Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Útoky a hacking v online prostředí a ochrana před nimi

Bc. Lukáš Gregora

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Lukáš Gregora

Informatika

Název práce

Útoky a hacking v online prostředí a ochrana před nimi

Název anglicky

Attacks and hacking in the online environment and protection against it

---

Cíle práce

Hlavním cílem diplomové práce je definování a simulace útoků v online prostředí a možné způsoby jak se jim bránit.
Součástí dílčích cílů je
- sestavení uceleného přehledu historického, současného a budoucího vývoje hackingu a technologií, které se v online prostředí využívají,
- sumarizace možných forem útoků v online prostředí a jejich četností, které budou implementovány na izolovaném prostředí s názornou ukázkou možných způsobů ochrany,
- zachycení aktuálního pohledu na hacking v online prostředí z právního hlediska,
- vytvoření příkladů využití zařízení, které umožňuje sledovaní provozu WiFi sítí.

Na základě zjištěních poznatků bude provedena diskuse a výsledky pozorování. Formulace závěrů.

Metodika

Teoretická část diplomové práce je založena na studiu odborných informačních zdrojů. Praktická část je zaměřena na sestavení uceleného přehledu metod použitých k útokům v online prostředí, způsoby ochran před nimi a srovnání jejich četností. Útoky budou simulovány na izolovaných webových stránkách, které budou záměrně obsahovat bezpečnostní nedostatky, na kterých budou demonstrovány formy útoků. K testování, simulaci a ověřování některých útoků bude využito zařízení WiFi Pineapple, které umožňuje sledovat provoz WiFi sítě. Na základě získaných poznatků ze simulací a praktického využití uvedeného zařízení bude provedena analýza výsledků, diskuze stavu zabezpečení sítě WiFi a chování uživatelů.

Doporučený rozsah práce

60 – 80 stran

Klíčová slova

útoky, hacking, ochrana, wifi, online, web

Doporučené zdroje informací

BEAVER, Kevin, DAVIS, Peter T.. Hacking Wireless Network For Dummies. 5. vydání. Vydavatel: John Wiley & Sons, Inc, 2005. ISBN 978-0764597305

CLARKE, Justin. SQL Injection Attacks and Defense. 2. vydání. Vydavatel: Syngress, 2012. ISBN 978-1597499637

CHAUHAN, Sudhanshu, PANDA, Nutan Kumar. Hacking Web Intelligence: Open Source Intelligence and Web Reconnaissance Concepts and Techniques. 1. vydání. Vydavatel: Syngress, 2015. ISBN 978-0128018675

Kümmel, Roman. Cross-Site Scripting v praxi. 1. vydání. Vydavatel: SOOM, 2011. ISBN 978-80-86062-34-1

SCAMBRAY, Joel, McCLURE, Stuart, KURTZ, George. Hacking bez tajemství. 1. vydání. Vydavatel: Computer Press, 2001. ISBN 80-7226-549-0

SCAMBRAY, Joel, SHEMA, Mike. Hacking bez tajemství – Webové aplikace. 1. vydání. Vydavatel: Computer Press, 2003. ISBN 80-7226-769-8

Předběžný termín obhajoby

2016/17 LS – PEF

Vedoucí práce

Ing. Václav Lohr, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 18. 10. 2016

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 24. 10. 2016

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 26. 02. 2017

Čestné prohlášení

Prohlašuji, že svou diplomovou práci „Útoky a hacking v online prostředí a ochrana před nimi“ jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 28. 3. 2017 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Václavu Lohrovi, Ph.D. za odborné vedení práce a cenné rady, které mi pomohly tuto práci zkompletovat. Děkuji katedře informačních technologií za zorganizování diplomantského semináře, který poskytl cenné zkušenosti, připomínky a poznatky. V neposlední řadě, bych chtěl poděkovat své rodinně, přítelkyni, přátelům a kolegům za pochopení a podporu, kterou mi při psaní této práce poskytli.

Útoky a hacking v online prostředí a ochrana před nimi

Souhrn

Diplomová práce je zaměřena na útoky a hacking v online prostředí a ochranu před nimi. V přehledu řešené problematiky byl definován pojem hacking a s ním spjaté pojmy, včetně rozdělení hackerů podle chování a smýšlení. V dalších částech byl zachycen historický, aktuální a budoucí vývoj hackingu s důležitým pohledem na právní legislativu, která je z hlediska právních systémů odlišná. Za využití aktuálních a hackery využívaných technologií, byla provedena sumarizace aktuálních typů útoků a u zvolených typů byla provedena jejich implementace v rámci izolovaných webových stránek s následným souhrnem možných ochran. Praktická část je zaměřena na využití zařízení WiFi Pineapple k analýze současné situace uživatelů využívajících veřejných Wi-Fi sítí a jejich zařízení. Za využití výše zmíněného zařízení, byl proveden výzkum formou pokusných měření a na základě jejich statistické a analytické analýzy bylo zjištěno, že až 17 % zaznamenaných zařízení je potencionálně napadnutelných zvolenou formou útoku. V rámci následné analýzy bylo provedeno vyhodnocení stanovených hypotéz, očekávání a předpokladů, které byly zaměřeny na vliv okolních aspektů a hodnoty zařízení na využívání veřejných Wi-Fi sítí.

Klíčová slova: útoky, hacking, bezpečnost, ochrana, online, internetové technologie, Wi-Fi

Attacks and hacking in the online environment and protection against it

Summary

The diploma thesis is focused on the attacks and hacking in online environment and protection against them. In the theoretical part was the definition of the hacking and related terms with him, including a distribution of hackers by their behaviour and mentality. In other parts was captured historical, current and future developments of hacking, with important insight into law legislation, that is different from the perspective of legal systems. With use of the current technologies used by hackers were summarized current types of attacks and for selected types, has performed their implementation in the isolated web pages with the subsequent summary of possible protections. The practical part is focused on the use of Wi-Fi Pineapple equipment to analyse the current situation of users utilizing public Wi-Fi networks and their devices. Using the above-mentioned apparatus was conducted research through experimental measurements and on the basis of statistical and analytical analysis showed that up to 17 % of the recorded devices (users) is potentially countervailable by selected form of attack. In a follow-analysis was evaluate the hypotheses, expectations and assumptions, which were focused on the effects of environmental aspects and price values of devices using public Wi-Fi networks.

Keywords: attacks, hacking, security, protection, online, internet technology, Wi-Fi

Obsah

Seznam obrázků

Seznam tabulek

Seznam grafů

1. Úvod

Teoretická část práce je zaměřena na sestavení historického, současného a budoucího přehledu bezpečnostních nedostatků a technologií, které se u nich využívají. Nedílnou součástí je i zachycení aktuálního pohledu na hacking v online prostředí z hlediska legislativy, která je z pohledu kontinentálního a angloamerického právního systému odlišná.

Součástí teoretické i praktické části práce je definování a simulace útoků v online prostředí, které jsou simulovány na izolovaných webových stránkách, které jsou dostatečně informativní ve věci jejich účelu, aby nedošlo k nechtěnému přístupu nezainteresovaných uživatelů. Na webových stránkách jsou prakticky ukázány bezpečnostní nedostatky, které byly vybrány na základě možnosti jejich implementace a způsoby, kterými se před nimi lze bránit. I přes skutečnost, že se vývojáři webových aplikací a stránek snaží dělat pro bezpečnost maximum, tak jejich důkladné otestování nezamezí možným bezpečnostním incidentům. Aplikace není možné připravit na doposud neznámé hrozby, které se v budoucnu mohou objevit, a proto je důležitá i následná údržba, která zajistí, že nedojde ke zneužití nově objevených bezpečnostních nedostatků.

Praktická část práce je založena na výzkumu, který se skládá z pokusných měření za účelem získání kvantitativních i kvalitativních dat pro následnou analýzu. Měření byla prováděna za využití zařízení WiFi Pineapple, které slouží pro monitorování provozu bezdrátových sítí Wi-Fi a za pomocí dostupných modulů, funkcí a dílčích součástí byl vytvořen dostatečný základ pro provedená měření. Získaná data byla standardizována o vlivy okolních aspektů a analyticky a statisticky zkoumána, za účelem ověření stanovených očekávání, předpokladů a hypotéz, které v konečném důsledku vypovídají o uživatelích veřejných Wi-Fi sítí. Na základě zjištěných poznatků, byla provedena diskuze nad úrovní bezpečnosti veřejných Wi-Fi sítí a chování uživatelů.

2. Cíl práce a metodika

2.1. Cíl práce

Hlavním cílem diplomové práce je definování a simulace útoků v online prostředí a možné způsoby jak se jim bránit.

Součástí dílčích cílů je:

- sestavení uceleného přehledu historického, současného a budoucího vývoje hackingu a technologií, které se v online prostředí využívají,
- sumarizace možných forem útoků v online prostředí a jejich četností, které budou implementovány na izolovaném prostředí s názornou ukázkou možných způsobů ochrany,
- zachycení aktuálního pohledu na hacking v online prostředí z právního hlediska,
- vytvoření příkladů využití zařízení, které umožňuje sledovaní provozu Wi-Fi sítí.

Na základě zjištěních poznatků bude provedena diskuse a výsledky pozorování. Formulace závěrů.

2.2. Metodika

Teoretická část diplomové práce je založena na studiu odborných informačních zdrojů. Praktická část je zaměřena na sestavení uceleného přehledu metod použitých k útokům v online prostředí, způsoby ochran před nimi a srovnání jejich četností. Útoky budou simulovány na izolovaných webových stránkách, které budou záměrně obsahovat bezpečnostní nedostatky, na kterých budou demonstrovány formy útoků. K testování, simulaci a ověřování některých útoků bude využito zařízení WiFi Pineapple, které umožňuje sledovat provoz Wi-Fi sítě. Na základě získaných poznatků ze simulací a praktického využití uvedeného zařízení bude provedena analýza výsledků, diskuze stavu zabezpečení sítě Wi-Fi a chování uživatelů.

3. Přehled řešené problematiky

Bezpečnost v online prostředí je v dnešní době nedílnou součástí každodenního života lidí. V době, která směřuje k stále větší integraci zařízení, které jsou připojené k celosvětové síti Internet tzv. **IoT**[1], narůstá riziko bezpečnostních incidentů. Z toho důvodu je kladen (měl by být kladen) stále větší důraz na bezpečnost uživatelských či klientských dat, protože únik dat je v dnešní době závažným a v některých případech i mediálně zveřejněným problémem, který dokáže otřást se stabilitou a důvěryhodností společnosti. (1)

V přehledu řešené problematiky je v úvodu vysvětlen, definován a rozdělen pojem *hacking* v takové míře, aby byla dostatečná pro následné řešení praktické části práce. Skládá se z několika odlišných oborů a celků, které určují, že hacker nemusí být jen záškodník a zloděj, ale může být společnosti prospěšný. Záleží jen na tom, jakou cestou se vydá.

V následujících podkapitolách byl sestaven ucelený přehled historického, současného a budoucího vývoje *hackingu*, který je doplněn o vhodné grafy znázorňující nárůst sledovaných útoků v průběhu času. Zaměření na právní aspekty, kauzy a technologie, které jsou v online prostředí útočníky využívány k odcizení citlivých dat.

Na základě znalosti technologií a poznatků z předcházejících kapitol, byly na izolovaném webovém prostředí implementovány vybrané formy útoků a bezpečnostních nedostatků, se kterými se může běžný uživatel setkat a současně s názornou ukázkou možných způsobů ochran.

3.1. Definice

Hacking je termín, který je často považován za škodlivou a protizákonnou činnost, která má za úkol vylákat z oběti požadované údaje, které jsou následně útočníkem zneužívány pro uspokojení jeho cílů. Ale jedná se i o činnost, která v dobrých rukou je společnosti prospěšná. (2)

[1] **IoT** (Internet of Things) lze přeložit jako Internet věcí a představuje propojení vestavěných zařízení s internetem, např. chytré pračky, ledničky, domy, televize, … které připojením k celosvětové síti Internet, umožní efektivní řízení a správu zdrojů.

Nejlépe ho lze vyjádřit následující definicí:

"Hacking je získávání přístupu (chtěného nebo nechtěného) k počítači a pozorování, kopírování nebo vytváření dat (zanechávání stop) bez záměru jejich poškození nebo s úmyslem poškodit počítač." (3 str. 1) Vlastní překlad

Hackera lze na základě definice rozdělit podle jeho chování, zkušeností, metod a technologií, které ke své činnosti využívá. Pokud se zaměříme na rozdělení podle chování, tak základní rozdělení je do tří skupin, na ty, kteří tak činí protizákonně, v souladu se zákonem a na ty, kteří stojí na pomezí. (4)

Úzce spjatým pojmem s hackingem je tzv. *cracking* nebo také crackování, je technika prolamování se do počítačů a aplikací. V podstatě se jedná o podmnožinu hackingu, protože jde o specifickou činnost, která se zaměřuje na způsobení škody nebo odcizení dat. Počínání crackerů je v posledních desetiletích úzce spjato s vývojáři her a programů, kterým jsou jejich výtvory pomocí reverzibilního inženýrství modifikovány a šířeny P2P[2] sítěmi mezi uživateli bez zakoupených licencí. Slibným řešením je technologie od společnosti DENUVO z roku 2014, která se opakovaným šifrováním a dešifrováním stává odolnou na běžné metody crackování. (5)

3.1.1. White Hat

Lze volně přeložit jako „*Bílá čepice*“ nebo také Ethical Hacker (etický[3] hacker), který se chová v souladu se svým etickým kodexem[4] a ten mu neumožňuje chovat se v rozporu se zákonem a etickými mravy, protože by to bylo v rozporu s jeho kodexem. Etický hacker bývá většinou vázán smlouvou, na základě které provádí bezpečnostní testy svěřené aplikace, webových stránek nebo systémů. (4)

Pro bezpečnostní testování se využívají zpravidla velmi zkušení programátoři nebo konzultanti, kteří mají mnohaleté zkušenosti a potřebné znalosti o tom, jak zkoumaná aplikace a technologie fungují. Často jsou rekrutováni z řad neetických hackerů, kteří si svojí protizákonnou činností získaly zkušenosti a reference z oboru. Při svém počínání využívají

[2] **P2P** je v počítačových sítích přenos informací mezi dvěma klienty
[3] Slovo **Etika** pochází z řeckého slova *„éthos“,* které vyjadřuje charakter člověka ve vztahu ke společnému mravu, způsobu jednání, postoji a smýšlení osob (49)
[4]**Kodex** je dokument, který upravuje pravidla práce v organizacích a profesích, příkladem může být Hippokratova přísaha nebo etický kodex advokáta

stejných nástrojů a technik, které jsou využívány black hat hackery. Oproti kterým, ale musí zároveň využívat plánování, specifické nástroje a komplexní testovací metody, které jim umožní opravit bezpečnostní problémy před útočníkem a zamezit tak jejich zneužití. (6)

3.1.1.1. Testování

V případě etického hackera není vhodné o jeho činnosti hovořit jako o hackování, protože svým počínáním provádí testování svěřené aplikace. Testy jsou zpravidla prováděny automatizovaným softwarem, u kterého se provede nastavení vstupních parametrů podle testované aplikace nebo webových stránek a následně je provedena analýzu výstupů. Testy, které provádí, se nazývají penetrační a zajišťují, že systém odolá známým bezpečnostním hrozbám, které byly prozatím odhaleny např. žebříček OWASP[5] Top 10. Výsledky testů analyzuje a případné nedostatky opraví nebo doporučí jejich opravu na základě svých zkušeností. Testování lze rozdělit do dvou základních kategorií:

Black Box – Jedná se o nejčastěji používanou formu testování, která je prováděna s neznalostí zdrojového kódu aplikace. Aplikace nebo webová stránka se stává pomyslnou bednou, do které útočník nevidí, ale snaží se do ní všemi dostupnými prostředky dostat. To umožní testerovi nastavit stejné podmínky, které by měl potencionální útočník.

White Box – Způsob testování, kdy jsou testerovi ze strany vlastníka poskytnuty informace o aplikaci a její struktuře, případně i zdrojové kódy. Tester tak může testovat aplikaci na úrovni zdrojového kódu a odhalit jeho škodlivé části nebo nedostatky. (7) Aplikace je tedy onou pomyslnou bílou/průhlednou bednou, do které může tester nahlížet a zkoumat její obsah a funkcionalitu.

3.1.2. Black Hat

V případě hackera, který se řadí do kategorie „*Černé čepice*“, hovoříme o úplném opaku etického hackera, neřídí se žádným kodexem a převážně se snaží působit co největší škodu nebo jedná v rámci naplnění vlastních cílů. Činnosti, které provádí, jsou protizákonné a jsou zaměřeny na napadání systémů a aplikací, za účelem získání informací nebo poškození subjektu. Získané informace využívají k vlastnímu prospěchu, který má převážně finanční charakter, případně informace předávají konkurenci nebo vydírají poškozené subjekty. (8)

[5]**OWASP** (Open Web Application Security Project) je neziskovou charitativní organizací, která se zaměřuje na zlepšení bezpečnosti aplikací (49)

Ve většině případu si počínají tak, aby jejich činnost nezanechala žádné stopy. K tomu využívají sofistikovaných metod, aplikací, operačních systémů a hardwaru, které jim umožní zůstat v úplné anonymitě a v ideálním případě bez náznaku úniku informací. Často používají i falešné stopy, kterými svedou vyšetřovatele na nastraženou stopu, kterou odvedou pozornost od své osobnosti nebo skutečného rozsahu incidentu. V některých případech se může jednat i o konkurenční rozepře, které mají za cíl poškodit jinou vládu, skupinu, společnost nebo instituci. (9)

3.1.2.1. Hacktivist

Aktuálně velmi se rozvíjející podkategorií *hackingu*, jedná se o skupiny aktivistů, kteří svým jednáním upozorňují na světové problémy, události a komentáře, mezi které lze zařadit vládní špionáže, války, politické události a fakticky veškeré dění okolního světa. Jejich počínání je v dobrém přesvědčení a pro veřejné dobro, ale stále se jedná o protizákonnou aktivitu. (9)

Skupiny hacktivistů bývají společností přijímány kladně, protože svým působením a smýšlením poskytují reálný pohled na okolní svět nezasažený cenzurou. Jedná se o jednu z jejich hlavních hodnot, která vychází z přesvědčení, že informace jsou určeny pro všechny, a proto prosazují jejich uveřejňování. Příkladem může být nejznámější hacktivistická skupina *Anonymous*, která upozorňuje na veřejné dění. (9)

3.1.3. Gray Hat

Na pomezí Black a White hat se nacházejí hackeři s označením "*Šedivé čepice*", kteří mohou porušovat zákony a etický kodex, ale nečinní tak se špatným úmyslem. Jejich činnost spočívá v zjišťování bezpečnostních nedostatků aplikací, serverů nebo webových stránek, kterými mohou uspokojovat svoji potřebu (dokazují sami sobě svoje zkušenosti) nebo je poskytovat vlastníkovi. Předání může být formou upozorněním na uvedený nedostatek, případně i s doporučením jak jej opravit nebo za příslušnou službu požadují finanční kompenzaci. (4)

Hlavní rozdíl oproti neetickému hackerovi spočívá v tom, že nalezené chyby nezneužívá a veřejně nezveřejňuje, ale nemusí to být pravidlem. Když se nesetká s pochopením ze strany vlastníka nebo je dokonce ignorován, tak často přistoupí k uveřejnění problému, aby vlastníkovi tzv. *otevřel oči*. To může být dosti razantním řešením, kterým vystavuje

v ohrožení sám sebe, i možná osobní data uživatelů, protože takové jednání je protizákonné, i když s možným dobrým úmyslem. (2)

Příkladem může být česká webová stránka *soom.cz,* na které působí převážné čeští a slovenští Gray Hat hackeři, kteří se zabývají psaním článků v oblasti počítačové bezpečnosti a upozorňující na webové stránky, které obsahují bezpečnostní nedostatky. (8)

3.2. Historie

Prvotní datovaná historie hackingu má počátek v roce 1960, kdy na MIT[6] u velmi zkušených programátorů v jazyce FORTRAN[7] a starších jazyků vznikají první *hacky*, které slouží jako jednoduché zkratky k obcházení nebo vylepšování operací systému. V počátcích byl tedy jako hacker považován zkušený programátor, který uměl využít program nad rámec svého určení. (10) (11)

1971 - John Draper (Captain Crunch) vynalezl metodu, která mu umožnila bezplatně telefonovat pomocí píšťalky, kterou získal z cereálií. Skupinám telefonních hackerů se začalo přezdívat „*phreakers*“ a patřili mezi ně i Steve Jobs a Steve Wozniak. Z důvodu zainteresovanosti těchto významných osobností, bylo jejich počínání součástí řady známých filmů. (11)

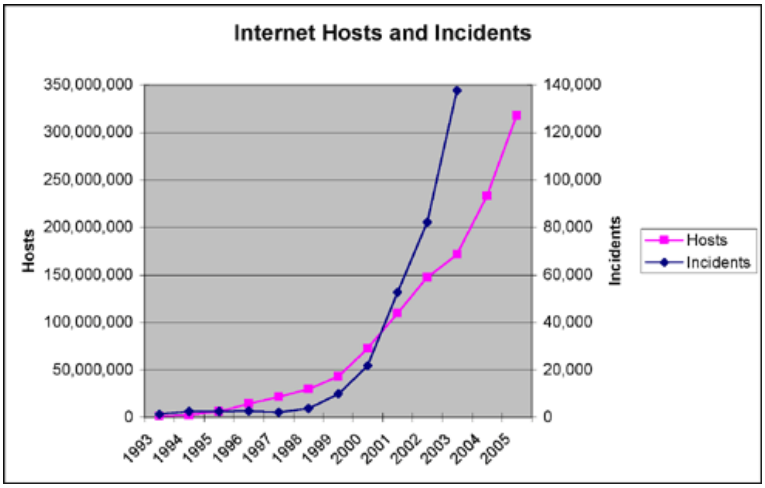
1980s – Vznikají první skupiny hackerů *Legion of Doom* a *Chaos Computer Club*, tematické publikace a v USA vstoupil v platnost zákon o zneužívání výpočetní techniky a sní spojené podvodné činnosti. Pro vykonávání a podporu zákona vznikl CERT[8], který měl za úkol odhalovat rostoucí množství útoků. V rámci nového zákona byl prvním obviněným Robert Tappan Morris, který vytvořil prvního „červa“[9], kterého vypustil na internet během svých studií na Cornellově univerzitě a k vypuštění využil počítače univerzity MIT. Červ způsoboval kromě dalšího šíření i cyklické infikování už napadeného počítače, to mělo za

[6] **MIT** (Massachusetts Institute of Technology) je soukromou výzkumnou univerzitou v USA, která klade silný důraz na vědecký a technologický výzkum.
[7] **FORTAN** – programovací jazyk z 50. let 20. století pro vědecké a numerické výpočty, který se používá do současnosti
[8] **CERT** (Computer Emergency Response Team) byl založen americkými bezpečnostními složkami a dodnes slouží jako zdroj bezpečnostních informací po celém světě pro soukromé i vládní subjekty (12)
[9] **Červ** pochází z anglického slova WORM, které je v počítačové terminologii známo jako program využívající replikace pro rozšíření se na další počítače

následek jeho zpomalení. Podle slov autora prvního červa, měl sloužit pouze pro měření počtu uživatelů připojených k síti internet. (10) (12)

1990s – V devadesátých letech 20. století s růstem počtu uživatelů celosvětové sítě Internet, začal růst počet bezpečnostních incidentů, jejichž růst je patrný z níže uvedeného grafu (viz. Graf 1). Z grafu lze pozorovat značný nárůst uživatelů v devadesátých letech z několika set tisíc uživatelů, na hodnotu vyšší než 50 miliónů, kteří představovali potencionální oběti, na které se útočníci mohli zaměřit.

Graf 1 - Graf vývoje uživatelů internetu a počtu incidentů v letech 1993-2005



Zdroj: OPPENHAIMER, Alan B., WHITAKER, CHARLES H. The rate of hacking incidents per year. [Online] Dostupné z: http://www.opendoor.biz/isfym/Chapter/2.4.html

S rostoucí popularizací sítě Internet roste i důmyslnost útočníků, kteří přicházejí na způsoby, kterými mohou využít „díry“[10] v operačním systému a vzdáleně ho ovládat. S tím, jak byly systémy vylepšovány a zbavovány svých bezpečnostních nedostatků, museli hackeři vyvíjet větší úsilí k získání „zadních vrátek“[10] do systému. Tím začal věčný souboj mezi vývojáři a útočníky, který neutichá a trvá dodnes. Současně pokračuje i hon na hackery, kteří páchají trestnou činnost na bankovní instituce a napadají webové stránky a aplikace, ve většině případů končí dopadením a odsouzením s jejich odnětím svobody. (11) (10)

2000s – Boj s internetovou kriminalitou stále pokračuje a nabývá na intenzitě, objevuje se stále větší množství hackerů, kteří sofistikovanými metodami útočí na společnosti, vládní

[10] **Díry** z anglického slova holes, jsou v počítačové terminologii chyby v kódu, které útočník využívá k vniknutí do systému, někdy jsou též nazývané jako zadní vrátka nebo backdoors. Tyto chyby mohou být neúmyslné, ale může se jednat o mstu nebo pojistku programátora.

a bezpečnostní složky. I přes značný pokrok v oblasti internetových technologií, se stále rozšiřují DDoS[11] útoky, které mají za cíl ochromit internetový obsah a vynucovat finanční prostředky od poškozených subjektů. Objevují se nové formy útoků, které se zaměřují na mobilní a herní zařízení, za účelem obcházení hesel nebo prolomení ochran tzv. *cracking*. (10) (11)

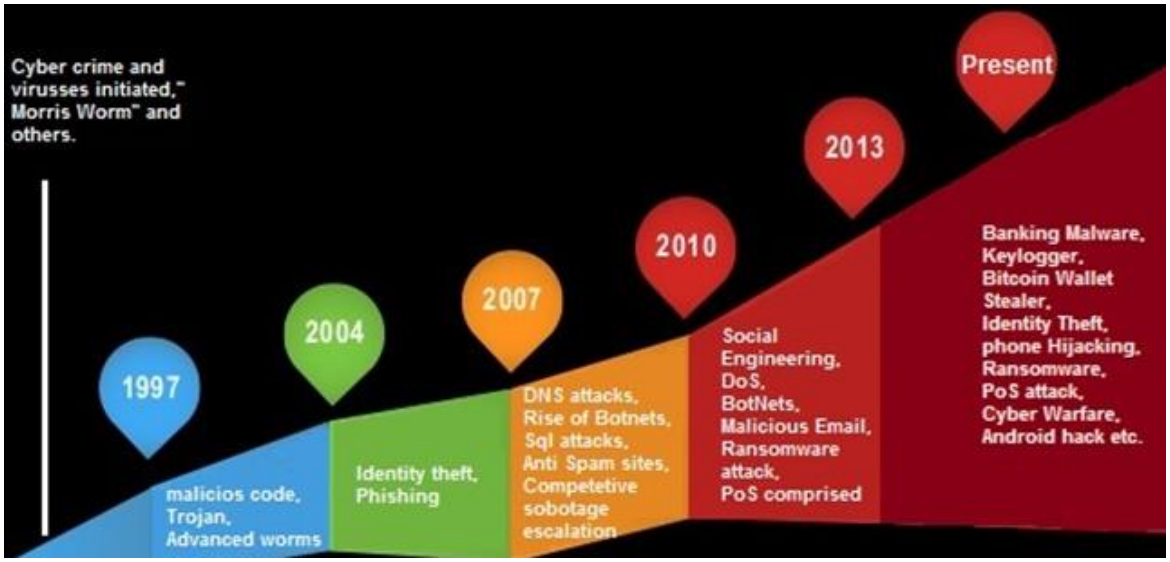
3.2.1. Aktuální situace

V dnešní době, která je zaměřena na internetifikaci do každodenních životů tzv. IoT, se rozrůstají počty potencionálních obětí. Dosud znamenala škoda, kterou hacker způsobil finanční ztráty, ale nyní je potencionálně ohroženo lidské zdraví a majetek, protože veškeré zařízení kolem nás začíná být internetifikováno včetně aut, domů, vlaků a spotřebičů, tím vzrůstá riziko jejich napadení.

Příkladem poslední doby je událost, kdy skupina hackerů využila k masivnímu DDoS útoku milióny kamer, termostatů, žárovek a dalších zařízení připojených k internetu. Při svém počínání se chytře zaměřily na uvedená zařízení, protože mají minimální bezpečnostní opatření a jsou tak snadno zneužitelná k dalším činnostem. (13)

Níže uvedená infografika (viz. Obrázek 1) znázorňuje vývoj útoků během posledních dvou desetiletí. V současné době jsou nejvíce rozšířené různé šifrovací viry tzv. *ransomware*, krádeže identit, útoky na platební terminály a zasílání podvodných zpráv tzv. *phising*. Útoky se tedy začaly zaměřovat na část komunikace, kde dochází k interakci s člověkem, protože se mnohdy jedná o nejslabší článek zabezpečení, který je zastoupen nezkušeným a neznalým uživatelem internetu.

[11] **DDoS** (Distributed Denial of Service) neboli odepření služby je typ útoku, který má za cíl ochromit internetové služby nebo webové stránky. K útoku bývá využívána distribuovaná síť počítačů (často napadena virem), která zahltí cílovou stanici požadavky.



Obrázek 1 - Infografika bezpečnostních hrozeb internetu za posledních 20 let

Zdroj: SHAKEEL, Irfan. Evolution in the World of Cyber Crime. [Online] 28. Červen 2016. Dostupné z: http://resources.infosecinstitute.com/evolution-in-the-world-of-cyber-crime/

3.2.2. Budoucí vývoj

Po rušném období roku 2015, kdy se útokům nevyhnul ani ředitel CIA John Brennan, lze podle názorů bezpečnostních expertů očekávat neutichající eskalaci útoků. V následujících letech je očekáván nárůst všech typů útoků, protože pro hackery jsou nezanedbatelným zdrojem finančních prostředků. Jedním z nich budou útoky na zařízení IoT, které jsou zkušeným útočníkem prolomena v řádu hodin až dnů. (14)

Největší nárůst útoků zaznamenalo zdravotnictví, které čelí o 340 % většímu množství útoků než jakékoliv jiné odvětví a vzhledem k přechovávaným údajům, lze očekávat zájem o zdravotnický segment i v budoucích letech. Zdravotnictví je ale řízeno zákony, které ukládají způsoby a postupy, podle kterých se musí s údaji manipulovat a přechovávat je, příkladem může být zákon HIPPA[12]. (14)

Mezi dalšími očekávanými trendy budou útoky typu *ransomware*, které po spuštění škodlivého kódu zašifrují uživatelská data a sám útočník poskytne řešení této situace – „*zaplať nebo přijdeš o data*“. Pokusy o dešifrování vlastními silami, bývají s aktuálním výpočetním výkonem bez znalosti šifrovacích algoritmů bezvýchodné. Lze také očekávat

[12] **HIPPA** (The Health Insurance and Accountability Act) je zákon z roku 1996 platný na území USA, který upravuje zacházení s osobními informacemi o zdravotním stavu pacienta, u kterých musí být mimo jiné logována veškerá aktivita a šifrován obsah (39)

neustupující vliv hacktivistických skupin, které působí celosvětově a zabývají se zveřejňováním utajovaných informací, které dle svých etických kodexů patří veřejnosti. To samozřejmě není jejich jediným cílem, zaměřují se i na boj se zločinem, nespravedlností, politikou a v základu veškerým veřejným děním, které je do určité míry kontroverzní. (9) (14)

3.3. Právní legislativa

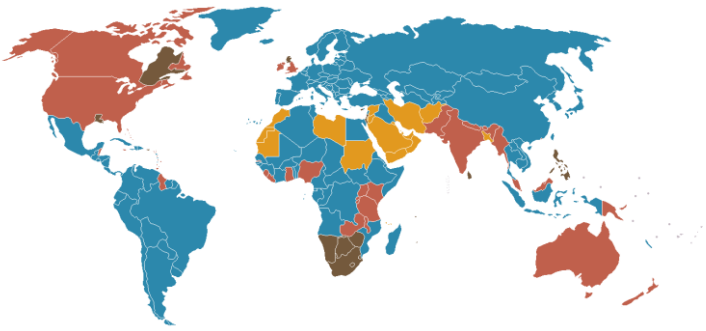
V současnosti žijeme v zajímavé době, ve které se právní svět a svět informační bezpečnosti stávají navzájem propleteny do takové míry, že dochází k přetěžování zdrojů obou systémů. Oba světy používají rozdílné jazyky, terminologie, a v minulosti se zaměřovaly na vlastní zájmy, cíle a procedury. Nikterak do sebe navzájem nezasahovaly, ale s tím, jak se z počítačů začala stávat platforma pro podnikání a páchání nových trestných činů, musely se dva rozdílné světy nezávisle přiblížit a začít spolupracovat v novém prostoru, který je často označováno jako *kybernetické právo* (z anglického slova *cyberlaw*). (2) (15)

Kybernetické právo je široký pojem, který zahrnuje mnoho elementů právní struktury, která je v kontaktu s tímto rychle se rozvíjejícím segmentem. Právní předpisy by měly být vytvářeny s bezpečnostními odborníky, kterým nejsou cizí. Nedorozumění u těchto neustále se rozvíjejících právních předpisů, může vzhledem k složitosti počítačových zločinů v krajních případech vyústit k obvinění nevinného nebo umožní viníkům zůstat na svobodě. (2)

Legislativci, vládní a soukromé bezpečnostní organizace soustavně upravují právní předpisy, zákony a související kriminalistické metody ve snaze čelit všem novým útokům, se kterými hackeři přijdou. Vývojáři bezpečnostních technologií a ostatní profesionálové se soustavně snaží přelstít sofistikované útočníky, kteří se naopak snaží zhatit jejich bezpečnostní opatření. V této souvislosti se zákony neustále upravují právními úpravami a představují neustále se měnící soubor pravidel, které se snaží udržet krok s novými typy útoků a jejich provedením. (2)

Na celém světě se můžeme setkat s různými zákony týkajících se kybernetiky. V základu můžeme světové právní systémy rozdělit na dva právní systémy současného světa kontinentální a angloamerický. Rozdíly mezi nimi jsou zřetelné především v oblasti soukromého práva, kdežto v oblasti veřejného práva je mezi nimi zřetelná souvislost.

Z uvedeného členění právních systémů vychází následující dvě podkapitoly, které se zabývají různými pohledy na oblast kybernetického práva. (16)



Obrázek 2 - Rozdělení právních systémů ve světě

Zdroj: PullUpYourSocks. Legal Systems Of The World Map. [Online] 6. Srpen 2014. Dostupné jako volné dílo z: https://commons.wikimedia.org/wiki/File:LegalSystemsOfTheWorldMap.png

Vysvětlivky k obrázku:

Kontinentální právo	Smíšené právo
Angloamerické právo	Fiqh

3.3.1. Kontinentální právo

Též nazývané jako občanské právo je celosvětově převládajícím právním systémem, který stojí na dualismu, tedy na dělení práva na veřejné a soukromé. Kontinentální právní systém je velmi členitý mezi zeměmi působení, to je způsobeno historickým vývojem, který se utvářel spontánně. Zákony jsou u kontinentálního systému tvořeny poslanci v zákonodárných sborech, to sebou přináší riziko přijmutí zákona, který je nedokonalý z důvodu nedostatečných odborných znalostí. Při vykonávání práva soudce právo pouze vyhledává, nevytváří jej. (17)

Skládá se z normativních právních aktů, které představují právní předpisy a obsahují obecná pravidla chování vydaná předepsanou formou. Jedná se o stěžejní prameny kontinentálního právního systému. Normativní právní akty mají svojí hierarchii právních předpisů, která je určena právní silou, kdy na jejím vrcholu stojí ústava a ústavní zákony, dále zákony a podzákonné právní předpisy. U hierarchie platí, že u právních předpisů nižší právní síly nesmí docházet k rozporu s předpisy vyšší právní síly. (17)

3.3.1.1. Česká republika

V roce 2011 vzniklo pod Národním bezpečnostním úřadem (dále jen NBÚ) Národní centrum kybernetické bezpečnosti (dále jen NCKB), úlohou centra je koordinace spolupráce na národní i mezinárodní úrovni při předcházení kybernetickým útokům, přijímání opatření při řešení bezpečnostních incidentů a proti probíhajícím útokům. NCKB spravuje vládní CERT (*Computer Emergency Response Team*) tzv. GOVCERT, který zajišťuje ochranu kritické informační infrastruktury a významných informačních systémů. Úlohou týmu je působit osvětu a podporu vzdělávání v oblasti kybernetické bezpečnosti a poskytovat prvotní zdroj bezpečnostních informací a pomoci pro orgány státu, organizace a občany. Mezi další poskytované služby týmu patří koordinační činnost a pomoc při řešení incidentů, zprostředkování kontaktů, sdílení dat infikovaných strojů v ČR, nasazování *honeypotů*[13], penetrační testování a zázemí forenzní laboratoře. (18) (15)

Úřad postupuje podle zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), který nabyl účinnosti 1. ledna 2015 a dalších vyhlášek. Zákon upravuje práva, povinnosti a působnost osob a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti. Zákon vymezuje pojmy z oblasti kybernetické bezpečnosti, stanovuje postupy bezpečnostních incidentů a systém zajištění kybernetické bezpečnosti. Na základě zákona má NBÚ pravomoci stanovovat stav kybernetického nebezpečí, který vyjadřuje úroveň ohrožení bezpečnosti informací v informačních systémech, bezpečnost a integritu sítí elektronických komunikací nebo ohrožení zájmů České republiky. (19)

Mezi další paragrafy, se kterými se na území České republiky pachatel internetové kriminality dostane do styku, jsou zejména z trestního zákona č. 40/2009 Sb. a konkrétně se jedná o níže uvedené paragrafy. (20)

§180 o neoprávněném nakládání s cizími údaji, který se zabývá neoprávněným zveřejněním, sdělením, zpřístupněním, jiným zpracováním nebo přisvojením osobních údajů, byť i z nedbalosti nebo jejich zpřístupnění třetí osobě

[13] Automatizovaná síťová past, která má za úkol přitahovat potencionální útočníky a zaznamenat jejich aktivitu.

§182 o porušení tajemství dopravovaných zpráv, který chrání všechny formy zpráv zasílané prostřednictvím sítě elektronických komunikací a neveřejné přenosy počítačových dat do počítačového systému a postihuje jejich zachytávání a zneužívání.

§183 o porušení tajemství listin a jiných tajných dokumentů uchovávaných v soukromí

§230 o neoprávněném přístupu k počítačovému systému a nosiči informací, který se zabývá neoprávněným přístupem k počítačovému systému nebo jeho části a neoprávněným užitím získaných dat ve smyslu odcizení, pozměnění, odstranění nebo vložení.

§231 opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat, je doplněk k předchozímu paragrafu 230 a ošetřuje případy, kdy dojde pachatelem k zneužití získaných informací nebo k jejich poskytnutí třetí osobě.

§232 o poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti

3.3.2. Angloamerické právo

Známé též pod pojmem anglosaské právo, je právní systém založený na obecném právu též nazývaném soudcovské právo, které je tvořené soudci skrze *precedenty*[14], které jsou primárními prameny práva. Soudcovské právo je tak právem jednotlivých případů, kde se právní normy vyvozují z jednotlivých konkrétních kauz, na rozdíl od psaného práva, pro které je značný vysoký stupeň zevšeobecnění. (16)

Je na první pohled méně členité než kontinentální, proto jsou si právní řády zemí, ve kterých je uplatňováno mnohem více podobné, než je tomu u zemí s kontinentálním právním systémem. Mezi nejvýznamnější země, které uplatňují angloamerický právní systém je možno zařadit Kanadu, Indii, Austrálii, Velkou Británii a Spojené státy americké. (16)

3.3.2.1. Spojené státy americké

V USA je zákon **18 USC Section 1029: The Access Device Statue**, který se zabývá zločiny, mezi které patří neoprávněné přístupy k účtu, krádeže peněz, produktů a služeb v online prostředí a obdobné zločiny. Mezi další zákony patří zejména zákony o počítačových sítích,

[14] Jsou soudní rozhodnutí, které jsou prvním řešením (rozhodnutím) daného případu a ty jsou aplikována na nynější obdobné případy. Soudy a správní úřady se od nich jen zřídka odchylují a zároveň platí, že nejsilnější jsou judikáty Ústavního a Nejvyššího soudu.

komunikaci, autorských právech a dodatek o nakládání s počítačovými zločinci. Roku 2002 vstoupil v platnost dodatek **Cyber Security Enhancement Act**, který umožňuje udělovat doživotní tresty za zločiny, které měly za následek už jen možné ublížení na zdraví nebo ohrožovaly veřejné zdraví a bezpečnost. (2)

USA jako jedna z největších mocností světa je pod neustálým útokem hackerů z celého světa, kteří prahnou po tajných vládních informacích a databázích společností. Z toho důvodu má propracovaný legislativní systém včetně organizací, které jej vykonávají a svoje zákony se snaží prosazovat v celosvětovém měřítku. Příkladem může být dohoda *ACTA*[15], která usilovala o vytvoření mezinárodního systému pro vynucování duševního vlastnictví a stala se terčem hacktivistického hnutí *Anonymous*, protože byla v rozporu s jejich kodexem o veřejném přístupu k informacím. Smlouva nakonec nebyla Evropskou unií (dále jen EU) ratifikována a tím nevstoupila v platnost na území EU.

3.4. Technologie

V kapitole zabývající se technologiemi, které jsou kyberútočníkem využívány, jsou především vysvětleny ty, které jsou provázány s webovými technologiemi a jsou stěžejní pro porozumění praktickým částem práce tj. zejména technologie HTML, PHP, JavaScript, databáze a bezdrátové sítě. V úvodu kapitoly je sestaven ucelený přehled vývoje webových technologií od počátku až po současnost a v samostatných podkapitolách jsou blíže specifikovány.

Počátek webových technologií je datován od roku 1989, kdy Tim Berners-Lee vyvinul hypertextový systém pro švýcarské výzkumné středisko CERN a o rok později vytvořil hypertextový editor. Dosáhl i dalšího milníku, když současně vytvořil první webový server, na kterém publikoval specifikaci základních standardů UDI, značkovací jazyk pro tvorbu webových stránek (HTML) a protokol, který umožňoval výměnu hypertextových dokumentů ve formátu HTML tzv. HTTP. Postupem času se rozšiřují počty webových serverů, stránek a vznikají první webové prohlížeče, které disponují grafickým rozhraním. To byl první krok směrem k masivnímu rozšíření webových stránek a vzniku organizace W3C, která stanovuje standardy webových technologií. Tím vznikl základ webových

[15] Obchodní dohoda proti padělatelství a ochraně duševního vlastnictví

technologií, který je využíván do současnosti a pravděpodobně bude i v horizontu blížících se let stále využíván. (21)

Postupem času se vyvíjely nové webové prohlížeče, vznikaly nové verze a s tím i podporované technologie. Vznikly *cookies*, které umožnily uchovávat malé množství dat z webového serveru přímo u uživatele a tím je mezi sebou rozlišit a v současnosti jim poskytovat i personalizovaný obsah, uchovávat přihlášení a další předdefinovatelné parametry. Vznikl skriptovací jazyk JavaScript, který umožnil určitou formu dynamizace stránky, která od té doby získala větší úroveň interakce s uživatelem. Postupně vznikaly další technologie např. *Flash* a kaskádové styly, které vznikly pro snadnější a centralizovanou správu stylů webových stránek zvlášť u rozsáhlejších webových struktur. (22)

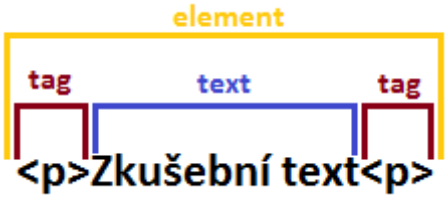
3.4.1. HTML

Zkratka pochází z anglického slovního spojení Hypertext[16] Markup Language (Hypertextový značkovací jazyk), který je používán pro tvorbu webových stránek. Veškeré webové stránky jsou vytvořeny pomocí HTML, který představuje stěžejní článek spojující grafiku, obsah a další informace v jeden funkční celek. HTML soubor, který vytváří webové stránky je jen kombinací běžného textu se speciálními prvky, které se nazývají značky. Značky s textem tak tvoří specifické sady instrukcí, které instruují webové prohlížeče. Prohlížeče vznikly za jediným účelem, kterým bylo čtení HTML instrukcí (značek) a zobrazování jejich výsledků formou webové stránky. Výhodou webových stránek je, že se prakticky jedná pouze o textový soubor, který umožňuje jejich úpravu a vytváření v jakékoliv aplikaci, která pracuje s textem např. poznámkový blok a Microsoft Word. Uvedené aplikace ale nejsou pro danou práci příliš efektivní a podporované. (23)

HTML se tedy skládá ze značek, které se umísťují mezi špičaté závorky < >, které tvoří značku (*tag*). Příkladem je uveden element ** Text... **, který se využívá pro označení odstavců a jedná se o element párový, který musí být ukončen druhou uzavírací značkou. Element se tedy skládá ze dvou značek, kdy značka ** **, je počáteční a jejím zadáním začíná odstavec a druhou značkou ** **, která odstavec ukončuje. Elementy jsou párové z důvodu, aby bylo možné například odlišit, kde odstavec končí a začíná. Na obrázku níže (viz.

[16] Speciální instrukce HTML, která povoluje textu odkazovat na něco jiného v kyberprostoru. Takové ukazatele se nazývají hyperlinky, které udržují World Wide Web (WWW) pohromadě. Ve webových prohlížečích jsou vizualizovány do textu modré barvy s podtržením. (22)

Obrázek 3), je znázorněno rozložení HTML elementu, který je tvořen značkami a obsahem. (23)



Obrázek 3 - Element v HTML kódu

Zdroj: vlastní zpracování

3.4.1.1. Kaskádové styly

Dříve se zobrazované prvky webových stránek stylovaly přes element **<style>**, kterým se upravovala veškerá vizuální podoba webové stránky tj. barvy, pozice a velikosti. S rostoucí komplexností webových stránek a přibýváním podstránek, byla správa stylů časově náročná. Proto došlo k vytvoření kaskádových stylů (CSS), které obsahovaly skoro veškeré styly prvků v jednom souboru. Výjimku mohou tvořit styly, které jsou na webové stránce unikátní a jejich umístění do souboru CSS by znamenalo stejnou úroveň pracnosti jako jejich umístění přímo do HTML kódu.

K rozlišení a přiřazení stylů k určitému prvku se využívá např. *třída*, která je v HTML kódu přiřazena k elementu a v kaskádových stylech nastylována pod stejným názvem *třídy*. Stylování je možné přiřadit i na veškeré konkrétní elementy nebo identifikátory.

Tabulka 1 - Nastylování HTML kódu pomocí kaskádových stylů

Výňatek z HTML kódu	**Výňatek z CSS souboru**	**Zobrazení ve webovém prohlížeči**
Nadpis 1. úrovně	.nadpis {color: red; font-size:20px}	Nadpis 1. úrovně

Zdroj: vlastní zpracování

3.4.2. PHP

Jedná se o rekurzivní zkratku hypertextového preprocesoru (*Hypertext Preprocessor*), který je zástupcem objektově orientovaných programovacích jazyků (*OOP*). Programování prostřednictvím objektů umožní modelovat úkoly skutečného světa, procesy a další myšlenky, na kterých je aplikace postavena. Při objektovém pohledu se na aplikaci nenahlíží

jako na řídící vlákno, které pracuje na principu předávání dat od jedné funkce k druhé, ale umožňuje modelovat aplikaci jako skupinu spolupracujících objektů, které jsou prováděny nezávisle. Oproti procedurálnímu programování je princip tříd a objektů a jejich způsob využití základní myšlenkou OOP, kdy procedurální je založeno na volání funkcí a globálních datových strukturách. (24) (25)

Objektové programování je založeno na základních principech, které jsou navzájem provázány a následující odstavec je zaměřen na jejich vyjasnění a specifikaci:

- **Třídy** – je vzor, podle kterého se vytvářejí objekty a vlastní kód, který definuje atributy (charakteristiky) a metody (chování)
    - **Atributy** – jsou vlastnosti, charakteristiky neboli data, které mají název a hodnotu, kterou lze v některých případech změnit
    - **Metody** – jsou funkce (schopnosti), které umí daný objekt vykonávat
- **Objekty** – jsou entity reálného světa (např. člověk, auto nebo databáze), které představují běžící instance třídy a které mají své atributy a metody (24)
- **Dědičnost** – jedná se o vytváření nových datových struktur na základě starých, kdy děděná třída má stejné vlastnosti jako rodičovská (příkladem je čtverec, který je speciálním případem obdélníku) (24)
- **Polymorfizmus** – umožňuje definovat jednu třídu, jakožto člena více kategorií tříd (příkladem může být telefon, který lze chápat jako „věc s obrazovkou“ a „věc s tlačítky“) (24)
- **Rozhraní** – je způsob, jak definovat funkcionalitu, kterou je objekt schopen poskytnout, aniž by bylo třeba definovat způsob jejího dosažení
- **Zapouzdření** – schopnost objektu chránit před přístupem svá interní data (24 str. 31)

3.4.3. JavaScript

Skriptovací jazyk, který se poprvé objevil v roce 1995 v prohlížeči *Netscape* a byl to nástroj původně zamýšlený na doplnění jednoduchých dynamických prvků na webových stránkách. Syntakticky vychází s jazyka C, některé standardní rozhraní se podobají jazyku Java a z pohledu funkcionálního modelu se autoři inspirovali jazyky Scheme a Self. *JavaScript* je umístěn na straně klienta nejčastěji přímo v HTML kódu stránky nebo v knihovnách, odkud je také spouštěn po načtení webové stránky nebo interakci uživatele. Z důvodu

možnosti spuštění po načtení webové stránky, je *JavaScript* často využíván útočníky k oklamání uživatele a testování zranitelností, kterým se blíže věnuje kapitola zaměřená na XSS (viz. Kapitola 3.5.1.2.). (26) (27)

Jeho prvotní funkce byla pro validace formulářů na straně klienta (správnost a úplnost zadaných údajů) a drobné efekty s obrázky. Takový kód obsahoval převážně pár jednoduchých řádků. S příchodem nové verze Internet Exploreru bylo umožněno skriptům přistupovat k objektovému modelu stránky, pomocí kterého mohl *JavaScript* manipulovat s obsahem webové stránky. (26) (28)

V současnosti vzniká a vznikalo poměrně početné množství různých *frameworků*[17] a knihoven, které mohou značně komplikovat počáteční orientaci a výuku skriptování. Jeho značné rozšiřování je příležitostí pro tvůrce webových prohlížečů, kteří se neustále předhánějí s rychlostí a optimalizací načítaní skriptů webových stránek.

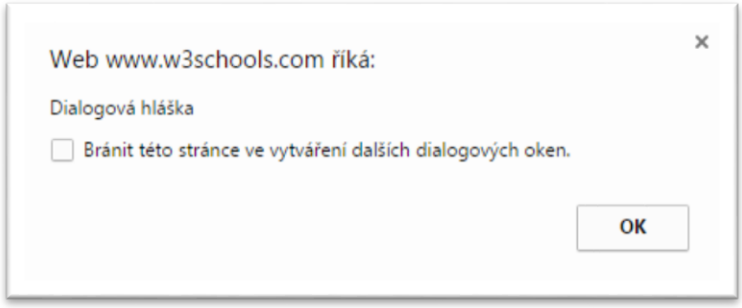
Skript může být napsán v samostatné knihovně, která se označuje příponou *.js* a obsahuje spustitelné funkce. V případě psaní skriptu přímo do HTML kódu stránky, je umístěn do párových značek ***<script>***text***</script>***, které vymezují začátek a konec skriptu. Takový skript může být spouštěn různou událostí, které jsou např.:

- při načtení stránky *onload*
- při uživatelské aktivitě kliknutí *onclick* nebo zmáčknutí klávesy *onkeypress*

Níže je uveden jednoduchý skript, který je často využíván pro zjištění a prezentaci bezpečnostních nedostatků webových stránek. Uvedený příklad je jednoduchý skript, který po načtení webové stránky zobrazí dialogovou hlášku.

[17] Software, který obsahuje knihovny, návrhové vzory, programy a slouží jako podpora při programování.

Tabulka 2 - Ukázka dialogové hlášky vyvolané skriptem

Ukázka skriptu	Dialogová hláška, která je vyvolána skriptem
<script> alert("Dialogová hláška"); **</script>**	

Zdroj: vlastní zpracování

3.4.4. Databáze

Jsou spolu s databázovými systémy základním prvkem života moderní společnosti, kdy většina z nás provádí každodenně akce, které vyžadují interakci s databázemi. A při rostoucím počtu počítačů můžeme říci, že databáze představují kritický prvek téměř v každém prostředí, které jejich služeb využívají. Včetně obchodu, výroby, medicíny, práva, vzdělávání, elektroniky a sociálních médií. (29)

Protože pojem *databáze* je běžně používán, tak je vhodné vysvětlit jednoduchou definicí, co je to databáze. **Databáze** je kolekcí (sbírkou) souvisejících dat, které představují známé skutečnosti, které mohou být zaznamenány a mající určitý význam. Databáze mají několik nepopiratelných vlastností:

- reprezentují aspekty reálného světa, někdy též nazývané *miniworld* nebo *universe of discourse (UoD),* kdy jejich změny jsou obsaženy v databázi (29)
- představují logicky spjaté kolekce dat s daným významem (náhodné uspořádání dat nemůže být korektně označováno jako databáze)
- je navržena, vytvořena a naplněna daty za konkrétním účelem pro určitou skupinu uživatelů a aplikací, které jsou těmito uživateli využívány

Jinými slovy mají databáze zdroje, ze kterých jsou získávána data, určitou úroveň interakce s událostmi skutečného světa a uživatele, kteří se aktivně zajímají o její obsah. Jejich konečný uživatel může provádět obchodní operace nebo události, které způsobují změny informací v databázi. K tomu, aby databáze byly přesné a spolehlivé, musí být skutečným zrcadlením *miniworldu*, a proto musí být změny ihned zobrazeny v databázi. (29)

V současnosti je nejrozšířenějším databázovým modelem relační a objektově orientovaný, mezi kterými jsou rozdíly především ve způsobu ukládání dat a vazeb mezi nimi.

3.4.4.1. Relační databáze

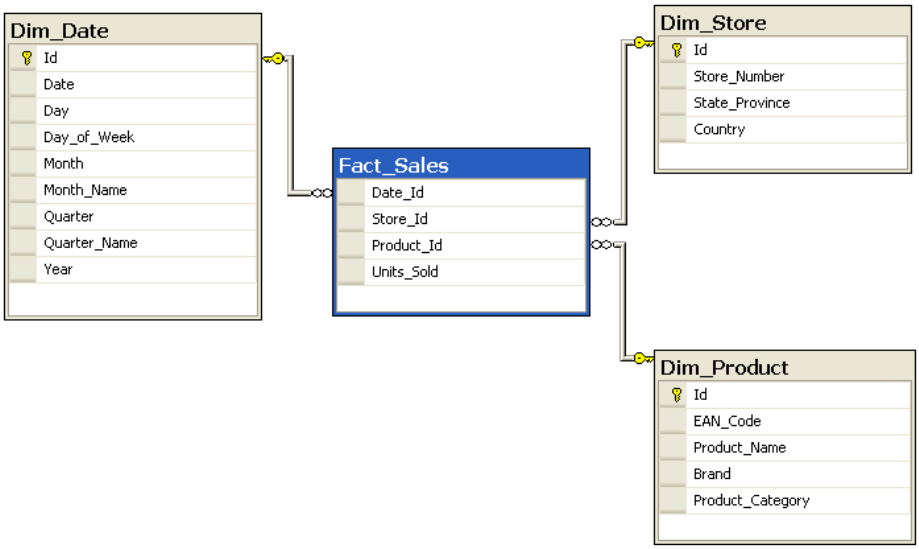
Byly původně navrženy tak, aby oddělovaly fyzické uložení dat od jejich abstraktního znázornění a poskytly tak matematický základ pro reprezentaci dat a dotazování. Model relačních databází umožnil použití programovacích jazyků vyšší úrovně, které poskytly alternativu k rozhraní programovacího jazyka a umožnily mnohem rychlejší psaní nových dotazů. Pro komunikaci s databázovými servery byl vyvinut jazyk SQL. (1) (30)

Prvotní pokusy s experimentálními relačními databázemi byly poměrně pomalé, protože nepoužívali *pointery*[18] na fyzickém úložišti nebo umístění záznamu pro přístup k souvisejícím datovým záznamům. S vývojem nových úložišť, *indexovacích*[19] technik, lepšímu zpracování dotazů a optimalizaci, se jejich výkonnost výrazně zvýšila. Tím se relační databáze začaly stávat nejrozšířenějším typem databázových aplikací, které se vyskytují na běžných počítačích i velkých serverech. (29)

Ovšem hlavní rozdíl oproti objektově orientovaným databázovým modelům je patrný z níže uvedené definice:

„Relační databáze ukládá data ve vztazích, které uživatel vidí jako tabulky. Každý vztah je složen z uspořádaných n-tic, neboli záznamů, a atributů, neboli polí.“ (31 str. 47)

[18] Datový typ, který zpřístupňuje data, která jsou na příslušné adrese v paměti uložena
[19] Pomocná databázová struktura, která slouží pro zrychlení vyhledávání a dotazovacích procesů v databázi



Obrázek 4 - Ukázka relační databáze

Zdroj: SqlPac. Star schema example. [Online] 28. Červen 2008. Dostupné pod licencí GNU Free z: https://en.wikipedia.org/wiki/File:Star-schema-example.png

U relačních databází jsou jednotlivé tabulky propojeny vazbami, které jsou realizovány pomocí klíčů – primárního, cizího a kandidátního. U každé vazby je určena kardinalita a stupeň vztahu. Ke komunikaci s databází se využívá SQL jazyk, který se liší v závislosti na použité databázi např. IBM DB2 využívá SQL PL, Oracle využívá PL/SQL a MySQL využívá SQL/PSM. Zformátováním dotazu v jazyce SQL můžeme vytvářet, upravovat nebo mazat databáze a provádět nad nimi dotazy pro práci s daty. (1) (32)

Typický dotaz napsaný v jazyce SQL může mít následující podobu:

```
SELECT * FROM zakaznici WHERE jmeno='Karel' AND prijmeni='Novák';
```

Uvedený dotaz slouží k vyhledání všech sloupců z tabulky **zakaznici**, kteří se křestním jménem jmenují **Karel** a příjmením **Novák**. Dotazy mohou využívat více typů příkazů a celý dotaz může být vnořen do jiného dotazu. Ukázka vnořeného dotazu:

```
SELECT * FROM zakaznici WHERE cenaObjednavky > (SELECT
AVG(cenaObjednavky) FROM zakaznici);
```

U uvedeného příkladu vnořeného dotazu se nejdříve provede dotaz v kulatých závorkách – získání průměrné ceny objednávky. Po získání průměrné ceny objednávky se vykoná část

dotazu, která není v závorce, která vyhledá zákazníky, u kterých byla cena objednávky větší než průměrná cena objednávky.

3.4.5. Bezdrátové sítě

Historicky první bezdrátový přenos informace bez použití fyzického přenosového média uskutečnil italský vědec Guglielmo Marconi, který v roce 1895 na vzdálenost přibližně dvou kilometrů přenesl rádiem informaci za použití technologie bezdrátového telegrafu. Svůj objev si nechal patentovat v roce 1896, následující rok svůj pokus vylepšil na vzdálenost patnácti kilometrů. Roku 1901 provedl první transatlantické bezdrátové spojení a v roce 1906 poprvé rádiovým spojením přenesl hlas.

Bezdrátová technologie si získala oblibu u námořnictva, které nemohlo využívat fyzického telegrafního spojení. Celkově se o masivní rozsah radiotelekomunikace zasloužila armáda a dvě světové války, kdy ve druhé světové válce se využívala přenosná radiovysílačka, která představovala důležitý komunikační prostředek na bitevním poli. (6)

Další milník nastal v padesátých letech, kdy začaly vznikat první návrhy mobilních rádiových systémů založených na podobné technologii, která se podobá dnešním sítím GSM. K první realizaci mobilního analogového přenosu došlo až v roce 1961. V osmdesátých letech začaly vznikat první digitální telefonní systémy, ze kterých jsou v Evropě stále provozované systémy GSM. Milník, ze kterého vychází následující kapitoly je vznik standardu IEEE 802.11[20], který popisuje bezdrátovou komunikaci mezi počítači. (6)

3.4.5.1. Wi-Fi

Nazývané též WLAN jsou bezdrátové sítě, které nás v dnešním světě obklopují téměř v každém ohledu a na každém místě. Setkáváme se s nimi v kancelářích, hotelech, kavárnách, veřejných místech, domácnostech atd. Jejich rozšíření začalo s expanzí celosvětové sítě Internet a v současnosti s příchodem internetu věcí, je jejich expanze do každodenního života ještě výraznější a vytvářející miliardový byznys. Bezdrátové sítě poskytují svým uživatelům pohodlí, mobilitu a finanční úsporu na implementaci kabelového řešení. (33)

[20] Zkratka pro **Institute Electrical and Electronics Engineers** (Institut pro elektrotechnické a elektronické inženýrství), kde číslo *802* reprezentuje vznik této skupiny - únor 1980 a. 11 odkazuje na podskupinu podílející se na uvedené skupině standardů. (29)

Obrázek 5 - Logo Wi-Fi aliance a ikona

Zdroj: Wi-Fi Alliance. Wi-Fi Logo. [Online] ©2017. Dostupné jako volné dílo z: https://commons.wikimedia.org/wiki/File:Wi-Fi_Logo.svg

V roce 2002 vznikla Wi-Fi Aliance, která je celosvětovým sdružením společností, které stanovují, zdali Wi-Fi technologie a produkty odpovídají normám. Je držitelem ochranné známky Wi-Fi, kterou by výrobci měli používat pro označení produktů otestovaných v nezávislých laboratořích aliance. Takové produkty mohou využívat označení Wi-Fi CERTIFIED, protože vykazují zpětnou kompatibilitu, nejvyšší úroveň zabezpečení a kvalitu. (34)

Při vytváření bezdrátového systému, ale nikdo nepočítal s jeho masivním rozšířením, které dalo podklad k možným bezpečnostním incidentům. „*Příkladem je společnost Microsoft, která je názorným příkladem toho, že čím jste větší a populárnější, tím více útoků je vůči vám vedeno.“* (33 str. 30) S příchodem výhod bezdrátové komunikace přicházejí i záplavy bezpečnostních rizik, které jsou oproti současným problémům úplně odlišné. Čemuž nepomohly ani široce publikované nedostatky zranitelnosti zabezpečení WEP u standardu IEEE 802.11, které mělo dosahovat obdobné úrovně bezpečnosti jako kabelové sítě.

3.4.5.1.1. Struktura

Každá Wi-Fi síť má svůj jednoznačný identifikátor SSID (*Service Set Identifier*), který je periodicky vysílán (10x až 100x za minutu) a nazývá se *beacon frame*. Taková forma vysílání umožní klientům/uživatelům si snadno zobrazit dostupné sítě a připojit se k přístupovým bodům. Druhým identifikátorem bezdrátové sítě je BSSID, které je MAC adresou vysílače. V případě komunikace mezi dvěma klienty tzv. ad-hoc sítě, se provádí vzájemná identifikace pomocí SSID (BSSID se nevyužívá). Sítě mezi dvěma klienty jsou použitelné u přenášení dat mezi chytrými telefony a u přenosu mezi počítači na krátké vzdálenosti.

Wi-Fi zařízení jsou zpravidla vybavena dodatečným softwarem, který správci umožňuje upravovat nastavení a přizpůsobovat funkci svým požadavkům, mezi možné funkce patří řízení přístupové politiky, přidělování IP adres, konfigurace firewallu a nastavování přístupového bodu.

3.4.5.1.2. Bezpečnostní protokoly

V počátcích byly bezdrátové sítě nezabezpečené až do roku 1990 a verze IEEE 802.11b. Starší verze standardu obsahovaly fyzické bezpečnostní slabiny, problémy s šifrováním a autentizací. (33)

To způsobilo vzestup útoků proti bezdrátovým sítím, proti kterým se postavily dva bezpečnostní standardy:

WPA je zkratkou Wi-Fi Protected Access (Wi-Fi chráněný přístup) a je nástupcem předchozí technologie WEP, oproti které nabízí vyšší úroveň zabezpečení a poučení se z jejich nedostatků. Předchozí technologie WEP byla v roce 2001 prolomena a odpovědí Wi-Fi Aliance bylo vytvoření nového standardu zabezpečení. Za zmínku stojí vylepšení šifrovacího algoritmu a správy šifrovacích klíčů, které ale měli vyšší výpočetní náročnost a některé počítače tak nedisponovaly dostatečnou výpočetní kapacitou, aby WPA podporovala. Na jedné síti lze používat pouze jeden bezpečnostní standard a nelze tedy kombinovat WEP a WPA. V dnešní době, je jejich náročnost na výkonnost výpočetní techniky marginální a úroveň jejich podpory a implementace všudypřítomná. Standard WPA byl jen přechodovým můstkem mezi jeho novější verzí a v současnosti je považován za stejně nebezpečný jako jeho předchůdce. (33) (6)

WPA2 neboli Wi-Fi Protected Access II je bezpečnostní protokol, který je certifikován Wi-Fi Aliancí. Jedná se o nástupce standardu WPA, oproti kterému poskytuje silnější algoritmus šifrování, který je doposud považován za neprolomený. Uživatel bezdrátové sítě se zabezpečením WPA2 je tak chráněn před útoky hrubou silou, tabulkovými útoky a odposlechy, ale nejslabším článkem řetězce mnohdy bývá samotný uživatel. Výhodou je, že pro zařízení, která nepodporují WPA2 je možné využít režimu WPA/WPA2, ve kterém se používá bezpečnější šifrování WPA2, ale zároveň se budou moci připojit i starší zařízení WPA. V současnosti, pokud chce Wi-Fi zařízení získat certifikát, musí být certifikováno pro zabezpečení WPA2. (33)

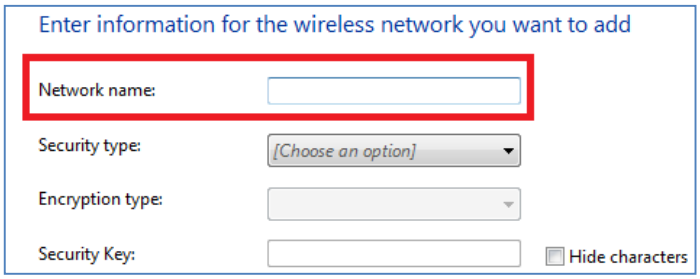
- Za slabý článek zabezpečení je považována funkcionalita WPS, která poskytuje důvěryhodným uživatelům, kteří znají 8místný číselný kód, možnost se připojit k síti, bez znalosti úplného přístupu k bezdrátové síti. Jenže zařízení neprovádí validaci všech zadaných znaků kódu, ale pokud jsou první čtyři správné, pak provede kontrolu dalších tří a poslední znak představuje kontrolní součet. Útočníkovi tak místo teoretických 100 miliónů kombinací, postačí vyzkoušet 11 tisíc kombinací k získání přístupu. (35)
- U WPA2 lze využít z dvou šifrovacích metod AES nebo TKIP, případně jejich kombinací. AES (*Advanced Encryption Standard*) je považován za doposud neprolomený a bezpečný způsob šifrování, který je prolomitelný útokem hrubou silou a bezpečnostními slabinami WPA2. Je použitelný jak pro standard WPA2, tak i starší verzi WPA, které poskytne dostatečnou úroveň zabezpečení. U šifry je možné zvolit sílu šifrovacího klíče v délce 128, 192 nebo 256 bitů. TKIP (*Temporal Key Integrity Protocol*), byl převážně využíván u předchozího standardu WPA, který byl odpovědí na nebezpečný standard WEP. V současnosti už není považován za bezpečný a měl by být použit jen v kombinaci s šifrou AES. (36)

3.4.5.1.3. Metody zabezpečení

V důsledku útoků a nežádoucích přístupů, je potřeba ochránit vysílač rozmanitými způsoby fyzického i softwarového charakteru. Zvýšené riziko je u zařízení, které disponují továrním nastavením, které je optimalizováno s důrazem na vysokou úroveň kompatibility s uživatelskou sítí. Potencionální útočník je schopen se k přístupovému bodu připojit i na velkou vzdálenost, využitím směrové antény, která mu umožní signál zachytit. Ochranou před takovými postupy a technologiemi, je určitá forma stínění signálu nebo skrytí vysílaných údajů o síti.

Skrytí SSID

Metoda, která zamezí přístupovému bodu vysílání SSID identifikátoru a ten je pak pro běžného uživatele nevyhledatelný. Identifikátor je sdělován zainteresovaným uživatelům jinou formou např. emailem, poštou, telefonem nebo tištěnou formou. Uživatelé se následně k Wi-Fi síti připojí manuálně zadáním poskytnutých parametrů.



Obrázek 6 - Manuální připojení k přípojnému bodu

Zdroj: vlastní zpracování

Nicméně, jednoduchost této metody je spojena i s její nízkou efektivitou, protože je možné SSID identifikátor odposlechnout pomocí specializovaných aplikací *inSSIDer*, *NetStumbler* nebo *Kismet*. Proto se jedná pouze o podpůrnou metodu zabezpečení bezdrátové sítě, která poskytuje téměř nulovou ochranu před většinou známých útoků. (37)

Filtrování MAC adres

Funkcionalita, kterou standardně disponují síťová zařízení a umožňující řídit politiku přístupů pomocí listu MAC adres[21], který může zahrnovat povolené (*White list*) i nepovolené adresy (*Black list*). Zároveň může disponovat i funkcí „*rodičovské kontroly*", která slouží pro časové nebo obsahové restrikce. Pokud se k přístupovému bodu připojuje zařízení, prvotně dojde k jeho ověření s dostupným listem povolených zařízení a v případě pozitivního nálezu je provedena autorizace. Nicméně se nejedná o metodu, která je použitelná samostatně, protože při zjištění MAC adresy povoleného zařízení se útočník/neoprávněný uživatel může za takové zařízení vydávat. K získání MAC adresy může být útočníkem využito odposlechu provozu Wi-Fi sítě, ve které je každý paket označen MAC adresou, aby bylo zajištěno, že se dostal do správného zařízení. Příkladem je aplikace *Wireshark* nebo *Achilles*, které slouží pro monitorování a analýzu síťové komunikace.

Stínění signálu

Metoda je využitelná v prostředí, ve kterém je vyžadováno omezení dosahu signálu, zejména mimo prostory budov. K odstínění signálu se využívají speciální barvy nebo fólie, které obsahují příměs stříbra nebo hliníku a takto vodivá vrstva zamezí prostupu Wi-Fi signálu, ale ostatní bezdrátové spojení zůstanou zachována např. televizní a telekomunikační. Uvedená metoda je nejen účinnou ochranou proti nežádoucím uživatelům a útočníkům, ale

[21] Jednoznačný identifikátor síťového zařízení

zamezí pracovníkům využívat Wi-Fi sítí mimo pracovní stanoviště např. na toaletě, v kuchyňce a různých odlehlých částech společnosti.

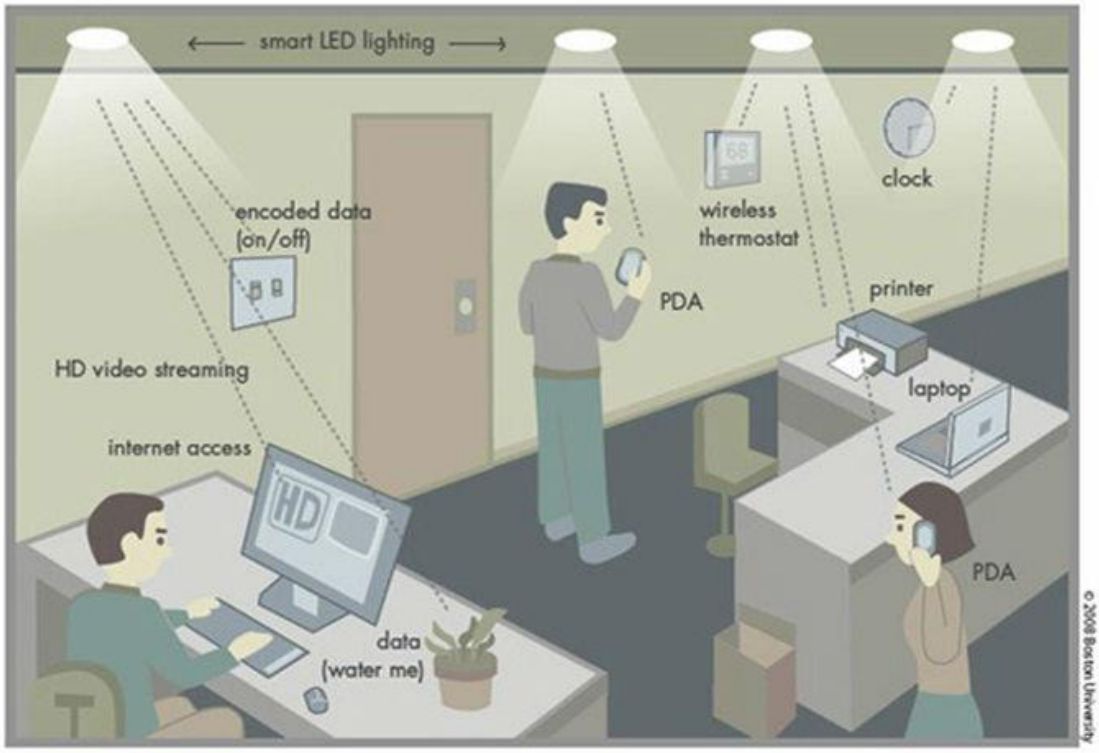
E2E šifrování

Bohužel, výše jmenované metody zabezpečení bezdrátové sítě jsou sami o sobě sledovatelné a jediným řešením je jejich kombinace s dostatečně silným šifrováním na straně koncových zařízení, které je na úrovni aplikační vrstvy. Při takovém provedení je komunikaci možno odposlechnout, ale útočník získá pouze zašifrované zprávy, u kterých by musel nejprve získat šifrovací klíč. K získání samotného šifrovacího klíče, by ale útočník musel využít sofistikovanějších metod softwarového inženýrství, za účelem oklamání uživatele nebo využití bezpečnostních nedostatků šifrovacího algoritmu.

3.4.5.1.4. Prognózy vývoje Wi-Fi sítí

Lze předpokládat, že v následujících letech bude postupovat rozšiřování Wi-Fi sítí, které budou propojovat každodenně používané zařízení s celosvětovou sítí Internet a umožňovat efektivní řízení zdrojů, sledování výdajů, plánování činností a mnohé další činnosti. Dnešní bezdrátové sítě využívají šíření rádiových vln, ale pro budoucí využití jsou plánovány média, která využívají k přenosu informací viditelného světla. Počátky komunikace založené na přenosu informací prostřednictvím světelných paprsků sahají až do 19. století k Alexandru Graham Bellovi, který je známý především vynálezem telefonu, ale i *fotofonu*, který využíval k přenosu zvuku měnící se intenzitu paprsku světla. Bohužel, nedostatečná úroveň technologií neumožnila jeho praktické využití a patent tak na dlouho upadl v zapomnění. (38)

Na přelomu tisíciletí se o Bellovu myšlenku a patent začal zajímat německý profesor Herald Haas, který se v rámci svého výzkumu začal zabývat přenosem informací prostřednictvím světla. Výsledkem jeho vývoje je technologie označována jako Li-Fi, která k přenosu informací využívá viditelného světelného spektra, které má vlnovou délku 400 až 800nm. Jeho výzkum bylo možné realizovat za pomoci Bellových nápadů, nynější úrovně technologií a LED světel, které oproti světlům využívaným Bellem umožňují rychlou změnu intenzity světla tzv. blikání, které je ale pro lidské oko nepostřehnutelné. (38)



Obrázek 7 - Vizualizace využití Li-Fi technologie

Zdroj: Boston University and Science Alert. Li-Fi Environment. [Online] 2008.

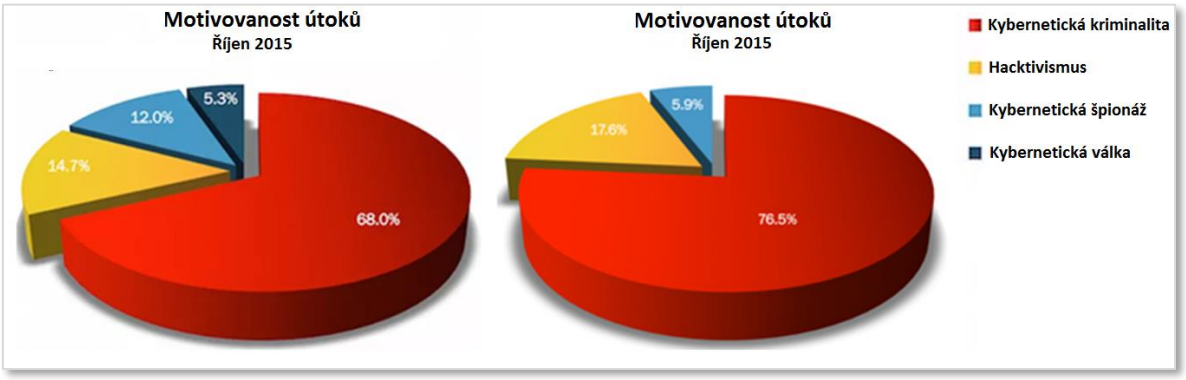
Výhodou technologie Li-Fi je její poměrně jednoduchá implementace s již existujícím LED osvětlením, ke kterému se implementuje řídící mikročip, který pro přenos informace využívá změnu intenzity světla. Změna intenzity světla je prováděna v takové rychlosti, že je lidským okem nepozorovatelná a nezpůsobuje viditelné blikání světla. V budoucnu by technologie umožnila automobilům mezi sebou komunikovat, poskytnout bezpečné hotspoty[22], monitorovat pacienty a navíc je technologie využitelná i pod vodní hladinou. V dnešní době vznikají i pokusy s fotovoltaickými články, které by kromě generování elektrické energie pro svůj provoz, poskytovaly i bezdrátové spojení a staly se tak nezávislými a široce využitelnými. (38)

3.5. Metody

V následující kapitole byly na izolovaných webových stránkách simulovány zvolené formy metod, které může útočník využít k získání informací, oklamání oběti nebo sledování komunikace. Metody jsou implementovány v takové formě, aby byly zjevně patrné jejich

[22] Přípojné body (zařízení), ke kterým se může uživatel bezdrátově připojit a komunikovat prostřednictvím nich v síti Internet

nedostatky i pro čtenáře, kteří nejsou odborníky v oblasti bezpečnostních technologií. Podstatnou částí realizace zvolených metod, jsou i názorné ukázky možných bezpečnostních opatření, které mohou být prováděny z hlediska vývojáře nebo uživatele. Realizaci zvolených metod předcházela sumarizace internetových útoků na základě jejich četnosti, motivace útočníků[23] a cílů útoků.



Obrázek 8 - Motivovanost útoků - porovnání října 2015 a 2016

Zdroj: PASSERI, Paolo. Cyber Attack Statistics. [Online] 19. Leden 2017. Vlastní překlad. Dostupné z: http://www.hackmageddon.com/category/security/cyber-attacks-statistics/

V posledních letech lze pozorovat nárůst útoků, které mají na svědomí členové *hacktivistických* hnutí, kterým je věnována kapitola 3.1.2.1 Hacktivist. K poměrné eskalaci útoků tohoto typu pravděpodobně přispěly světové události zejména: válka v Sýrii, volby v USA a teroristické útoky na území Evropské unie. V určitých ohledech je graf oproti předešlým obdobím odlišný, protože v říjnu 2016 nebyla detekována žádná forma kybernetické špionáže, která měla vliv na výslednou podobu grafu a růst ostatních sledovaných typů útoků. Na základě porovnání hodnot z předešlých let se hodnoty

[23] Motivace útočníků znamená důvod, který stojí za realizací útoku. Takový důvod může být politický, špionážní, válečný nebo s prostým účelem zisku.

kybernetických zločinů a špionáže pohybují u špionáže mezi 4 % a 12 % a zločinů mezi 60 % až 80 %. Situace je značně proměnlivá a reflektuje světové dění. (39)

Tabulka 3 - Srovnání forem útoků za říjen 2015 a 2016

Říjen 2016	
Typ útoku	Podíl útoků
Neznámý	27,45 %
Malware/PoS* Malware	21,57 %
Krádeže účtů	17,65 %
Cílené útoky	13,73 %
DDoS	9,80 %
Přesměrování DNS	1,96 %
Local File Inclusion**	1,96 %
Získávání emailů	1,96 %
Obsahové útoky	1,96 %
Šíření malwaru reklamou	1,96 %

Říjen 2015	
Typ útoku	Podíl útoků
Neznámý	34,70 %
Cílené útoky	18,70 %
Obsahové útoky	12 %
SQLi	12 %
Krádeže účtů	5,30 %
DDoS	4 %
Šíření malwaru reklamou	4 %
SQLi Magento***	2,70 %
Malware	2,70 %
Elektronická zařízení	1,30 %
Bitcoin transakce	1,30 %
PoS* Malware	1,30 %

Vysvětlivky k tabulce:

*__PoS__ (Point Of Sale) – platební terminály

**__LFI__ (Local File Inclusion) – vkládání souborů na server prostřednictvím webového prohlížeče

***__Magento__ – systém pro internetové obchody

Zdroj: PASSERI, Paolo. Cyber Attack Statistics. [Online] 19. Leden 2017. Vlastní překlad. Dostupné z: http://www.hackmageddon.com/category/security/cyber-attacks-statistics/

Ve srovnání s rokem předcházejícím, jsou útoky motivované především za účelem získání osobních informací, které vyústí v jejich zneužití. Útočník se pokouší získat přístup k cizímu účtu, u kterého se v případě sociálních sítí, emailů a dalších komunikačních nástrojů následně pokouší vylákat z kontaktů napadeného účtu finanční prostředky nebo pokračuje v šíření svého plánu. V posledním roce došlo k zásadnímu rozšíření útoků typu *Malware* a *Ransomware*, které se šíří komunikačními médii a formou *phisingových* zpráv a snaží se oklamat svou oběť. Se ziskem finančních prostředků jsou spojeny i útoky typu *DDoS*, u kterých se za stejné období minulého roku zvýšil výskyt dvojnásobně. Útočníci se u typu útoku *DDoS* pokouší o znepřístupnění cílového serveru, jehož výpadek představuje značné finanční ztráty a napadený subjekt je v krajních případech nucen zaplatit požadovanou částku za pozastavení útoku. Těmto útokům napomáhá i stále rozšířenější zařízení *IoT*, které

disponují minimálním bezpečnostním opatřením a jsou tak ideálním nástrojem útočníků. (1) (39)

Oproti minulému období došlo k značnému poklesu útoků typu *SQLi* (viz. Kapitola 3.5.1.1) a forem vandalismu, které je v počítačové terminologii označováno jako forma určité modifikace nebo záškodnictví, prostřednictvím kterého útočník smaže databázi, napíše na webovou stránku zprávu nebo změní její kontext. Také lze pozorovat změnu forem útoků, které jsou ovlivněny aktuálními trendy v tomto sektoru. Jedná se o prostou příležitost útočníků ke generování zisku, která dokáže přilákat další subjekty chtějící si utrhnout svůj vlastní pomyslný díl koláče a tak se množství útoků rozšíří jako infekce. (39)

3.5.1. Příprava prostředí

Vybrané zranitelnosti byly implementovány na vlastním webovém prostoru, který je pro náhodného uživatele dostatečně informativní, že se nachází na pokusných webových stránkách, vytvořených za účelem simulace útoků v rámci diplomové práce. Nicméně, po obsahové stránce jsou prakticky neškodné a neobsahují útočné prvky, které by potencionálního návštěvníka jakkoliv poškodili a jejich význam je tak pouze demonstrativní.

Pro simulaci útoků bylo využito technologií HTML, PHP, CSS a SQL databáze. Webová stránka byla vytvořena s důrazem na funkčnost a vypovídající hodnotu implementovaných bezpečnostních nedostatků, a proto veškeré prvky neobsahují funkční základ. Stránka je určena pro implementaci útoků typu *SQLi*, *XSS* a *Session hijacking*. Pro účely simulace útoku založeného na sledování komunikace bylo využito specifického softwaru.

Obrázek 9 - Úvodní přihlašovací formulář demonstrativní webové stránky

Zdroj: vlastní zpracování

Proces přihlášení uživatele je z funkčního hlediska kompletní, pouze nebyla implementována funkcionalita registrace, protože je pro zpracování simulace útoku nepodstatná. Za účelem autentizace je vyžadováno vyplnění přihlašovacích údajů, které jsou následně ověřeny v databázi. Na základě zpracovaného dotazu databází je uživateli poskytnut nebo odepřen přístup. Součástí přihlašovacího procesu je generování *PHPSESSID*, které představuje jednoznačný identifikátor každé relace, která k webovému formuláři přistoupila. Identifikátor je uložen v dočasné paměti webového prohlížeče tzv. *cookies* a je využíván webovým prohlížečem v komunikaci s dotčeným serverem a pomocí uložených cookies server rozpozná přistupujícího klienta a může ověřit jeho oprávnění, bez opětovné potřeby autentizace (soubory cookies mají zpravidla omezenou platnost, zvlášť ty které uchovávají číslo relace).

Veškeré zdrojové kódy, které byly využity pro tvorbu webových stránek, jsou součástí příloh diplomové práce. U částí, které nelze prostě zkopírovat (databáze) je přiložena její struktura a obsah z vývojového prostředí (viz. Příloha A a B). Prostředí bylo vytvořeno na základě studia odborných informačních zdrojů, vlastních zkušeností a návodů, které jsou dostupné z webových stránek *FormGet* a *W3Schools*. (40)

3.5.1.1. SQL Injection

Zkráceně útok typu SQLi je zranitelností, která vzniká v případech, kdy je dána útočníkovi příležitost ovlivnit strukturovaný dotazovací jazyk (SQL), prostřednictvím kterého aplikace předávají dotazy databázi. K ovlivnění dotazu, může útočník využít syntaxe a schopností samotného jazyka SQL, stejně tak výkonu, funkcí a funkcionalit operačního systému, které má databáze k dispozici. Jedná se o zranitelnost, která se netýká výhradně jen webových aplikací, ale každý kód, který přijímá vstupy od neznámého zdroje a předává je formou SQL dotazu databázi, může být zranitelný. (41) (42)

Zranitelnost typu SQLi pravděpodobně existuje od prvního připojení webové aplikace k SQL databázi. První datovanou publikací, která způsobila zájem veřejnosti o danou zranitelnost, byl dne 25. 12. 1998 zveřejněný článek s názvem „*NT Web Technology Vulnerabilities*“, jehož autor vystupoval pod pseudonymem Rain Forest Puppy (skutečným jménem Jeff Forristal). Autor článku se později roku 2000 prezentoval svojí další publikací, která popisovala způsob, kterým prostřednictvím SQLi hacknul webovou stránku Packet Storm, která poskytuje bezpečnostní nástroje, popisy chyb a bezpečnostní upozornění. (41)

3.5.1.1.1. Předmluva k simulaci

Pro simulaci zranitelnosti SQL Injection, bylo příhodné použít webový přihlašovací formulář, který se skládá z webové prezentační části a databáze. V případě, že uživatel vyplní přihlašovací údaje, webová aplikace shromáždí dvě části informace – přihlašovací jméno a heslo. Aplikace vložené parametry zpracuje a vytvoří SQL příkaz, který shromáždí požadovaný typ informací z databáze. Příkladem je webová stránka *prihlaseni.php* (viz. Příloha C), která naváže spojení s databázovým serverem. Připojení pak může být udržováno nebo se vytvářet při každém pokusu o přístup k databázi. Nutno zmínit, že webový server používá vlastní přihlašovací jméno a heslo k databázi, aby mohl spouštět SQL příkazy. (30)

Po navázání spojení dojde k předání SQL příkazu do databáze, která jej příjme, zpracuje a odpoví. Odpověď může být reprezentována binárně, kdy hodnota 1 znamená, že uživatelské jméno a heslo v databázi existuje anebo hodnota 0, která vyjadřuje, že uvedená kombinace uživatelského jména a hesla se v databázi nenachází. Na základě odpovědi z databáze, je uživateli umožněn nebo zamítnut přístup. (30)

Teoretickým vysvětlením principu komunikace databáze a webového serveru, byl vytvořen základ pro pochopení následujících simulací praktického použití zranitelnosti SQL injection, která je vytvořena v základní formě, tak aby byla pochopena širším okruhem odborné veřejnosti. Veškeré zdrojové kódy, které byly implementovány pro simulování zranitelnosti, jsou umístěny v přílohách práce jako Příloha A, B, C a D.

3.5.1.1.2. Popis prostředí a funkcionalit

Při každém pokusu o přihlášení je provedeno odeslání požadavku prostřednictvím metody POST, který obsahuje parametry USERNAME a PASSWORD. Přenášené parametry jsou následně v rámci SQL příkazu zpracovány databází. Formulář je možné odeslat i metodou GET, která neposkytuje dostatečná bezpečnostní opatření pro odesílání webových formulářů. Výsledné složení POST požadavku může mít následující podobu:

Tabulka 4 - Struktura POST požadavku

POST požadavek	
http://world.8u.cz/skola2/index.php	Adresa webové stránky, z které se uživatel pokouší přihlásit
username=admin	Parametr pro přihlašovací jméno
password=test	Parametr pro heslo

Zdroj: vlastní zpracování

V databázi spuštěný SQL příkaz, který obsahuje přijaté parametry z webového formuláře, má v základní podobě následující strukturu:

```
SELECT * FROM login WHERE username='$username' AND password='$password';
```

Kde **$username** a **$password** jsou parametry, které zasílá formulář z webového rozhraní.

```
SELECT * FROM login WHERE username='admin' AND password='test';
```

V uvedeném ukázkovém případě (viz. SQL příkaz výše), by databáze spustila SQL příkaz, na základě kterého by se databáze pokusila vyhledat uživatelské jméno **admin**, a zdali je jeho heslo **test**.

SELECT * FROM `login`

id	username	password	email
1	admin	test123	admin@seznam.cz

Obrázek 10 - Struktura a obsah databázové tabulky LOGIN

Zdroj: vlastní zpracování

Databázový server vyhodnotil, že uvedená kombinace se v databázi nenachází a informoval o této skutečnosti webový server, který zprávu prezentuje uživateli ve formě textového dialogu „*Nesprávné jméno nebo heslo*“ a znemožní mu přístup k uživatelské sekci. Z obrázku výše (viz. Obrázek 10), který byl pořízen z databáze, je patrné, že uvedená kombinace přihlašovacího jména a hesla skutečně neodpovídá a chování obou systémů bylo korektní.

3.5.1.1.3. Praktická ukázka útoku

Následující ukázka je zaměřena na možnost modifikace SQL příkazu, tak aby bylo umožněno získat přístup k systému, i bez znalosti hesla k některému z účtů. Při uvedené technice vycházíme z toho, že známe přihlašovací jméno některého z účtů. V opačném případě by muselo být postupováno metodou pokus-omyl nebo za použití sofistikovanějších metod.

Struktura použitého SQL příkazu se skládá z funkcí, proměnných a technických znaků, které mohou svým použitím způsobit transformaci celého příkazu. Při vkládání řetězcových hodnot do databáze se vždy vymezují apostrofy, které mohou být jednoduché nebo dvojité. Na to je potřeba pamatovat i při vytváření SQL příkazu ve webové aplikaci. Dalším znakem, který je v SQL syntaxi používán, je znak pro křížek, mřížku nebo též nazývaný *hash*, který slouží pro zakomentování příkazu. V průběhu vývoje databázových systémů bylo objeveno, že vložením znaků ze syntaxe SQL do části příkazu, lze provést jeho nežádoucí úpravu. Vložením jednoduchého znaku pro zakomentování tak způsobovalo, že se část příkazu, která se nacházela za vloženým znakem, neprovedla. V praxi by uživatel zadal jako přihlašovací jméno **admin#** a jeho odesláním, by došlo k vykonání příkazu, bez červeně označené části (viz. Příkaz níže). (41)

```
SELECT * FROM login WHERE username='admin#'  AND password='test';
```

Bohužel uvedený příkaz by nejspíše skončil chybou nebo by se pokusil vyhledat uživatele s přihlašovacím jménem **admin#**. Možným řešením by byla kombinace znaku pro vymezení

řetězcových hodnot a komentáře. Potencionální útočník by tak mohl dokázat přesvědčit systém, že autentizace se skládá pouze z ověření přihlašovacího jména (viz. Příkaz níže).

```
SELECT * FROM login WHERE username='admin'#'  AND password='test';
```

Útočník v takovém případě dokázal SQL příkaz modifikovat do takové podoby, že provedl vložení přihlašovacího jména ve formátu **admin'#**. To způsobilo uzavření řetězce a zároveň zakomentování zbytku kódu, který byl databází proveden v útočníkem požadovaném formátu (viz. Příkaz níže).

```
SELECT * FROM login WHERE username='admin';
```

Útočník pomocí jednoduché metody SQLi získal přístup k účtu s právy administrátora, bez znalosti přístupového hesla (viz. Obrázek 11).

Obrázek 11 - Úspěšný pokus o přihlášení za využití SQLi

Zdroj: vlastní zpracování

3.5.1.1.4. Zabezpečení před útokem

Ochrana před SQLi by měla být vždy implementována na straně webového serveru, který je první linií obrany a záleží na něm, co poskytne uživateli za informace. Základní možností obrany sestávají z omezení přístupových práv uživatelského účtu webového serveru, který nemusí mít oprávnění k provádění zápisů do Master databáze nebo provádět zálohování. (30)

Z hlediska dalších způsobů ochran, je potřeba zabezpečit schéma databáze tzn. strukturu SQL databáze, která by neměla být zobrazována v HTML kódu, zejména její názvy tabulek, sloupců a struktury. Jejich zobrazováním bychom útočníkovi ušetřili čas a usnadnili práci. S tím je spjato i zobrazování chybových hlášek a stavů, které by měli být všeobecné a nikdy by neměly zobrazovat systémové informace, proměnné nebo jiná data, na základě kterých

útočník odhaluje zranitelnosti buď manuálně, automaticky nebo robotem prohledávajícím obsah internetu. (30)

Jednoduchý způsob ochrany, který byl implementován na pokusných webových stránkách, spočívá v ošetření vstupních znaků, za využití funkce *mysql_real_escape_string()*. Použitá funkce je založena na metodě **escapování**, která ošetřuje potencionálně nebezpečné znaky, prostřednictvím kterých lze pozměnit výslednou podobu SQL příkazu. Funkce před každý znak, který má v SQL databázi technickou funkci, vkládá zpětné lomítko. Pomocně vložený znak je aktivní pouze po dobu zpracování a do databáze se nezapisuje ani není součástí výběrů z databáze. Při využití skriptovacího jazyka PHP, jsou k dispozici funkce *magic_quotes_gpc()* a *stripslashes()*, které vkládání zpětných lomítek provádějí automaticky, s každým požadavkem. (43)

Na praktické ukázce webové stránky, která tvoří prostředí pro simulaci zvolených útoků, by bylo dostačující k přihlašovacímu PHP kódu implementovat níže uvedené dva řádky, které by znemožnily využití simulovaného útoku typu SQLi k získání přístupu. Samozřejmě se nejedná o úplnou ochranu před útokem typu SQLi, ale minimálně před jeho základní demonstrovanou podobou.

```
$username = mysql_real_escape_string($username);
$password = mysql_real_escape_string($password);
```

3.5.1.2. XSS

Je zkratkou pro metodu **Cross-Site Scripting**, která představuje zranitelnost na straně webového serveru. Studie z roku 2010 uvádí, že až 71 % všech webových aplikací je na zranitelnost typu XSS náchylných, dokonce bývá některými odborníky v oboru bezpečnosti podceňovaná. (44)

Zranitelnost je založena na skriptovacích jazycích vykonávajících se na straně klienta, které vytvářejí dynamický vzhled a obsah stránky. Skripty vytvářejí aktivní obsah pomocí malých spustitelných souborů nebo skriptů, které jsou prohlížečem spouštěny pro vytvoření dynamického obsahu a mohou tak převzít velkou část zatížení serveru. Prvními skriptovacími jazyky využívajícími se pro tvorbu dynamického obsahu webových stránek, byl JavaScript a Java od Sun Microsystems[24], která disponovala vynikajícím bezpečnostním

[24] V roce 2009 byla společnost Sun Microsystems odkoupena společností ORACLE

modelem a stala se tak jedním z dominantních vývojových nástrojů pro Internet. Nicméně, mezi tvůrci webových aplikací se nejvíce ujal JavaScript, který si je získal svou jednoduchostí a rozšířením. (30) (44) (42)

Při využívání sofistikovanějších XSS útoků musí být útočníkova úroveň znalosti skriptovacích jazyků na pokročilé úrovni a zároveň mít povědomí o technologiích tvořících obsah webových stránek – HTML, CSS a DOM[25]. Pro simulaci útoku bylo primárně využito funkcí JavasScriptu, který je stěžejní pro spuštění škodlivého kódu v rámci pokusných webových stránek. Útok je ve své základní podobě prezentován formou dialogové hlášky, za využití metody *alert()*, která je pro útočníka indikátorem napadnutelnosti webové stránky metodou XSS. (30) (44)

Nyní teoreticky k samotnému průběhu útoku, během kterého se útočník s využitím skriptovacího jazyka pokouší na webové stránce spustit svůj skript, který následně ovlivní výslednou podobu webové stránky. Takto pozměněná webová stránka může být u jednoduchých metod např. přebarvená nebo pozměněn text, ale u metod sofistikovanějších může zobrazovat jiné formuláře, měnit její kontext, zobrazovat dialogy a nepřeberné množství dalších funkcionalit *JavaScriptu*. Jeho nebezpečnost tkví v tom, že může být spuštěn nejen z parametru URL odkazu, ale může být i součástí hlaviček požadavku nebo umístěn přímo v databázi. (44)

Útoky typu XSS lze rozdělit do tří skupin:

- **Stored** (persistent) - jsou typy útoků u kterých oběť nemusí na webové stránky přistupovat přes upravený odkaz, aby došlo ke spuštění útočného skriptu, ale ten už je uložen v databázi cílového serveru a je spuštěn při zaslání požadavku
- **Reflected** (non-persistent) - jedná se o nejběžnější typ XSS útoku, protože je i nejjednodušší a je nejčastěji umístěn v parametru URL odkazu a je spuštěn načtením cílové webové stránky
- **DOM** – obdoba reflected XSS, ale využívá DOM již existujícího klientského skriptu, který využije k přenesení vlastního kódu do skriptu stránky (44)

[25] Document Object Memory(DOM) je objektový model dokumentu, prostřednictvím jehož metod a vlastnosti jednotlivých uzlů přistupujeme k samotným objektům umístěných na webové stránce (36)

3.5.1.2.1. Praktická ukázka útoku

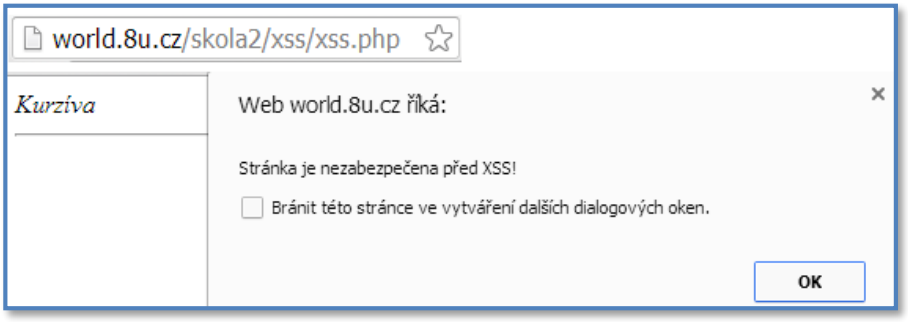
Na výzkumné webové stránce byl vytvořen jednoduchý formulář, který simuluje vkládání textových komentářů např. k článkům, obrázkům, filmům, produktům atp. Po vložení textu do textového pole a následném odesláním se provede jeho uložení do samostatného textového souboru *komentare.txt,* z kterého jsou následně načítány ve formě obsahu na webovou stránku (viz. Příloha K). Na uvedeném příkladu byla simulována metoda reflected XSS (non-persistent), která je založena na předání skriptu GET/POST požadavkem, pod některým z přenášených parametrů.

Pokud v rámci formuláře pro vkládání textového komentáře dojde k vložení HTML elementu např. **Kurzíva**, pak se zobrazí text zvýrazněný kurzívou „*Kurzíva*“. V případě, že se text skutečně zobrazí kurzívou, pak se může jednat o prvotní indikátor, který by útočníkovi prozradil, že je stránka náchylná na útok typu XSS. V dalším kroku následuje pokus, v rámci kterého se útočník pokouší spustit skript při načtení webové stránky, který je v případě úspěchu reprezentován dialogovým oknem. Útočník se samozřejmě mohl ihned pokusit spustit skript a vynechat využití HTML elementu, ale cíl práce je především založen na vysvětlení problematiky dané zranitelnosti.

Spuštěný skript může mít následující podobu:

```
<script>alert('Stránka je nezabezpečena před XSS!');</script>
```

Z obrázku níže (viz. Obrázek 12) je patrné, že útočný skript byl skutečně načten prostřednictvím formuláře pro vkládání komentářů. Pro útočníka by se jednalo o indikaci, že je webová stránka zranitelná prostřednictvím útoku typu XSS a mohl by se pokusit implementovat sofistikovanější metody k oklamání uživatele. Pro hledání webových stránek s XSS zranitelností se často využívají webový roboti prohledávající obsah internetu.



Obrázek 12 - Načtení XSS skriptu webovou stránkou

Zdroj: vlastní zpracování

3.5.1.2.2. Ochrana před útokem

Při ochraně před útokem typu XSS je nutné zmínit, že JavaScript je spouštěn na straně klienta a z toho důvodu je potřeba provést opatření v skriptu, vstupních parametrech a požadavcích, protože útočník může persistent útoky spouštět přímo z databáze.

Ochrana na straně klienta – Je zvlášť obtížná, protože útok se může skrývat pod každým odkazem, především na webových stránkách, které obsahují pochybný a útočný obsah. Navíc v kombinaci s dalšími metodami např. *phising* se uživatel může stát obětí podvodné zprávy, která odkazuje na odkaz, který uživatele může přesměrovat na skutečnou stránku, ale se spuštěným aktivním obsahem útočníka. Praktické rady spočívají ve vypnutí aktivního skriptování ve webovém prohlížeči, tím dojde k zabránění webovým serverům a e-mailovým červům ve snadném shromažďování informací. (30)

Ochrana na straně serveru - Spočívá v zajištění validace všech vstupních hodnot aplikace. Validační funkce by měly odstraňovat speciální znaky nebo je nahrazovat a ukládat v jiné formě. To spočívá hlavně v odstraňování špičatých závorek < >, které uzavírají skriptovací *tagy* využívající se ke spuštění aktivního obsahu na webových stránkách. Dalším způsobem ochrany je využití funkce **escapování**, která funguje na principu vkládání zpětného lomítka před potencionálně nebezpečné speciální znaky (nebo jejich převádění do entitní podoby). (30)

Speciální znaky jsou tak přenášeny a ukládány v kódované podobě, která pozmění jejich význam na prostý text:

Znak & je odeslán jako **&**

Znak < je odeslán jako **<**

Znak > je odeslán jako **>**

Znak " je odeslán jako **"**

Znak ' je odeslán jako **'**

Znak / je odeslán jako **/**

3.5.1.3. Session hijacking

Typy útoků, které jsou založeny na speciálních souborech *cookies*, též přezdívaných drobečky, které slouží k uchovávání stavů, informací a dalších specifických parametrů o uživatelské návštěvě webové stránky. Pomocí těchto souborů uložených ve webovém prohlížeči uživatele, dojde k jeho rozpoznání webovým serverem, který mu tak umožní např. zobrazení osobního obsahu, cílení reklamy nebo uchovávání relací. (30)

Často jsou soubory *cookies* nastavovány v rámci relace, která je uchovává v operační paměti a jejich platnost je buď omezena zavřením webového prohlížeče, nebo vypršením jejich doby platnosti. V dřívějších dobách, ve kterých byl nejpoužívanějším prohlížečem Internet Explorer, se cookies ukládali ve speciální systémové složce, nicméně s příchodem a rozšiřováním konkurenčních webových prohlížečů, došlo k jejich decentralizaci a prohlížeče je začali uchovávat pod svými profily.

Zranitelnost založená na *session hijacking* neboli ukradení relace umožňuje útočníkovi na základě odcizení souborů cookies získat přístup k důvěrným informacím nebo identitě uživatele. Metody, které se za tímto účelem využívají, jsou založeny na odposlouchávání komunikace sítě tzv. *spoofing* nebo důmyslnějších způsobech, které mohou využívat aktivního obsahu. Po získání souborů cookies je útočník odešle cílovému serveru, který mu např. zpřístupní osobní obsah „okradeného“ uživatele. K odposlechu síťové komunikace lze využít softwarového nástroje **Achilles**, který je založen na odposlouchávání síťové komunikace mezi serverem a uživatelem (formou proxy serveru), ze které lze v případě nezabezpečeného spojení zachytit soubory *cookies*. (30)

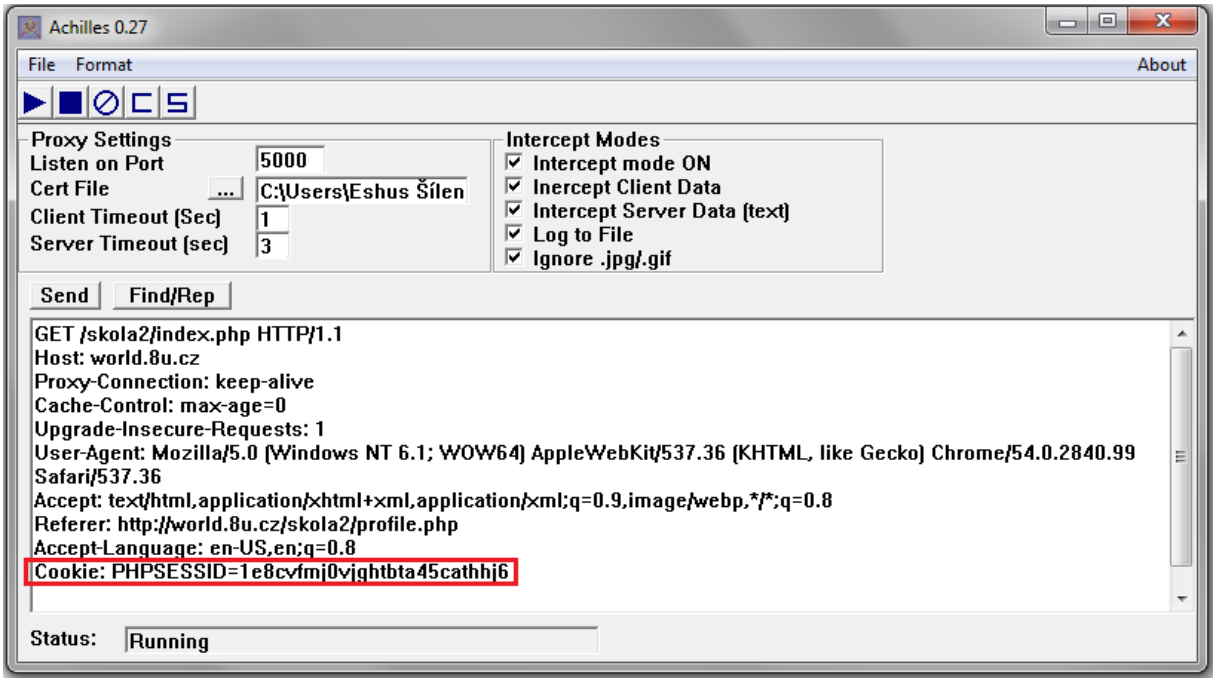
Soubory cookies mohou mít prakticky jakoukoliv podobu, od jednoznačného identifikátoru po specifický text, kdy jejich podoba je závislá na jejich užití. V případě cookies, která ve formě jednoznačného identifikátoru slouží k rozpoznání relace, by měla být odolná proti

běžným metodám útoků, založených na hrubé síle. Proto jejich hodnoty běžně nabývají náhodných řetězců tzv. *hashů,* které jsou proti těmto metodám chráněny např. hodnota **kq176duiu33nn1n2hrok1lso55.** Každá cookies disponuje doménou, ke které je určena a datem exspirace. Pro uživatele jsou informace o uložených souborech cookies běžné dostupné a mohou s nimi manipulovat pomocí různých doplňků a modulů webových prohlížečů.

3.5.1.3.1. Praktická ukázka

Prvotně je potřebné provést počáteční nastavení programu Achilles a webového prohlížeč, aby veškerá komunikace směřovala prostřednictvím *proxy* serveru, který je reprezentován programem Achilles. Ve webovém prohlížeči je potřeba nastavit *proxy* server na lokální síť 127.0.0.1 a port 5000, na kterém program naslouchá. Součástí programu je řada funkcí, které poskytují správu logů, ignoraci obrázků, získávání klientských nebo serverových dat a *intercept* mode, který umožní nastavit chování programu jako *proxy* serveru nebo ve formě prostředníka. (45) (42)

Na obrázku níže, který byl pořízen z programu Achilles je zachycen záznam komunikace mezi pokusnou webovou stránkou a serverem, během které se odesílají požadavky a součástí jejich hlaviček jsou i soubory cookies. Zachycené soubory cookies jsou využívány jako identifikátor relace a v případě jejich nedostatečného zabezpečení, získá útočník jejich odcizením přístup k účtu oběti. Útočník je následně využije v komunikaci se serverem, který jej bude považovat za originálního vlastníka. Úprava souborů *cookies* je snadná pomocí řady doplňků a pluginů např. *EditThisCookie*, protože jsou uloženy v paměti webového prohlížeče. (42)



Obrázek 13 - Zachycení komunikace programem Achilles

Zdroj: vlastní zpracování

3.5.1.3.2. Ochrana před útokem

Možné způsoby ochrany jsou opět rozděleny z hlediska pohledu uživatelského a serverového. Pro uživatele jsou platná obecná pravidla a doporučení, která doporučují nevstupovat na podezřelé webové stránky, využívat šifrovaného spojení a být na pozoru před webovými stránkami využívající cookies. V dnešní době je zvlášť poslední ze zmiňovaných doporučení velmi sporadicky řečeno a problematicky realizovatelné, protože cookies jsou využívány pro uchování relace, analytickými nástroji pro měření a vyhodnocování uživatelských dat. Nicméně, moderní webové prohlížeče disponují funkcionalitou, která umožňuje vypnutí souborů cookies, ale tím se uživatel vystaví nedostupnosti webových stránek, které nejsou bez vytvoření relace přístupné (zejména pak webové stránky vyžadující přihlášení).

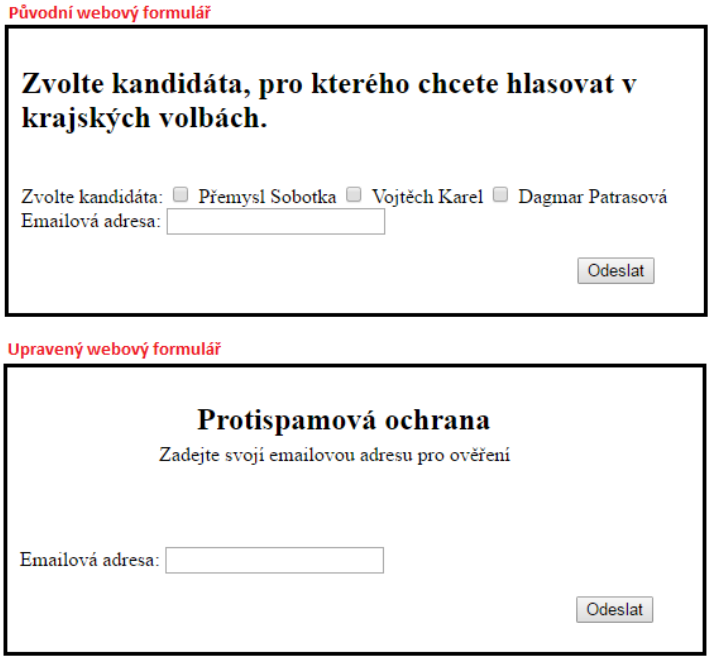
Při zaměření se na ochranu ze strany serveru, se lze setkat v publikacích z počátků 21. století s radami, které nabádají k úplnému vyhnutí se souborům cookies. Nicméně, dnešní doba se ubírá jiným směrem a bezpečnost je na výrazně vyšší úrovni než byla dříve. Na straně serveru by měla být zajištěna ochrana před zneužitím souborů cookies při případném odcizení a to zejména používáním omezeného data exspirace, využit cookies s delší lhůtou exspirace mohou využít sledovací cookies, ale rozhodně ne ty, které uchovávají ID relace!

Jako další způsob ochrany lze využít ověřování IP adres, kdy při využití cookies prostřednictvím jiné IP adresy než které byla určena, se stává neplatnou.

3.5.1.4. Clickjacking

Typy útoků, které jsou zaměřeny na koncové uživatele a jsou úzce provázány se zranitelností typu CSRF (Cross-Site Request Forgery), která je útočníky využívána k přimění uživatele, provést nechtěný požadavek vůči aplikaci, ke které je přihlášen. Zranitelnost využívá rámů a ve své elementární podobě, může fungovat jako prostředek pro agresivní reklamu a přesměrovávání uživatelů. Takto útočné prvky se nacházejí zejména na webových stránkách s pochybným a nebezpečným obsahem, které uživatele při klikání na prvky stále přesměrovávají nebo jim zobrazují reklamy. (44)

Ve své sofistikovanější podobě útočník využije rámů, aby na své webové stránce provedl zobrazení cílového formuláře, který je ale umístěn na jiné webové stránce. Útočník následně provede modifikace, které za pomocí kaskádových stylů a dalších rámů, způsobí změnu kontextu formuláře. Výsledná podoba formuláře může být diametrálně odlišná od jeho původní podoby, protože v rámci stylování webové stránky lze ponechat jen vybraná pole, text nebo aktivní prvky. V moci útočníka je provést změnu existujícího formuláře, který je např. určen pro hlasování, odesílání emailů nebo přesměrování zpráv, aby byl pro příchozího uživatele navenek neškodný a kompletně odlišný od své původní podoby.



Obrázek 14 - Ukázka upraveného formuláře pomocí clickjackingu

Zdroj: vlastní zpracování

Výsledný útok může mít podobu protispamové ochrany (viz. Obrázek 14), která je pro uživatele navenek neškodná, ale její původní účel je zcela odlišný. Útočník v rámci své webové stránky provede vložení formuláře pocházejícího z cizí webové stránky formou rámu (na obrázku uveden jako *Původní webový formulář*). Původní účel formuláře může být prakticky libovolného rázu. Pro simulaci útoku byl využit fiktivní webový formulář pro krajské volby, který je dostupný po přihlášení v rámci volebních stránek. Následně útočník provede překrytí nechtěných částí dalším rámem, v rámci kterého provede vložení vlastního obsahu sloužícího k oklamání uživatele. Následný příchozí uživatel vyplní svou emailovou adresu v přesvědčení, že se jedná o protispamovou ochranu (na obrázku uvedena jako *Upravený webový formulář*), ale jejím vyplněním a odesláním formuláře, provede volbu kandidáta do krajských voleb. Zdrojové kódy ze zmiňované simulace, jsou součástí přílohy práce jako Příloha E a F.

3.5.1.4.1. Ochrana před útokem

Pro uživatele platí obecné rady a doporučení, které jsou založeny na prevenci, tzn. nevstupovat na pochybné stránky a být obezřetný. Vývojáři mají z hlediska prevence *clickjackingu* více možností, protože se jedná o útok, který je založen na načtení cílové stránky v rámci útočné stránky, proto by tato možnost měla být regulována. První možností,

která je dlouhodobě využívána je krátký JavaScriptový kód, který kontroluje, zdali je stránka na vrcholu hierarchie DOM, pokud není, tak dojde k přepsání vlastnosti *location* a stránka se stane kořenovým dokumentem. Bohužel, i způsob ochrany založený na JavaScriptu má své nedostatky, protože se jedná o řešení na straně klienta, který může mít zakázáno spouštění skriptů, na kterých je ochrana založena. (44)

V reakci na rozšiřující se zneužívání clickjackingu, vznikla nová HTTP hlavička *X-FRAME-OPTIONS*, kterou lze použít s upřesňujícím nastavením načítání obsahu do rámů:

Tabulka 5 - Nejpoužívanější MIME typy X-FRAME-OPTIONS

DENY	Zákaz jakéhokoliv načítání stránky do rámu
SAMEORIGIN	Stránku mohou načítat do rámu pouze stránky stejné domény
ALLOW-FROM	Umožňuje definovat povolené zdroje

Zdroj: KÜMMEL, Roman. Nejpoužívanější MIME typy. (44 str. 92)

Další možnost ochrany je založena na bezpečnostní politice *Content Security Policy*[26], která obsahuje direktivu *FRAME-ANCESTORS*. Uvedená bezpečnostní politika umožňuje definovat zdroje pomocí HTTP hlavičky, které mohou danou stránku načítat do rámu. (44)

[26] Obsahuje definice a mechanismy, pomocí kterých mohou webový vývojáři určit zdroje, které konkrétní webová stránka může načítat nebo spouštět, stejně tak obsahuje několik relevantních bezpečnostních rozhodnutí příslušné politiky.

4. Praktická část práce

Na základě postupující integrace bezdrátových prvků do okolního prostředí, roste riziko ztráty soukromí a možnosti realizace sofistikovanějších útoků za použití nejen technologií, ale i psychologických poznatků.

Praktická část práce byla vytvořena se zaměřením na možnosti využití bezdrátového zařízení, které umožňuje monitorování provozu a komunikace bezdrátových sítí. Zařízení nebylo použito za účelem poškozování cizího majetku, omezování osobní svobody ani k sledování přepravovaných informací, ale k získání informací o uživatelích, kteří se připojují k veřejným bezdrátovým sítím a to na základě volně poskytovaných identifikátorů. Aby nedošlo k zásahu do práv osob k zařízení připojených, bylo potřebné brát ohled na charakter shromažďovaných informací, které byly získávány za účelem vyhodnocení výsledků pozorování, ze kterých byly vyvedeny patřičné závěry.

Výzkum byl realizován za pomocí veřejné bezdrátové sítě Wi-Fi, prostřednictvím které je poskytováno internetové připojení na základě autorizace uživatele tzn. odsouhlasení podmínek a řádu veřejné Wi-Fi sítě (viz. Příloha I). Součástí zmiňovaného souhlasu je informace o účelu uvedeného projektu a čestné prohlášení, které pojednává o úmyslech autora výzkumu. V rámci prohlášení je definován způsob zacházení se získanými informacemi, které nebudou využity za účelem marketingové komunikace, ani poskytnuty třetím osobám. Soubor informací, které jsou o připojených uživatelích a zařízeních získávány, je uveden v následných podkapitolách práce, aby byla dodržena obsahová struktura práce.

Zařízení bylo sestaveno z několika dílčích částí, které ve svém funkčním celku disponují dostatečnou mobilitou a provozuschopností v řádu desítek hodin, které je dosaženo za využití přenosného zdroje elektrické energie, bezdrátového zařízení, paměťové karty a zdroje internetového připojení, které bude realizováno formou mobilního internetu. Soustava zařízení je při své kompaktnosti umístitelná např. ve veřejné dobíjecí stanici pro elektrická zařízení, batožinách, bezpečnostních schránkách nebo na jiných místech, která budou pro účely projektu stanovena jako vyhovující. Při výběru měřených lokalit bylo postupováno na základě jejich potencionálního zájmu, ze strany okolních uživatelů, kteří by mohli využít služeb veřejné Wi-Fi sítě. Pro měření byly záměrně vybírány lokality, které byly na základě okolních faktorů vyhodnoceny jako zajímavé. A za účelem potvrzení

hypotéz, očekávání a předpokladů, byly provedeny měření i v oblastech stanovených jako nezajímavé z hlediska provádění výzkumu.

Na základě zjištěných poznatků pozorování, byla provedena analýza a prezentace výsledků, které vypovídají o podílu uživatelů využívajících veřejných Wi-Fi sítí, vlivu hodnoty zařízení na využívání veřejných Wi-Fi sítí a dalších průzkumných charakteristik. Uživatelé využívající nezabezpečených Wi-Fi sítí, mnohdy netuší o nebezpečích, kterým se svým počínáním vystavují. V případě realizace útoku prostřednictvím přípojného bodu, může docházet k sledování komunikace, shromažďování osobních informací nebo k aplikování metod sociálního inženýrství a psychologie, za účelem oklamání uživatele.

4.1. Použitá zařízení

Pro sběr kvantitativních i kvalitativních dat prostřednictvím monitoringu bezdrátových sítí, bylo potřeba využít kombinace zcela odlišných zařízení, které v konečném důsledku vytvořili vysoce mobilní jednotku, kterou je možné využít v prostředí se stálým zdrojem elektrické energie i v terénu, díky použitému záložnímu zdroji elektrické energie. V následujících podkapitolách jsou uvedeny technické vlastnosti použitých zařízení, případně jejich nedostatky a jejich primární účel použití.

Veškerá zařízení byla pořízena z finančních prostředků autora práce a jejich použití není v rozporu se zákony a vyhláškami České republiky, zejména se zákony §182 Porušení tajemství dopravovaných zpráv a §230 Neoprávněný přístup k počítačovému systému a nosiči informací. I přes oficiální nedostupnost zařízení na území ČR a potencionálního nebezpečí plynoucího z využívání souboru zařízení, bylo zařízení slovy autora využito ke svému primárnímu účelu – penetrační testování. Data získaná z jeho provozování, slouží pro analýzu současné situace bezpečnosti bezdrátových zařízení, uživatelů a použitých zařízení.

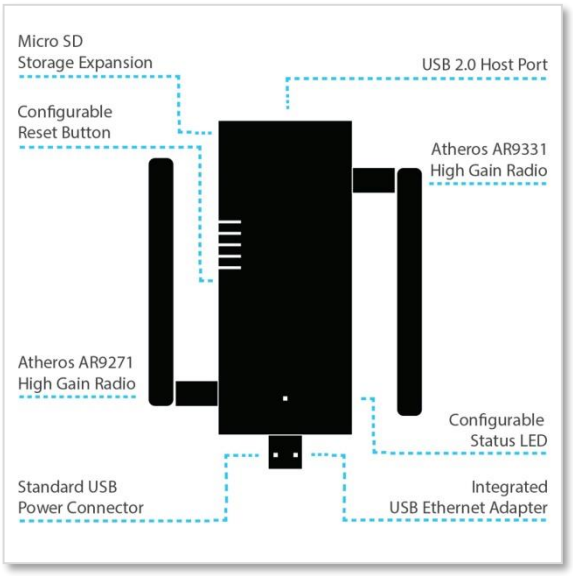
Obrázek 15 - Zkompletovaná měřící soustava zařízení

Zdroj: vlastní zpracování

4.1.1. Bezdrátový přípojný bod

Pro potřeby výzkumu bylo využito multifunkčního zařízení WiFi Pineapple, které je šestou generací a ve svém provedení NANO kombinuje výkon technologicky výkonnější verze TETRA s důrazem na mobilitu. Zařízení byla za dobu svého osmiletého vývoje postupně zdokonalována, aby poskytla stabilní prostředí pro vykonávání penetračního testování bezdrátových Wi-Fi sítí.

Zařízení přes své kompaktní rozměry 122 mm x 47 mm (bez připojených periferií) disponuje dvěma čipy pro bezdrátové Wi-Fi sítě (viz. Obrázek 16) s podporou standardů IEEE 802.11 b/g/n. Prvním z čipů je ***Atheros AR9331***, který disponuje větším výkonem, a zařízením je primárně využíván pro skenování okolních přípojných bodů, uživatelů a jejich monitorování. Druhým čipem je **Atheros AR9271**, který je využíván pro správu přístupových bodů, ke kterým se klienti připojují a k hostování přístupového bodu pro správu zařízení tzv. *management interface*.



Obrázek 16 - Diagram zařízení WiFI Pineapple NANO

Zdroj:Hak5. Nano diagram. [Online] ©2017. Dostupné z: https://www.wifipineapple.com/pages/nano

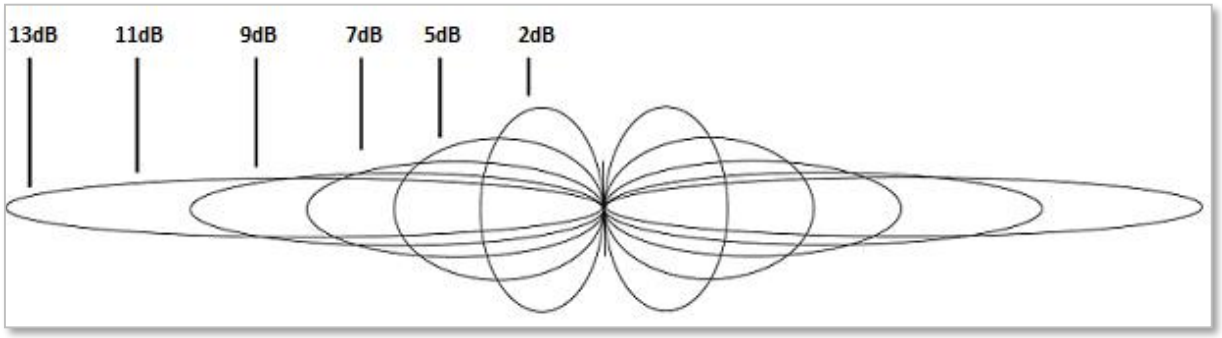
Zařízení disponuje přednastaveným operačním systémem Linux v distribuci OpenWRT, který je určen pro *embedded* (vestavěné) síťové prvky a pro použití v zařízení WiFi Pineapple byl speciálně modifikován, aby odpovídal specifickým požadavkům. Z hlediska použití operačního systému, který je dimenzován pro zařízení s nízkým výpočetním výkonem je odpovídající i operační paměť o velikosti 64MB typu *DDR2* a interního elektronicky nezávislého úložiště typu EEPROM (*Electrically Erasable Programmable Read-Only Memory*) s kapacitou 16MB. Kapacita interního úložiště může být prostřednictvím Micro SD slotu rozšířena paměťovou kartou.

Pro zvýšení dosahu vyzařovaného signálu přípojných bodů, ke kterým se připojují koncoví uživatelé, byla na základě kompromisu mezi výkonem, spotřebou elektrické energie a vyzařovacím úhlem, zvolen všesměrová anténa se silnějším ziskem, druhá anténa byla ponechána nezměněná.

"Zisk antény G je jedním z podstatných ukazatelů kvality antény. Je definován jako poměr intenzity vyzařování U v daném směru vůči celkovému vstupnímu výkonu P_{in} vyzářeného izotropickou anténou děleném 4π." (46 str. 125)

Oproti původní anténě se ziskem 2dBi, byla zvolena anténa se ziskem 9dBi, která poskytne větší dosah vyzařovaného signálu (viz. Obrázek 17) v rámci horizontálního úhlu (při

standardním použití antény dle pokynů výrobce). Bohužel, větší dosah vyzařovaného signálu je kompenzován snížením prostorového pokrytí na vertikální ose. Nicméně, uvedená kompenzace je pro výzkum výhodná, protože je prováděn převážně v otevřených prostranstvích a v případě uzavřených objektů s případnými výškovými výkyvy, je možné anténu vyměnit pro dosažení vyšší úrovně vertikálního pokrytí.



Obrázek 17 - Srovnání vyzařovaného signálu podle zisku antény (vertikální pohled)

Zdroj: ALFA NETWORK. Wireless Antenna Properties. [Online] ©2011. Dostupné z: https://www.alfa.com.tw/faq_show.php?sn=10

4.1.2. Datové úložiště

Z důvodu omezené kapacity použitého bezdrátového zařízení (viz. Kapitola 4.1.1), bylo potřebné implementovat dodatečné úložiště dat, které by navýšilo interní kapacitu zařízení pro uložené soubory. Pro navýšení kapacity z původních 14.2 MB (celková kapacita interního úložiště je 16MB), má zařízení k dispozici slot pro paměťové karty typu Micro SD. Dalším důvodem pro využití externího paměťového úložiště tkví v poskytnutí veškerých paměťových kapacit operačnímu systému, který využije externí úložiště pro uchování logů, dočasných souborů a pro načítání HTML souborů připojeným uživatelům (zejména souborů, které jsou použity na přihlašovací webové stránce).

Pro zařízení byla vybrána datová karta **Sony micro SDHC 16 GB Class 10**, která disponuje kapacitou 16GB a rychlostní třídou 10, která dosahuje rychlosti čtení a zápisu až 90MB/s. Takové hodnoty jsou pro provedený výzkum značně naddimenzované, ale v době jejího pořízení nebyla specifikována struktura pořizovaných dat a jejich rozsah. Současně je karta v provedení, které je schopné odolávat vysokým teplotám, nárazům a poskytuje počítačový software pro záchranu poškozených nebo smazaných souborů.

4.1.3. Zdroj internetového připojení

Zařízení disponuje dvěma všesměrovými anténami, USB typu *male* s podporou Ethernetu a USB portem 2.0 typu *female* (viz. Obrázek 16). Uvedené konektory a síťové prvky umožňují získávat internetové připojení zcela odlišnými způsoby. Zařízení může využívat jednu z integrovaných antén pro příjem bezdrátového signálu a poskytovat ho prostřednictvím druhé antény připojeným uživatelům. Funguje tedy jako určitý typ přemosťovače signálu. Bohužel, přemostění signálu není pro výzkum použitelné, protože při použitém nastavení pracuje WiFi Pineapple v režimu, který využívá obou bezdrátových vysílačů současně.

Další možnosti jsou si vzájemně velmi podobné, první z nich je založena na připojení zařízení prostřednictvím konektoru USB typu *male* s podporou Ethernetu k počítači, který disponuje internetovým připojením. Typ připojení nehraje klíčovou roli a může se jednat o bezdrátové nebo kabelové připojení, které uživatel přemostí a umožní připojenému WiFi Pineapplu využívat sdíleného připojení. Jedná se o jednu z metod použitelnou pro výzkum, ale je velmi závislá na zdroji internetového připojení a elektrické energii, tudíž není příliš vhodná pro déletrvající a terénní měření. Druhá metoda využívá zdroje internetového připojení prostřednictvím zařízení disponujícího mobilním internetovým připojením, které je sdíleno prostřednictvím USB konektoru. Moderní mobilní telefony a tablety umožňují prostřednictvím USB propojení sdílet internetové připojení pomocí technologie nazývané *USB Tethering*. Uvedená metoda je oproti předchozí variantě minimálně energeticky závislá a poskytuje určitou úroveň nezávislosti a mobility při měření, proto je při výzkumu nejčastěji využívána za použití mobilního telefonu **Samsung Galaxy S7 Edge**. Pro minimalizaci energetické závislosti je možné využít USB adaptéru, který disponuje SIM kartou s internetovým připojením.

Třetí možnost je založena na první metodě, ale k získání internetového připojení využívá dodatečné antény, která je připojena k zařízení Pineapple prostřednictvím USB typu *female*. V tomto případě dochází k přemosťování internetové připojení z dostupných okolních bezdrátových sítí uživatelům připojeným k přípojným bodům vysílaných zařízením WiFi Pineapple.

4.1.4. Zdroj elektrické energie

Pro využití zařízení nezávisle na zdroji elektrické energie, byl pořízen přenosný zdroj elektrické energie **Xiaomi Power Bank 20000mAh White**. Bohužel, je rozsáhlým marketingovým trikem, u zdrojů externího napájení, uvádět kapacitu při odběru elektrického napětí ve výši 3.7 Voltů, ovšem odběr většiny zařízení připojených přes rozhraní USB odebírá elektrické napětí na úrovni 5 Voltů a tím je ovlivněna výsledná kapacita zdroje na 12700mAh. Zařízení je kromě externího zdroje elektrické energie možné připojit k jakémukoliv zdroji elektrické energie, který umožní připojení prostřednictvím USB (viz. Kapitola 4.1.1).

V závislosti na využívání připojených komponent (bezdrátový přípojný bod a zdroj mobilního internetu), které mohou za hodinu provozu spotřebovat od 500 do 2000mAh kapacity baterie, je teoreticky dosažitelná výdrž sestavy zařízení v rozmezí 6 až 25 hodin. Odhadovaná výdrž externí baterie je pro provedení výzkumu v terénu dostatečná, protože je z důvodů většího pohybu osob prováděn v nejvíce aktivních částech dne a na místech, s vysokým výskytem osob, proto zjištěnou výdrž baterie nepřekročí.

4.2. Stanovení očekávání, předpokladů a hypotéz

Před započetím výzkumu bylo vhodné si stanovit očekávání, předpoklady a hypotézy, na základě kterých bude možno stanovit východiska a zhodnocení výzkumu diplomové práce. Práce je zaměřena na útoky v online prostředí, které jsou převážně vedeny proti koncovým klientům (uživatelům), kteří bývají nedostatečně informováni (gramotní) nebo neberou dostatečně v zřetel možná rizika plynoucí z operování v online prostředí prostřednictvím veřejných Wi-Fi sítí. Výzkum je prováděn prostřednictvím Wi-Fi přístupových bodů pracujících v určité formě *promiskuitního* režimu, který je blíže popsán v následujících kapitolách zabývajících se implementací zařízení.

Základní otázkou, na kterou se výzkum snaží nalézt odpověď je: **Využívají uživatelé veřejné bezdrátové sítě Wi-Fi bez ohledu na možná rizika? A jsou veřejné sítě bezpečné**? Je vysoce pravděpodobné, že podstatný vliv na tuto skutečnost mají klimatické podmínky[27], zkoumaná oblast a cílová skupina klientů, na kterých je výzkum prováděn,

[27] V souvislosti s podílem výskytu a fyzickou aktivitou osob, která je přímo závislá na okolní teplotě

a proto je metodou váženého bodového součtu provedeno zjištění funkce užitku jednotlivých měření.

Výzkum je dále složen z dílčích částí, ve kterých jsou analyzovány získaná data za pomoci vhodných analytických a statistických nástrojů, které poskytnou obecný přehled o uživatelích připojujících se k veřejným Wi-Fi sítím. Zejména bude docházet k identifikaci připojených uživatelů na základě dvou úrovní, které budou závislé na stupni aktivity uživatele, která poskytne detailnější data o připojených klientech a jejich zařízení. Kromě získání obecného přehledu o uživatelích, byla stanovena hypotéza, která předpokládá, že hodnota zařízení nemá vliv na využívání Wi-Fi sítí. Hypotéza vychází z teoretického poznatku, že uživatelé disponující zařízením s vyšší cenovou hladinou, nevyužívají veřejných Wi-Fi sítí, protože takový uživatelé disponují dostatečnými finančními prostředky pro pořízení mobilních dat.

V neposlední řadě je výzkum prováděn v odlišných prostředích, které vykazují vysoký výskyt osob a lze předpokládat vyšší míru jejich aktivity. Ovšem odlišují se úrovní dostupnosti a variabilitou veřejných Wi-Fi sítí a dalšími okolními faktory. Před započetím výzkumu lze konstatovat, že je bezpředmětné provádět měření v oblastech s nízkou koncentrací osob – periferie měst a oblasti s všeobecně známou nízkou úrovní osídlení, ale pro vyloučení špatného úsudku, bude provedeno kontrolní měření, které uvedený předpoklad potvrdí nebo vyvrátí.

4.3. Příprava prostředí

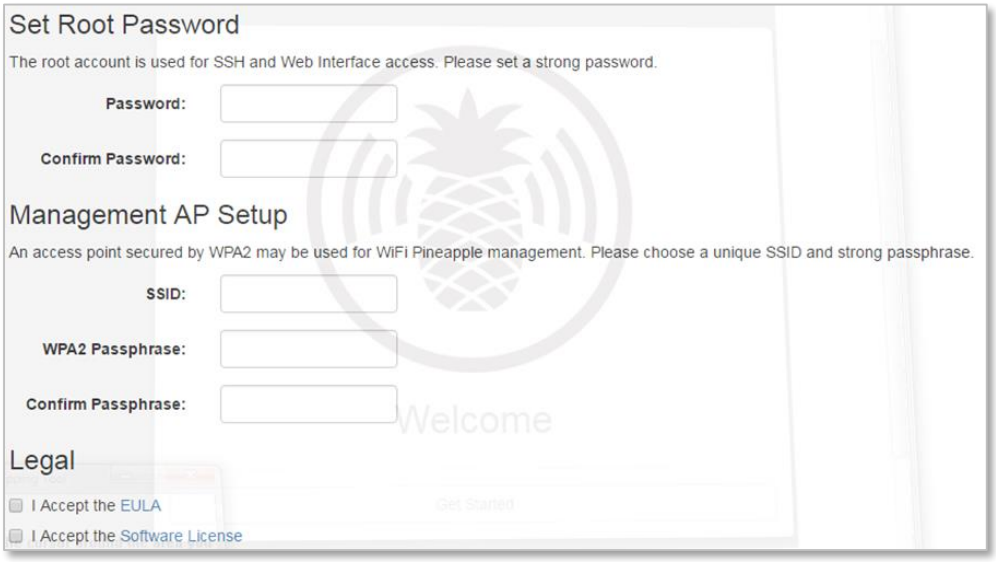
V předcházející kapitole 4.1, byla představena použitá zařízení z technického hlediska s důrazem na *hardware*. V následující kapitole je popsáno *softwarové* řešení, které umožní ve svém funkčním celku získávat potřebná výzkumná data, která budou použita pro analýzu, ověření hypotéz a k prezentaci výsledků výzkumu a celé diplomové práce. Při vytváření, optimalizaci a úpravě prostředí, bylo vycházeno z teoretických poznatků popsaných v přehledu řešené problematiky (viz. Kapitola 2), zejména z podkapitol zabývajících se technologiemi, metodami používanými k útokům v online prostředí a možnými způsoby ochran.

4.3.1. Prvotní inicializace zařízení

Po připojení zařízení k elektrickému zdroji napětí prostřednictvím větveného USB kabelu (zapojení obou konektorů k zdroji elektrického napětí není vyžadováno, ale v případě nedostatečného zdroje napětí, může dojít k nesprávné funkci nebo k poškození zařízení), dojde ke spuštění zavaděče operačního systému, tento proces je doprovázen blikáním modré LED diody. Uživatel je informován o úspěšném zavedení operačního systému indikační diodou, která začne soustavně vyzařovat světlo modré barvy a poskytne informaci pro uživatele, že zařízení je připraveno k použití.

V závislosti na uživatelově operátorském přístupu, který může být veden prostřednictvím webového rozhraní nebo prostřednictvím mobilní aplikace *WiFi Pineapple Connector*, nastane automatické nebo manuální přesměrování operátora na lokální webovou stránku http://**172.16.42.1:1471/**, na které je umístěno administrační rozhraní zařízení WiFi Pineapple, prostřednictvím responzivního webového rozhraní.

Při prvotní inicializaci je operátor uvítán a je vyzván k zadání údajů, které slouží k budoucím přístupům do administrace zařízení (viz. Obrázek 18). Operátor je vyzván, aby zadal heslo pro *root* uživatele, pod kterým bude probíhat operátorské přihlášení do administračního rozhraní a nastavení přístupového bodu, který je určen pro přístup k *management interface* zařízení WiFi Pineapple.



Obrázek 18 - Úvodní konfigurace zařízení WiFi Pineapple

Zdroj: vlastní zpracování

4.3.2. Nastavení zařízení

Zařízení je určené pro penetrační testování bezdrátových Wi-Fi sítí a je dostupné pro široký okruh veřejnosti, která sdílí své poznatky a znalosti prostřednictvím diskusního fóra pod záštitou tvůrců, kteří své vědomosti sdělují účastníkům a získávají cenné odezvy. Na základě hojné uživatelské základny je dostupná řada modulů (aktuálně je k verzi NANO dostupných 38 modulů, které jsou včetně grafického rozhraní) a funkcí, které jsou soustavně vyvíjeny, vylepšovány a v případě vysoké úrovně zájmu implementovány přímo do přednastaveného operačního systému zařízení.

Při realizaci prostředí, které umožní provedení výzkumu, bylo vhodné využít modulů, které jsou dostupné a schopné vykonávat potřebné kroky pro získání požadovaných výzkumných dat. Opětovné vytváření již vyvinutých modulů by bylo značně kontraproduktivní a nebylo by dosaženo takové kvality již existujících modulů, které jsou vyvíjeny v řádu let. Pro realizaci výzkumu se jevili jako vhodné moduly zejména: **EvilPortal** (umožňující přesměrovat uživatele na připravenou webovou stránku), **Cabinet** (souborový manažer umožňující práci s Unixovou strukturou) a **ConnectedClients** (poskytující informace o připojených klientech). Jedná se o stručný výčet modulů, které jsou pro získávání dat kritické a kterým se věnují následující podkapitoly. Zároveň byly využity funkcionality předinstalovaných doplňků pro logování aktivit a správu přípojných bodů – **PineAP**.

4.3.3. EvilPortal

Modul umožňující definovat tzv. *landing page*, která slouží jako záchytná webová stránka pro klienty přihlašující se prostřednictvím vysílaných přístupových bodů. V ideálním případě, by veškeré klientovi požadavky směrem do sítě, byly přesměrovány na *landing page* dokud není provedena autorizace. Bohužel, vzhledem k šifrované komunikaci některých webových stránek, nelze takové stránky přesměrovat, protože by vznikl problém s bezpečnostním certifikátem a pravděpodobně by prohlížečem byla vyvolána chybová zpráva. Z tohoto důvodu je možné autorizovat pouze klienty, kteří provádějí načítání prostřednictvím nezabezpečeného HTTP spojení nebo jsou vyzvání prostřednictvím systémové služby mobilního telefonu (případně jiného zařízení s podporou Wi-Fi) k přihlášení. Bohužel zvláště u starších mobilních telefonů nemusí být tato pop-up funkcionalita podporována.

4.3.3.1. Realizace landing page

Prostřednictvím modulu byla vytvořena *landing page* (viz. Obrázek 19), která byla implementována za použití technologií HTML, PHP, CSS a JavaScript, které jsou stručně vysvětleny v přehledu řešené problematiky (viz. Kapitola 3.4). Pro obrázek pozadí byla zvolena fotografie, která je veřejně dostupná a šiřitelná pod licencí *Creative Commons* od autora Valerii Tkachenko. (47)

Obrázek 19 - Vizuální podoba landing page

Zdroj: vlastní zpracování

Zdrojový kód webové stránky je pro zachování přehlednosti práce součástí příloh (viz. Příloha G). Nedílnou součástí záchytné webové stránky je skript v jazyce PHP, který slouží k zachycení klientem zadaných parametrů po odeslání formuláře a k zobrazení informativní zprávy o stavu autorizace (viz. Příloha H). Součástí webové stránky je i odkaz na dokument, který obsahuje provozní řád sítě (viz. Příloha I), součástí kterého je sdělení, které poukazuje na fakt, že se jedná o výzkum v rámci diplomové práce.

Proces autorizace spočívá ve zpracování údajů, které byly klientem poskytnuty odesláním formuláře ve formě POST požadavku s parametry. Při autorizaci jsou klientské údaje ukládány v následujícím formátu:

YYYY-MM-DD hh:mm:ss EMAIL ; USER-AGENT

Získané údaje jsou využity pro vyhodnocení stanovených hypotéz, předpokladů, očekávání a k analýze chování uživatelů veřejných Wi-Fi sítí.

4.3.4. Cabinet

Samotné zařízení neposkytuje nativně správu souborů prostřednictvím webového rozhraní, ale je možné využít aplikace *WinSCP*, která poskytuje rozhraní pro přístup k adresářové struktuře nebo se prostřednictvím zabezpečeného komunikačního protokolu (SSH) připojit k příkazové řádce Linuxu a využívat příkazů *Unixového shellu* k ovládání zařízení.

Pro méně zkušené operátory, kteří nedisponují znalostí Linuxových příkazů nebo je nepraktické až nemožné se vzdáleně připojovat k zařízení prostřednictvím programu *WinSCP*, je možné využít připraveného modulu **Cabinet**. Modul umožňuje pracovat s Linuxovou adresářovou strukturou ve zjednodušeném prostředí webového rozhraní, které poskytuje operátorovi funkce pro vytváření, mazání a editaci souborů a složek. Bohužel má modul i určité nedostatky, které je nutné kompenzovat vzdáleným připojením prostřednictvím klienta s podporou FTP, SFTP např. *PuTTY, WinSCP* nebo *Total Commander*, kteří umožní nastavování práv souborům a složkám, a nahrávání souborů.

4.3.5. ConnectedClients

Modul poskytující zjednodušený a ucelený přehled o aktuálně připojených klientech a základní informace o jejich zařízení. Prostřednictvím modulu je možné skrze responzivní webové rozhraní pozorovat a vyhodnocovat aktuální situaci připojených klientů, bez nutnosti pracovat s *logy*, které jsou ve své textové podobě nepřehledné a práce s nimi by byla kontraproduktivní v situaci, kdy existuje modul, který čerpá z *logů* a filtruje zobrazované výsledky.

Zobrazovaný pohled je rozdělen do několika sekcí – tabulek, které zobrazují konkrétní druh informací. První tři tabulky zobrazují aktuálně připojené klienty k některému z rozhraní zařízení WiFi Pineapple. Tyto rozhraní jsou rozděleny podle způsobu použití na:

- *wlan1* je využíváno pro skenování okolních přípojných bodů, uživatelů a jejich monitorování – nedochází tedy k přímé interakci s uživateli a tabulka je ve většině

případů prázdná (může dojít k zásahu do nastavení nebo k vysílání přípojného bodu z uvedeného rozhraní a tabulka pak reflektuje připojené klienty)

- *wlan0-1* reflektuje připojené klienty k administrativnímu rozhraní prostřednictvím přípojného bodu, který byl definován v rámci prvotní inicializace zařízení (viz. Kapitola 4.3.1) a umožňující operátorovi provádět audit neoprávněných pokusů o připojení k administrativní části zařízení a oddělit aktivitu operátora od výzkumných dat
- *wlan0* zobrazuje klienty připojené k rozhraní prostřednictvím přípojných bodů, které mohou být přímo vysílány nebo vytvářeny na základě *probe* požadavků (viz. Kapitola 4.3.6)

O klientech jsou ve zmíněných tabulkách uchovávány hodnoty o přiřazených IPv4 adresách DHCP serverem, MAC adresa zařízení a název připojeného zařízení. Během vykonávání výzkumu v lokalitě s vysokým počtem okolních zařízení, došlo vlivem špatné konfigurace k vyčerpání přiřaditelných IPv4 adres. K danému jevu došlo v důsledku omezení ze strany masky sítě, která byla nastavena na hodnotu 255.255.255.0 a teoreticky umožňovala spravovat až 254 připojených zařízení, ale vlivem dodatečných nastavení síťování, byl rozsah přiřaditelných IPv4 adres v rozmezí 172.16.42.100 až 172.16.42.254. Bohužel při pokusech o změnu masky sítě, docházelo k problémům s nastavením tzv. *landing pag*e (viz. Kapitola 4.3.3), na kterou jsou automaticky směrovány veškeré požadavky neautorizovaných zařízení. Alternativním řešením bylo založeno na úpravě omezení, které bylo součástí nastavení síťování. Upravením parametru *option start* na hodnotu 10, bylo dosaženo zvýšení rozsahu přiřaditelných adres v rozpětí 172.16.42.10 až 172.16.42.254 tzn. 244 přiřaditelných IPv4 adres, které s platností přidělení 4 hodin poskytly dostatečnou kapacitu pro provedení jednotlivých měření (měření byla nejčastěji prováděna v délce trvání několika hodin). V případě vyčerpání adres, bylo možné vytvořit zálohu přiřazených IPv4 adres pro potřeby logování a následně vynulovat tabulku s jejich záznamy.

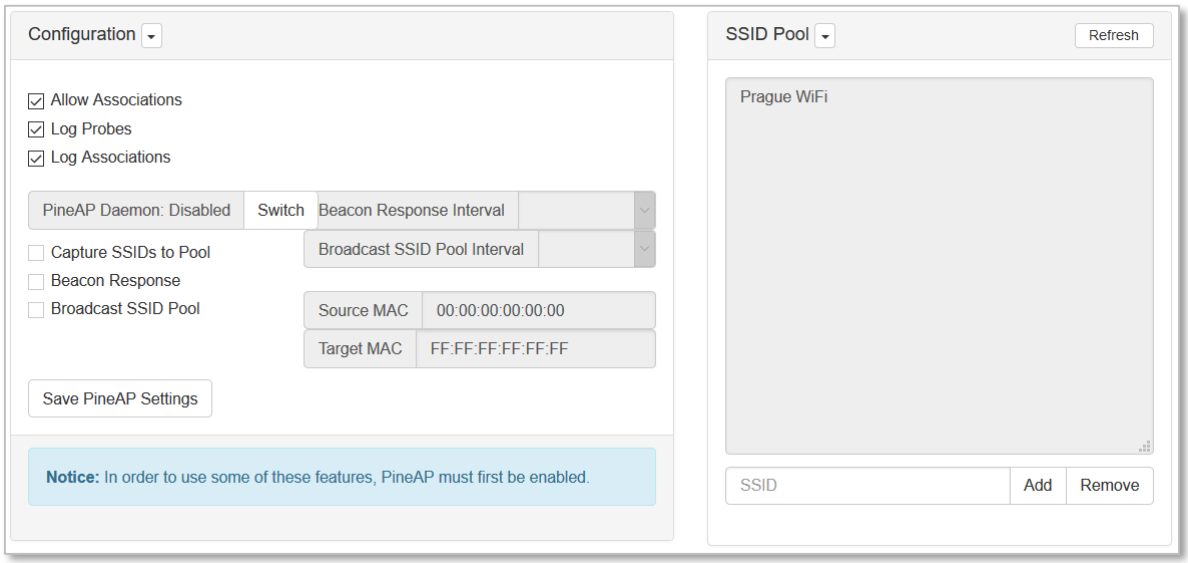
4.3.6. PineAP

Jedná se o funkcionalitu, která je předinstalovanou součástí zařízení, poskytující rozhraní pro realizace útoků typu *Karma* a vysílání přípojných bodů. Celý název aplikace je *PineAP Daemon* a ke svému provozu vyžaduje použití obou rádiových vysílačů současně, které jsou využívány pro zachytávání požadavků, vysílání přípojných bodů a obsluhu klientů. Ve své

podstatě zařízení na jedné rádiové anténě zachycuje okolní komunikaci bezdrátových sítí a na druhé vysílá přístupové body.

Samotný princip zařízení je nejlépe uvést na příkladu z reálného života: Uživatel si na svém mobilním telefonu (případně na jiném zařízení s podporou Wi-Fi – tablet, notebook atd.) zvolí možnost pro vyhledání okolních Wi-Fi sítí, ke kterým by se mohl připojit. Uživatelovo zařízení začne vysílat tzv. *probe request*, který představuje požadavek pro získání informací od okolních přípojných bodů a pokouší se vyhledat doposud uložené sítě. V případě, že se v okolí nachází dostupné přípojné body, vrátí se uživatelovi odpověď (*probe response*) s informacemi od okolních přípojných bodů a pokud má uživatel některý z nalezených přípojných bodů uložený, automaticky se k němu připojí (v závislosti na nastavené bezpečnostní politice zařízení).

V případě, že se v okolí uživatele nachází aktivní *PineAP Daemon,* zachytí *probe request* od uživatelova zařízení a odešle mu odpověď (*probe response)*, že se v okolí nachází přípojný bod, který se uživatelovo zařízení pokouší vyhledat. V této chvíli nastala situace, při které se uživatelovo zařízení připojilo k podvrženému SSID, které ale vykazuje stejné parametry jako v uživatelově zařízení uložená síť a jeho komunikace začne procházet skrze zařízení *WiFi Pineapple*.



Obrázek 20 - Webové rozhraní pro nastavení PineAP Daemon

Zdroj: vlastní zpracování

Zároveň aplikace disponuje službou pro vysílání tzv. *beacon frames*, které jsou nastavitelné prostřednictvím SSID Pool (viz. Obrázek 20) a představují výčet přípojných bodů, které bude zařízení vysílat prostřednictvím vysílače do okolí. Okolní zařízení zachycují tyto rámce a jejich prostřednictvím se mohou připojit k definovanému přípojnému bodu. V rámci výzkumu byly využity obě varianty pro maximalizaci rozsahu připojitelných zařízení.

4.4. Seznam měřených lokalit

Měření probíhalo ve vybraných lokalitách, které byly pro výzkum vyhodnoceny jako potencionálně zajímavá z hlediska výskytu osob, pocitu nedostatku veřejných Wi-Fi sítí a na základě funkce užitku, vypočítané pomocí metody váženého bodového součtu.

Tabulka 6 - Seznam provedených měření

Datum	Lokalita	Počasí	Doba (minuty)	Funkce užitku
16. 2. 2017	Pražský Hrad	Slunečno	90	1
16. 2. 2017	Pražský Hrad/ Karlův Most	Oblačno	90	0,45
17. 2. 2017	Pražský Hrad	Slunečno	60	0,95
18. 2. 2017	Pražský Hrad	Oblačno	90	0,85
18. 2. 2017	OC Metropole Zličín	Zataženo	130	0,2
19. 2. 2017	Pražský Hrad	Slunečno	90	1
19. 2. 2017	Pražský Hrad	Polojasno	90	0,6
20. 2. 2017	Anděl	Zataženo	210	0,15
21. 2. 2017	Anděl	Oblačno	60	0,1
23. 2. 2017	Areál ČZU	Zataženo	345	0,35
24. 2. 2017	Pražský Hrad	Zataženo	60	0,8
25. 2. 2017	Pražský Hrad	Slunečno	120	0,95
26. 2. 2017	Karlův Most	Zataženo	90	0,6
4. 3. 2017	Pražský Hrad	Slunečno	90	0,95
12. 3. 2017	Pražský Hrad	Zataženo	60	0,7

Zdroj: vlastní zpracování

4.5. Naměřená data

Během výzkumu bylo provedeno 15 měření v souhrnné délce trvání 27 hodin a 55 minut, prostřednictvím kterých byl získán soubor kvantitativních dat, které byly pomocí

analytických nástrojů analyzovány, aby poskytli ve své kvalitativní formě odpovědi na stanovené očekávání, předpoklady a hypotézy.

Během prováděných měření bylo zaznamenáno 43155 *probe requestů* tzn. okolních pokusů o připojení k Wi-Fi síti, které pocházely od 5720 unikátních zařízení. Z těchto unikátních zařízení došlo v 993 případech k realizaci připojení k vysílanému přípojnému bodu tzv. *asociaci*, během které bylo zařízením DHCP serverem přiřazena IPv4 adresa. Poslední úroveň konverze představuje *autorizace*, kterou podstoupilo celkem 108 uživatelů, kteří jejím prostřednictvím poskytli emailovou adresu a detailnější pohled na využité zařízení.

4.6. Analýza dat

Pro analýzu dat bylo využito nástrojů Microsoft Excel, pro statistickou analýzu *SAS 9.4* a *business intelligence* nástroje QlikView, který je využíván pro analýzu dat, tvorbu reportů a jejich vizualizaci. Příprava dat spočívala v jejich strukturalizaci, která umožnila v analýzách zohledňovat jejich původ a získané parametry.

Z důvodu realizace měření v odlišných prostředích, bylo potřeba určitou formou standardizovat vlivy, které mohou měření ovlivnit. Proto bylo využito vícekriteriální analýzy variant, kdy se za pomoci metody váženého součtu (viz.

Tabulka 7) vypočítá funkce užitku pro každé měření, kdy její hodnoty leží v intervalu <0,1> a vyšší hodnotou jsou reprezentovány výhodnější varianty. Na základě logického uvažování byly jako zásadní faktory, které ovlivňují výsledky měření stanoveny tyto kritéria: klimatické podmínky, výskyt osob, pocit nedostatku Wi-Fi přípojných bodů a fluktuace osob. Pro provedení metody váženého součtu je vyžadováno, aby veškeré kritéria byla maximalizační tzn., aby nejlepší hodnoty byly ohodnoceny nejvyšší bodovou hodnotou. Uvedené podmínce bylo potřebné přizpůsobit minimalizační kritérium fluktuace osob, které vyjadřuje rychlost pohybu osob, která má zásadní vliv na připojení k Wi-Fi síti.

Zároveň bylo potřebné u každého kritéria stanovit jeho váhu podle míry, kterou daný faktor ovlivňuje výsledek výzkumu. Jedná se o značně subjektivní vyjádření, které u daných kritérií nelze s přesností odhadnout, ale lze očekávat, že míra výskytu osob je kritická a z toho důvodu byla ohodnocena vahou 0,4. Mezi ostatní kritéria se rovnoměrně rozložila zbytková váha po 0,2 váhových jednotkách, protože vážená hodnota ze všech kritérií musí v součtu udávat hodnotu 1.

Tabulka 7 - Metoda váženého součtu

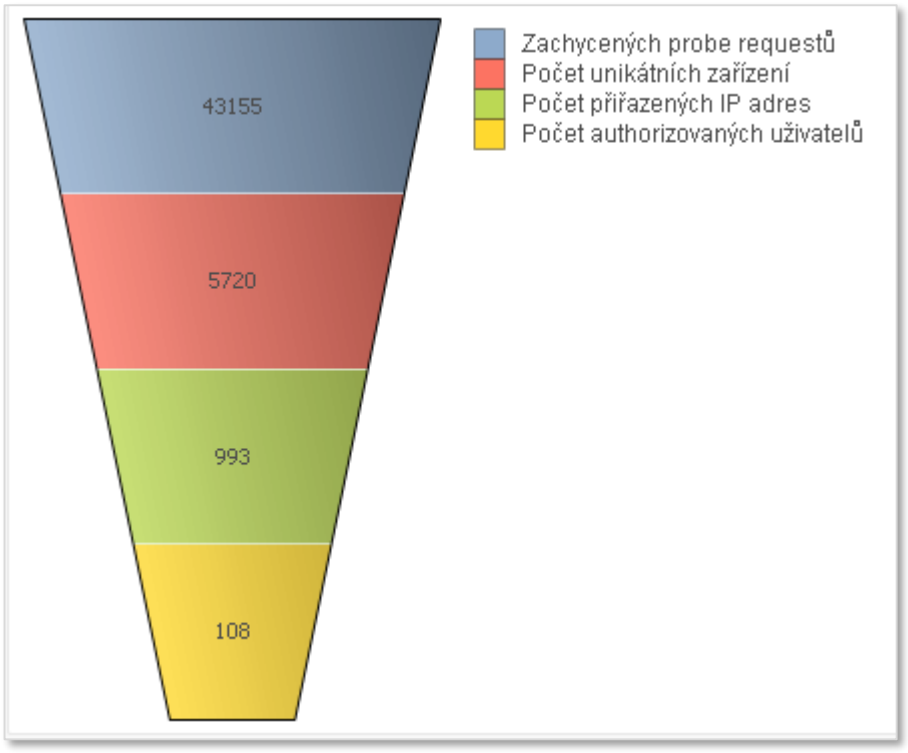
Datum	Měření	Klimatické podmínky	Výskyt osob	Pocit nedostatku Wi-Fi	Fluktuace osob	Funkce užitku
16. 2. 2017	1	1	1	1	1	**1**
16. 2. 2017	2	0,5	0,25	1	0,25	**0,45**
17. 2. 2017	1	0,75	1	1	1	**0,95**
18. 2. 2017	1	0,25	1	1	1	**0,85**
18. 2. 2017	2	0,25	0,25	0	0,25	**0,2**
19. 2. 2017	1	1	1	1	1	**1**
19. 2. 2017	2	0,75	0,25	1	0,75	**0,6**
20. 2. 2017	1	0,25	0	0,25	0,25	**0,15**
21. 2. 2017	1	0	0	0,25	0,25	**0,1**
23. 2. 2017	1	0,25	0,5	0,25	0,25	**0,3**
24. 2. 2017	1	0,25	1	1	0,75	**0,8**
25. 2. 2017	1	0,75	1	1	1	**0,95**
26. 2. 2017	1	0,25	1	0,75	0	**0,6**
4. 3. 2017	1	0,75	1	1	1	**0,95**
12. 3. 2017	1	0,25	0,75	1	0,75	**0,7**
	Váha	0,2	0,4	0,2	0,2	

Zdroj: vlastní zpracování

4.6.1. Analýza konverzí

Měřené hodnoty jsou uzpůsobeny pro zjišťování konverzních poměrů a vytvářejí tak podklad pro následnou analýzu trychtýřovým grafem (*Funnel chart*). Analýza dat proběhla v nástroji QlikView, který umožňuje analytickou práci s velkým množstvím dat a jejich úpravou.

Graf 2 - Konverzní poměry měření



Zdroj: vlastní zpracování

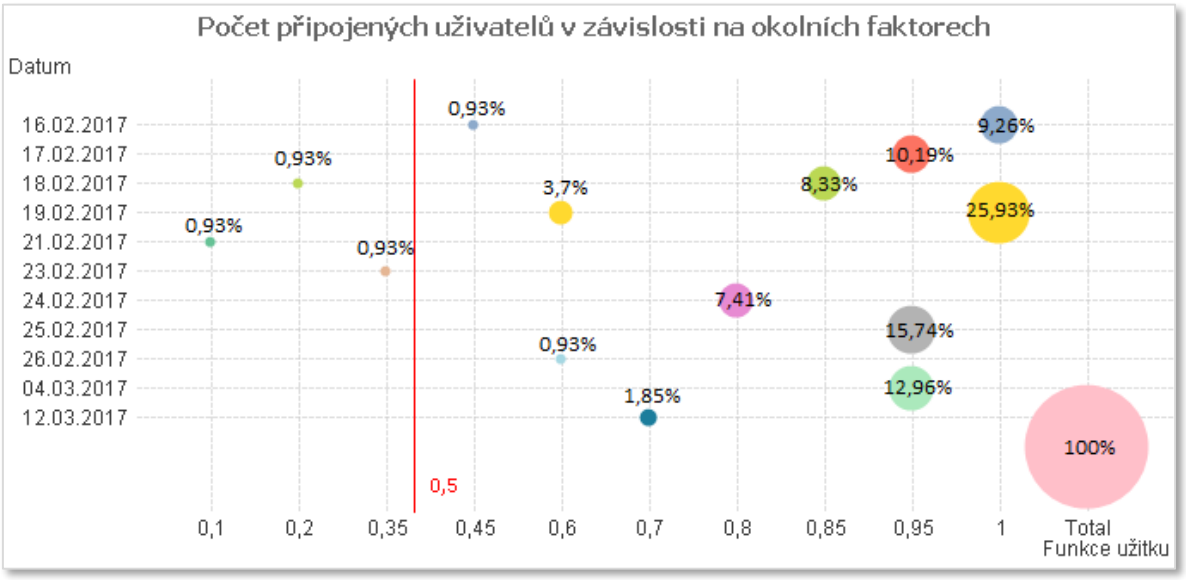
Pro získání odpovědi na stanovenou otázku týkající se využívání veřejných Wi-Fi síti bez ohledu na možná rizika poskytuje největší vypovídající hodnotu 1, 2 a 3 úroveň grafu, které vyjadřují počet zachycených *probe requestů* tzn. počet pokusů o připojení, počet unikátních zařízení pokoušejících se připojit a počet skutečně připojených zřízení. Zjištěná úroveň konverze dosahuje 17 % připojených zařízení z počtu okolních unikátních zařízení. Vůči těmto připojeným uživatelům by bylo možné realizovat různé typy útoků, na bázi sociálního inženýrství nebo sledovat jejich síťovou komunikaci. Lze tedy konstatovat, že každé páté zařízení s aktivním Wi-Fi modulem je zneužitelné. Je vysoce pravděpodobné, že na tuto naměřenou hodnotu mají značný vliv okolní faktory, které byly specifikovány v kapitole 4.5, a v následující kapitole je analyzován jejich vliv na naměřené hodnoty.

4.6.2. Analýza vlivu okolních faktorů

Pro analýzu vlivu okolních faktorů byl využit bublinový graf (*Grid chart*), který umožní nejlépe prezentovat vliv zvolených kritérií na počet připojených uživatelů. Graf byl vytvořen v analytickém nástroji *QlikView*, kterému předcházela úprava struktury dat v tabulkovém editoru *Microsoft Excel*.

Z grafu níže (viz. Graf 3) je patrná koncentrace připojených uživatelů v pravé části grafu, která reprezentuje vysokou funkci užitku a tedy i skutečnost, že připojení uživatelů je závislé na okolních faktorech. Levá část grafu naopak reprezentuje nízkou úroveň funkce užitku a tedy i nízký počet připojených uživatelů. Na základě provedené analýzy lze konstatovat, že uživatelé vyhledávají veřejných Wi-Fi sítí v prostředích s dobrými klimatickými a povětrnostními podmínkami (zejména za bezdeštného podnebí) a při nízké fyzické aktivitě (např. stání ve frontě, při posezení). A zásadní logické faktory, které rozhodují o počtu připojených uživatelů, je jich samotný výskyt a nízká variabilita veřejných Wi-Fi sítí.

Graf 3 - Vliv funkce užitku na připojené uživatele



Zdroj: vlastní zpracování

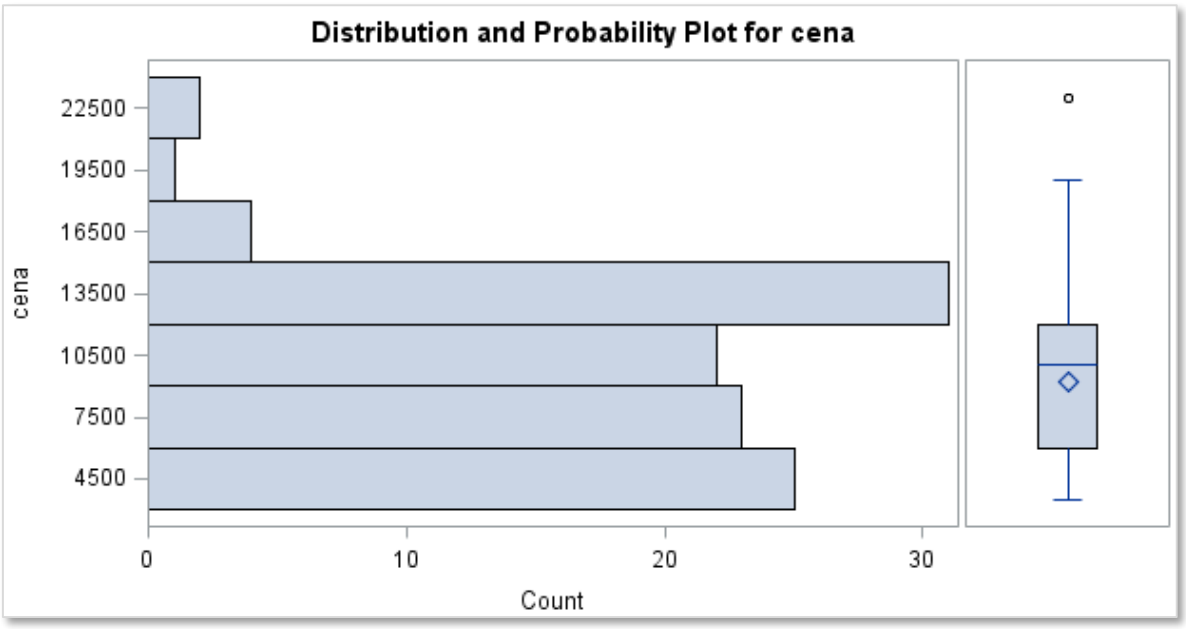
4.6.3. Vlivy ceny zařízení

Pro otestovaní stanovené hypotézy, která předpokládá, že hodnota zařízení nemá vliv na využívání veřejných Wi-Fi sítí, bylo využito statistického analytického softwaru SAS 9.4, který poskytl dostatečné rozhraní pro otestování normality souboru.

Testování normality souboru probíhá na úrovni konverze, která obsahuje uživatele, kteří prošli autorizačním procesem a získali přístup k internetu. Autorizační proces je definován v kapitole 4.3.3, kdy k autorizaci dochází, pokud uživatel vložením svého emailu a kliknutím na tlačítko *Vstoupit* odsouhlasí podmínky a řád veřejné Wi-Fi sítě. Bohužel musela být normalita otestována na tomto stupni konverze z důvodu nedostatku

kvalitativních dat na konverzi předchozí, která neshromažďuje detailní data o připojených zařízeních. Přesto se jedná o dostatečný vzorek pro otestování stanovené hypotézy.

Graf 4 - Boxplot ukazatele CENA



Zdroj: vlastní zpracování

Výstup z programu SAS (viz. Graf 4) pro ukazatel ceny vykazuje znaky, které se neslučují s normálním rozdělením. Zejména se zde vyskytují odlehlé (extrémní) pozorování, které mohou představovat chyby v měření, chyby v přepisu dat nebo neobvyklé extrémy. Zároveň umístění mediánu značí asymetrické rozdělení hodnot sledovaného znaku směrem k maximu. Nicméně grafické zobrazení je vhodné pro testování normality u malých souborů, proto nelze hypotézu vyjadřující, že výběr pochází z normálního rozdělení potvrdit ani zamítnout.

Tabulka 8 - Testy normálního rozdělení výběru

Goodness-of-Fit Tests for Normal Distribution				
Test	Statistic		p Value	
Kolmogorov-Smirnov	D	0.15176669	Pr > D	<0.010
Cramer-von Mises	W-Sq	0.32445312	Pr > W-Sq	<0.005
Anderson-Darling	A-Sq	2.31778254	Pr > A-Sq	<0.005

Zdroj: vlastní zpracování

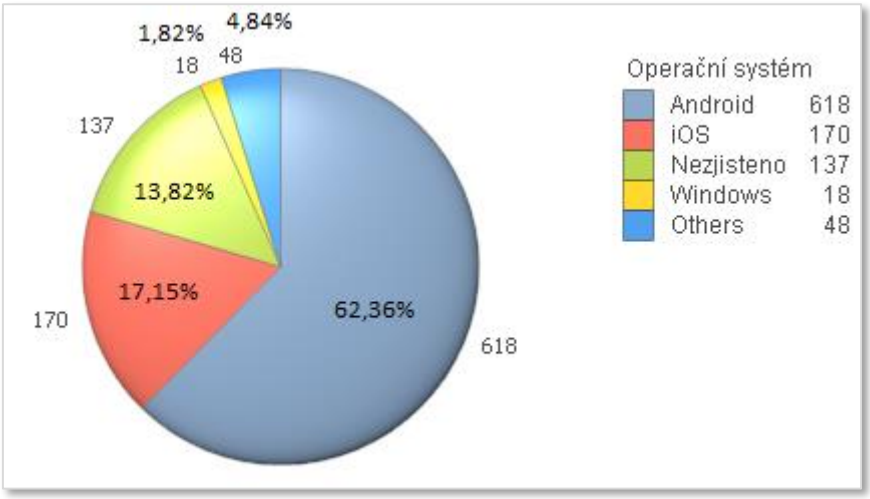
V případě jednovýběrového *Kolmogorovova-Smirnovova* testu nulovou hypotézu zamítáme, pokud pozorovaná hodnota překročí tabelovanou kritickou hodnotu $D_n(\alpha)$, která je při 5 % hladině významnosti a počtu prvků větším než 40 vypočtena dle vzorce $\frac{1,36}{\sqrt{n}}$. U zvoleného výběru je hodnota p=0,010 a tedy platí, že $p<D_n(\alpha)$. Protože pozorovaná hodnota (0,010) nepřekročila kritickou hodnotu Kolmogorova-Smirnonova testu (0,1517) s hladinou významnosti 0,05, tak nulovou hypotézu nezamítáme a můžeme prohlásit, že výběr pochází z normálního rozdělení.

Na základě poznatků zjištěných ze statistické analýzy můžeme konstatovat, že finanční hodnota zařízení nemá vliv na využívání veřejných bezdrátových Wi-Fi sítí a cenová hladina zařízení je rovnoměrně rozložena okolo Gaussovy křivky.

4.6.4. Analýza zařízení

Při provádění měření bylo získáno poměrně velké množství kvantitativních dat, ze kterých lze získat data, která mají určitou vypovídající hodnotu o použitých zařízeních, operačních systémech a případně rozložení jejich verzí u napozorovaného souboru zařízení.

Graf 5 - Rozložení operačních systémů připojených zařízení

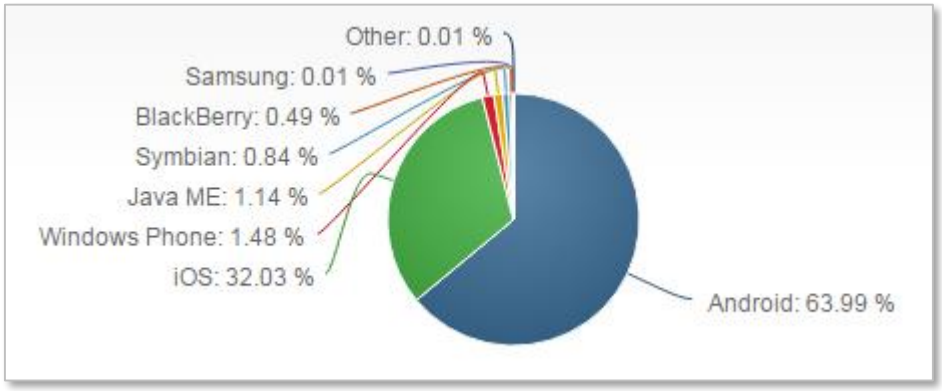


Zdroj: vlastní zpracování

Na výše uvedeném výsečovém grafu (viz. Graf 5), který je výstupem analytického nástroje QlikView je vyjádřeno rozložení operačních systémů připojených zařízení. V porovnání s procentuálním zastoupením trhu, který je zobrazen na Graf 6 je rozložení mobilních operačních systémů v naměřeném souboru prakticky shodné. Určitý vliv na výslednou

podobu grafu mají zařízení, u kterých nebylo možné rozpoznat použitý operační systém. Lze tedy konstatovat, že typ operačního systému nemá výrazný vliv na využívání veřejných Wi-Fi sítí.

Graf 6 - Procentuální zastoupení mobilních operačních systému na trhu

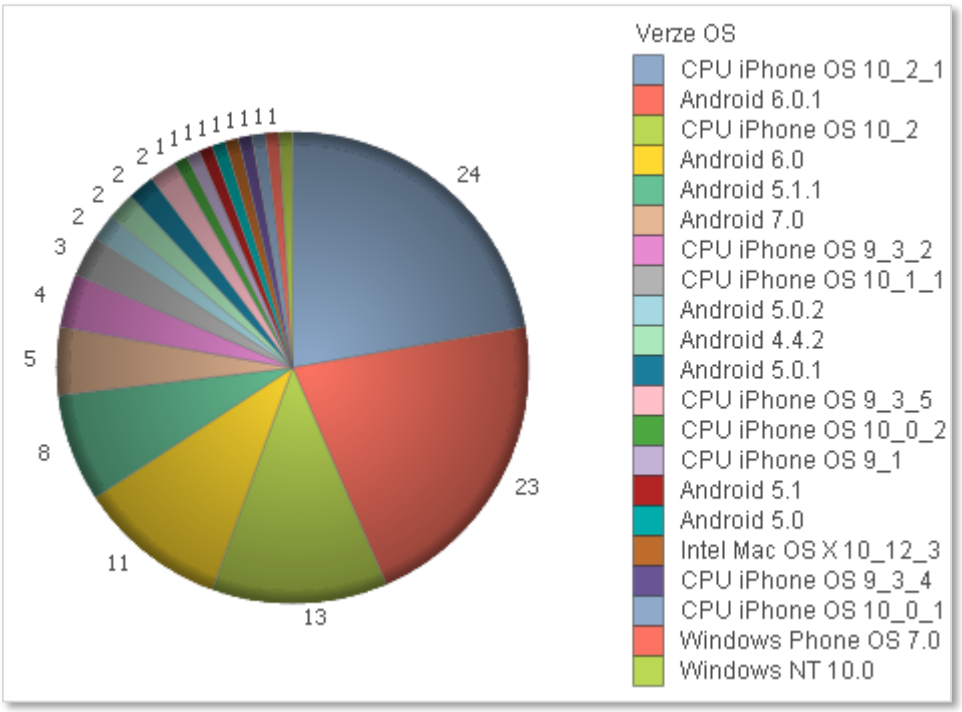


Zdroj: Net Applications. Mobile/Tablet Operating System Market Share. [Online] ©2006-2017. Dostupné z: https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=8&qpcustomd=1

4.6.4.1. Verze operačních systémů

Při sestupu na nižší úroveň konverze, která představuje autorizované uživatele, lze z parametru *UserAgent*, který je z uživatelského zařízení získáván při odsouhlasení podmínek a provozního řádu Wi-Fi sítě, získat konkrétní verzi mobilního operačního systému (viz. Graf 7).

Graf 7 - Rozložení verzí OS v souboru



Zdroj: vlastní zpracování

Pro srovnání nebylo možné získat z internetových zdrojů relevantní aktuální data, k dispozici jsou pouze data z poloviny roku 2016, která jsou ale vůči hodnotám aktuálním nevypovídající. Přesto lze ze získaných dat pozorovat, že většina uživatelů využívá zařízení s poměrně aktuální verzí operačního systému a zbytečně se nevystavují možným hrozbám z jeho neaktuálnosti. Na tuto skutečnost mají pravděpodobně velký vliv výrobci samotných zařízení, kteří z mobilních zařízení vytvářejí zboží se spotřebním charakterem.

4.7. Způsoby ochran

Útoky toho typu jsou natolik sofistikované, že odolávají standardním obraným metodám a všeobecná rada, která je zmiňována jako ochrana před různým typem útoků – ostražitost uživatele, je v konkrétním případě velmi irelevantní. Útok je veden takovým způsobem, který dokáže obejít i autentizační proces zabezpečených Wi-Fi sítí a v případě nezabezpečených sítí mu nejsou kladeny téměř žádné překážky.

Základní, bohužel též velmi sporadicky řečená rada zní, nepřipojovat se k veřejným Wi-Fi sítím, které i v případě těch celosvětově rozšířených *Eduroam, McDonald's, KFC* nebo *Starbucks* mohou být jednoduše využity k odposlouchávání komunikace. V případě

hlubšího pohledu, se jeví jako bezpečné řešení využití VPN (*Virtuální privátní síť*), která zprostředkovává zabezpečení a šifrování komunikace. Případně nevstupovat na webové stránky, které nedisponují bezpečnostním SSL certifikátem a ujistit se, že webový prohlížeč podporuje funkcionalitu HSTS (*HTTP Strict Transport Security*), která chrání spojení před tzv. *downgrade* útoky formou vynuceného šifrovaného spojení v HTTP hlavičce. Uvedená funkcionalita je ale též napadnutelná útokem typu MANA, který využívá snížení komunikace na nezabezpečený přenos a umožní též překonat nebo odklonit mechanismus HSTS.

Z hlediska zaručené ochrany je nutné upozornit, že zařízení ve svém promiskuitním módu využívá uložených Wi-Fi sítí v cílovém zařízení a proto zamezením jejich ukládání je zařízení proti uvedenému režimu chráněno. Při manuálním zadávání identifikátorů sítě je zařízení chráněno do té doby, než útočník provede cílenou deautentizaci, při které se útočník pokouší vynutit, aby se zařízení připojilo k jeho přípojnému bodu. Na základě výše uvedených poznatků, lze konstatovat, že zaručená metoda ochrany zařízení před WiFi Pineapple, tkví v úplné deaktivaci Wi-Fi sítě a využívání mobilních sítí nebo ve využití VPN. Bohužel se jedná o zranitelnost Wi-Fi sítí, která je prozatím přehlížena, pravděpodobně z důvodu malého rozšíření útoků typu Karma, MANA atp.

4.8. Právní aspekty

Výzkum byl prováděn v rádiovém pásmu 2.4GHz a v souladu s nařízeními, které jsou na území ČR regulovány Českým telekomunikačním úřadem (dále jen ČTU), který provoz ve zmíněném pásmu upravuje všeobecným oprávněním č. VO-R/10/05.2014-3 o využívání rádiových kmitočtů a o provozování zařízení krátkého dosahu.

Zároveň ČTÚ stanovuje případy, kdy provozování veřejné Wi-Fi sítě podléhá ohlašovací povinnosti a případné licenci. Ohlásit tuto skutečnost ČTÚ vzniká u osob, které provádějí podnikání v elektronických komunikacích za účelem zisku. Jelikož byl výzkum součástí diplomové práce a nebyl prováděn za účelem zisku, nevznikla povinnost ohlašovat jeho působení ČTÚ.

4.8.1. Vyjádření od poskytovatele mobilního připojení

Na základě poznatků a připomínek vedoucího práce, bylo před započetím výzkumu potřebné, si v souladu s všeobecnými podmínkami operátora (dále jen VPO), vyjasnit

některé body smluvních podmínek. Během výzkumu dochází k poskytování služeb operátora třetím stranám, kdy dané počínání je v rozporu s VPO, jakožto nestandardní využívání služeb, které musí být podloženo tzv. smlouvou o propojení. Z tohoto důvodu byl kontaktován operátor, za účelem poskytnutí oprávnění k provedení výzkumných měření s jeho vědomím a za využití jeho služeb.

Na základě odpovědi od operátora, bylo po objasnění náplně a tématu diplomové práce umožněno nestandardní využití služeb, za účelem dosažení stanovených cílů práce. Povolení bylo poskytnuto v rámci elektronické komunikace a schváleno právním oddělením operátora, které vymezilo pro účely výzkumu propůjčenou SIM kartu a vymezilo platnost uděleného povolení.

5. Výsledky a diskuse

Výzkum, který spočíval v analýze zařízení a chování uživatelů veřejných Wi-Fi síti, byl proveden za využití zařízení WiFi Pineapple a spolupracujících dílčích částí, které vytvořily mobilní jednotku pro sběr kvantitativních a kvalitativních dat. Data byla dále vyhodnocena, analyzována a verifikována za použití statistických (*SAS*) a analytických nástrojů (*QlikView* a *Microsoft Excel*), které poskytly hlubší pohled na zkoumanou problematiku a umožnily vyhodnotit stanovené hypotézy, očekávání a předpoklady.

Sběr dat probíhal v prvním čtvrtletí roku 2017, za nepříliš příznivých klimatický podmínek, které následně byly zohledněny i v analýze okolních vlivů na výsledky měření. Data byla shromažďována v několika konverzních úrovních, které závisely na úrovni aktivity připojujícího se uživatele. Konverze jsou prezentovány v rámci kapitoly č. 4.6.1 Analýza konverzí a jsou členěny na úrovně: počet zachycených požadavků o připojení, počet unikátních zařízení, počet skutečně připojených zařízení a počet autorizovaných uživatelů. Z analýzy konverzí bylo zjištěno, že k vysílané skupině veřejných Wi-Fi přípojných bodů, se připojilo až 17 % ze zachycených okolních zařízení, které v okolí zařízení vysílaly požadavek o připojení k Wi-Fi síti (*probe request*). Jedná se o poměrně znepokojující procentuální hodnotu, která v konečném důsledku vyjadřuje počet zařízení, vůči kterým by mohl být veden útok formou sociálního inženýrství, sledování síťové komunikace nebo jinou sofistikovanou formou. Je třeba zdůraznit, že se jedná o aktivity, jejichž provozováním v reálném provozu se útočník dopouští jednání, které je v rozporu se zákony ČR a autor práce se s nimi neztotožňuje, ani neposkytuje návod k jejich realizaci. Z tohoto důvodu byl výzkum prováděn takovou formou, která nikterak nepoškozuje připojené uživatele, pouze jim poskytuje možnost připojení k internetové síti prostřednictvím přípojného bodu veřejné Wi-Fi sítě a to na základě jejich potřeb.

Následný soubor analýz založený na statistických a analytických verifikací odhalil, že naměřené hodnoty jsou značně ovlivňovány okolními faktory, které byly za pomocí metody váženého bodového součtu znormovány, aby umožnily objektivní znázornění jejich vlivu na měřené hodnoty. Analýza byla provedena formou proporcionálního bublinového grafu, na kterém byla na osu *X* nanesena funkce užitku, na osu *Y* datum měření a pro znázornění proporcí počet připojených uživatelů. Následnou analýzou, která byla založena na testování normality výběrového souboru cenové hladiny připojených zařízení, která byla doplněna

o běžné ceny použitých zařízení, bylo v rámci grafického znázornění *boxplotu* možné pozorovat odlehlé hodnoty, které vylučují normální rozdělení výběru. Z důvodu použití výběru, který má větší množství měření než 30, tak bylo použito *Kolmogorovova-Smirnovova* testu. Použitý test nezamítnul (potvrdil) nulovou hypotézu, která vyjadřovala, že výběr pochází z normálního rozdělení a na základě které bylo možné stanovit, že hodnota zařízení nemá vliv na využívání veřejných Wi-Fi sítí.

Zařízení byla analyzována z hlediska použitého operačního systému a aktuálnosti jeho verze. Při analýze typu operačního systému, došlo k prakticky identické shodě rozložení použitých zařízení s jejich rozdělením na trhu, které vycházelo z analýzy společnosti *Net Applications.com*. Detailnější rozbor zaměřený na verzi operačního systému poukázal na fakt, že zaznamenaná mobilní zařízení disponují poměrně aktuálními verzemi operačního systému a tím i větší bezpečností zařízení. Důležitou roli zde zastupuje fakt, že mobilní zařízení jsou spotřební elektronikou, která se pod tlakem výrobců neustále obměňuje, a tím se převážně dostávají nové verze operačního systému do oběhu.

Analýzou zabezpečení veřejných Wi-Fi sítí bylo zjištěno, že bezpečnostní nedostatky kterými disponují, jsou technického charakteru a jejich případné úpravy by postihli celkovou funkcionalitu sítí. Uživatel se může v rámci veřejných Wi-Fi sítí bránit útokům na základě prevence, která je založena na jejich nevyužívání a orientovat se směrem k mobilnímu připojení třetí a čtvrté generace (sítě druhé generace jsou prostřednictvím falešných telefonních věží napadnutelné – downgrade šifrování). Z hlediska aktivní ochrany se jako účinné jeví využívání VPN, případně přistupovat k zabezpečeným webovým stránkám s prohlížečem podporujícím HSTS.

6. Závěr

Na základě cílů stanovených v zadání práce, byl zpracován přehled řešené problematiky, která na základě studia odborných informačních zdrojů obsahuje definici *hackingu*, který je v samotné práci stěžejní. Zpracování uceleného přehledu historického vývoje *hackingu* až po současnost, včetně předpokládaného vývoje a legislativní pohled v závislosti na aplikovaném právním systému. V dalších kapitolách teoretické rešerše, byla provedena sumarizace použitých technologií a vybraných útoků v online prostředí. Zvolené útoky byly simulovány na izolovaných webových stránkách, za účelem prezentace jejich průběhu a možných způsobů ochran před nimi z pohledu systému i koncového uživatele. Přehled řešené problematiky byl zpracován s důrazem na následné využití v praktické části práce, jako její teoretická východiska.

Praktická část byla založena na realizaci výzkumu, prostřednictvím zařízení WiFi Pineapple a jeho dílčích součástí, který měl nalézt odpovědi na stanovené očekávání, předpoklady a hypotézy. Během výzkumu byla provedena řada měření, které pocházely z diametrálně odlišných prostředí, a bylo potřeba standardizovat vliv okolních aspektů pomocí vícekriteriální analýzy variant. Během měření se vyskytla řada technologických problémů a nedostatků, které ale byly optimalizovány a poskytly provozuschopnou platformu pro provedení výzkumných měření.

Výsledkem měření byly soubory kvantitativních a kvalitativních dat, které byly na základě statistických a analytických nástrojů zkoumány, analyzovány a testovány. Zejména došlo ke zjištění, že se uživatelé připojují (17 % uživatelů) k veřejným sítím bez ohledu na možná rizika, která mohou být založena na sledování komunikace nebo různých typů útoků např. na bázi sociálního inženýrství. Z pohledu uživatele se ovšem jedná o problematiku, které může předcházet jen velmi omezeným souborem opatření, kdy základním obecným doporučením je nevyužívat veřejných Wi-Fi sítí a v opačném případě využívat zabezpečeného připojení, VPN serveru a prohlížeče s podporou HSTS.

Zároveň na základě statistické analýzy došlo k ověření hypotézy, která předpokládala vliv hodnoty zařízení na využívání veřejných Wi-Fi sítí. Hypotéza byla na základě testu normality zamítnuta, protože výběrový soubor s cenami zařízení, vykazoval znaky normálního rozdělení v rámci grafického znázornění, ale i na základě *Kolmogorovova-*

Smirnovova testu, který mohl být použit, protože byl splněn požadavek na velikost výběrového souboru.

Během dalších analýz byl zjištěn značný vliv okolních aspektů na výsledky měření, kdy se jednalo o vlivy klimatické, počty okolních osob, úroveň fluktuace osob a nedostatek okolních přípojných bodů. Na základě analýzy připojených zařízení byl pozorován podíl zařízení srovnatelný s rozložením zařízení v rámci trhu a poměrně vysoká úroveň aktuálnosti verzí operačních systémů, které v konečném důsledku zvyšují bezpečnost samotného zařízení a zjištěná úroveň aktuálnosti operačních systémů, je pravděpodobně způsobena charakterem mobilních zařízení jakožto spotřební zboží.

7. Citovaná literatura

1. **CHAUHAN, Sudhanshu a PANDA, Nutan Kumar.** *Hacking Web Intelligence - Open Source Intelligence and Web Reconnaissance Concepts and Techniques. 1. vydání.* Waltham : Syngress, 2015. ISBN 978-0128018675.

2. **HARPER, Allen, a další.** *Gray Hat Hacking The Ethical Hackers Handbook. 4. vydání.* místo neznámé : McGraw-Hill Publishing, 2015. ISBN 978-0-07-183850-4.

3. **Ei0nN.** Hacking. *Urban Dictionary.* [Online] 22. Srpen 2014. [Citace: 2016. Září 21.] Dostupné z: http://www.urbandictionary.com.

4. **SNJIB, Sinha.** Ethical Hacking - For Absolute Beginners. *Leanpub.* [Online] [Citace: 21. Září 2016.] http://samples.leanpub.com.

5. **DENUVO.** What we do. *DENUVO.* [Online] DENUVO GmbH, 2014. [Citace: 21. 10 2016.] Dostupné z: http://www.denuvo.com.

6. **SURYNEK, Jiří.** PROBLEMATIKA BEZDRÁTOVÝCH SÍTÍ, Bakalářská práce. *Vysoké učení technické v Brně.* [Online] 2010. [Citace: 15. 1 2017.] https://www.vutbr.cz/.

7. **SHARPE, Isaac.** *HACKING Guide to Basic Security, Penetration Testing and Everything Else Hacking.* místo neznámé : CreateSpace Independent Publishing Platform, 2015. ISBN 978-1512300772.

8. **KÜMMEL, Roman a KLUBAL, Martin.** SOOM.cz. *SOOM.cz.* [Online] SOOM.cz, © 2017. [Citace: 21. 10 2016.] Dostupné z: www.soom.cz. ISSN 1804-7270.

9. **JACKSON, Dexter.** *Ultimate Beginner's Guide to Computer Hacking in 2016.* [Dokument] místo neznámé : CreateSpace Independent Publishing Platform, 2016. ISBN 978-1537369761.

10. **KUCAN, Berislav, ZORZ, Mirko a ZORZ, Zeljka.** The History Of Hacking. *HELPNETSECURITY.* [Online] Help Net Security, 2017. [Citace: 22. 10 2016.] Dostupné z: www.helpnetsecurity.com.

11. **DARELL, Richard.** Hacking History – A Timeline Of Hack Tactics. *BIT REBELS.* [Online] 2015. [Citace: 22. 10 2016.] Dostupné z: http://www.bitrebels.com.

12. **TRIGAUX, Robert.** A history of hacking. *St. Petersburg Time.* [Online] 2010. [Citace: 24. 10 2016.] Dostupné z: http://www.sptimes.com.

13. **The Associated Press.** Hackers used 'internet of things' devices to cause Friday's massive DDoS cyberattack. *CBC News.* [Online] 22. 10 2016. [Citace: 25. 10 2016.] Dostupné z: http://www.cbc.ca.

14. **WAGSTAFF, Keith.** Hack to the Future: Experts Make 2016 Cybersecurity Predictions. *NBC NEWS.* [Online] 2. 1 2016. [Citace: 26. 10 2016.] Dostupné z: http://www.nbcnews.com.

15. **CZOKL.** Legislativní pohled na napadání sítí v České republice. *Security-Portal.cz.* [Online] 22. 7 2010. [Citace: 31. 10 2016.] Dostupné z: http://www.security-portal.cz.

16. **PTÁČEK, Ing. Vladimír.** Angloamerický právní systém, Diplomová práce. *Masarykova univerzita v Brně.* [Online] 2010. [Citace: 10. 2 2017.] Dostupné z: https://is.muni.cz/. ISSN 1802-128X.

17. **HEGEROVÁ, Klára.** *Velké právní systémy.* Brno : Diplomová práce. Masarykova univerzita v Brně, 2010.

18. **NCKB.** Co je NCKB. *Národní centrum kybernetické bezpečnosti.* [Online] Národní bezpečnostní úřad, 2017. [Citace: 29. 10 2016.] Dostupné z: https://www.govcert.cz/.

19. **Parlament ČR.** Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). *Sbírka zákonů.* [Online] 2014. [Citace: 15. 2 2017.] Dostupné z: https://www.nbu.cz/.

20. **Parlament ČR .** Zákon č. 40/2009Sb.,. *Trestní zákoník.* [Online] 2009. [Citace: 15. 2 2017.] Dostupné z: http://www.mvcr.cz.

21. **PALAS, Petr.** Historie Webu z pohledu vývojáře. *Fakulta informatiky.* [Online] 4 2001. [Citace: 1. 11 2016.] http://www.fi.muni.cz. ISSN 1802-128X.

22. **Google Chrome team.** The Evolution of the Web. [Online] 2012. [Citace: 31. 10 2016.] Dostupné z: http://www.evolutionoftheweb.com/.

23. **TITTEL, Ed a NOBLE, Jeff.** *HTML, XHTML & CSS for DUMMIES.* místo neznámé : Wiley Publishing, Inc., 2011, 7. vydání. ISBN: 978-0470916599 .

24. **LECKY-THOMSON, Ed a NOWICKI, Steven D.** *PHP 6 Programujeme profesionálně.* Brno : Computer Press, 2010. ISBN 978-80-251-3127-5.

25. **ČÁPKA, David.** Úvod do PHP a webových aplikací. *IT network.* [Online] © 2017. [Citace: 13. 3 2017.] Dostupné z: http://www.itnetwork.cz. ISSN 2464-6326.

26. **MAJDA, David.** Do hlubin implementací JavaScriptu: 1. díl – úvod. *zdroják.cz.* [Online] 30. 10 2008. [Citace: 2. 11 2016.] Dostupné z: https://www.zdrojak.cz. ISSN 1803-5620.

27. **ŽÁRA, Ondřej.** *JavaScript Programátorské techniky a webové technologie.* Brno : Computer Press, 2015. ISBN 978-80-251-4573-9.

28. **JANOVSKÝ, Dušan.** JavaScript - návody na použití jazyka. *Jak psát web.* [Online] [Citace: 2. 11 2016.] https://www.jakpsatweb.cz/. ISSN 1801-0458.

29. **ELMASRI, Ramez a NAVATHE, Shamkant B.** *Fundamentals of Database Systems.* místo neznámé : Pearson, 2015, 7.vydání. ISBN: 978-0133970777 .

30. **SCAMBRAY, Josel a SHEMA, Mike.** *HACKING bez tajemství - webové aplikace.* Brno : Computer Press, 2003. ISBN 80-7226-769-8.

31. **HERNANDEZ, M. J.** *Návrh databází.* Praha : Grada, 2006. ISBN 9788024709000.

32. **VŠE v Praze.** Základy relačních databází, jejich využití v programování webu. *Rozvoj oboru Multimédia v ekonomické praxi pro lepší uplatnění absolventů v praxi.* Praha : VYSOKÁ ŠKOLA EKONOMICKÁ V PRAZE, 2014. Číslo projektu: CZ.2.17/3.1.00/34129.

33. **BEAVER, Kevin a DAVIS, Peter T.** *Hacking Wireless Networks for DUMMIES.* místo neznámé : Wiley Publishing Inc., 2005. ISBN 978-0764597305.

34. **Wi-Fi Alliance.** Who We Are. *Wi-Fi Alliance.* [Online] © 2017. [Citace: 13. 11 2016.] Dostupné z: http://www.wi-fi.org/.

35. **DUCKLIN, Paul.** Using WPS on your Wi-Fi router may be even more dangerous than you think. *Naked Security.* [Online] 2. 9 2014. [Citace: 14. 11 2016.] Dostupné z: https://nakedsecurity.sophos.com.

36. **HOFFMAN, Chris.** Wi-Fi Security: Should You Use WPA2-AES, WPA2-TKIP, or Both? *How-To Geek.* [Online] 12. 12 2014. [Citace: 15. 11 2016.] Dostupné z: https://www.howtogeek.com.

37. **HEDDINGS, Lowell.** Debunking Myths: Is Hiding Your Wireless SSID Really More Secure? *How-To Geek.* [Online] 15. 8 2014. [Citace: 20. 1 2017.] https://www.howtogeek.com/.

38. **VYLEŤAL, Martin.** Fenomén Li-Fi: budeme se k Internetu místo WiFi připojovat přes LED žárovky? *LUPA.cz.* [Online] 10. 7 2014. [Citace: 22. 11 2016.] Dostupné z: http://www.lupa.cz.

39. **PASSERI, Pablo.** Cyber Attacks Statistics. *HACKMAGEDDON.* [Online] 2017. [Citace: 12. 3 2017.] Dostupné z: http://www.hackmageddon.com.

40. **AGARWAL, Neeraj.** PHP Login Form with Sessions. *FormGet.* [Online] © 2017. [Citace: 2. 12 2016.] Dostupné z: https://www.formget.com/.

41. **CLARKE, Justin.** *SQL Injection Attacks and Defense. 2. vydání.* Burlington : Syngress Publishing, Inc., 2012. ISBN 978-1597499637.

42. **SCAMBRAY, Joel, McCLURE, Stuart a KURTZ, George.** *Hacking bez tajemství. 1. vydání.* Brno : Computer Press, 2001. ISBN 80-7226-549-0.

43. **VEČERA, Zdeněk.** Jak na to: SQL injection. *Zdeněk Večera.* [Online] 21. 3 2009. [Citace: 3. 12 2016.] Dostupné z: http://blog.zdenekvecera.cz.

44. **KÜMMEL, Roman.** *Cross-Site Scripring v praxi.* Zlín : Tigris s.r.o., 2011. ISBN 978-80-86062-34-1.

45. **CARDONA, Roberto.** *Achilles Documentation.* [Dokumentace programu] místo neznámé : DigiZen Security Group, 2000.

46. **DVORSKÝ, Marek.** *Základy bezdrátových komunikací pro integrovanou výuku VUT a VŠB-TUO.* [Online] Ostrava : Vysoká škola báňská - Technická univerzita Ostrava, 2014. ISBN 978-80-248-3557-0.

47. **TKACHENKO, Valerii.** *The best place in the east Europe is Prague in morning at sunrise.* Wikimedia Commons, Praha : 2012.

48. **GREGORA, Lukáš.** *Cloud computig - bezpečnost dat.* Praha : Bakalářská práce. Česká zemědělská univerzita v Praze, 2015.

49. **BERAN, Aleš.** Etika a morálka – úvod. *Aleš Beran.* [Online] 2015. [Citace: 20. 10 2016.] Dostupné z: http://www.eapraha.cz.

50. **KONDA, Matt a CURIEL, Johanna.** OWASP. [Online] OWASP Foundation, 2016. [Citace: 8. 11 2016.] Dostupné z: https://www.owasp.org.

8. Přílohy

Příloha A - Databázová struktura

Struktura databáze uchovávající přihlašovací údaje uživatelů.

	#	Název	Typ	Porovnávání	Vlastnosti	Nulový	Výchozí	Další
☐	1	**id** 🔑	int(6)			Ne	*Žádná*	AUTO_INCREMENT
☐	2	**username**	varchar(30)	utf8_general_ci		Ne	*Žádná*	
☐	3	**password**	varchar(30)	utf8_general_ci		Ne	*Žádná*	
☐	4	**email**	varchar(50)	utf8_general_ci		Ne	*Žádná*	

Příloha B - Obsah databáze

Obsah databáze uchovávající přihlašovací údaje uživatelů.

id	username	password	email
1	admin	test123	admin@seznam.cz

Příloha C - Zdrojový kód úvodní stránky

Úvodní webová stránka, která disponuje přihlašovacím formulářem se zranitelností typu SQLi.

```
<?php
include('login.php');
if(isset($_SESSION['login_user'])){
header("location: profile.php");}
?>
<!DOCTYPE html>
<html>
<head>
<title>Přihlašovací formulář</title>

<link rel="stylesheet"
href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.c
ss"
integrity="sha384-
BVYiiSIFeK1dGmJRAkycuHAHRg32OmUcww7on3RYdg4Va+PmSTsz/K68vbdEjh4u"
crossorigin="anonymous">
</head>

<div class="panel panel-default">
<h1>Vstupujete na výzkumnou webovou stránku</h1>
<div class="panel-body">Nacházíte se na webové stránce, která slouží k
demonstrování bezpečnostních nedostatků
webových aplikací v rámci diplomové práce na ČZU. Veškerou aktivitu na
webových stránkách
provádíte na vlastní zodpovědnost! Odesílaná data nejsou nikterak
uchovávána!</div>
</div>
<body>
<div class="container" id="main" style="width: 350px;">
<form class="form-signin" action="" method="post">
<div id="login">
<h2 class="form-signin-heading">Přihlašte se prosím</h2>
<label for="name" class="sr-only">Uživatelské jméno</label>
<input type="text" id="name" name="username" class="form-control"
placeholder="Uživatelské jméno" required autofocus>
<label for="heslo" class="sr-only">Heslo</label>
<input type="password" id="heslo" name="password" class="form-control"
placeholder="Heslo" required>
<button class="btn btn-lg btn-primary btn-block" type="submit" value="
Login " name="submit">Přihlásit se</button>
<span><?php echo $error; ?></span>
</div>
</form>
</div>
<br>
</body>
</html>
```

Příloha D - PHP skript pro přihlášení

Skript, který vstupní údaje přenáší prostřednictvím dotazu do MySQL databáze a ověřuje oprávnění k přístupu.

```
<?php
session_start();
if (isset($_POST['submit'])) {
if (empty($_POST['username']) || empty($_POST['password'])) {
$error = "Chyba";
}
else
{
//Definování proměných
$username=$_POST['username'];
$password=$_POST['password'];

//Připojení k databázi
$connection = mysql_connect("localhost", "ridik81480443246", "s6r9Fsfm");

//Zakomentované ošetření před SQLi z kapitoly 2.5.1.1.1 Zabezpečení před
SQLi
/*$username = mysql_real_escape_string($username);
$password = mysql_real_escape_string($password);*/

//Výběr databáze
$db = mysql_select_db("ridik81480443246", $connection);

//SQL příkaz, který ověří, jestli se zadaná kombinace hodnot nachází v
databázi
$query = mysql_query("select * from login where username='$username' AND
password='$password'", $connection);
$rows = mysql_num_rows($query);
if ($rows == 1) {
$_SESSION['login_user']=$username;
header("location: profile.php"); //Přesměrování při úspěšném přihlášení.
} else {
$error = "<div style=color:red;>Nesprávné jméno nebo heslo</div>";
}
mysql_close($connection); // Closing Connection
}
}
?>
```

Příloha E - Názorné zobrazení funkcionality clickjackingu

Využití rámců k pozměnění formuláře, který může být prostřednictvím rámce vložený na vlastní webové stránky a za využití rámců a kaskádových stylů pozměněn jeho kontext.

```
<html>
<head></head>

<body>
<div style="width: 550px;position: absolute;left: 150px; top: 100px;
border-style: solid;">
<div style="padding: 10px">
<div><h2>Zvolte kandidáta, pro kterého chcete hlasovat v krajských
volbách.</h2><div>
<br>


<form action="demo_form.asp">
<label>Zvolte kandidáta:</label>
  <input type="checkbox" name="vehicle" value="Bike"> Přemysl Sobotka
  <input type="checkbox" name="vehicle" value="Bike"> Vojtěch Karel
  <input type="checkbox" name="vehicle" value="Bike"> Dagmar Patrasová
<br>

<label>Emailová adresa:</label>
<input type="email" name="vehicle" value="" checked><br><br>

  <input type="submit" value="Odeslat" style="position: absolute; left:
450px"><br>
</form>
</div>
</div>

<iframe src="frame.html"
 style="position: absolute; top: 0px; left: 0px;
 width: 550px; height: 141px; border: medium none;" scrolling="no">
 </iframe>

</body>
</html>
```

Příloha F - Iframe překrývající obsah

Rámec sloužící k překrytí podstatných částí originálního rámce (např. s formulářem) za účelem pozměnění jeho kontextu.

```
<html>
<head></head>
<body style="background-color: white">
<div>
<h2 style="position:absolute; left: 150px">Protispamová
ochrana</h2><br><br>
<p style="position:absolute; left: 120px">Zadejte svojí emailovou adresu
pro ověření<p><br><br><br><br><br>
</div>
</body>
</html>

<iframe src="frame.html"
style="position: absolute; top: 0px; left: 0px;
width: 550px; height: 141px; border: medium none;" scrolling="no">
</iframe>
```

Příloha G - Landing page z WiFi Pineapple

Landing page, která slouží k autorizaci klienta prostřednictvím formuláře vyžadující zadání emailové adresy.

```
<?php
$destination = "http://" . $_SERVER['HTTP_HOST'] . $_SERVER['HTTP_URI'] . "";
require_once('helper.php');
?>
<html>
  <head>
    <title>Prague WiFi</title>
    <meta charset='UTF-8'>
    <meta name="robots" content="noindex, nofollow">
    <script src="jquery-2.2.1.min.js"></script>
    <script type="text/javascript">
      function redirect() {
        document.getElementById('user').value = navigator.userAgent;
        setTimeout(function() {
          window.location = "/captiveportal/index.php";
        }, 100);}
    </script>
    <style>
    .container{max-width:350px;background-color:
white;opacity:0.8;padding:10px;margin:auto;text-align:center;}
    body{background-image:url("/bgrd.jpg"); background-size: auto auto;
background-repeat: no-repeat;background-position: top;background-color:
#8f7561;}
    #prohlaseni {font-size:9px;}
    input[type=text] {border: 2px solid red;border-radius: 4px;min-
width:220px;text-align:center;height:50px;font-size:16px;}
    button[type=submit] {background-color: #4CAF50;border: none;color:
white;padding: 16px 32px;text-decoration: none;margin: 4px 2px;cursor:
pointer;font-size:20px;}
    </style>
  </head>
  <body>
    <div class="container">
      <h1>Prague WiFi</h1>
        <form method="POST" action="/captiveportal/index.php"
onsubmit="redirect()" class="authForm">
          <p>Pro přístup k internetovému připojení Prague Wifi, vložte svojí
emailovou adresu</p><br>
          <input type="hidden" name="target" value="<?=$destination?>">
              <input type="hidden" name="user" id="user" value="">
          <input type="text" name="email" placeholder="Vložte emailovou adresu"
title="Zadejte email ve formátu xxxx@xxxx.xx"
            pattern="[a-zA-Z0-9._%+-]+@[a-z0-9.-]+\.[a-z]{2,3}$"
required><br><br>
          <button name="login" type="submit">Vstoupit</button>
          <p id="prohlaseni">*Kliknutím na tlačítko vstoupit  <a
href="/pravidla.pdf">souhlasím s podmínkami a řádem</a> Prague WiFi</p>
        </form>
    </div>
  </body>
</html>
```

Příloha H - PHP skript zachycující parametry požadavků

Skript v jazyce PHP zachycující parametry, zaslané z autorizačního formuláře na landing page a zobrazující zprávy při ne/úspěšné autorizaci.

```
<?php namespace evilportal;
class MyPortal extends Portal
{
    public function handleAuthorization()
    //Zápis parametrů získaných autorizací do textového souboru na SD kartě
    {
        if (!is_dir('/sd/evilportal-logs/')) {
          mkdir('/sd/evilportal-logs/');
        }
        if (isset($_POST['email'])) {
            $email = isset($_POST['email']) ? $_POST['email'] : 'email';
            $user = isset($_POST['user']) ? $_POST['user'] : 'user';
            file_put_contents("/sd/evilportal-logs/auth-login.txt",  date('Y-m-d
H:i:s') .  " {$email} ; {$user}\n", FILE_APPEND);
        }
        parent::handleAuthorization();
    }
    public function showSuccess()
    //Zobrazení zprávy při úspěšné autorizaci
    {
        parent::showSuccess();
    }
    public function showError()
    //Zobrazení zprávy při neúspěšné autorizaci
    {
        parent::showError();
    }
}
?>
```

Příloha I - Provozní řád Wi-Fi sítě

Konkrétní ukázka obsahu dokumentu provozního řádu sítě.

Provozní řád sítě Prague Wi-Fi

1. Úvodní ustanovení

1.1. Provozní řád sítě Prague Wi-Fi (dále jen „Provozní řád“, nebo „Řád“) upravuje podmínky využívání sítě Prague Wi-Fi

1.2. Sítí Prague Wi-Fi se rozumí skupina přípojných bodů provozovaných na frekvenci 2,4 GHz, jejichž specifikace je uvedena níže:

1.2.1. Prague WiFi

1.2.2. Prazsky Hrad

1.2.3. Prague Castle

1.2.4. Karluv Most

1.2.5. Karl’s Bridge

1.3. Uživatel se připojením k síti zavazuje, k plnění podmínek a provozního řádu

1.3.1. Připojením se rozumí zadání emailové adresy pro získání přístupu (emailová adresa je určena pouze pro účely diplomové práce a nebude dále šířena, ani využívána k marketingovým účelům)

2. Řízení provozu v síti

2.1. V síti jsou zakázány aktivity, které jsou v rozporu se zákony České republiky, ustanovením Evropské unie a veřejnými mravy

2.2. Při porušování provozního řádu je postupováno podle jeho ustanovení a zákonů ČR

3. Závěrečná ustanovení

3.1. Připojením k síti je uživatel vázán tímto Provozním řádem

3.2. Síť je poskytována v rámci výzkumu diplomové práce a nedochází na ní k narušování dopravovaných zpráv, poskytování informací třetím osobám ani k jakékoliv protiprávní aktivitě

Příloha J - Simulace útoku typu XSS

PHP skript pro vkládání textových komentářů náchylný na zranitelnost typu XSS.

```
<?php
if($_POST['content']!=null){
        $fp = fopen('komentare.txt','a');
        fwrite($fp, $_POST['content'] . "<hr/>");
        fclose($fp);
}
echo nl2br(file_get_contents('komentare.txt'));
?>

<!DOCTYPE html>
<html>
<meta charset='UTF-8'>
<title>XSS formulář</title>
<head>
</head>

<body>
  <h3>Vložení komentáře</h3>
  <form action="xss.php" method="post">
    <textarea name="content" rows="3" cols="50"><script>alert('Stránka je
nezabezpečena před XSS!');</script></textarea>
    <br/>
    <input type="submit" value="Odeslat"/>
  </form>
</body>
</html>
```

Příloha K - Infografika výzkumu

Infografika, která byla vytvořena za účelem prezentace výstupů výzkumu.