://web.archive.org/web/20161122071258/https://www.secureidentityalliance.org/index.php/blog/item/20-eidas-eu-identity-assurance/20-eidas-eu-identity-assurance

[25] COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502. EUR-Lex: Acces to European Union law [online]. 2015, 9.9.2015 [cit. 2020-03-11]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2015_235_R_0002

[26] Dokument konkretizující minimální požadavky na kvalifikované systémy elektronické identifikace a na prostředky pro elektronickou identifikaci v rámci nich vydávané a používané [DKP IDP]: v3.1. In: . Ministerstvo vnitra České republiky, 2019. [cit. 2020-03-12].

[27] SCHWALLER, Mgr. Jan. EIDAS elektronická identita, elektronický podpis - příprava, dopad do praxe …. 2016. [cit. 2020-03-12].

[28] DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. EUR-Lex: Acces to European Union law [online]. 2015, 25.11.2015 [cit. 2020-03-15]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02015L2366-20151223

[29] PSD2 Explained: What is it and why does it matter? TransferWise [online]. 2018, 12.12.2016 [cit. 2020-03-15]. Dostupné z: https://transferwise.com/

[30] Co znamená silné ověření klienta (SCA) a proč se o něm všude mluví? GoPay [online]. 2019, 7.3.2019 [cit. 2020-03-15]. Dostupné z: https://www.gopay.com/blog/co-znamena-silne-overeni-klienta-sca-a-proc-se-o-nem-vsude-mluvi/

[31] COMMISSION DELEGATED REGULATION (EU) 2018/389. EUR-Lex: Acces to European Union law [online]. 2018, 13.3.2018 [cit. 2020-03-15]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R0389

[32] Nařízení (EU) č. 2018/389 - nová pravidla pro poskytovatele platebních služeb. Epravo.cz [online]. 2019, 12.4.2019 [cit. 2020-03-18]. Dostupné z: https://www.epravo.cz/top/clanky/narizeni-eu-c-2018389-nova-pravidla-pro-poskytovatele-platebnich-sluzeb-109129.html

[33] Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures. © 2006-2016 PCI Security Standards Council, LLC. All Rights Reserved., 2016. [cit. 2020-03-20].

[34] Bezpečnostní standardy v oblasti karetních plateb: Jak ochránit platební data svých klientů v souladu s mezinárodními požadavky? Deloitte.: dReport [online]. 2019, 4.12.2019 [cit. 2020-03-20]. Dostupné z: https://www.dreport.cz/blog/bezpecnostni-standardy-v-oblasti-karetnich-plateb-jak-ochranit-platebni-data-svych-klientu-v-souladu-s-mezinarodnimi-pozadavky/

[35] Payment Card Industry (PCI) Payment Application Data Security Standard: Requirements and Security Assessment Procedures. © 2006-2016 PCI Security Standards Council, LLC. All Rights Reserved. 2016. [cit. 2020-03-24].

[36] Appendix E: Mobile Financial Services. FFIEC: IT examination handbook infobase [online]. 2016 [cit. 2020-04-03]. Dostupné z: https://ithandbook.ffiec.gov/it-booklets/retail-payment-systems/appendix-e-mobile-financial-services.aspx

[37] Types of Mobile Payments. Blogs ICEMD [online]. 2016 [cit. 2020-04-12]. Dostupné z: http://blogs.icemd.com/blog-moma-trends-mobile-payments/types-of-mobile-payments/

[38] NFC platby mobilem (NÁVOD). Alza.cz [online]. 2016, 18.5.2020 [cit. 2020-04-15]. Dostupné z: https://www.alza.cz/nfc-platby-mobilem

[39] SOLAT, Siamak. Security of Electronic Payment Systems: A Comprehensive Survey. ResearchGate, 2017. [cit. 2020-04-15]

[40] Haselsteiner, Ernst, and KlemensBreitfuß. Security in near field communication (NFC). Workshop on RFID Security RFIDSec. 2006 [cit. 2020-04-15]

[41] Francis, Lishoy, et al. "Potential misuse of NFC enabled mobile phones with embedded security elements as contactless attack platforms." Internet Technology and Secured Transactions, 2009.ICITST 2009. International Conference for. IEEE, 2009 [cit. 2020-04-16]

[42] The Mobile Money Revolution: Part 1: NFC Mobile Payments. ITU Committed to connecting the world [online]. 2013 [cit. 2020-04-15]. Dostupné z: https://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000200001PDFE.pdf

[43] ENISA. Security of Mobile Payments and Digital Wallets. European Union Agency For Network and Information Security, 2016. [cit. 2020-04-20]

[44] OWASP Mobile Top 10. OWASP [online]. 2016 [cit. 2020-05-15]. Dostupné z: https://owasp.org/www-project-mobile-top-10/

[45] OWASP Mobile Top 10: A Comprehensive Guide For Mobile Developers To Counter Risks. Appsealing [online]. 2020 [cit. 2020-05-15]. Dostupné z: https://www.appsealing.com/owasp-mobile-top-10-a-comprehensive-guide-for-mobile-developers-to-counter-risks/

[46] What is two-factor authentication, and which 2FA solutions are best? PCWorld: from IDG [online]. 2019 [cit. 2020-05-20]. Dostupné z: https://www.pcworld.com/article/3225913/what-is-two-factor-authentication-and-which-2fa-apps-are-best.html

[47] Biometric Two-Factor Authentication (2FA) – Pros and Cons. JumpCloud: Directory-as-a-Service [online]. [cit. 2020-05-23]. Dostupné z: https://jumpcloud.com/blog/biometric-totp-2fa

[48] RASP 101: What Is Runtime Application Self-Protection? RAPID7 Blog [online]. 2019 [cit. 2020-06-04]. Dostupné z: https://blog.rapid7.com/2019/09/04/rasp-101-what-is-runtime-application-self-protection/

[49] JAŠEK, Roman a David MALANÍK. Bezpečnost informačních systémů. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013, 1 online zdroj. ISBN 9788074543128 [cit. 2020-06-07]. Dostupné také z: http://hdl.handle.net/10563/25821

[50] STALLINGS, William, Lawrie BROWN, Michael D BAUER a Michael HOWARD. Computer security: principles and practice. 2nd ed. Boston: Pearson, c2012, xxii, 788 s. ISBN 9780132775069 [cit. 2020-06-09].

[51] Mobile apps are unsecured against hacking attacks and threats - your financial data and users at gunpoint. Talsec [online]. [cit. 2020-06-15]. Dostupné z: https://talsec.app/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

2FA	Dvoufaktorová autentizace je druhá vrstva zabezpečení pro ochranu účtu nebo aplikace.
API	Application Programming Interface - rozhraní mezi 2 systémy/aplikacemi.
CIA	Triáda kybernetické bezpečnosti složena ze tří atributů: C-Confidentiality (důvěrnost); I-Integrity (celistvost); A-Availability (dostupnost).
CVV	Card Verification Value je kód, který se nachází na zadní straně platební karty.
eIDAS	Je zkratka pro nařízení Evropské unie č. 910/2014 o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním evropském trhu.
GDPR	Obecné nařízení o ochraně osobních údajů (anglicky General Data Protection Regulation).
HCE	Emulace hostitelské karty (anglicky Host card emulation, HCE) je softwarová architektura sloužící k přenosu informací mezi terminálem, poskytujícím radiový přenos NFC, a aplikací mobilního telefonu s NFC, imitující bezdrátovou platební kartu.
KB	Zkratka pro kybernetickou bezpečnost.
MFS	Mobile Financial Services; mobilní finanční služby. V této práci často spojováno s přílohou E vydanou americkou FFIEC.
MITM	Man-in-the-middle je název útoku na kryptografii. Jeho podstatou je snaha útočníka odposlouchávat komunikaci mezi účastníky tak, že se stane aktivním prostředníkem.
OTP	Jednorázové heslo (anglicky One-Time Password) je heslo, které je platné pouze pro jedno přihlášení nebo pro provedení operace.
OWASP	Open Web Application Security Project je komunitou vývojářů, která vytváří metodiky, dokumentaci, nástroje a technologie v oblasti zabezpečení webových a mobilních aplikací.
PA-DSS	Payment Application Data Security Standard, tedy standard zabezpečení dat platebních aplikací.

PAN Číslo platební karty, číslo primárního účtu (anglicky Primary Account Number).

PCI DSS Jde o mezinárodní bezpečnostní standard (anglicky Payment Card Industry Data Security Standard), který má za cíl zamezit krádežím, únikům a následnému zneužití dat o držitelích platebních karet.

RASP Runtime application self-protection je bezpečnostní technologie, která využívá runtime zařízení k detekci a blokování útoků využitím informací z uvnitř spuštěného softwaru.

SCA Anglicky Strong Customer Authentication je silné ověření zákazníka. Jedná se o bezpečnostní mechanismus, který má za cíl snížit riziko vzniku podvodů v důsledku kompromitovaného hesla.

SE Secure Element (SE) je čip odolný proti neoprávněné manipulaci s bezpečným mikrokontrolérem, který je navržen pro bezpečné ukládání důvěrných a kryptografických dat. SE je kritickou součástí každé mobilní platební aplikace.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK