Kybernetické útoky v síťových a distribuovaných informačních systémech

Cyber attacks in networked and distributed information systems

Bc. Lukáš Krynes

Diplomová práce
2014

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2013/2014

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Lukáš Krynes**
Osobní číslo:	**A12421**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Počítačové a komunikační systémy**
Forma studia:	**prezenční**
Téma práce:	**Kybernetické útoky v síťových a distribuovaných informačních systémech**
Téma anglicky:	**Cyber Attacks in Networked and Distributed Information Systems**

Zásady pro vypracování:

1. **Zpracujte literární rešerši na téma kybernetické útoky v síťových a distribuovaných systémech.**
2. **V teoretické části zpracujte základní pojmy a tvrzení teorie uspořádaných množin a teorie svazů. Tvrzení formulujte bez důkazů a uveďte přehledné příklady.**
3. **Formulujte základní vlastnosti uzávěrových operátorů na uspořádaných množinách a větu o pevném bodě s konkrétními příklady.**
4. **V praktické části zpracujte přehledně základní pojmy a tvrzení formální konceptuální analýzy a uvedtě konkrétní příklady kontextů a jejich konceptuálních svazů v dané oblasti.**
5. **Metodami formální konceptuální analýzy proveďte rozbor kybernetických útoků na síťové a distribuované systémy.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. GANTER, Bernhard a Rudolf WILLE. Formal concept analysis: mathematical foundations. New York: Springer, x, 284 p. ISBN 35-406-2771-5.
2. BĚLOHLÁVEK, Radim. Konceptuální svazy a formální konceptuální analýza [online]. [cit. 2014-02-06]. Dostupný z WWW: http://belohlavek.inf.upol.cz/publications/Bel_Ksfka.pdf.
3. CHAJDA, Ivan. Algebra 3. Olomouc: Univerzita Palackého, 1998. 125 s. ISBN 80-7067-803-8.
4. KOPKA, Jan. Svazy a booleovy algebry. Ústí nad Labem: Univerzita J. E. Purkyně, 1991. 244 s. ISBN 80-7044-025-2.
5. HARZHEIM, By Egbert. Ordered sets. New York: Springer, 2005. ISBN 978-038-7242-224.
6. JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. 1. vyd. Praha, 2007, 284 s. ISBN 978-80-247-1561-2.
7. ENDORF, Carl. Detekce a prevence počítačového útoku. 1. vyd. Praha: Grada, 2005, 355 s. ISBN 80-247-1035-8.
8. MIRKOVIC, Jelena. Internet denial of service: attack and defense mechanisms. Upper Saddle River, N.J.: Prentice Hall Professional Technical Reference, 2005, xxii, 372 p. ISBN 01-314-7573-8.

Vedoucí diplomové práce: **RNDr. Jiří Klimeš, CSc.**
Ústav matematiky

Datum zadání diplomové práce: **7. února 2014**

Termín odevzdání diplomové práce: **27. května 2014**

Ve Zlíně dne 7. února 2014

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

prof. Ing. Vladimír Vašek, CSc.
děkan

prof. Ing. Karel Vlček, CSc.
ředitel ústavu

ABSTRAKT

Práce je v teoretické části zaměřena na popis poznatků z oblasti počítačových sítí, kybernetických útoků, teorie svazů, uzávěrových operátorů a věty o pevném bodě. Popis jednotlivých kybernetických útoků je rozčleněn do několika základních částí podle povahy jednotlivých útoků. Dále je popsán také Hasseův diagram, který se ke grafickému znázornění svazů využívá. Praktická část se skládá z obecného popisu formální konceptuální analýzy a především z konkrétní analýzy kybernetických útoků. Tato analýza je rozdělena na více části, kde každá část je zaměřena na útoky stejné povahy. Jako atributy k analýze slouží vlastnosti útoků a principy jejich činnosti.

Klíčová slova: Formální konceptuální analýza, objekt, atribut, formální koncept, formální kontext, konceptuální svaz, kybernetický útok, denial of service, man in the middle, malware.

ABSTRACT

The thesis is in the theoretical part focused on the description of knowledge in the field of computer networks, cyber attacks, lattice theory, closure operators and fixed point theorem. Description of individual cyber attacks is divided into several parts according to the nature of individual attacks. Futhermore Hasse diagram is also described which is used to graphical representation of lattices. The practical part consists of a general description of formal concept analysis and especially of a specific analysis of cyber attacks. This analysis is divided into several parts, each part focuses on attacks of the same kind. As attributes to the analysis are used the characteristic of attacks and principles of their activities.

Keywords: Formal concept analysis, object, attribute, formal concept, formal context, concept lattice, cyber attack, denial of service, man in the middle, malware.

Chtěl bych touto formou poděkovat panu RNDr. Jiřímu Klimešovi, CSc. za vedení diplomové práce, odborné rady a doporučení. Poděkování patří rovněž mojí rodině za jejich podporu při studiu.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně ……

podpis diplomanta

OBSAH

ÚVOD

Kybernetické útoky představují jeden z nejvážnějších problémů bezpečnosti v informačních technologiích. Jejich postupný narůstající počet je úzce spjat s rozvojem komunikačních technologií a Internetu. K jejich velkému rozmachu tedy začalo docházet na počátcích devadesátých let. Lze je rozdělit do mnoha skupin podle určitých kritérií, kterými mohou být například metody použité k provedení útoku, anebo důsledky, které dané útoky v napadnutém systému vyvolaly. Může tedy dojít k odposlouchávání komunikace mezi odesílatelem a příjemcem, ale i k modifikaci této komunikace, což nemusí odesílatel ani příjemce zaznamenat a při komunikaci potom předpokládají, že komunikují pouze spolu, i když tomu tak není. Dále může dojít k odepření určité služby pomocí útoků, které mají za úkol znepřístupnit prvek, který danou službu poskytuje. V posledních letech se velké množství kybernetických útoků odehrává na aplikační úrovni, což umožňuje také přístup útočníkům k uživatelským datům a komunikaci a společně s tím roste i tlak na softwarové vývojáře, kteří jsou zodpovědní za chyby v aplikacích, které potom útočníci využívají. Ti mají také ve velké oblibě využívání škodlivého software, který může být schopen šířit se sítí a usnadňovat útočníkům přístup do napadnutého systému, nebo provádět další škodlivé aktivity. Dalším častým jevem je provádění distribuovaných útoků, kdy je útok veden obvykle z více než jednoho místa.

Útočníky k provádění kybernetických útoků vede více důvodů, mezi nimi i pomsta, ctižádost nebo například nesouhlas s politickými poměry. Hlavním důvodem ovšem zůstává hmotný prospěch, který útočníkovi napadnutí daného systému může přinést. V dnešní době probíhá pomocí Internetu často manipulace uživatelů s financemi, na což se útočníci také s oblibou zaměřují. Při získání přihlašovacích údajů určitého uživatele k jeho internetovému bankovnictví, tak mohou uskutečňovat převody finančních částek na své účty, nebo prostřednictvím napadnutého uživatele nakupovat zboží v internetových obchodech. V neposlední řadě je důležitá také osvěta samotných uživatelů, kteří často velmi zbytečně, usnadňují útočníkům provádění útoků, které jsou právě založeny na selhání lidského faktoru. Jelikož lze kybernetické útoky rozdělit do mnoha skupin podle jejich povahy, kdy určité útoky mohou mít společné vlastnosti, tak je lze použít jako objekty pro rozbor pomocí formální konceptuální analýzy FKA. Atributy těchto objektů jsou poté vlastnosti kybernetických útoků.

I. TEORETICKÁ ČÁST

1 ZÁKLADNÍ POJMY

1.1 Kyberprostor

Tento pojem se poprvé objevil v povídce Williama Gibsona *Burning Chrome*. To bylo v roce 1982. V reálném světě má ale základy již v práci Norberta Wienera, který v roce 1947 definoval pojem kybernetika, kterou popisuje jako řízení a sdělování u organismů a strojů ve stejnojmenné knize. Velmi významné se staly také práce Claude Elwood Shannona, který definoval kvantitativní a pravděpodobnostní pojetí informace. Poslední ze základních milníků bylo vytvoření prvního tranzistoru v Bellových laboratořích, kdy se první modely začaly komerčně prodávat již na začátku padesátých let. Poté již začalo docházet k prudkému rozmachu technologií, vytváření prvních integrovaných obvodů a později i procesorů. [1]

Důležité je si uvědomit, že člověk je součástí kyberprostoru například i při pouhém telefonování. Skutečný rozmach zapojení běžného člověka v kyberprostoru nastal ale až na počátku osmdesátých let s vytvořením prvních personálních počítačů a veřejných počítačových sítí. Po komercializaci internetu v roce 1994 vznikl z pohledu člověka ke kyberprostoru velký zlom, protože se tím otevřely další cesty jak jeho prostřednictvím komunikovat a dostávat se k informacím.

1.1.1 Kybernetický útok

Je jakékoliv protiprávní jednání útočníka nebo skupiny útočníků z kyberprostoru, nejčastěji z internetu, které je proti zájmům dané osoby. Pro útočníky existuje více druhů motivací pro tvorbu kybernetického útoku, jak je již naznačeno v úvodu. Samotný útok poté nemusí být směřován proti konkrétní osobě, jelikož výběr oběti bývá často náhodný. U obětí kybernetického útoku může dojít ke ztrátě důvěrnosti informací, porušení integrity dat, anebo například k odepření určité služby. Poškození kybernetickým útokem není pouze otázkou software, ale důsledek útoku může vést i k zničení hardwarových částí systému. Škodlivý kód může mít například za následek zvyšování teploty určitých částí počítače, což může vést až k jejich nevratnému poškození. [2], [3]

1.2 Počítačová síť

Je to skupina hardwarových prostředků, jako jsou počítače, přepínače, směrovače, servery a další periferie, jenž jsou mezi sebou propojeny tak, aby byla možná jejich vzájemná komunikace. K propojování jednotlivých částí sítě existuje mnoho druhů médií od měděných vodičů, přes optické spoje až k bezdrátovému přenosu. Počítačové sítě mohou být soukromé i veřejné a je možné je rozdělit podle mnoha aspektů, z nichž nejčastějším je dělení sítí podle přepojování. U sítí s přepojováním okruhů probíhá komunikace po předem sestaveném spojení, data se posílají po tomto spojení a jsou doručována ve správném pořadí. U sítí s přepojováním paketů se každý paket posílá individuálně a v uzlových bodech, což mohou být například směrovače, se rozhoduje, jakou cestou se paket pošle dál k příjemci. Důležité je také rozdělení z hlediska role a postavení jednotlivých prvků. V sítích klient-klient jsou si všechny prvky v síti rovny. Druhým základním typem je síť klient-server, ve které jsou prvky klienti podřízení nadřazenému prvku nebo prvkům, tzv. serverům, kteří poskytují klientům určité služby.

Dalším nejčastějším rozdělením sítí je dělení podle velikost. Nejmenšími sítěmi jsou osobní sítě Personal Area Network PAN sloužící k připojení osobních elektronických zařízení nejčastěji některou z bezdrátových technologií. Další z hlediska velikosti jsou lokální počítačové sítě Local Area Network LAN, jejichž prvky se rozprostírají v ohraničeném prostoru na vzdálenosti stovek metrů. Příkladem může být škola nebo nemocnice. Větším celkem je poté metropolitní počítačová síť Metropolian Area Network MAN, které se lokálním sítím dosti podobají, ale slouží k propojování prvků na vzdálenosti až několika kilometrů a využívají i veřejné telekomunikační sítě. Největším celkem jsou rozlehlé počítačové sítě Wide Area Network WAN, u kterých může docházet i k mezikontinentálnímu propojení. Co se velikosti týká, jsou omezeny pouze velikostí Země. Sítě WAN jsou ve většině případu veřejné, ale existují i soukromé. Počítačové sítě mohou mít i různou topologii, podle které jsou vytvořeny. Ta říká, jak jsou prvky v síti uspořádány. Mezi základní topologie patří sběrnicová, kruhová, hvězdicová a páteřní. Každá s topologií má své výhody a nevýhody.

1.2.1 Základní prvky sítě

Základními prvky jsou koncová zařízení jako počítače nebo notebooky, potom servery, na kterých jsou uložena data a které poskytují počítačům, nebo obecně klientům určité služby

a programy. K řízení provozu v síti se nejčastěji používají přepínače pracující na druhé vrstvě modelu ISO/OSI. Pracují tedy s Media Access Control MAC adresami, které si v Content Addressable Memory neboli CAM tabulce přiřazují ke svým portům. Dalším důležitým prvek sítě jsou směrovače, které pracují na třetí vrstvě referenčního modelu ISO/OSI a tím pádem pracují s Internet Protocol IP adresami. Existují ovšem i přepínače pracující na třetí a vyšších vrstvách modelu referenčního modelu ISO/OSI, který je popsán i s jeho jednotlivými vrstvami dále. Důležitá je také brána sítě, což je uzel spojující dvě sítě s odlišnými protokoly. Brána musí vykonávat i funkci směrovače, proto se v hierarchii síťových zařízení řadí výše. Pojem výchozí brána označuje směrovač, přes který se ostatní prvky sítě dostanou do Internetu. Pro řízení sítě existují i primitivnější prvky pracující na úrovni první vrstvy modelu OSI. Těmito prvky jsou opakovače signálu, různé převodníky vedení a rozbočovače. Známým zařízením pracujícím na druhé vrstvě modelu ISO/OSI je tzv. můstek, který slouží k oddělení provozu dvou segmentů sítě podle MAC adres. V neposlední řadě je třeba zmínit firewall, což je síťové zařízení, které slouží k zabezpečení síťového provozu. Na firewallu jsou definovány pravidla, podle kterých je provoz řízen. Firewally se podle složitosti a schopnosti zabezpečení dělí do více skupin. [4]

1.3 Distribuovaný systém

Výpočty distribuovaných systému lze považovat za speciální typ paralelních výpočtů. Spolupráce mnoha procesorů při výpočtu je náročný proces vyžadující řízení určitým distribuovaným algoritmem. Z bezpečnostního hlediska je u distribuovaných systémů problém hlavně v množství komponentů, ze kterých se skládá, protože s růstem jejich množství roste i možnost vzniku poruch a bezpečnostních hrozeb. Když nějaký prvek v systému selže, tak je jeho činnost většinou nahrazena ostatními prvky systému. Komunikace mezi jednotlivými procesory probíhá pomocí zasílání zpráv. Distribuované systémy nalézají uplatnění v mnoha aplikacích, ať již třeba při řešení složitých výpočtů, nebo například v databázových systémech. Jejich hlavními výhodami jsou spolehlivost, rozšiřitelnost, vysoká výkonnost, ale i ekonomická výhodnost díky dobrému poměru cena/výkon.

Řízení počítačové sítě je u komplexnějších sítí dosti náročný proces, a proto se využívá rozdělení do více vrstev, kde každá má zodpovědnost za určitou část řízení. Každá z těchto vrstev je v podstatě distribuovaným systémem využívající komunikační protokoly. [5]

1.4 Referenční model ISO/OSI

Úkolem modelu je rozdělení sítě do sedmi vrstev, kde každá má zodpovědnost za určitou část celkové přenosu dat od odesílatele k příjemci. Mezi jednotlivými vrstvami funguje vertikální komunikace, při které nižší vrstva poskytuje služby vyšší. Každá z vrstev obsahuje protokoly pro horizontální komunikaci s protilehlým systémem.

7. Aplikační – Přístup a spolupráce síťových aplikací s komunikačním systémem, předepisuje, v jakém formátu mají být data dodána.
6. Prezentační – Komprese a dekomprese zpráv, jejich úprava pro síťové aplikace, převody datových struktur.
5. Relační – Přístup uživatele k aplikačním programům, eviduje provoz na sítí a stará se o přístupová práva, vytváří relace, kde nejčastěji je jedna relace jeden transportní spoj.
4. Transportní – Tvorba transportních spojů, práce s porty, rozklad zprávy na stejně velké úseky, spoléhá se na služby nižších vrstev.
3. Síťová – V této vrstvě probíhá adresování a směrování dat od odesílatele k příjemci přes různý počet prvků nacházejících se ve WAN. Realizována je nejčastěji datagramovou službou IP nebo virtuálním spojením. V této vrstvě se vytváří z datagramů nebo segmentů pakety. Tyto pakety obsahují metadata a uživatelská data. Metadata obsahují řídící informace pro přenos paketu sítí, jako je adresa zdroje a cíle, kontrolní součty a informace o pořadí.
2. Linková – Pracuje s MAC adresami. Zajištění přenosu mezi sousedními propojenými prvky v LAN síti. V této vrstvě se se vytváří rámce z paketů, které obsahují: přenášená data, údaje o adresování, zabezpečení proti chybám a údaj o rozpoznání začátku rámce.
1. Fyzická – Vlastnosti přenosového média, charakteristika a vlastnosti přenosového signálu, reprezentace logických nul a jedniček, přenos jednotlivých bitů přes komunikační kanál bez ohledu na jejich význam.

Tab. 1: Vrstvy referenčního modelu OSI

1.5 Protokoly v TCP/IP

Tyto protokoly se v drtivé většině případů nezabývají fyzikou a linkovou vrstvou. Protokol IP přenáší datagramy mezi vzdálenými počítači a odpovídá síťové vrstvě. IP datagram má v záhlaví adresu příjemce, podle které se datagram doručí. Jednotlivé datagramy se posílají samostatně a není zaručeno jejich doručení v pořadí odeslání. Protokoly User Datagram Protocol UDP a Transmission control protocol TCP odpovídají transportní vrstvě. TCP dopravuje data pomocí segmentů a UDP pomocí datagramů. Rozdíl v obou je i v tom, že TCP je spojovaná služba a příjemce tak potvrzuje přijímaná data. Aplikační protokoly TCP/IP jsou v podstatě tři zredukované vrstvy OSI modelu. Jedná se o relační, prezentační a aplikační vrstvu. Patří sem celá řada známých protokolů jako HyperText Transfer protocol HTTP, což je bezstavový protokol, jehož hlavním úkolem je přenos hypertextových informací, tedy textových dat, které jsou doplněny o odkazy. Dalším příkladem může být File Transfer Protocol FTP. Aplikační protokoly využívají buďto TCP nebo UDP, popřípadě oba dva. K rozlišení jednotlivých aplikačních protokolů se používají porty, což jsou v podstatě číselná označení. Každé síťové spojení aplikace je pak označeno číslem portu, spolu transportním protokolem a adresou příjemce.

1.5.1 IPv4 a IPv6

Protokol IPv4 je používaný v sítích s přepojováním paketů. IP adresa identifikuje umístění prvků v síti. Je to 32 bitová adresa zapisovaná pomocí 4 osmibitových čísel v rozmezí 0 – 255. Skládá se ze dvou částí, z nichž první je síťová a druhá hostitelská. K určení adresy sítě slouží síťová maska, což je 4 bajtové číslo. Adresa sítě se z IP adresy získá logickým součinem IP adresy a masky sítě vyjádřených ve dvojkové soustavě. Jelikož síťových zařízení a požadavků na adresy přibývá, tak IPv4 již nestačí pokrýt růst poptávky a v roce 2011 byly rozděleny poslední bloky adres. U IPv6 jsou adresy v šestnáctkové soustavě, protože adresa je šestnáctibajtová. Osm čtveřic šestnáctibitových čísel se odděluje dvojtečkami. S nástupem IPv6 vzrostla i kapacita IP adres, které tak vydrží pro celý svět na mnoho let dopředu.

1.5.2 MAC adresa

MAC je jedinečný identifikátor síťové karty, který využívají protokoly druhé vrstvy modelu OSI. MAC adrese se také říká fyzická adresa, protože je přiřazena síťové kartě již

při její výrobě. Ethernetová MAC adresa obsahuje 48 bitů zapsaných standardně jako tři skupiny čtyř hexadecimálních čísel. Nejčastěji se zapisuje jako šestice dvojciferných hexadecimálních čísel oddělených pomlčkami, či dvojtečkami. Jedinečnost označení MAC adresy je celosvětová. Speciálním typem je všesměrová adresa označující všechna připojená zařízení. Tato adresa obsahuje samé jedničky, tedy ff:ff:ff:ff:ff:ff. [6]

1.5.3 Domain Name System

Je to celosvětově distribuovaná databáze, jejíž části jsou umístěny na tzv. name serverech. Jsou v ní definovány vazby mezi doménovými jmény a IP adresami prvků. Založeno na principech klient-server architektury. Uživatel zadává do internetového prohlížeče doménové jméno, které DNS server převede na IP adresu.

1.5.4 Dynamic Host Configuration Protocol

Tento protokol se používá pro automatickou konfiguraci prvků v síti. DHCP server poskytuje klientům nejčastěji IP adresu, masku sítě, IP adresu výchozí brány a DNS serveru. Platnost těchto údajů je ale omezena. Jelikož DHCP je také založeno na klient-server architektuře, tak na zařízení, které o přidělení adres žádá je umístěn DHCP klient, který adresy obnovuje.

1.5.5 Internet Control Message Protocol

Využívají ho operační systémy a zařízení jako routery k posílání chybových a řídících zpráv ostatním zařízením. Zprávy ICMP se vytvářejí nad IP vrstvou nejčastěji z IP datagramu, který vytvoření ICMP zprávy zapříčinil. [7]

1.5.6 Address Resolution Protocol

Protokol Address Resolution Protocol ARP je povinným standardem sady protokolů TCP/IP. Tento protokol překládá IP adresy na MAC adresy. Umožňuje zjistit adresu zařízení formou vyslání dotazu na všechny prvky a zjištěním, komu patří daná přiložená IP adresa. Když některý prvek zjistí, že jde o jeho adresu tak odpoví a ARP si do tabulky přiřadí k dané IP adrese jeho adresu MAC. [8]

2 ROZDĚLENÍ A POPIS KYBERNETICKÝCH ÚTOKŮ

S růstem a rozvojem počítačových sítí začalo vznikat i čím dál více druhů kybernetických útoků na tyto síťové systémy. Základní rozdělení je na kybernetické útoky aktivní a pasivní. Pasivní útoky se snaží především o získání důvěrných informací, které by mohly být zneužity. Při tomto útoku nedochází k žádnému poškození ani změnám na hardware, software ani na datech napadnutého systému. Jedná se především o monitorování provozu napadnuté sítě a odposlouchávání dat. Oproti tomu aktivní útok způsobuje poškození hardware, software nebo pravosti dat a může do napadnutého systému injektovat škodlivý kód. Aktivní útoky se sice dají snadněji detekovat, ale způsobují také větší škody.

2.1 Denial of service

Tyto útoky bývají často označovány zkratkou DOS. Český význam je odmítnutí nebo odepření služby. Jedná se o aktivní typ útoku. Mají za následek znepřístupnění určité služby, zařízení, nebo dokonce celé sítě. Vyskytují se v různých obměnách již několik desítek let, ale v dnešní době jsou v popředí hlavně útoky využívající chyb programů, operačních systémů, nebo síťových protokolů. DOS útoky jsou často využívány až jako doplňková akce k jinému typu útoku, aby zametly stopy po útočníkovi. [9],[10]

2.1.1 Útoky využívající chyb a vyčerpání systémových prostředků

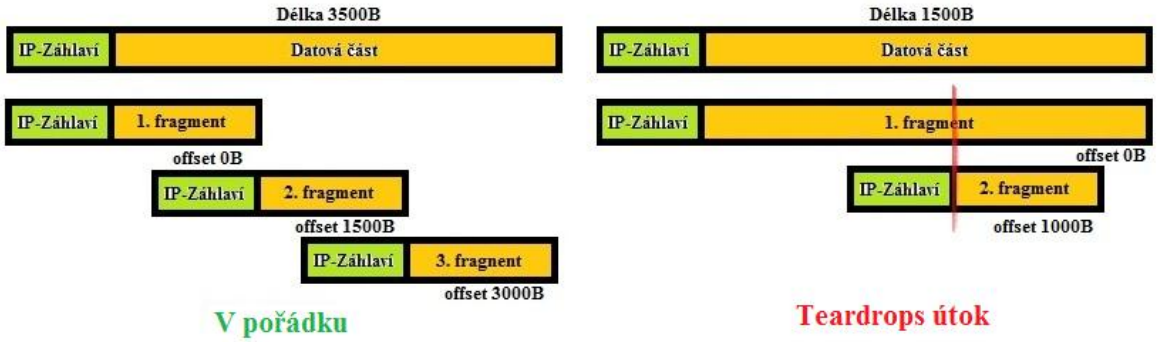
Ping of death

Ping neboli Packet InterNet Groper je příkaz udávající čas, který paket potřebuje na cestu ze zdrojového do cílového prvku a zpátky. Parametrem příkazu je adresa cílového zařízení, nebo jeho doménové jméno, které přeloží DNS server. Program využívá protokol ICMP.

Ping of death patří k nejstarším DOS útokům využívající chyby v TCP/IP. Je-li velikost paketu větší než 1500 bajtů, dochází k jeho fragmentaci a následnému složení zpět do původní podoby u příjemce. Aby mohl příjemce paket sestavit, tak potřebuje informaci o offsetu, aby věděl kam, který fragment paketu patří. Útok spočívá v úpravě fragmentu, kdy po složení paketu je jeho velikost větší než 65 535 bajtů. To má za následek havárii, zamrznutí a nedostupnost daného napadnutého prvku. Důvodem je přetečení paměti vyhrazené pro daný upravený paket.

Teardrops

Jedná se také o útok využívající chyby, který je Ping of death podobný v tom, že také využívá situace při sestavování fragmentů paketu. Na obrázku 1 je na levé straně vidět správné sestavení paketu ze segmentů, kde v IP záhlaví je uloženo pořadí jednotlivých paketů, jejich délka a také offset. Na pravé straně obrázku 1 je ilustrován Teardrops útok, kde je patrné, že se dva fragmenty překrývají, protože první fragment je stejně dlouhý jako celý paket. Problém nastává při sestavování paketu, kdy v kopírovací funkci vyjde záporná návratová hodnota. Systém totiž očekává hodnotu kladnou, a tak tedy onu zápornou hodnotu převede na velké kladné číslo. Toto číslo je ovšem tak velké, že při pokusu o kopírování dojde k chybě, která také může vyřadit celý prvek sítě. Tento typ útoku může na starších operačních systémech přivodit až jejich pád a tím i nedostupnost daného prvku v síti.



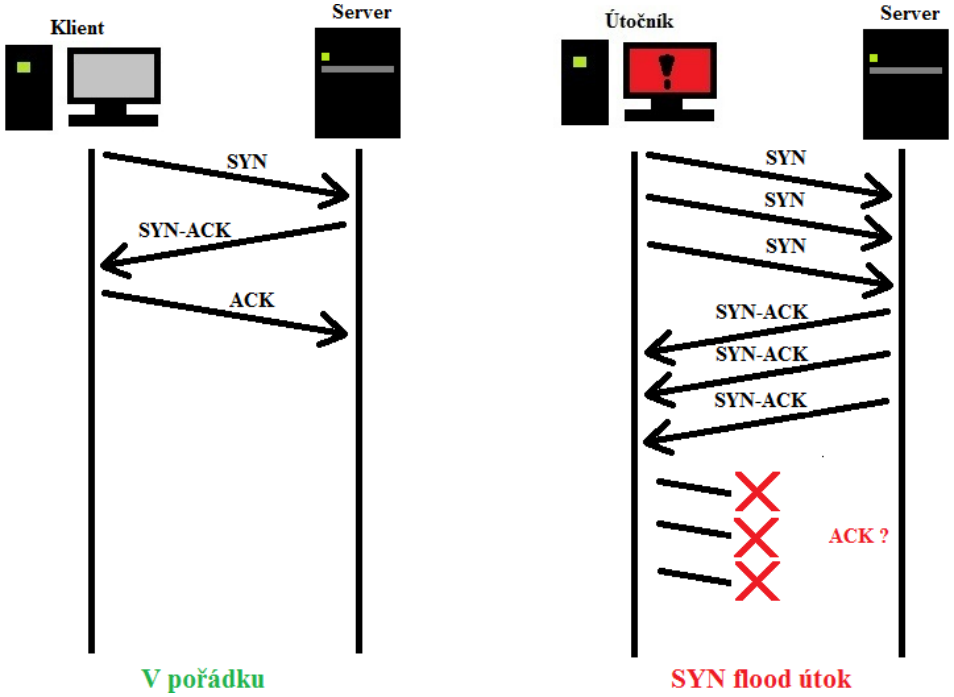
Obr. 1: Teardrops útok

SYN flood útok

Navázání komunikace probíhá v TCP pomocí handshake, neboli potřesení rukou. Protokol transportní vrstvy TPC se používá ve většině webových služeb, jelikož je bezpečnější než UDP. Klient odešle příjemci nejdříve TCP paket s nastaveným synchronizačním příznakem. Pokud server příjme spojení tak pošle zpět klientovi paket s potvrzením ACK a také nastaví příkaz SYN, čím nastaví spojení i z druhé strany. Klient nakonec serveru odešle také potvrzení ACK, čímž je proces navázání spojení u konce a může se přejít k přenášení samotných dat.

SYN flood útok spočívá v tom, že útočník posílá na server stále jen SYN paket, jehož velikost je velmi malá, což je pro útočníka výhodné. Pokaždé když server příjme SYN paket tak odešle zpět SYN-ACK a alokuje pro spojení systémové zdroje. Poté čeká na

potvrzení ACK, ale od útočníka žádné potvrzení nepřichází. Čím více SYN paketů útočník na server pošle, tím více zatíží systémové zdroje serveru, což vede až k jeho nedostupnosti pro ostatní klienty sítě. Moderní obrana proti útoku spočívá ve využití SYN cookies, kdy se systémové prostředky serveru alokují až po úplném navázání spojení. Tento útok je záplavového typu, ale jelikož využívá chyby, tak je zařazen do této kategorie.



Obr. 2: SYN flood útok

NetKill

Tento útok je podobný útoku předešlému. Využívá chyby v implementaci TCP protokolu což má za následek spotřebování operační paměti prvku. Na rozdíl od SYN flood útoku zde dochází k navázání úplného spojení. Útočník se však již dál o toto spojení nezajímá a navazuje další spojení, přičemž se snaží, aby jich navázal co nejvíce. Systém serveru pro každé spojení poskytuje prostředky, které znovu uvolní až po několikaminutovém čekání, když útočník neodpovídá. Ten se mezitím snaží navazovat další spojení, aby vyčerpal co nejvíce systémových zdrojů prvku

Land útok

Útok spočívá v posílání zfalšovaných paketu oběti. Tyto pakety mají nastavenou stejnou zdrojovou i cílovou IP adresu, která patří oběti. To vyústi v situaci, kdy oběť posílá data

sama sobě a tím se uvrhne do smyčky. Útok se nedá považovat za nebezpečný, protože firewall takovéto pakety může snadno vyfiltrovat.

Fork bomb útok

Tento typ útoku je použitelný pouze k útočení na lokální prvek. Při útoků se využívají programy, které samy sebe spouští donekonečna. To vede k vyčerpání systémových prostředků a zatuhnutí nebo pádu systému. Výsledky některých jiných DOS útoků mohou vypadat stejně jako výsledek Fork bomb.

WinNukes

K útoku se zde využívají programy, tzv. nukes, které slouží k provádění DOS útoků využívajících chyb. Nebezpečí z jejich použití tkví především v tom, že jsou s nimi schopni pracovat i úplní začátečníci. Počet nukes programů naštěstí není příliš velký a nový se objeví jen jednou za několik let.

NBName

K útoku se využívá program, který využívá zranitelnosti NetBiosu. Program nabízí i mnoho možností diagnostiky. DOS útok pomocí tohoto programu je velice silný a jeho důsledek je nemožnost připojení do lokální sítě počítačům s nainstalovaným operačním systémem Windows. [11], [12]

2.1.2 Záplavové DOS útoky

Jedná se o jednoduché, přitom ale velmi nebezpečné typy útoků. Na obrázku 3 je patrné, že pokud je rychlost připojení útočníka například 512 Kb/s a rychlost připojení oběti pouze 128 Kb/s, může dojít k úplnému zahlcení 128 Kb/s linky. Mezi servery poskytovatele Internet service Provider ISP to nevadí, jelikož tyto spoje mívají mnohem větší kapacitu než 512 Kb/s. V dnešní době se tyto útoky využívají k ochromení koncového uživatele, anebo na servery, jejichž rychlost připojení není příliš vysoká. U serverů s vyšší rychlostí linky se používají k jejich znepřístupnění distribuované DOS útoky, které budou popsány dále.

Obr. 3: Příklad záplavového útoku

Tyto útoky jsou nebezpečné především v tom, že uživatel není proti útoku většinou nijak chráněn. Když se pokusí danou komunikaci odfiltrovat přes firewall, tak linka bude stejně pořád zatěžována. Tuto komunikaci je možné filtrovat již u ISP, ten ale často takovou možnost uživatelům nenabízí. Pokud ale ISP takovouto filtraci provede, tak pro útočníka stejně není problém útok modifikovat a zaútočit znovu. Poté bývá řešením úplné odpojení oběti od linky a následný pokus dohledat útočníka. Tyto útoky se již řadu let objevují ve stejné podobě a jsou založeny většinou na nějakém protokolu.

ICMP flood

Mezi nejznámější patří ICMP flood, kdy útočník na server posílá ICMP echo request a server mu posílá zpátky odpověď ICMP reply. Přitom zůstává zachována velikost paketu. Útočník zfalšuje adresu odesílatele a to má za následek dvojnásobné zatížení sítě. Je to obyčejný záplavový útok, který je velmi jednoduché provést.

UDP flood

Využívá zranitelnosti služeb echo a chargen. Při útoku jsou data odeslána na port echo a je zfalšována zdrojová IP adresa spolu s portem. Zfalšování probíhá tak, že se IP adresa nastaví na počítač poskytující službu echo nebo chargen a port se nastaví na příslušnou službu. Tím se docílí toho, že oběť útoku a prvek, jemuž patří zfalšovaná IP adresa, si budou posílat data dokola. Pokud má prvek se zfalšovanou IP adresou vysokou rychlost připojení, může útočník zahltit i prvky, který mají vyšší rychlost připojení než on. V dnešní době není protokol UDP tolik využívaný jako v minulosti, ale i tak je tento útok nebezpečný.

TPC flood

Jsou založeny na protokolu TPC, mají mnoho názvů a jedním z nich je i SYN flood popsaný v předešlé kapitole, který se od ostatních liší. Mezi ostatní patří ACK flood, RST

flood, PSH flood, URG flood a FIN flood. Název závisí na nastaveném příznaku v TCP paketu. Význam ostatních je vždy pokus zahltit linku oběti.

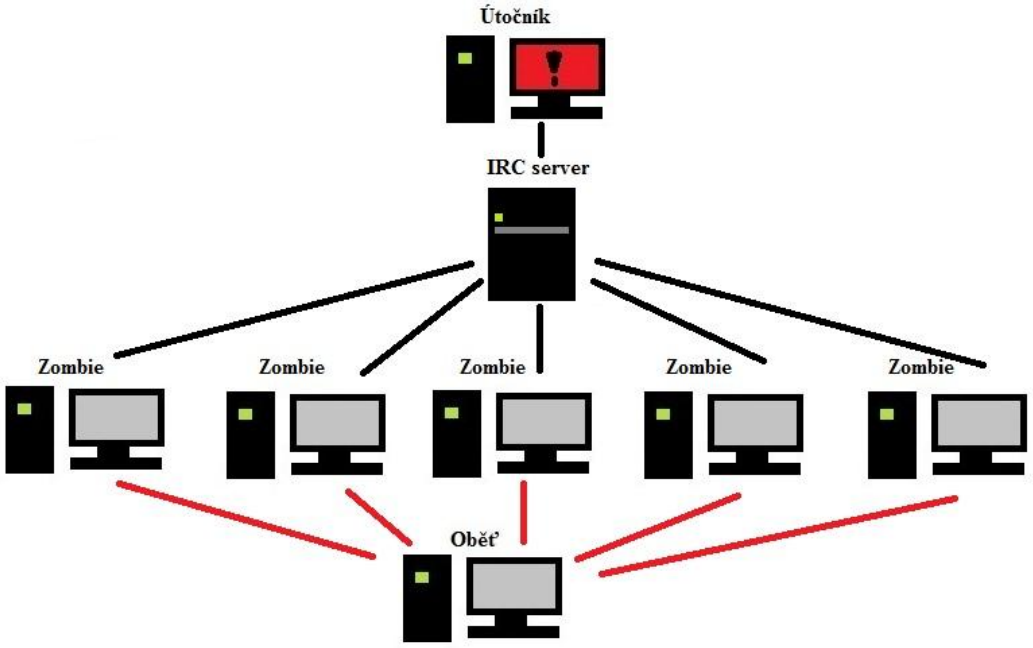
Mass mailing a Email bombs

Další skupinou jsou záplavové útoky způsobující zahlcení emailové schránky. Mezi ně lze zařadit útok Mass mailing, kdy útočník zaregistruje vybranou emailovou adresu na určitých stránkách, nejčastěji s pornografií, odkud je získávají spameři, kteří potom zahlcují danou emailovou adresu. Dalším typem tohoto útoku je Email bombs, kdy útočník pomocí programu vytváří email, kterými poté danou schránku také zahlcuje a může se pokusit i o znepřístupnění poštovního serveru. [13]

2.1.3 Distributed denial of service

Jak již název napovídá, jedná se o distribuované DOS útoky, které bývají vedené z většího množství prvků. Toto větší množství může dosahovat až řádů tisíců, ve výjimečných případech milionů. Důležité také je, že tyto prvky mohou být rozprostřeny po celém světě, takže při útoku může být jeden útočící prvek například z Evropy a další z USA. Přitom útočník obvykle bývá jen jeden. Dříve sice tyto útoky fungovaly na principu více spolu domluvených útočníků, ale to je již v dnešní době nepodstatné. K tomu, aby útočník dosáhl útoku z tak velkého množství počítačů, využívá škodlivý software, tzv. bot. Těmito boty se potom snaží infikovat další počítače tzv. zombie, ze kterých poté bude DDOS útok veden. Přitom majitelé těchto zombie počítačů o tom, že je z jejich počítače veden Distributed Denial Of service DDOS útok ani netuší. Napadení počítače botem se dosti podobá napadení virem, s tím rozdílem, že flexibilita botu ztěžuje uživateli jeho odhalení a odstranění ze systému.

Samotné útoky jsou většinou záplavového typu. Zombie se pomocí botu připojí na IRC server, kde čeká na útočníkovy příkazy. Jakmile příkaz přijde, tak zaútočí na oběť. Síla útoku tkví především ve velkém množství útočících počítačů a bývá o mnoho nebezpečnější než běžný záplavový DOS útok. [14]



Obr. 4: Schéma DDOS útoku

2.1.4 Reflektivní útoky

Jedná se o reflektivní útoky z toho důvodu, že data jejich prostřednictvím neprocházejí stále stejnou cestou, ale během útoku se mění prvky, od kterých se útok reflektuje. V drtivé většině se tyto útoky vyskytují v distribuované verzi. K zahlcení linky oběti se snaží útočník využít jiné prvky, které slouží jako prostředníci. Útočník si vytvoří seznam takovýchto prvků a poté na ně postupně začne posílat pakety se zfalšovanou zdrojovou IP adresou, která patří oběti. Počet paketů bývá obvykle deset, což je záměrně málo, aby nedošlo k žádnému podezření. Prvky, na které tyto pakety pošle, poté odpovídají oběti a tím zatěžují její linku.

2.1.5 Zesilující útoky

I zde je název velmi výstižný. Ve své podstatě jsou to záplavové reflektivní útoky, kde se ono zesílení dosáhne právě pomocí prostředníků, protože útočník posílá menší počet dat, než která nakonec dorazí k oběti.

Smurf útok

Jedná se o ICMP flood útok, ke kterému je přidáno ono zesílení a reflektivita. Echo request se zde pošle na adresu celé sítě, přičemž je zdrojová IP adresa nastavena na IP adresu oběti.

Velikost zesílení tím pádem závisí na počtu prvků dané sítě, protože každý z těchto prvků posílá zpět reply na zfalšovanou adresu oběti. Tento útok se dá považovat za nejstarší ze všech zesilujících útoků a i když jsou většinou adresy sítí filtrovány, tak stále představuje reálné nebezpečí.

Fraggle útok

Tento útok se velice podobá Smurf útoku, navíc pochází i od stejného autora. Princip je skoro stejný s tím rozdílem, že se na IP adresu sítě neposílá ICMP paket, nýbrž se využívá UDP protokol a služeb Echo a Chargen. Jelikož ne všechny prvky používají tyto služby, tak má tento útok menší zesílení než Smurf. V dnešní době se tyto služby prakticky nevyužívají již skoro vůbec, proto se dá tento útok označit za malou hrozbu.

TTL Expiration flood

Je to typ reflektivního zesilujícího útoku, přičemž ale nevyžaduje dopředu mapovat síť a vytvářet seznam prvků. Útok využívá hodnotu Time to live TTL, která je nastavena v rozmezí 64 až 255. Při průchodu dat přes zařízení pracující s protokolem IP je vždy tato hodnota snížena o 1 a to do té doby, než dorazí k cíli. Průměrně je hodnota TTL při dosažení cíle menší o 10, než byla její hodnota při o odeslání. Jedná se o jakýsi typ ochrany, neboť pokud by se data na cestě k příjemci ztratila, tak zařízení, které by hodnotu TTL snížilo z 1 na 0, by je už dál neposlalo. Poté by odeslalo odesílateli zprávu o tom, že vypršela doba životnosti. Hodnoty TTL se využívá i k zjišťování trasy k cíli.

Z hlediska útoku se jako odesílatelova IP adresa nastaví adresa oběti. Dále se nastaví hodnota TTL na nízké číslo, aby došlo k tomu, že se zmenší až na 0. Poté až TTL hodnota skutečně dosáhne 0, je oběti odeslána zpráva. U tohoto útoku je hodnota zesílení dosti nízká zhruba jen 1,7. Na druhou stranu je výhodná jednoduchost jeho implementace, a pokud nefiltruje uživatel příchozí zprávu o vypršení životnosti TTL přes firewall, tak je tento útok možné bez problému používat.

SYN flood

Útok SYN flood je popsán již dříve, ale zde se jedná o modifikovanou reflektivní zesilující verzi, kde je opět zfalšována zdrojová IP adresa na adresu oběti. Pří útoku si vytvoří útočník seznam prvků, které k útoku využije. Poté na ně začne posílat TPC pakety s nastaveným příznakem SYN, kde je i nastavena ona zfalšovaná IP adresa odesílatele. Prvky ze seznamu začnou posílat odpověď SYN-ACK. Jelikož o tom oběť nemá tušení tak

RST zpět neodešle, navíc bývá toto pravidlo i často filtrováno. Prvky ze seznamu poté předpokládají, že se jejich odpověď SYN-ACK asi někde ztratila a většinou ji ještě odešlou čtyřikrát. Z toho plyne i fakt že má tento útok zesílení podle toho, kolikrát prvky ze seznamu SYN-ACK odešlou oběti. Jedná se o velmi nebezpečný typ útoku, kde tkví výhoda ve snadné dostupnosti prvků, které se k útoku využijí.

DNS amplification útok

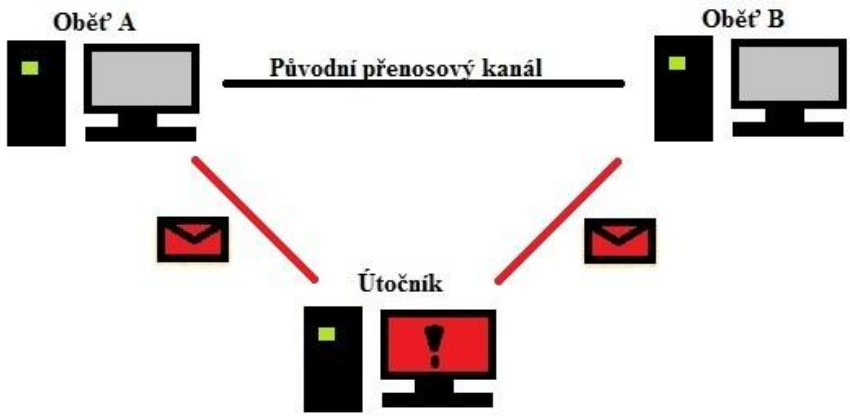
Tento útok bývá označován za jeden z nejnebezpečnějších ze všech DOS útoků. I zde dochází ke zfalšování zdrojové IP adresy a následnému odesílání DNS dotazů. Jediný nutný prvek k útoku je veřejný relay DNS server. Tento DNS server zpracuje ony odeslané DNS dotazy a je dostupný všem prvkům v Internetu. Běžný DNS server využívá protokoly TPC a UDP. Častější je využití UPD, kdy odpověď DNS serveru může mít velikost do 512 bajtů. Dotaz na DNS může mít ale pouze 70 bajtů. Tím se získá vysoké zesílení. Při použití rozšířeného DNS, tzv. Extension mechanisms for DNS může být odpověď serveru až 4 kilobajty. Aby byla odpověď takto veliká, tak útočník povětšinou napadne nějakou doménu, do které vloží své záznamy. Po vytvoření těchto záznamů si útočník sestaví seznam veřejných relay DNS serverů, které k útoku využije.

Následně konečně započne útok spočívající v tom, že útočník DNS serverům ze seznamu začne posílat dotazy na svou předem napadnutou doménu a u těchto dotazů změní zdrojovou IP adresu na adresu oběti. DNS servery budou posílat oběti odpovědi, přičemž se dosáhne onoho zesílení, které dosahuje i hodnot kolem 70. [15]

2.2 Man in the middle MITM

Již podle názvu je zde patrné, že se zde jedná o útok, kdy je útočník připojen na komunikační kanál někde mezi odesílatelem a příjemcem. Fyzicky se však mezi nimi nacházet nemusí. Když útočník monitoruje provoz a odchytává komunikaci, jedná se o pasivní útok. Pokud ale odchycené zprávy modifikuje, tak je to již útok aktivní. Při úspěšném útoku si odesílatel myslí, že komunikuje s příjemcem a naopak, ale ve skutečnosti je jejich komunikace modifikována útočníkem uprostřed. To je i demonstrováno na obrázku 5, kde oběť A a oběť B si myslí, že spolu komunikují přes původní komunikační kanál, ale ve skutečnosti je jejich komunikace vedena přes útočníka. Nebezpečí tohoto útoku může být sníženo dobrým šifrováním komunikačního kanálu

pomocí asymetrické kryptografie nebo použitím elektronického podpisu s certifikátem. Útoky se nejčastěji vyskytují v lokálních sítích, kde jsou prvky připojeny k přepínači. Speciálním typem je útok man in the browser, tedy muž v prohlížeči. Zneužívá se hlavně při bankovních převodech. Útočník ani nepotřebuje být připojen k sítí, protože převod bez vědomí oběti za něj uskuteční škodlivý software, který byl do sítě předtím útočníkem vložen. [16]



Obr. 5: Man in the middle

2.3 Útoky využívající MITM

V této části budou popsány útoky v lokálních sítích využívající principů man in the middle.

2.3.1 ARP Cache poisoning

Při tomto útoku je využita slabina protokolu ARP. Jelikož je tento protokol dost starý, tak neobsahuje žádné ochranné mechanismy. Důležité je definovat prvek brána, což je prvek, který zprostředkovává ostatním prvkům v síti připojení do Internetu. Ostatní potom při přístupu do Internetu komunikují přes tuto bránu.

Toho využije útočník tak, že oběti odešle paket, který obsahuje informaci o tom, že MAC adresa brány a útočníka je stejná. Potom se skutečné bráně odešle další paket s informací o tom, že MAC adresa oběti a útočníka je stejná. To má za následek to, že při vzájemné komunikaci budou prvky do odesílaných dat dosazovat MAC adresu útočníka a přepínače mu poté data odešlou. Tím pádem má přehled o veškeré komunikaci oběti. Po příchodu dat

si tato data prohlédne a pošle je dále s tím rozdílem, že MAC adresu opraví na správnou hodnotu.

2.3.2 MAC flooding

Přepínače vlastní CAM tabulku. Útok je založen na tom, že pokud přepínač v CAM tabulce nemá cílovou MAC adresu prvku, tak paket pošle na všechny porty, kromě portu odesílatele. Při útoku nejprve posíláním paketů dojde k zahlcení CAM tabulky napadnutého prvku. Tyto pakety mají zdrojovou a cílovou MAC adresu náhodně vygenerovanou, což způsobí, že si přepínač vždy udělá záznam do CAM tabulky a paket pošle na všechny porty, kromě portu odesílatele. Tím se nakazí i další přepínače pokud nejsou odděleny například směrovačem. U modernějších přepínačů je velikost CAM tabulky dostačující i pro statisíce záznamů. Další možnost je nastavení cílové MAC adresy příjemce na útočníkovu a zdrojovou náhodně vygenerovat. Pokud příjme přepínač takový paket, udělá si záznam do CAM tabulky, zjistí, že příjemce se nachází na stejném portu a paket už dál nepošle. To ztíží odhalitelnost útoku, ale znemožní nakažení dalších přepínačů.

Jakmile dojde k zahlcení CAM tabulky, tak se většinou každý přepínač přepne do stavu, kdy funguje jako rozbočovač, ale není to pravidlo. Po nějaké době dojde k promazání záznamu v přepínači a právě na to čeká útočník, který dané místo zaplní svou položkou. Tento útok je poněkud obtížnější a hůře proveditelný než předchozí.

2.3.3 Port stealing

Při tomto útoku dochází k odcizení portu. Útok je založen na skutečnosti, že přepínač si při příjmu paketu aktualizuje CAM tabulku. Útočník si nejprve zjistí MAC adresu oběti a poté začne odesílat pakety, jejichž cílová adresa je nastavena na MAC adresu útočníka a zdrojová MAC adresa je nastavena na MAC adresu oběti. Jakmile takový paket dorazí na přepínač, tak ten bude předpokládat, že oběť je připojena na příchozím portu paketu a proto si aktualizuje záznam v CAM tabulce. Paket už přepínač nikam nepošle, protože cílová adresa je nastavena na stejném portu. Pokud je oběť připojena na jiném přepínači, tak je třeba cílovou adresu nastavit jako všesměrovou, aby paket k danému přepínači dorazil. Když následně na přepínač přijde paket pro oběť, tak ho přepínač pošle útočníkovi. Útočník si jej prohlédne a následně pošle oběti. Proto, aby to mohl udělat, tak musí

poupravit znova CAM tabulku. Tabulku opraví za pomoci paketu ARP request, na který oběť odpoví ARP reply a až se tento paket dostane na přepínač, tak ten si podle zdrojové MAC adresy opět opraví CAM tabulku.

2.3.4 DHCP spoofing

Útok je založen na protokolu DHCP, kde se při útoku předpokládá, že na jediné síti může být využíváno více DHCP serverů. Útok spočívá v tom, že útočník na dané síti vytvoří nový DHCP server a až se oběť připojí tak ji podstrčí své údaje. V podstrčených údajích se většinou zfalšuje adresa DNS serveru nebo brány. Pokud je zfalšována adresa brány, tak přes útočníkův prvek na dané adrese budou procházet všechna data směřující do Internetu. Data směřující z Internetu ale dorazí na nepodvrženou bránu a ta je pošle cílovému prvku. Pokud se zfalšuje adresa DNS serveru, tak lze zachytit oba směry toku dat, tedy do i z Internetu. Zde bude útočník na všechny dotazy odpovídat svou IP adresou a ze svého počítače udělá zdánlivý proxy server. To je zařízení, které funguje jako prostředník mezi zdrojovým a cílovým prvkem. Překládá klientské požadavky a vůči cílovému prvku vystupuje jako sám zdrojový klient. Přijatou odpověď poté skutečně zdrojovému klientovi posílá. Pomocí DOS útoků se snaží ochromit původní DHCP servery, aby nemohly posílat odpovědi.

2.3.5 ICMP redirect

Při tomto útoku se využívají ICMP zprávy s jejichž pomocí se optimalizuje směrování dat v dané síti. Existuje více podtypů těchto zpráv, ale nejrozšířenější je přesměrování hostitele. Pokud na bránu dorazí data určená do další sítě a brána zjistí, že přenos přes jinou bránu by byl rychlejší, tak o tom právě pomocí ICMP podá zprávu. Útok je potom založen na posílání těchto falešných ICMP zpráv. Některé systémy pomocí firewallů nebo kontroly dat takovéto zprávy filtrují, ale i tak je velká šance, že na napadnuté síti tato filtrace neprobíhá.

2.3.6 DNS spoofing

Uživatel používá k překladu doménových jmen DNS resolver, což je sada volání sloužících pro práci s DNS protokolem. Při útoku se jedná o podvržení IP adresy paketu, který se vrací jako odpověď DNS serveru na žádost o překlad doménového jména. Existuje více

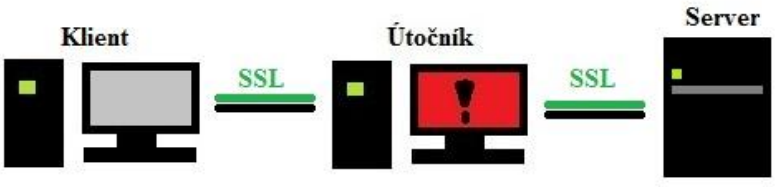
možností provedení tohoto útoku. Důsledek útoku může být až přesměrování tisíců prvků. Zde je možné útok přesměrovat i mimo lokální síť. V případě, že se jedná o útok v lokální síti, tak DNS protokol využívá protokoly TCP i UDP. Jednoduší je útok na UDP, kde není potřeba zjišťovat sekvenční čísla. Je však nutné zjistit IP adresu DNS serveru, který je využíván obětí. Je nutné také zjistit, na jakou doménu se oběť ptá. Dokonce je potřeba ještě znát port odkud dotaz na DNS přišel a ID dotazu, s jehož pomocí se přiřazuje dotaz k odpovědi. Při útocích využívajících špatnou implementaci resolveru stačí většinou znát port a ID dotazu. Někdy je potřeba zamezit rychlé odpovědi legitimního DNS serveru a k tomu se často využívají DOS útoky. [17]

2.3.7 DNS Cache Poisoning

Při tomto typu útoku je potřeba, aby útočník provozoval vlastní DNS server, přičemž se může jednat o cizí DNS server, který naboural. Tento server bude poté poskytovat útočníkovy falešné záznamy. Poté útočník zvolí další DNS server, který napadne. To provede zasláním požadavku na tento nový napadený DNS server. V požadavku je žádost o překlad, který poskytuje jen jeho vlastní DNS server. Protože napadený DNS server tento záznam nevlastní, tak si jej vyžádá od DNS serveru útočníka. Útočníkův DNS server napadnutému serveru poskytne daný překlad spolu s dalšími zfalšovanými záznamy. [18]

2.3.8 Útok na SSL a TLS

Secure Sockets Layer SSL je vrstva umístěná mezi aplikační a transportní vrstvou ISO/OSI modelu. Protokol této vrstvy se využívá k zabezpečení šifrováním a ověřováním komunikujících stran. Transport Layer Security TSL je novějším následovníkem SSL.



Obr. 6: Příklad útoku na SSL

Útok odposloucháváním se provede přesměrováním oběti nějakým jiným útokem jako je DNS spoofing nebo ARP cache poisoning ještě než započne komunikace s jiným prvkem, například serverem, jak je vidět na obrázku 6. Dojde tedy k odesílání dat k útočníkovi, kde

jeho počítač bude fungovat jako proxy server. Při šifrování bude situace vypadat tak, že oběť bude komunikovat šifrovaně s útočníkem a útočník bude komunikovat šifrovaně se serverem. Tím pádem si oběť a server budou myslet, že komunikují spolu. [17]

2.3.9 Útoky na vybrané protokoly CISCO

Firma CISCO vyrábí velké množství komponentů počítačových sítí a také vytváří programy a protokoly pro správu sítě. Velké množství těchto protokolů nevyžaduje žádné ověření uživatele, a když ano, tak je tato možnost většinou implicitně vypnuta. Někdy se obětí kybernetického útoku stanou právě tyto správní protokoly. K těmto útokům lze využít program Yersinia.

Útok na Spanning tree protokol

Spanning tree protokol STP je protokol zabraňující vzniku cyklů v sítích s redundantními spoji. Pomocí tohoto protokolu se dá snadno realizovat DOS útok, nebo se může stát nástrojem pro odposlouchávání síťové komunikace. Protokol STP používá pakety, které mají cílovou MAC adresu nastavenou na stejnou známou hodnotu. K útoku je zapotřebí připojení alespoň ke dvěma prvkům v dané síti. Při připojení jen k jednomu zařízení je zapotřebí k provedení útoku přestavění cest mezi zařízeními. Protokol vytváří Bridge Protocol Data Unit BPDU pakety, které při útoku může vytvářet i útočník. Počet těchto paketů vyslaných útočníkem je v řádu tisíců, přičemž tyto útoky mají náhodně vygenerovánu MAC adresu. Při jiném typu útoku na STP útočník předstírá, že získal roli kořenového přepínače nebo mostu. Kořenový přepínač má nastavenu nejnižší hodnotu ID. Útok předstírá nové síťové zařízení, které se chce k STP připojit a má nejnižší ID. Tím pádem se kořenovým přepínačem stane toto podvržené zařízení. Tento útok způsobuje nestabilitu sítě.

Útok na VLAN Trunking protkol

VLAN trunking protokol VTP slouží k centralizované správě virtuálních LAN sítí. Virtuální LAN se používají k vytvoření oddělených sítí na společných síťových zařízeních. Prvky sítě si za pomoci tohoto protokolu vyměňují informace o změnách. Důsledkem útoku většinou bývá přidání nebo odebrání určité VLAN.

Útok na Dynamic Trunking protokol

Dynamic Trunking protkol DTP slouží k automatickému přiřazování sdružených portů. Přes sdružený port lze posílat data z několika VLAN. Přes sdružený port jsou většinou propojeny dva síťové prvky. Při útoku se na portu, kde je připojen útočník, vyjedná spojení pomocí DTP. Tím se získá přístup k prvkům ve VLAN. [17]

2.4 Klasifikace škodlivého malware

Mnoho útočníku využívá škodlivý malware k usnadnění přístupu do napadnuté sítě, nebo jako zadní vrátka pro další přístup. Některé škodlivé kódy rozšířené v síti mohou způsobit až přerušení funkčnosti některých prvků a tím i nedostupnosti dané sítě.

2.4.1 Virus

Je analogií k biologickému viru. Jedná se o kód nebo program, který sám sebe replikuje do dalších souborů, stejně jako biologický virus, který vkládá svůj kód do živých buněk. Primárním úkolem viru je sebereplikace. Ta zatěžuje celý prvek a plýtvá jeho systémovými zdroji. To také může vést k poškození funkce daného prvku v síti. Virus může být i nositelem dalšího škodlivého kódu, který například maže soubory a muže být spuštěn až nějakou dobu po napadení prvku virem. V dnešní době viry nepředstavují tak závažnou hrozbu jako červi šířící se sítí.

2.4.2 Červ

Tento škodlivý program vytváří a šíří kopie sebe sama. Na rozdíl od viru bývá v infikovaném prvku většinou jen jednou a snaží se prostřednictvím sítě šířit co nejvíce ven. Nejčastěji je prvek infikován kvůli neopravené chybě operačního systému nebo pomocí komunikace na síti. Jako sekundární činnost nese červ obvykle nějaký další škodlivý kód. Tento kód může poškodit napadnutý prvek, nebo snížit hodnotu jeho zabezpečení, případně modifikovat a manipulovat s daty uloženými v daném napadnutém prvku.

2.4.3 Trojský kůň

Jeho nebezpečí tví především v tom, že se navenek tváří jako užitečný neškodný program, který po spuštění uživatelem může značně oslabit zabezpečení prvku. Na rozdíl od virů a

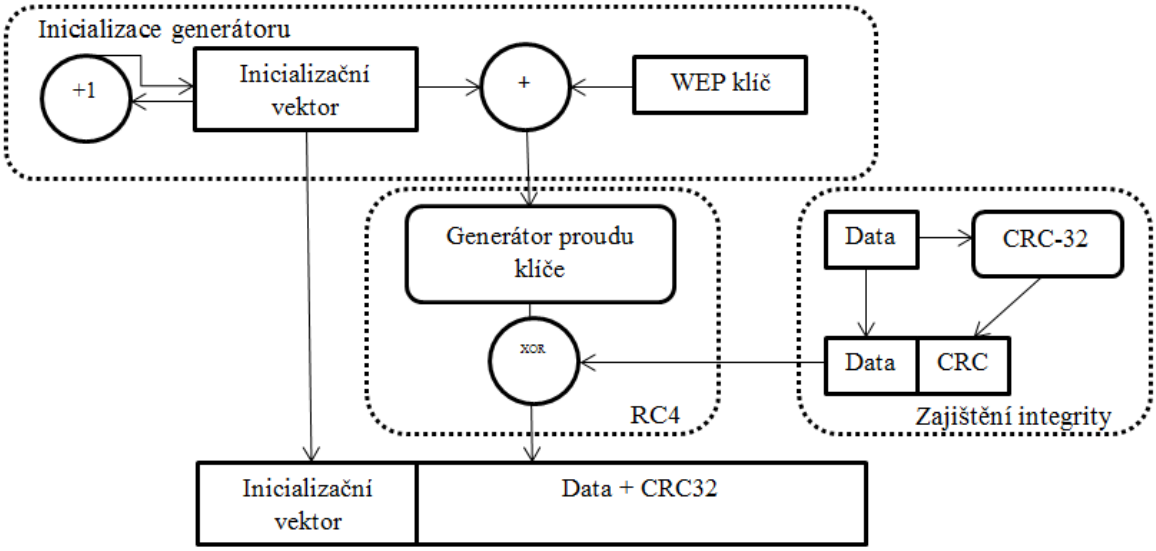
červů se nereplikuje ani nekopíruje. Škodlivý kód může mít mnoho účelů, z nichž nejčastější jsou funkce jako sniffer, což je odchytávač citlivých údajů. Dále potom keylogger, který čte zadané znaky na klávesnici. Nepříjemná je také funkce spam serveru, kdy jsou z napadnutého prvku rozesílány zprávy dalším prvků. Může fungovat dokonce jako spyware, což je program, který odesílá data o tom, jaké stránky uživatel navštěvuje a další jeho aktivity na síti. Pokud se do prvku trojský kůň dostane jinak než po síti, tak většinou obsahuje zadní vrátka, která útočníkovi umožní přístup do sítě, ve které je napadnutý prvek umístěn. Využívá i neopatrnosti uživatele, a také skrytých souborových přípon v operačních systémech Windows, kdy si uživatel myslí, že otevírá obrázek, a přitom se jedná o škodlivý soubor. Z toho lze odvodit, že je využívají i sociotechnické metody popsané dále. [19]

2.5 Útoky na protokoly bezdrátových sítí

K přenosu dat se v bezdrátových sítích se používají technologie bezdrátové komunikace, kdy se nejčastěji jedná o přenos pomocí elektromagnetických vln. Základním prvkem je zde přístupový bod, který poskytuje připojení ostatním prvkům v dané bezdrátové síti. Nevýhoda zde plyne hlavně z toho, že data se zde přenáší vzduchem, což může útočníkovi značně usnadnit práci. Proto byly vytvořeny určité protokoly, které mají za úkol tento bezdrátový přenos dat chránit. K útokům na bezdrátové sítě vzniklo mnoho programů jako Aircrack, Airsnort nebo Wireshark.

2.5.1 Útok na WEP

Wired Equivalent Privacy WEP je šifrovací protokol pracující na úrovní druhé vrstvy modelu ISO/OSI, šifruje tedy rámce. WEP využívá proudovou šifru RC4, ale k jejímu prolomení došlo již v roce 2000. WEP existuje ve více variantách lišících se délkou šifrovacího klíče. WEP, který je 64 bitový obsahuje 40 bitový klíč s připojeným 24 bitovým inicializačním vektorem IV. WEP, který je 128 bitový používá 104 bitový klíč s 24 bitovým IV. Existují i verze s delšími klíči jako 256 bitový WEP. Nevýhodou WEP je, že klíč je sdílený pomocí inicializačního vektoru. K zabezpečení obsahu Integrity Check Value ICV se používá cyklický kód určený pro detekci chyb CRC-32 .Dále jsou vypsány některé algoritmy, které se k prolomení WEP používají.



Obr. 7: Zpracování dat pomocí WEP

Útok hrubou silou

Tato metoda je prakticky použitelná pouze pro 64 bitový WEP, jelikož útočník musí vyzkoušet všechny možné kombinace klíče, případně využije slovníkový útok, při kterém útočník zkouší všechna slova daného jazyka. John Ellch vytvořil několik programů, jako jsou JC wepcrack nebo PS3 wepcrack pro distribuované lámání těchto klíčů.

Útok na Shared-key autentizaci

Shared-key autentizace má za úkol zabránit neautorizovanému přístupu do sítě. Pro získání klíče je zapotřebí znát původní i šifrovaný text, přičemž problém nastává hlavně v získání původního textu. Útočník tedy musí zachytit druhý autentizační rámec vyslaný přístupovým bodem, ve kterém je nezašifrovaná výzva. Následně zachytí třetí autentizační rámec od přístupového bodu, získá podobu zašifrovaného textu a pomocí operace XOR mezi šifrovaným a nešifrovaným textem získá klíč.

Injekce rámců

Při tomto útoku dochází k úpravě hlavičky paketu, části paketu nebo celého paketu. WEP zašifruje a pomocí ICV zabezpečuje pouze datovou část rámce. Další vlastností WEP je to, že umožňuje opakování IV, přičemž klíč je statický. To umožňuje znovu odeslat libovolný zachycený rámec. Ten ale nesmí být identifikován jako zdvojený, takže je potřeba změnit číslo sekvence. Pomocí tohoto útoku lze napadat tok dat, zvýšit celkový provoz na sítí

s cílem zachycení co nejvíce IV pro další útoky jako FMS nebo KoreK, které jsou popsány dále.

Fragmentační útok

Při tomto útoku se využívá vlastností fragmentace, s jejíž pomocí se velký rámec rozdělí na fragmenty, které se potom odesílají samostatně. Po příjmu je paket znovu složen přístupovým bodem, zašifrován novým klíčem a dále odeslán jako jediný fragment. Útok je potom založen na tom, že z přeposlaného paketu je útočník schopen dopočítat nový klíč.

FMS

V roce 2001 Fluhrer, Mantin a Shamir, odtud FMS, předvedli, že algoritmus RC4 má slabinu v tom, že pro něj existují skupiny bajtů, při kterých se s jistou pravděpodobností některý bajt z této skupiny přenese do prvního bajtu výstupního proudu. Takové IV, které odhalují bajty klíče, se nazývají slabé. Poté při zachytávání dvojic slabé IV a prvního bajtu RC4 proudu je možné prohledáváním podle statického výskytu zjistit použitý tajný klíč.

Arbaugh indukce

Útok umožňuje prodloužit známý klíč RC4 určité délky na libovolnou délku. K tomu se využívá ICV a zašifrovaného rámce bajt po bajtu. Postup se poté dá rozdělit na část získání inicializační hodnoty klíče a na indukční krok. Inicializační hodnotu klíče určité délky lze získat například za pomoci ARP zpráv. Tím lze získat klíč k danému IV.

KoreK chopchop

Tento útok umožňuje dešifrování jakýchkoliv rámců, které byly předtím pomocí WEP zašifrovány. Není zde nutné znát klíč, pomocí kterého byl rámec zašifrován. Útok vychází z Arbaughova indukčního útoku a je jeho jakousi inverzí. Útočník separuje poslední bajt datové části a odhadne jeho hodnotu. Poté když jej přístupový bod přepošle, tak zjistí, že postupoval správně a pokračuje dále.

KoreK

Je to statická metoda sloužící ke zjištění tajného klíče. Na rozdíl od FMS se nezaměřuje na slabé IV. Často dochází ke společné realizaci s FMS útokem. Při útoku záleží na stavu chování algoritmů Key Sheduling Algorithm KSA a PseudoRandom Generator Algorithm PRGA. Pro Korek není možné určit konkrétní hodnoty IV. [20]

2.5.2 Útok na Pre-Shared key (PSK) u WPA a WPA2

Kvůli nedostatečnému zabezpečení, které nabízí protokol WEP, bylo třeba vytvořit protokoly nové. Jedním z nich je WiFi Protected Access WPA, jehož úkolem bylo opravit všechny bezpečnostní slabiny, které měl WEP, ale také nutnost fungování na stávajících zařízeních. WPA je založen na protokolu Temporary Key Integrity Protocol TKIP. Využívá také dočasný klíč Pairwise Transient Key PTK a 48 bitový IV, který ale nenese informace o klíči. WPA2 je novější variantou, která nabízí širší spektrum možností zabezpečení bezdrátového přenosu. Zde ovšem je již vyžadována i hardwarová podpora. K šifrování využívá 128 bitovou šifru AES. U WPA2 se již nepoužívá IV, ale místo něj je zavedeno číslování paketů Packet Number PN. Při útoku na PSK nelze použít zachytávání IV, jelikož se klíč mění dynamicky. Jedním z možných útoků na WPA je opět použití útoku hrubou silou nebo slovníkového útoku na klíč. Při slovníkovém útoku je nejprve třeba získat čtyřcestný handshake neboli potřesení rukou, který probíhá mezi přístupovým bodem a klientem. Je možné jej získat přihlášením určitého klienta, nebo lze provést i deautentizaci připojeného klienta. Autentizační metody jsou u WPA i WPA2 téměř identické.

2.5.3 Útok na WPA-TKIP

Útok se podobá chopchop útoku u WEP. Slouží k získání klíče. Po získání klíče je možné zasílat data danému klientovi. K provedení útoku je nutné, aby šifrování mezi přístupovým bodem a klientem bylo realizováno pomocí TKIP. Dále je zapotřebí znát co nejvíce bajtů IP adresy, dlouhý časový interval mezi změnami klíče a podpora Quality of service QoS. Při samotném útoku je potřeba nejprve zachytit šifrovaný ARP request nebo response. Poté se použije modifikovaný chochop útok. Po úspěšném útoku může útočník získat další klíč během pěti minut. [21]

2.5.4 DOS útoky na bezdrátových sítích

Provedení DOS útoků u bezdrátového přenosu je dosti jednoduché a po jeho realizaci nastává okamžitý účinek. Většina těchto DOS útoků nezpůsobuje trvalé účinky na danou síť, jelikož po skončení útoku skončí také jeho účinek.

Rušení pásma

K tomuto útoku lze využít rušičky signálu na příslušných frekvencích, nebo lze využít i ovladač bezdrátové LAN karty, aby odesílala jednotlivé rámce bez časových prodlev a zahlcovala tak kanál náhodnými daty. Útoky, kde se používá rušení pásma, jsou náročné zejména na hardwarové vybavení útočníka a spotřebovanou energii. Z pohledu zabezpečení tento útok není vážnou hrozbou.

Útok na RTS/CTS

Request To Send a Clear To Send jsou řídící rámce pro požadavek na vysílání a povolení vysílat. Cílem útoku je zahltit kanál a zabránit komunikaci. Záplavy RTS rámců se využívají v sítích s mnoha skrytými uzly. CTS rámce slouží k vyhrazení kanálu na danou dobu. Posílají ho jednotlivé stanice, anebo přístupový bod jako odpověď na rámec RTS. Při útoku se nastavuje doba trvání na velké hodnoty.

Zahlcovaní paměti

Levnější přístupové body dokáží obsloužit jen poměrně malé množství stanic. Při DOS útoku se útočník snaží zaplnit tabulky, které jsou v paměti uloženy. Obsahem tabulek bývají informace o připojených stanicích. Po zaplnění tabulek již přístupový bod nemá možnost obsloužit žádnou další stanici. [22]

2.6 Útoky na úrovni aplikační vrstvy

Tyto útoky se většinou snaží napadnout servery, na kterých jsou aplikace umístěny. Útok má poté za cíl způsobit chybu systému nebo dané aplikace. Chybu, kterou útočník vyvolá, následně využije k překonání systémové ochrany. Následkem toho může získat kontrolu nad danou aplikací, celým systémem, či dokonce nad celou sítí. Po získání kontroly může číst, mazat nebo jinak modifikovat data. Může také napadnutý systém dále infikovat škodlivým kódem, nebo způsobit nedostupnost systému. Útoků na úrovní aplikační vrstvy existuje velké množství, mezi tyto útoky se řadí i některé typy DOS útoků. [16]

2.6.1 Útoky hrubou silou

Útočník se pomocí těchto útoků snaží dopátrat nejčastěji přihlašovacího hesla do určitého systému. Principem útoku je vyzkoušení všech možných kombinací znaků. Z toho plyne, že čím je heslo delší, tím déle trvá útočníkovi najít správnou kombinaci. Důležité také je, aby

se heslo sestávalo z širokého spektra znaků, jako je kombinace malých a velkých písmen, čísel a dalších symbolů. [1]

2.6.2 Buffer overflow

Jedná se o mechanismus využívaný útočníky k přetečení zásobníku nějaké aplikace. Funkce v takové aplikaci může očekávat při zadávání dat nebo navazování spojení *n* bajtů a poté dojde ke skoku, či návratu do části paměti s řídícím programem. Při útoku se využívá fakt, že není ošetřeno množství vložených bajtů. Útočník tedy odešle data, pro jejichž množství nebude kapacita zásobníku dostatečná a dojde k jeho přetečení. Poté dojde ke skoku na určitou adresu, která často obsahuje části s rizikovým řídícím kódem. Jakmile útočník pomocí přetečení zásobníku k tomuto kódu získá přístup, tak bude mít možnost spouštět své vlastní příkazy a převzít celkovou kontrolu nad daným napadnutým prvkem. [23]

2.6.3 SQL injection

Structured Query Langue SQL je standardizovaný dotazovací jazyk pro práci s daty v relačních databázích. Dotazování probíhá za pomoci SQL dotazů. Při útoku dochází k podvržení dat odesílaných na server jako dotaz, tak aby byla nějakým způsobem pozměněna odpověď serveru na tento dotaz. Pro útočníka je nejideálnější, pokud zná strukturu tabulek v dané databázi. To mu velice zjednoduší útok. Proto je velice důležité, aby ze skriptů na webových stránkách nebyla tato struktura tabulek rozpoznatelná. Z hlediska ohrožení hrozí přístup útočníka k citlivým údajům, jeho získání přístupu k administrátorskému účtu, jeho přístup ke všem účtům najednou nebo smazaní a další manipulace s daty, jenž jsou v tabulkách uloženy. [24]

2.6.4 Cross site scripting

Útok Cross site scripting, zkráceně XSS, je založen na vložení škodlivého kódu, většinou skriptu, útočníkem a tím i změně funkčnosti napadnutých webových stránek. Může tak například jednoduše nastavit, aby se při přihlašování uživatelů odesílaly jejich jména a hesla k němu. Nejčastějším typem útoku je perzistentní XSS, který je postaven na trvalém umístění škodlivého kódu na napadnutém webu. Obvyklým případem je vložení příspěvku do diskuzního fóra, kde tento příspěvek kromě běžného textu obsahuje i škodlivý kód.

Příspěvek je uložen do databáze a následně se zobrazuje všem návštěvníkům fóra spolu se spuštěním daného skriptu vloženého útočníkem. Takto podstrčený skript napsaný v javascriptovém kódu se potom v prohlížeči provádí v kontextu dané stránky. To umožní útočníkovi přístup i do uživatelova cookies, což je malé množství dat, kde se ukládají uživatelovy předvolby. WWW server je odesílá prohlížeči a při dalším připojení na server je prohlížeč zase odešle zpět danému serveru. Útočník může poté ukrást aktuální Session ID s platným přihlášením do určité aplikace. [25]

2.6.5 Cross site request forgery

Podobá se předešlému útoku, ale využívá zcela jiných zranitelností. Jedná se o útok na webovou aplikaci nebo službu. Zkratka útoku XSRF znamená podvržení požadavku mezi různými stránkami. Základem pro útočníka je znalost aplikace, na kterou útočí. K útoku často využívá metodu GET, nebo při rozšíření útoku metodu POST. Metoda GET je zranitelnější, jelikož nevyžaduje zapnutý javascript. Vykonavatelem útoku je jiný uživatel, zpravidla ten, kdo má administrátorský přístup k napadnuté aplikaci. Následek útoku může být například vytvoření trvalého platebního příkazu na útočníkův bankovní účet z účtu oběti, nebo sledování emailů oběti. Velké nebezpečí zde hrozí i pro redakční systémy, což jsou systémy pro správu obsahu, u kterých hrozí smazání veškerých dat útokem. Automatický útok je možný v tom případě, že oběť navštíví útočníkovy stránky, ze kterých se odešle předem připravený formulář. [26]

2.6.6 Cross-site tracing

Při tomto útoku se zkratkou XST dochází nejčastěji ke kombinaci XSS a metody TRACE z HTTP, která se používá k zjištění příjemce daného požadavku na aplikační vrstvě. TRACE také umožňuje klientovi zjistit, co je přijato na druhé straně spojení a použít data pro diagnostiku a testování. Oproti XSS, tak umožňuje útočníkovi získat nejen cookies oběti, ale i její přihlašovací údaje. [27]

2.6.7 HTTP response splitting

Tento útok využívá zranitelnosti webové aplikace při nesprávné kontrole uživatelských vstupů. Toho využije útočník tím, že předá dané aplikace podvržené vstupy, které rozdělí odpovědi serveru na více částí, které pak útočník může využít k vykonání dalších útoků

jako XSS popsaný výše. Na technice HTTP response splitting je založen i útok Cache poisoning, kde je cílem útočníka donutit webový prohlížeč, aby uložil danou stránku do své cache. [28]

2.6.8 HTTP Request Smuggling

Při tomto útoku se využívá rozdílného zpracování dat různými prvky sítě, jako jsou proxy servery nebo webový aplikační firewall, které se nachází v toku dat mez klientem a serverem. Smuggling znamená pašování což je zde velmi výstižné, protože se útočník pokouší propašovat žádost do jednoho systému, aniž by si toho byly ostatní systémy vědomy. Tento útok se často kombinuje s dalšími jako XSS. Pro úspěšnost útoku jsou důležité určité vstupní podmínky, jako je přítomnost určitého proxy systému nebo zranitelnost XSS ve webovém serveru. Tento útok je v prostatě vytvoření HTTP žádosti, která zapouzdřuje další HTTP žádost ve stejném záhlaví. [29]

2.6.9 Session hijacking

Server, na který se přihlásí určitý klient, tomuto klientovi odešle jedinečný identifikátor řetězce náhodných znaků. Toto odeslání provede buďto prostřednictvím Uniform Resource Locator URL za pomoci metody GET, nebo pomocí cookies. Název tohoto identifikátoru je Session ID SID. Server si tento identifikátor přiřadí k danému uživateli a poté každého kdo mu tento identifikátor pošle, považuje za daného uživatele a umožní mu přístup již bez zadávání přihlašovacích údajů. Po odhlášení uživatele dochází ke smazání SID na serveru.

Útok spočívá v získání SID od již přihlášeného uživatele, což útočníkovi umožní přístup bez zadávání přihlašovacích údajů. K útokům se využívá více metod, z nichž nejznámější jsou:

- fixace Session, při které útočník oběti odešle odkaz obsahující konkrétní SID a čeká na přihlášení oběti,
- Session Sidejacking, při kterém útočník pomocí snifferu odchytává komunikaci a snaží se ukrást Session cookie,
- útok s fyzickým přístupem, který umožní útočníkovi získat příslušný soubor v paměti na příslušné části počítače nebo serveru,

- XSS, při kterém útočník na uživatelově počítači spustí kód, jenž je považován za důvěryhodný a útočníkovi je poté umožněno získat kopii cookie nebo provádět i jiné operace. [30], [31]

2.6.10 JavaScript Hijacking

Zde se útočník zaměřuje na aplikace, které využívají JavaScript Object Notation JSON. Jestliže aplikace nabízí v tomto formátu data pro uživatele, může být na ně zaměřen útok. K útoku dojde, pokud přihlášená oběť navštíví útočníkovy stránky se škodlivým kódem, kdy nastane zkopírování JSON dat a dojde k jejich následnému přesunu na server útočníka.

2.6.11 Clickjacking

Jedná se o techniku, při které je na webové stránce obsah a tlačítko, které zdánlivě s tímto obsahem souvisí, ale ve skutečnosti se jedná o tlačítko jiné aplikace. To vede ke skutečnosti, že uživatel očekává po kliknutí na tlačítko určitou operaci, jako je například smazání textového pole. Místo toho se však provede nevědomé spuštění útočníkovy aplikace, které může mít za následek smazání obsahu z redakčního systému, nákup zboží v nějakém e-shopu a další problémy. [32]

2.6.12 Útok na SSH

Secure Shell SSH je zabezpečovací komunikační protokol v síťových systémech, využívajících TCP/IP. Protokol umožňuje transparentní šifrování přenášených dat, zachování jejich integrity a možnost bezztrátové komprese. K ověřování se využívá veřejný klíč, kde si každý prvně připojený klient vytvoří otisk daného klíče. Při dalším připojení jej vytvoří znovu a porovná s minulým. Existují dvě verze SSH, přičemž se pro každou verzi používá jiný klíč. Útočník se snaží přimět oběť komunikovat prostřednictví verze, kterou nepoužívá. K útokům na SSH se většinou využívají programy jako Ssharp nebo Cain & Abel. Při útoku se hledají podobné otisky klíčů. [17]

2.7 Útoky využívající sociotechnických metod

Základem těchto metod je využívání selhání lidského faktoru. Nejprve útočník zkoumá volné a dostupné informace, nejčastěji webových stránek firmy, facebooku a podobně. Poté začne vytvářet vztahy s vytypovanými osobami, snaží se získat jejich důvěru. Tu potom

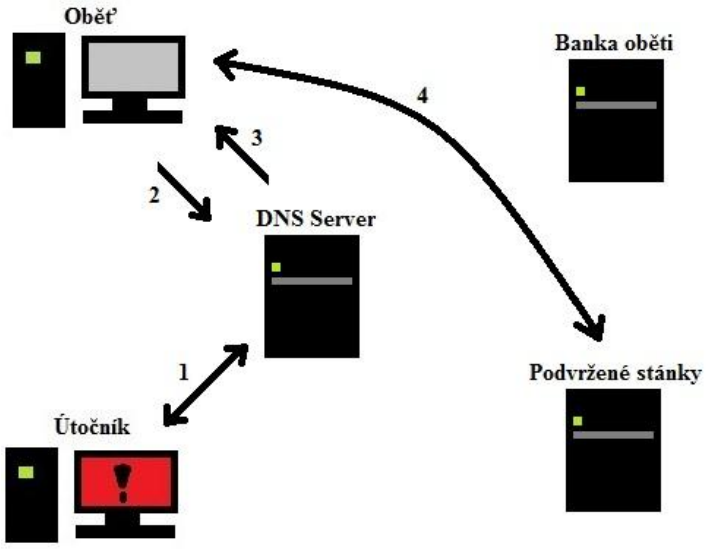
zneužije k získání daných informací. Sociotechnické útoky se odehrávají ve fyzické, ale i v psychologické úrovni. Existuje více metod provádění těchto útoku, ale všechny mají jeden společný cíl a tím je přelstění oběti. [1]

2.7.1 Phishing

Phishing neboli rybaření je typ kybernetického útoku, který má za cíl vylákání citlivých údajů uživatele prostřednictví elektronické komunikace. Mezi tyto citlivé údaje patří přístupová hesla, čísla kreditních karet nebo například osobní údaje a dokumenty oběti. Po praktické stránce se jedná o emailovou zprávu, která dorazí k oběti a obsahuje odkaz na podvodnou stránku, která je vzhledově co nejvíce podobná stránce oficiální. Jakmile oběť prostřednictvím odkazu v emailu na tuto podvodnou stránku vstoupí, tak je vyzvána k zadání osobních údajů. Jelikož je tato stránka podvrhem útočníka, tak se tyto zadané osobní údaje dostanou přímo do jeho rukou a on je může dále zneužít bez vědomí oběti. Při boji s phisingem je důležitá zejména uživatelská osvěta. Uživatel by neměl zadávat osobní údaje na stránky, které se mu jeví podezřelé. Existují i specializované softwarové a antivirové programy, které taktéž dokáží phishing odhalit. Jelikož se jedná o problém celosvětového měřítka, tak vzniklo i mnoho organizací na boj s phishingem a mnoho států se touto problematikou zabývá i v legislativě. [33]

2.7.2 Pharming

Česky tento termín znamená farmaření a jedná se o jakousi vylepšenou novější verzi útoku Phishnig. Při útoku se využívá překladu doménového jména serveru na IP adresu, tedy službu, kterou poskytují DNS servery. Principiální schéma útoku je uvedeno na obrázku 8, kde jsou i očíslovány jednotlivé kroky útoku. Nejprve se útočník zaměří na službu DNS užívanou obětí, kde změní IP adresu přiřazenou k doménovému jménu bankovního serveru oběti, za IP adresu serveru podvrženého. Poté se oběť dotáže DNS serveru jaká je IP adresa doménového jména mé banky? DNS server oběti odpoví předáním IP adresy, která je ale podvržená útočníkem a oběť tak přesměruje na podvržené stránky útočníka, které ovšem vypadají jako původní stránky banky, takže oběť nic nepozná. Problém zde je že podvržené stránky vypadají velice věrohodně a tak ani zkušení uživatelé nemusí poznat rozdíl.



Obr. 8: Schéma Pharming útoku

2.7.3 Vishnig

Při tomto útoku se zneužívá technologie Voice over IP, která umožnuje přenos digitalizovaného hlasu pomocí paketů protokolů IP, TCP nebo UDP. Vishingové útoky jsou úspěšné právě kvůli důvěře uživatelů, ale ti si neuvědomují, že na druhé straně nemusí být člověk u sluchátka, nýbrž počítač. Po praktické stránce útok vypadá zhruba tak, že útočník nejprve vybere telefonní čísla v dané oblasti a nakonfiguruje na ně vytáčení. Pokud oběť hovor příjme tak automatický záznamník ji upozorní, že byla s jejím účtem provedena podezřelá aktivita a že je nutné, aby zavolala bezprostředně na číslo, které je jí při té příležitosti nadiktováno. Pokud oběť na toto číslo skutečně zavolá, tak je vyzvána k zadání buďto čísla kreditní karty, pinu, čísla bankovního účtu nebo jiných osobních údajů, které potom útočník zneužije. [34]

3 TEORIE SVAZŮ

3.1 Relace uspořádání

Je to binární relace na určité množině, kde pro $\forall(x, y, z) \in G$ platí zákony zákony:

- reflexivity $a \leq a$,
- antisymetrie $x \leq y, y \leq x \Rightarrow x = y$,
- transitivity $x \leq y, y \leq z \Rightarrow x \leq z$.

Relace $R \subseteq M \times M$ je částečné uspořádání právě když R je reflexivní, antisymetrické a transitivní.

3.2 Uspořádané množiny

Definice 3.2.1 Uspořádaná množina je dvojice $(M, \leq)$, kde M je množina a $\leq$ je relace uspořádání. Říkáme, že uspořádání R na M je lineární, pokud jsou každé dva prvky množiny M srovnatelné v R.

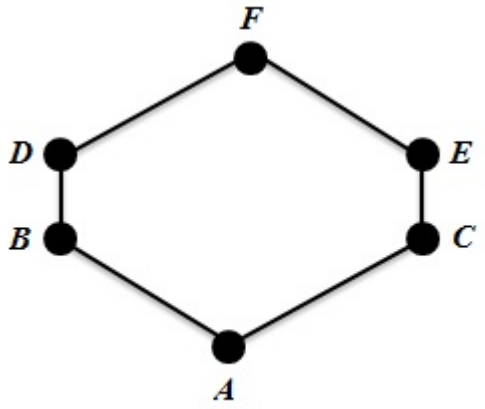
Příklad 3.2.1 Nechť $(\mathrm{N}, \leq)$, kde N je množina všech přirozených čísel a je uspořádanou množinou. Relace $\leq$ zde má obvyklý význam. Dalším příkladem může být množina všech přirozených čísel s relací dělitelnosti, toto uspořádání ovšem není lineární.

Definujeme $(M, \leq)$ jako uspořádanou množinu. Poté prvek $x \in M$ je minimální právě když pro $\forall y \in M$ platí tvrzení, jestliže $y \leq x$, pak $x \leq y$. Tedy x je minimální právě tehdy, když neexistuje prvek ostře menší než x. Analogicky x je maximální, když pro $\forall y$ platí, jestliže $x \leq y$, pak $y \leq x$. Tedy x je maximální právě když neexistuje žádný ostře větší prvek. O x můžeme říci, že je nejmenší právě když pro $\forall y$ platí $x \leq y$. Opačně potom x je největší právě když pro $\forall y$ platí $y \leq x$.

Dále řekneme, že $x \in M$ pokrývá $y \in M$ právě když $x \neq y$, $y \leq x$ a neexistuje žádné $z \in M$, pro které by platilo $x \neq z, y \neq z$ a $y \leq z \leq x$. Potom také $x \in M$ je dolní závora neboli mez množiny $A \subseteq M$ právě když platí $x \leq y$ pro $\forall y \in A$. A naopak $x \in M$ je horní závora množiny $A \subseteq M$ právě když platí $y \leq x$ pro $\forall y \in A$. [35]

3.3 Hasseův diagram

Tento graf se často využívá k vykreslení uspořádaných množin. Název získal podle jména německého matematika Helmuta Hassea. Vrcholy tohoto grafu představují prvky množin. Hrana mezi prvky A a B vyjadřuje, že $A < B$ a zároveň, že neexistuje C, pro které by platilo $A < C < B$. Proto mezi prvky A a E není hrana i když $A < E$ a to z toho důvodu, že mezi A a E se nachází prvek B. [36]



Obr. 9: Hasseův diagram

Teorie svazů je součástí matematické algebry, kde se z uspořádaných množin zaobírá těmi, které zachovávají supremum $\sup(x, y)$ a infimum $\inf(x, y)$. Svaz je množina prvků, kde ke každým dvěma z nich existuje supremum a infimum. Supremum je jakési zobecnění největšího prvku množiny. Pokud má množina největší prvek, tak má i supremum, kterým je onen největší prvek. Toto tvrzení však naopak platit nemusí, čehož je důkazem například shora omezený otevřený interval na množině reálných čísel. Pokud supremum v množině skutečně existuje tak je vždy jedno. Je tedy určeno jednoznačně. Jinak řečeno, $x \in M$ je supremum množiny $A \subseteq M$, právě když x je nejmenší horní závora množiny A. Opakem suprema je infimum, tedy zobecnění nejmenšího prvku.

3.4 Polosvazy

Definice 3.4.1 Prvek x grupoidu $(G,\cdot)$ se nazývá idempotentní, pokud $x \cdot x = x$. Polosvaz je komutativní idempotentní pologrupa, což je grupoid $(G,\cdot)$, pro jehož každé tři prvky $\forall(x, y, z) \in G$ platí:

- zákon asociativity $x \cdot (y \cdot z) = (x \cdot y) \cdot z$,
- zákon komutativity $x \cdot y = y \cdot x$,
- zákon idempotence $x \cdot x = x$.

Podle předchozí definice je i prázdný grupoid zachovávající zákony asociativity a komutativity polosvazem.

Věta 3.4.1. Nechť $(G,\cdot)$ je komutativní pologrupa. Pak množina všech idempotentních prvků tvoří podgrupoid pologrupy $(G,\cdot)$, který je polosvazem.

Věta 3.4.2. Nechť $(G,\leq)$ je uspořádaná množina, ve které k libovolným dvěma prvkům $x, y \in G$ existuje supremum $x \vee y$. Pak $(G,\vee)$ je polosvaz. Navíc pro $\forall (x, y) \in G$ platí $x \leq y \Leftrightarrow x \vee y = y$.

Věta 3.4.3. Nechť $(G,\leq)$ je polosvaz. Potom relace $\leq$, daná vztahem $x \leq y \Leftrightarrow x \vee y = y$ pro $\forall (x, y) \in G$, je uspořádání na G, ve kterém pro $\forall (x, y) \in G$ je $x \cdot y$ supremum množiny $\{x, y\}$ v $(G,\leq)$.

Z těchto vět plyne fakt, že polosvazy jsou identické s uspořádanými množinami, kde ke každým dvěma prvkům existuje supremum.

Princip duality. Nechť $(G,\leq_1)$ je uspořádaná množina. Pokud definujeme novou relaci $\leq_2$ na G pro $x, y \in G$ jako $x \leq_2 y \Leftrightarrow x \leq_1 y$, pak je $(G,\leq_2)$ také uspořádaná množina, kde supremum v $(G,\leq_1)$ je infimem v $(G,\leq_2)$. Toto platí i obráceně. [37]

Příklad 3.4.1. Při zavedení relace $x|y$ na množině přirozených čísel N, kde x dělí y je $|$ uspořádáním na N a $\forall (x, y) \in \mathrm{N}$ je:

- supremum $\sup(x, y)$ = nejmenší společný násobek x a y, označujeme $NSN(x, y)$,
- infimum $\inf(x, y)$ = největší společný dělitel x a y, označujeme $NSD(x, y)$.

Potom (N, NSD) a (N, NSD) jsou polosvazy. [38]

3.5 Svazy

Definice 3.5.1. Svaz je uspořádaná množina $(L,\leq)$, kde ke každým dvě prvků $x, y \in L$ existuje supremum $\sup(x, y)$ a infimum $\inf(x, y)$. Je to také uspořádaná množina se dvěma binárními operacemi zachovávajícími zákony:

- asociativity $(x \wedge y) \vee z = x \wedge (y \vee z), x \vee y = y \vee x, x \vee y \wedge z = x \vee (y \wedge z)$,
- komutativity $x \wedge y = y \wedge x, x \vee y = y \vee x$,
- idempotence $x \wedge x = x, x \vee x = x$,
- absorbce $x \vee (y \wedge x) = x, x \wedge (y \vee x) = x$.

Věta 3.5.1. Nechť $(L,\leq)$ je svaz. Pro libovolné prvky $x, y \in L$ označíme jejich supremum jako $x \wedge y$ a jejich infimum $x \vee y$. Poté jsou $(L,\wedge)$ a $(L,\vee)$ polosvazy a obě operace jsou spolu svázány absorpčními zákony, tedy pro $\forall(x, y) \in L$ platí:

- $x \vee (y \wedge x) = \sup(x, \inf(x, y)) = x$,
- $x \vee (y \wedge x) = \inf(x, \sup(x, y)) = x$.

Dále pro $x, y \in L$ platí:

- $x \wedge y = x \Leftrightarrow x \leq y \Leftrightarrow x \vee y = y$.

Věta 3.5.2 Nechť $(L,\wedge,\vee)$ je množina se dvěma idempotentními, asociativními a komutativními operacemi, které jsou spolu svázány absorpčními zákony. Jestliže toto platí, tak:

- Pro $\forall(x, y) \in L$ také platí $x \wedge y = x \Leftrightarrow x \vee y = y$,
- pokud definujeme na L relaci $\leq$ tak, že pro libovolné dva prvky $x, y \in L$ klademe $x \leq y \Leftrightarrow x \vee y = y$, pak $\leq$ je uspořádání na L takové, že $(L,\leq)$ je svaz, ve kterém pro libovolné prvky $x, y \in L$ je prvek $x \vee y$ jejich supremum a prvek $x \wedge y$ je jejich infimum.

Z výše uvedených vět je patrné, že svazy jsou totéž co algebraické struktury $(L,\wedge,\vee)$ se dvěma idempotetními, asociativními a komutativnímu operacemi, svázanými navzájem absorpčními zákony. Proto se i tyto struktury $(L,\wedge,\vee)$ nazývají svazy.

Princip duality. Je-li $(L,\vee,\wedge)$ svaz, pak i $(L,\wedge,\vee)$ je svaz. Obecně platí, že pokud v nějakém platném tvrzení o svazech dojde k systematické záměně:

- supremum $\leftrightarrow$ infimum,
- $\wedge \leftrightarrow \vee$,
- $\leq \leftrightarrow \geq$,

tak dostaneme opět platné tvrzení o svazech. Jelikož není zapotřebí zdůrazňovat, jestli máme na mysli svaz jako uspořádanou množinu nebo algebraickou strukturu se dvěma operacemi, tak v následujícím textu, nebude-li to z nějakého důvodu vhodné či nepostradatelné, nebudou uspořádání či operace vyznačeny.

Věta 3.5.3. V libovolném svazu L pro každou trojici prvků $x, y, z \in L$ platí tzv. distributivní nerovnosti:

- $(x \vee y) \wedge (x \vee z) \geq x \vee (y \wedge z)$,
- $(x \wedge y) \vee (x \wedge z) \leq x \wedge (y \vee z)$.

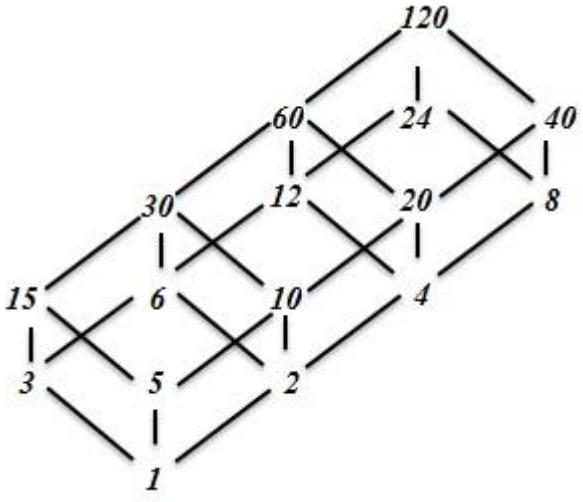
Je-li navíc $z \leq x$, tak platí tzv. modulární nerovnost:

- $(x \wedge y) \vee z \leq x \wedge (y \vee z)$.

Věta 3.5.4. Nechť L je svaz a $n \in \mathrm{N}$. Poté pro libovolné prvky $x_1,...,x_n \in \mathrm{N}$ platí, že $x_1 \vee ... \vee x_n$ je supremum množiny $\{x_1,...,x_n\}$ a $x_1 \wedge ... \wedge x_n$ je infimum množiny $\{x_1,...,x_n\}$.

Příklady 3.5.1.

- Nechť N je množina přirozených čísel, $x \vee y$ je $NSN(x,y)$ a $x \wedge y$ je $NSD(x,y)$, potom $(\mathrm{N},\vee,\wedge)$ je svaz,
- nechť n je přirozené číslo, $P(n)$ je množina všech dělitelů čísla n. Potom $(P(n), NSN, NSD)$ je svaz. Množina $X = \{1,2,3,4,5,6,8,10,12,15,20,24,30,40,60,120\}$ všech dělitelů čísla 120 je svaz a může být zobrazena Hasseovým diagramem jako je na obrázku 10. [37],[39]



Obr. 10: Svaz dělitelů čísla 120

3.5.1 Podsvazy

Definice 3.5.2. Nechť $(L,\vee,\wedge)$ je svaz a M je podmnožina jeho nosné množiny L. Řekneme, že M je podsvaz svazu $(L,\vee,\wedge)$, jestliže je M podgrupoidem grupoidu $(L,\wedge)$ a současně podgrupoidem grupoidu $(L,\vee)$. $M \subseteq L$ je tedy podsvazem svazu L, právě když pro $\forall (x,y) \in M$ platí $x \vee y \in M$ a $x \wedge y \in M$.

Věta 3.5.5. Nechť $(L,\vee,\wedge)$ je svaz. Potom platí:

- pro každý prvek $x \in L$ je $\{x\}$ podsvaz svazu $(L,\vee,\wedge)$,
- každý interval svazu $(L,\vee,\wedge)$ je jeho podsvaz,
- má-li L prvky 0 a 1, potom $L = [0,1]$.

Příklady 3.5.2.

- Každá jednoprvková podmnožina svazu je jeho podsvazem,
- prázdná množina je podsvazem jakéhokoliv svazu,
- každý svaz je zároveň svým podsvazem. [37],[38]

3.5.2 Ideály a filtry

Definice 3.5.3. Nechť L je svaz, $M \subseteq L$ je jeho podmnožina. Platí, že M je ideál svazu L, pokud M je podsvazem svazu L a navíc splňuje podmínku, že pro $\forall m \in M$ a $\forall x \in L$ platí:

- $x \leq m \Rightarrow x \in M$.

Duálně je možné tvrdit, že M je filtr svazu L, pokud M je podsvazem svazu L a navíc splňuje podmínku, že pro $\forall m \in M$ a $\forall x \in L$ platí:

- $x \geq m \Rightarrow x \in M$.

Ideál svazu je tedy podsvazem, který s každým svým prvkem m obsahuje i všechny prvky svazu, které jsou menší než m. Filtr svazu je podsvaz, jenž s každým svým prvkem m obsahuje i všechny prvky svazu, které jsou větší než m.

Věta 3.5.6. Průnik libovolného neprázdného systému podsvazů (respektive ideálů, filtrů) daného svazu je opět podsvaz (respektive ideál, filtr) tohoto svazu.

Nechť L je svaz, $M \subseteq L$ je jeho podmnožina. Jak vyplývá z předchozí věty, tak můžeme definovat ideál $M\downarrow$ svazu L generovaný množinou M jako průnik všech ideálů tohoto svazu, které obsahují množinu M. Duálně potom filtr $M\uparrow$ svazu L generovaný množinou M jako průnik všech filtrů tohoto svazu, které obsahují množinu M.

Pokud $M = \{m\}$, tak píšeme stručněji $m\downarrow$ namísto $\{m\}\downarrow$, nebo $m\uparrow$ namísto $\{m\}\uparrow$. Potom mluvíme o hlavním ideálu, či hlavním filtru, který je generován prvkem m. Ideál M ve svazu L se tedy nazývá hlavní, právě když existuje prvek $m \in L$, pro který platí $M = (\leftarrow, m\rangle$. Pokud $0 \in L$, pak ideál $\{0\}$ se nazývá nulový. Duálně potom filtr M ve svazu L se nazývá hlavní, právě když existuje prvek $m \in L$, pro který platí $M = \langle m, \rightarrow)$. Pokud $1 \in L$, pak filtr $\{1\}$ se nazývá jednotkový. Z toho také plyne, že podmnožina $M \subseteq L$ je ideálem svazu L, právě když $M\downarrow = M$ a je filtrem svazu L, právě když $M\uparrow = M$.

Věta 3.5.7. Nechť L je svaz, $M \subseteq L$ je jeho podmnožina. Pro ideál $M\downarrow$ generovaný množinou M platí:

- $M\downarrow = \{x \in G; \exists n \in \mathrm{N} \exists m_1, ..., m_n \in M : x \leq m_1 \vee ... \vee m_n\}$.

Duálně pro filtr $M\uparrow$ generovaný množinou M platí:

- $M\uparrow = \{x \in G; \exists n \in \mathrm{N} \exists m_1,...,m_n \in M : x \leq m_1 \wedge ... \wedge m_n\}$.

Příklady 3.5.3.

- Každý svaz je svým ideálem i filtrem,
- prázdná množina je ideálem i filtrem jakéhokoliv svazu. [37]

3.5.3 Homomorfismus

Definice 3.5.4. Nechť $(L,\leq_L)$, $(H,\leq_H)$ jsou uspořádané množiny a $f : L \to H$ zobrazení množiny L do množiny H. Řekneme, že je f izotonní zobrazení, jestliže pro $\forall (x, y) \in L$ platí implikace:

- $x \leq_L y \Rightarrow f(x) \leq_H f(y)$.

Řekneme, že f je izomorfismus uspořádaných množin, je-li f bijekce a obě zobrazení f i f^{-1} jsou izotonní.

Nechť L a H jsou svazy, $f : L \to H$ je zobrazení. Potom je f svazový homomorfismus, jestliže pro $\forall (x, y) \in L$ platí:

- $f(x \wedge y) = f(a) \wedge f(b)$,
- $f(x \vee y) = f(a) \vee f(b)$.

Řekneme, že f je svazový izomorfismus, jestliže je f bijektivní homomorfismus. Protože každý svaz je také uspořádaná množina, má smysl se ptát, zda svazový homomorfismus je též izotonní zobrazení.

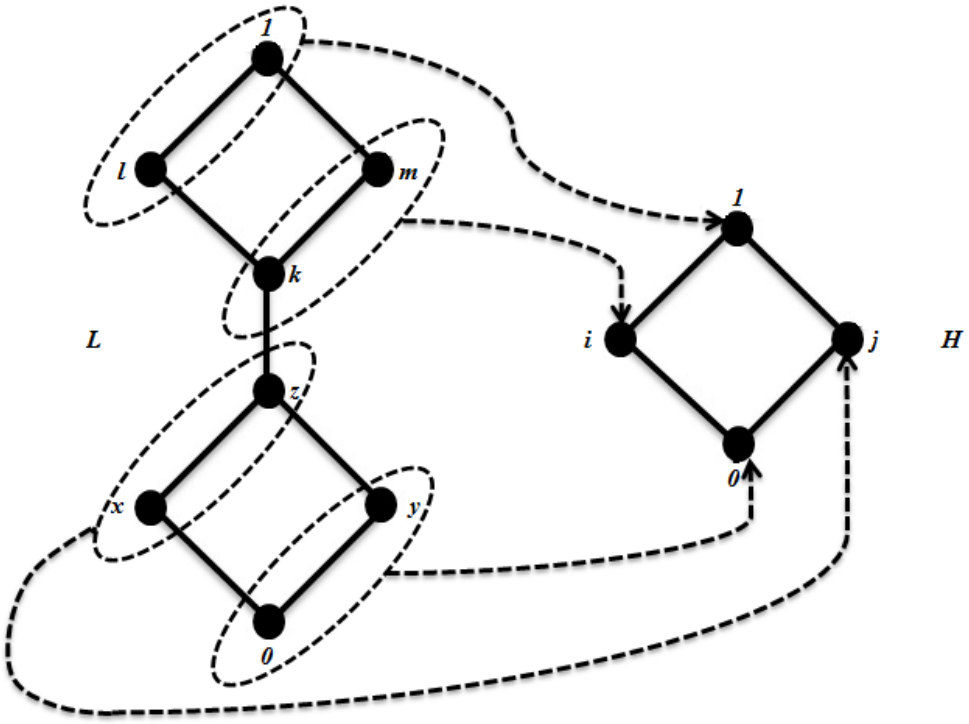
Věta 3.5.8. Nechť L a H jsou svazy, $f : L \to H$ je zobrazení. Je-li f svazový homomorfismus, pak f je izotonní zobrazení a homomorfní obraz $f(G) = f\{f(x); x \in L\}$ je podsvazem svazu H. Zobrazení f je izomorfismus uspořádaných množin. [11],[12]

Příklad 3.5.4. Nechť L a H jsou svazy, $f : L \to H$ je zobrazení definováno jako:

- $f(0) = f(y) = 0$,
- $f(x) = f(z) = j$,

- $f(k) = f(m) = i,$
- $f(l) = f(1) = 1.$

Potom zobrazení f je svazovým homomorfismem L na H. [13]



Obr. 11: Svazový homomorfismus L na H

3.6 Úplné svazy

Definice 3.6.1. Uspořádaná množina, ve které pro každou podmnožinu existuje supremum a infimum se nazývá uplný svaz. Nechť L je svaz a A je podmnožina svazu L. Tedy $A \subseteq L$. Potom infimum podmnožiny A ve svazu L je největší dolní závora podmnožiny A ve svazu L. Tato dolní závora je prvek $x \in L$ takový, že pro $\forall a \in A$ platí $x \leq a$. Pokud A je prázdná množina, tak je tato podmínka splněna pro všechna $x \in L$, odtud tedy plyne, že každý prvek svazu L je v L dolní závorou prázdné množiny. Z toho důvodu je infimem prázdné množiny ve svazu L největší prvek svazu L. Duálně potom supremem prázdné množiny ve svazu L je nejmenší prvek svazu L.

Věta 3.6.1. Nechť $(L, \leq)$ je uspořádaná množina. Potom jsou následující podmínky vůči sobě ekvivalentní:

- $(L,\leq)$ je úplný svaz,
- $(L,\leq)$ má nejmenší prvek a každá neprázdná podmnožina množiny L má v uspořádané množině $(L,\leq)$ supremum,
- $(L,\leq)$ má největší prvek a každá neprázdná podmnožina množiny L má v uspořádané množině $(L,\leq)$ infimum.

Věta 3.6.2. Nechť L je svaz. Pak existuje uplný svaz U, obsahující podsvaz H, který je izomorfní se svazem L.

Příklady 3.6.1.

- Prázdný svaz není úplný, jelikož pro jeho jedinou prázdnou podmnožinu neexistuje supremum ani infimum. Jinak řečeno prázdný svaz nemá nejmenší ani největší prvek, protože nemá žádný prvek,
- pro libovolnou množinu X je $(2^X,\subseteq)$ úplný svaz,
- pro libovolnou nekonečnou množinu X tvoří množina všech konečných podmnožin množiny X spolu s inkluzí $\subseteq$ svaz, který není úplným svazem. [37]

3.7 Součin svazů

Definice 3.7.1. Nechť $(L,\vee,\wedge)$ a $(H,\vee,\wedge)$ jsou svazy. Na kartézském součinu $L\times H$ jsou definovány nové operace $\vee$ a $\wedge$ tak, že pro $\forall(x_1,x_2)\in L$ a $\forall(y_1,y_2)\in H$ klademe:

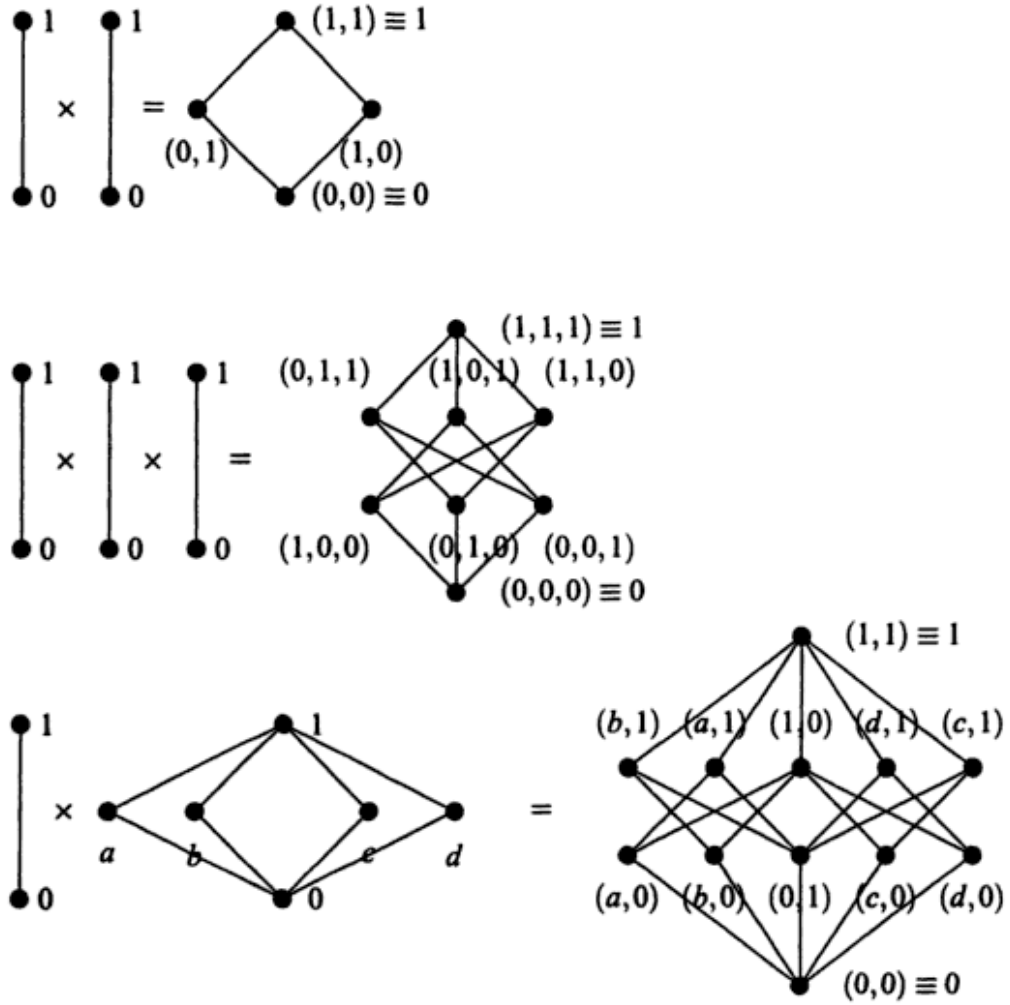
- $(x_1,y_1)\vee(x_2,y_2)=(x_1\vee x_2,y_1\vee y_2)$,
- $(x_1,y_1)\wedge(x_2,y_2)=(x_1\wedge x_2,y_1\wedge y_2)$.

Věta 3.7.1. Při splnění předpokladů, popsaných v předchozí definici tvoří součin $(L\times H,\vee,\wedge)$ svaz.

V součinu svazů platí všechny rovnosti platné v obou svazech. Vlastnosti, které není možné vyjádřit jako konjunkci rovností, už ale součin svazů zdědit nemusí. Což lze demonstrovat na následujícím příkladu. Pro každé dva prvky x,y platí $x\leq y$ nebo $x\geq y$. To je možné zapsat za pomoci svazových operací jako podmínky $x\wedge y=x$ nebo $x\wedge y=y$. Nejedná se ovšem o konjunkci rovností, nýbrž o disjunkci.

Obdobně jako součin dvou svazů je možné definovat součin n svazů kde $n \in \mathrm{N}$. Potom na kartézském součinu nosných množin těchto n svazů se nové operace $\wedge$ a $\vee$ definují po jednotlivých složkách. [37]

Příklad 3.7.1. Na obrázku 12 jsou ilustrovány příklady kartézských součinů svazů od jednodušších až ke složitějším.



Obr. 12: Příklady kartézských součinů svazů [40]

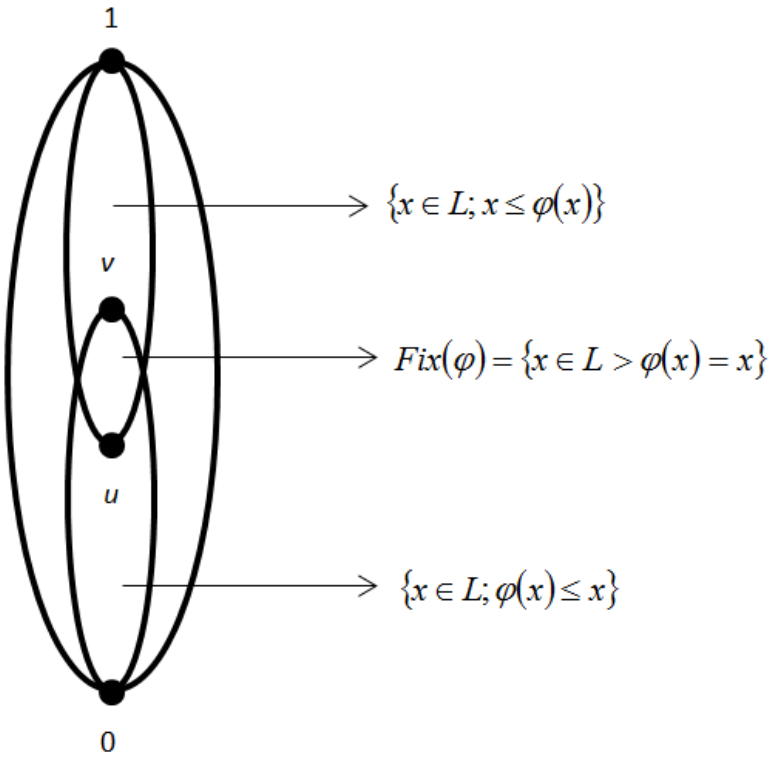
4 VLASTNOSTI UZÁVĚROVÝCH OPERÁTORŮ A VĚTA O PEVNÉM BODĚ

Tarského věta o pevném bodě našla široké uplatnění při definicích sémantik programovacích jazyků, ale i v dalších odvětvích výpočetní techniky.

Věta 4.1. Nechť L je úplný svaz a $\varphi : L \to L$ je izotonní zobrazení. Pak existuje prvek $x \in L$ tak, že $\varphi(x) = x$, což znamená, že x je pevný bod zobrazení φ.

Dále existuje největší pevný bod v zobrazení φ, pro který platí $v = \sup\{x \in L : x \leq \varphi(x)\}$ a nejmenší pevný bod u zobrazení φ, pro který platí $u = \inf\{x \in L : \varphi(x) \leq x\}$.

Také platí, že množina pevných bodů každého izotonního zobrazení daného úplného svazu do sebe tvoří také úplný svaz. Podle Tarského věty o pevném bodě platí i ta skutečnost, že existenci pevného bodu každého izotonního zobrazení lze použít pro charakterizaci úplnosti svazů. Jestliže každé izotonní zobrazení daného svazu do sebe má pevný bod, pak je daný svaz úplný. Potom platí tato charakterizace úplnosti pro svazy, podle které je svaz L úplný právě tehdy, když každé izotonní zobrazení svazu L do sebe má alespoň jeden pevný bod. [38]



Obr. 13: Největší a nejmenší pevný bod v úplném svazu

Na teorii uzávěrových operátorů stojí mnoho oblastí matematiky, z nichž zajímavá je například definice konceptů ve formální konceptuální analýze popsané dále.

Definice 4.1. Zobrazení $\varphi : L \to L$ uspořádané množiny L do sebe se nazývá uzávěrový operátor, jestliže pro $\forall (x, y) \in L$ platí:

- $x \le \varphi(x)$,
- $x \le y$ implikuje $\varphi(x) \le \varphi(y)$,
- $\varphi(x) = \varphi(\varphi(x))$.

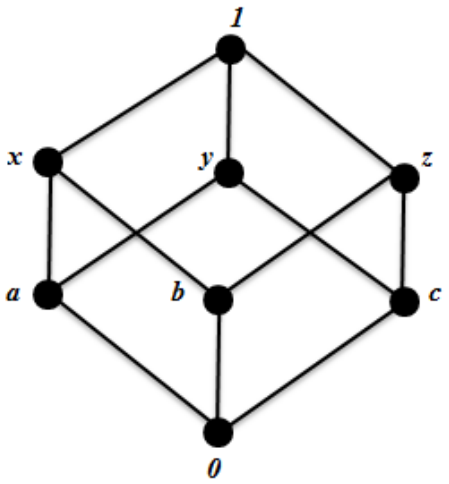
Věta 4.2. Libovolné zobrazení φ uspořádané množiny L do sebe je uzávěrový operátor právě tehdy, když pro všechna $x, y \in L$ platí ekvivalence:

- $x \le \varphi(y) \Leftrightarrow \varphi(x) \le \varphi(y)$.

Věta 4.3. Je-li φ uzávěrový operátor na úplném svazu L, pak množina všech pevných bodů $Fix(\varphi) = \{x \in G : x = \varphi(x)\}$ tvoří úplný svaz, ve kterém největší prvek je roven 1.

Na větě 4.3. je založena hlavní věta formální konceptuální analýzy, která tvrdí, že množina všech konceptů každého kontextu tvoří, vzhledem k uspořádání množinovou inkluzí, úplný svaz, tzv. konceptuální svaz. [37],[38]

Příklad 4.1. Mějme svaz $L = \{0, a, b, c, x, y, z\}$, jenž je pomocí Hasseova diagramu zobrazen na obrázku 14.



Obr. 14: Hasseův diagram svazu L

	0	a	b	c	x	y	z	1
f	0	a	b	1	x	1	1	1
g	0	y	z	c	1	y	z	1
$g \circ f$	0	y	z	1	1	1	1	1
$f \circ g$	0	1	1	1	1	1	1	1

Tab. 2: Definice uzávěrových operátorů f, g a jejich složení

Uzávěrové operátory f a g ve svazu L jsou definovány tabulkou 2. Pro množiny pevných bodů těchto uzávěrových operátorů platí:

- $Fix(f) = \{0, a, b, x, 1\}$,
- $Fix(g) = \{0, c, y, z, 1\}$,

přičemž tyto množiny tvoří úplné svazy. V tabulce 2 jsou definovány také složená zobrazení $g \circ f$ a $f \circ g$ vytvořená z uzávěrových operátorů f a g. Při prozkoumání těchto složení zjistíme, že složení $f \circ g$ splňuje všechny podmínky přechozí definice a tím pádem je také uzávěrovým operátorem. Pro množinu pevných bodů tohoto složení potom platí:

- $Fix(f \circ g) = \{0,1\}$.

Oproti tomu složení $g \circ f$ není uzávěrovým operátorem na svazu L, jelikož nesplňuje podmínku $\varphi(x) = \varphi(\varphi(x))$. Což je možné pozorovat podle:

- $(g \circ f)(a) = y$, ale $(g \circ f) \circ (g \circ f)(a) = 1$.

Z toho vyplývá fakt, že složení dvou uzávěrových operátorů netvoří vždy uzávěrový operátor, navzdory tomu, že množina pevných bodů takového složení:

- $Fix(g \circ f) = \{0,1\}$,

tvoří úplný svaz.

4.1 Modulární svazy

Podle věty 3.5.3. v libovolném svazu L pro každou trojici prvků $x, y, z \in L$ takovou, že $z \leq x$, platí modulární nerovnost:

- $(x \wedge y) \vee z \leq x \wedge (y \vee z)$.

Definice 4.1.1. Svaz L se nazývá modulární, pokud pro každou trojici prvků $x, y, z \in L$ takovou, že $z \leq x$, platí modulární nerovnost:

- $(x \wedge y) \vee z = x \wedge (y \vee z)$,

a podle principu duality:

- $(x \vee y) \wedge z = x \vee (y \wedge z)$.

Věta 4.1.1. Podsvaz modulárního svaz je modulární svaz.

Věta 4.1.2. Svaz L je modulární, jestliže pro každou trojici prvků $x, y, z \in L$ platí:

- $(x \wedge y) \vee (x \wedge z) = x \wedge (y \vee (x \wedge z))$.

Věta 4.1.3. Svaz L je modulární, jestliže pro každou trojici prvků $x, y, z \in L$ platí implikace:

- $x \geq z, x \wedge y = z \wedge y, x \vee y = z \vee y \Rightarrow x = z$.

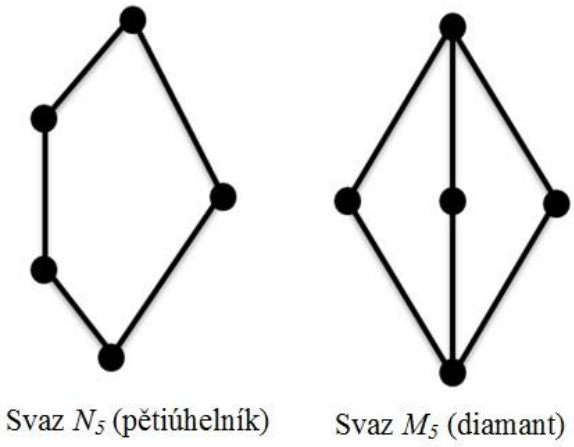
Věta 4.1.4. Svaz L je modulární, jestliže neobsahuje podsvaz izomorfní se svazem N_5 (tj. pětiúhelník, viz. obrázek 15) .

Příklad 4.1.1. Podle předchozí věty svaz N_5, neboli pětiúhelník modulární není. Ale svaz M_5, nazývaný diamant modulární je. Jestliže označíme $0 < z < x < 1$, což jsou čtyři prvky, jenž jsou v Hassově diagramu svazu N_5 umístěny nad sebou vlevo a y je jeho pátý prvek. Potom nerovnost:

- $(x \wedge y) \vee z = 0 \vee z = z < x = x \wedge 1 = x \wedge (y \vee z)$,

ukazuje, že svaz N_5 není modulární. Nyní dokážeme, že svaz M_5 modulární je. Označíme nejmenší prvek tohoto svazu jako 0 a největší prvek jako 1. Nechť $x, y, z \in M_5$ jsou prvky tohoto svazu takové, že $z \leq x$. Pokud $x = z$, potom plyne modulární rovnost z absorpčních

zákonů. Jestliže $z < x$, potom na Hasseově diagramu svazu M_5 je patrné, že buď $z = 0$ a nebo $x = 1$. Z obou případů je zřejmá modulární rovnost. [37]



Obr. 15: Ilustrace svazů pětiúhelník a diamant

4.2 Distributivní svazy

Podle věty 3.5.3. v libovolném svazu L pro každou trojici prvků $x, y, z \in L$ platí distributivní nerovnosti:

- $(x \vee y) \wedge (x \vee z) \geq x \vee (y \wedge z)$,
- $(x \wedge y) \vee (x \wedge z) \leq x \wedge (y \vee z)$.

Definice 4.2.1. Svaz L se nazývá distributivní, jestliže pro každou trojici prvků $x, y, z \in L$ platí distributivní rovnost:

- $(x \wedge y) \vee (x \wedge z) = x \wedge (y \vee z)$.

Věta 4.2.1. Nechť L je distributivní svaz. Pak pro každou trojici prvků $x, y, z \in L$ platí následující distributivní rovnost:

- $(x \vee y) \wedge (x \vee z) = x \vee (y \wedge z)$.

Věta 4.2.2. Každý distributivní svaz je modulární.

Věta 4.2.3. Podsvaz distributivního svazu je distributivní svaz.

Věta 4.2.4. Součin distributivních svazů je distributivní svaz. Homomorfní obraz distributivního svazu je distributivní svaz.

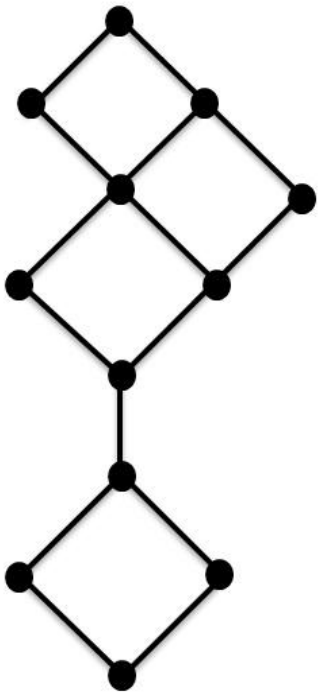
Věta 4.2.5. Svaz L je distributivní, právě když pro každou trojici prvků $x, y, z \in L$ platí implikace:

- $x \wedge y = z \wedge y, x \vee y = z \vee y \Rightarrow x = z$.

Svaz L je distributivní, právě když neobsahuje ani podsvaz izomorfní se svazem N_5 a ani se svazem M_5. (Viz. obrázek 15)

Definice 4.2.2. Prvek svazu L se nazývá $\vee$- nedosažitelný, pokud pro $\forall (y, z) \in L$ takové, že $x = y \vee z$, platí $x = y$ nebo $x = z$.

Příklad 4.2.1. Na obrázku 14 je znázorněn příklad distributivního svazu neobsahujícího podsvazy N_5 ani M_5. [37]



Obr. 16: Distributivní svaz

II. PRAKTICKÁ ČÁST

5 FROMÁLNÍ KONCEPTUÁLNÍ ANALÝZA

Formální konceptuální analýza, zkráceně FKA patří k základním metodám analýzy tabulkových dat. Je možné se také setkat s názvem metoda konceptuální svazů. O těchto konceptuálních svazech bude řeč dále.

5.1 Tabulková data

Při prací s FKA se vychází z tabulkových dat. Základním pojmem je objekt, což je nějaký prvek okolního světa. Může se jednat o lidi, zvířata, věci a podobně. Tyto objekty mívají určité atributy, což jsou jejich vlastnosti. U objektu počítač může existovat například atribut mít určitou velikost paměti Random Access Memory RAM. Pro daný objekt a atribut tedy může platit:

- objekt má daný atribut,
- objekt nemá daný atribut,
- objekt má daný atribut do jisté míry (např. IBM vyrábí levné základní desky),
- objekt má daný atribut s jistou hodnotou (počítač má v sobě obsažen slot čtyřikrát).

Vzájemný vztah mezi objekty a atributy je velice často vyjádřen tabulkou, kde řádkům tabulky odpovídají jednotlivé objekty a sloupcům atributy těchto objektů. Jednotlivé položky tabulky potom odpovídají objektům x a jím příslušným atributům y. Tyto položky potom poskytují informaci o tom, zda anebo s jakou hodnotou má daný objekt x atribut y. Tabulková data jsou jedna z nejzákladnějších a nejpřehlednějších možností reprezentace dat pro jejich další široké spektrum analýzy a zpracování.

5.2 Historie FKA

Úplné základy problematiky FKA položil americký matematik Garrett Birkhoff a norský matematik Øystein Ore. Garrett Birkhoff viděl v této problematice možnosti využitelnosti nejen pro matematiku. Ovšem za hlavního tvůrce FKA je považován Rudolf Wille, který navázal na jejich práce. Zabýval se konceptuálními svazy, pro jejichž teorii se snažil nalézt praktické využití. Své poznatky shrnul v knize *Restructuring lattice theory: an approach based on hiearchies of conceps* a také v *Formal concept analysis: Mathematical Foundations.* V dnešní době je problematika FKA velmi diskutovanou a využívanou části

matematické analýzy, která se využívá v mnoha odvětvích vědeckého světa, zejména proto, že přináší o trochu jiný pohled na data, než konvenční metody analýzy.

5.2.1 Základní pojmy FKA

Jak již bylo naznačeno dříve, tak jako vstup pro práci s FKA slouží tabulková data. FKA je metoda průzkumové analýzy dat. Přináší uživateli netriviální informace o zkoumaných datech. Může přinášet o datech nové poznatky, které nejsou z dat na první pohled patrné a mohou být využity při jejich dalším zpracování. Zpracovaná data pomocí FKA přináší dva základní výstupy:

- konceptuální svaz, což je hierarchicky uspořádaná množina tzv. formálních konceptů, které jsou přítomny i ve vstupních tabulkových datech,
- atributové implikace, které popisují jisté závislosti mezi jednotlivými atributy tabulky dat.

Při nejzákladnější analýze pomocí FKA se využívají pouze bivalentní logické atributy, což znamená, že daný objekt x buďto má anebo nemá daný atribut y. To je možno pozorovat i z následující tabulky, kde hodnota 1 znamená, že x má atribut y a 0, že x nemá atribut y. [41]

	y_1	y_2	y_3	y_4
x_1	1	0	1	1
x_2	0	0	0	1
x_3	1	1	0	0

Tab. 3: Objekty a bivalentní logické atributy

5.2.2 Galoisovy konexe

Definice 5.2.1. Nechť A a B jsou uspořádané množiny a $f : A \to B, g : B \to A$ jsou zobrazení. Potom dvojice zobrazení (f, g) je Galoisovou konexí mezi A a B, pokud platí:

- zobrazení f a g jsou antifonní,
- pro $\forall x \in A$ a $\forall y \in B$ platí, že $x \leq g(f(x)), y \leq f(g(y))$.

FCA je založena na Galoisových konexích mezi svazy všech podmnožin množiny objektů a atributů. [42]

5.2.3 Formální kontext

Definice 5.2.2. Je to trojice $\langle X, Y, I \rangle$, kde:

- X je množina objektů,
- Y je množina atributů,
- I je binární relace mezi X a Y.

Formální kontext reprezentuje tabulková data mezi objekty a atributy. Zápis $\langle x, y \rangle \in I$ znamená, že objekt x vlastní atribut y. Každý kontext $\langle X, Y, I \rangle$ indukuje zobrazení $^{\uparrow}: 2^X \to 2^Y$ a $^{\downarrow}: 2^Y \to 2^X$ předpisem:

- $A^{\uparrow} = \{ y \in Y \mid \forall x \in A : \langle x, y \rangle \in I \}$ pro $A \subseteq X$,
- $B^{\downarrow} = \{ x \in X \mid \forall y \in B : \langle x, y \rangle \in I \}$ pro $B \subseteq Y$.

Zobrazení $f: 2^X \to 2^Y$ a $g: 2^Y \to 2^X$ tvoří Galoisovu konexi mezi X a Y, jestliže pro $A, A_1, A_2 \subseteq X$ a $B, B_1, B_2 \subseteq Y$ platí:

- $A_1 \subseteq A_2$ implikuje $f(A_2) \subseteq f(A_1)$,
- $B_1 \subseteq B_2$ implikuje $g(B_2) \subseteq g(B_1)$,
- $A \subseteq g(f(A))$,
- $B \subseteq f(g(B))$.

Pro binární relaci $I \subseteq X \times Y$ tvoří indukovaná zobrazení $^{\uparrow I}$ a $^{\downarrow I}$ Galoisovu konexi mezi X a Y. Jinak řečeno, pokud tvoří f a g Galoisovu konexi mezi X a Y, tak existuje binární relace $I \subseteq X \times Y$ tak, že $f = ^{\uparrow I}$ a $g = ^{\downarrow I}$. To dává jednoznačný vzájemný vztah mezi Galoisovými konexemi mezi X a Y a binárními relacemi mezi X a Y. Obecně

podle tzv. zákona obráceného poměru rozsahů a obsahů platí, že čím více je objektů, tím mají méně společných vlastností. [41], [43]

5.2.4 Formální koncept

Nejprve je důležité definovat slovo *pojem*. Vytváření obecných pojmů a následná práce s nimi je nedílnou součástí života lidí. Díky nim je člověk schopen vyznat se v obrovském množství faktů a věcí našeho světa. Pojem vymezuje určité seskupení nějakých objektů, jinak též shluk. Tento shluk vyjadřuje, že dané objekty k sobě patří. Rozhodující je to, o čem si myslíme, že je důležitý shluk nebo pojem.

V FKA je uvažován tento pojem podle tzv. Port-Royalské logiky, která definuje pojem tím, že jej tvoří:

- rozsah – seskupení všech objektů, patřící pod daný pojem,
- obsah – seskupení všech atributů, které patří pod daný pojem.

Jako příklad můžeme uvést pojem kybernetický útok. Rozsah zde bude seskupení všech druhů kybernetických útoků a obsahem seskupení všech atributů všech kybernetických útoků, například *způsobovat nedostupnost napadnutého prvku*, nebo *odposlouchávat komunikaci oběti*.

Z matematického hlediska lze tedy pojem chápat jako dvojici prvků (A,B), z nichž A je množina objektů a B množina atributů daného pojmu. Ovšem ne všechny dvojice (A,B) je možné považovat za pojem. Aby je za pojem bylo možné považovat, tak A musí být množina všech objektů sdílející všechny atributy z množiny B. To platí také naopak, takže množina atributů B musí množinou všech atributů společných všem objektům z množiny A.

FKA pojem neboli dvojici (A_i, B_i), která splňuje požadavky popsané v předchozím odstavci, chápe jako tzv. koncept, nebo formální koncept. Tyto koncepty poté odpovídají vzájemně a jednoznačně maximálním obdélníkům vyplněnými jedničkami v tabulkových datech. Důležité je také definovat podpojem a nadpojem. Definujeme, že koncept (A_1, B_1) je podpojem konceptu (A_2, B_2). Potom je první koncept nejvýše tak obecný jako druhý. Jestliže platí, že každý objekt z A_1 patří do A_2, nebo každý atribut B_2 z patří do B_1. Tato

tvrzení značíme jako $(A_1, B_1) \leq (A_2, B_2)$. Takže například pojem „odepření služby“ je podpojmem pojmu „kybernetický útok“.

Definice 5.2.3. Nechť $\langle X, Y, I \rangle$ je formální kontext a dvojice (A, B) tvoří formální koncept v tomto kontextu. Pro (A, B) platí $A \subseteq X$, $B \subseteq Y$ a jsou takové, že $A^{\uparrow} = B$ a $B^{\downarrow} = A$.

Formální koncept je tedy pevným bodem Galoisovy konexe podle $^{\uparrow}$ a $^{\downarrow}$. Množina všech formálních konceptů v $\langle X, Y, I \rangle$ značená $\beta\langle X, Y, I \rangle$:

- $\beta\langle X, Y, I \rangle = \{(A, B) \mid A \subseteq X, B \subseteq Y, A^{\uparrow} = B, B^{\downarrow} = A\}$.

Pro dva formální koncepty (A_1, B_1), (A_2, B_2) klademe $(A_1, B_1) \leq (A_2, B_2)$, právě když $A_1 \subseteq A_2$ a $B_1 \subseteq B_2$. Formální koncept lze snadno definovat jako největší obdélník kontextové tabulky. Obdélník v $\langle X, Y, I \rangle$ je tedy pár $\langle A, B \rangle$, pro který platí $A \times B \subseteq I$, jinak řečeno pro $\forall x \in A$ a $\forall y \in B$ máme $\langle X, Y \rangle \in I$. [41],[43]

G	y_1	y_2	y_3	y_4
x_1	1	0	1	1
x_2	0	1	1	1
x_3	0	0	1	1
x_4	0	1	0	1

Tab. 4: Vyznačení jednoho formálního konceptu

V předcházející kontextové tabulce je možné pozorovat vyznačený koncept, ale nejedná se o jediný koncept této tabulky. Dalšími koncepty jsou:

- $\langle A_2, B_2 \rangle = \langle \{x_1\}, \{y_1, y_3, y_4\} \rangle$,
- $\langle A_3, B_3 \rangle = \langle \{x_2\}, \{y_2, y_3, y_4\} \rangle$,
- $\langle A_4, B_4 \rangle = \langle \{x_2, x_4\}, \{y_2, y_4\} \rangle$,

- $\langle A_5, B_5 \rangle = \langle \{x_1, x_2, x_3, x_4\}, \{y_4\} \rangle$,
- $\langle A_6, B_6 \rangle = \langle \{\ \}, \{y_1, y_2, y_3, y_4\} \rangle$.

5.2.5 Konceptuální svaz

Definice 5.2.4. Nechť je množina $\beta\langle X, Y, I \rangle$ spolu s relací $\leq$ definovanou na množině $\beta\langle X, Y, I \rangle$ předpisem $(A_1, B_1) \leq (A_2, B_2)$, právě když $A_1 \subseteq A_2$ nebo ekvivalentně $B_2 \subseteq B_1$.

Množina obsahů všech kontextu z $\beta\langle X, Y, I \rangle$ se značí $Int(I)$. Označíme $Int(I) = \{B \subseteq Y | \langle A, B \rangle \in \beta(X, Y, I)\}$ pro určitou $A \subseteq X$. Dále $B \subseteq Y$ je obsahem nějakého konceptu z $\beta\langle X, Y, I \rangle$. Relace $\leq$ je relací mezi podpojmem a nadpojmem, které byly popsány v kapitole 5.2.4.

Hlavní věta o konceptuálních svazech. Nechť $\langle X, Y, I \rangle$ je formální kontext. Potom $\beta\langle X, Y, I \rangle$ je vzhledem k $\leq$ úplný svaz, ve kterém jsou infima a suprema dána jako:

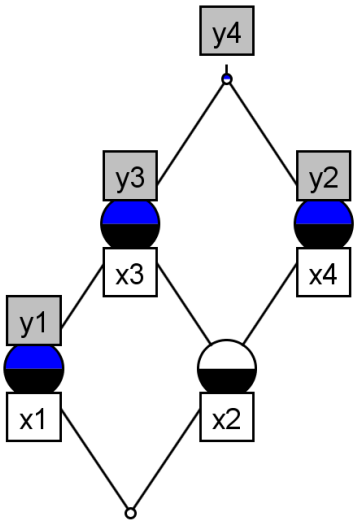
- $\bigwedge_{k \in K} \langle A_k, B_k \rangle = \left\langle \bigcap_{k \in K} A_k, (\bigcap_{k \in K} A_k)^{\uparrow} \right\rangle = \left\langle \bigcap_{k \in K} A_k, (\bigcup_{k \in K} B_k)^{\downarrow\uparrow} \right\rangle$,
- $\bigvee_{k \in K} \langle A_k, B_k \rangle = \left\langle (\bigcap_{k \in K} B_k)^{\downarrow}, \bigcap_{k \in K} B_k \right\rangle = \left\langle (\bigcup_{k \in K} A_k)^{\downarrow\uparrow}, \bigcap_{k \in K} B_k \right\rangle$.

Daný úplný svaz $L = \langle Z, \leq \rangle$ je izomorfní s $\beta\langle X, Y, I \rangle$ právě když existují zobrazení $\gamma : X \to Z$ a $\mu : Y \to Z$, pro která je $\gamma(X)$ supremálně hustá v L, $\mu(Y)$ infimálně hustá v L a $\langle x, y \rangle \in I$ platí právě když $\gamma(x) \leq \mu(y)$ pro $\forall x \in X$ a $\forall y \in Y$. Množina $K \subseteq Z$ je supremálně hustá v L, právě když pro $\forall z \in Z$ existuje $K_v \subseteq K$, tak že v je supremem množiny K_v,obdobně to platí i pro hodnotu infima. [41],[43]

Konceptuální svaz se vykresluje pomocí Hasseova diagramu, kde jsou jednotlivé koncepty v tomto diagramu znázorněny jako uzly. Určité koncepty K_i a K_j jsou v diagramu spojeny, jestliže platí $K_i \leq K_j$ přičemž je K_j umístěn výše než K_i. [44]

K vykreslení grafů je možné s výhodou použít program conexp. Tento program funguje jako kalkulačka FKA. Nejprve se nastaví počet objektů a atributů, načež se do tabulky vyplní křížky podle toho, jestli má daný objekt daný atribut. Program je poté schopen

vykreslit graf konceptuálního svazu, kde je možné i vyznačit jednotlivé objekty a atributy popiskem u příslušných uzlů jak je vidět i na následujícím obrázku.



Obr. 17: Konceptuální svaz
z konceptu v tabulce 4

5.2.6 Atributové implikace

Definice 5.2.5. Atributová implikace nad množinou Y atributů je výraz ve tvaru $A \Rightarrow B$, kde $A, B \subseteq Y$. Pro implikaci $A \Rightarrow B$ a množinu $E \subseteq Y$ definujeme, že $A \Rightarrow B$ platí v E, nebo že E je modelem $A \Rightarrow B$ pokud platí $A \subseteq E$ i $B \subseteq E$. Obecněji tedy pro množinu $M \subseteq 2^Y$, kde Y je množina atributů, a množinu implikací $V = \{A_k, B_k | k \in K\}$ říkáme, že V platí v M, nebo že M je model pro V, pokud $A_k \Rightarrow B_k$ platí v N pro $\forall N \in M$ a všechny $A_k \Rightarrow B_k \in T$.

5.2.7 Vícehodnotové škálování

Vícehodnotové kontexty jsou rozšířením formálních kontextů, kdy je možné vstupní data zpracovat nejen s bivalentními atributy.

Definice 5.2.6. Čtveřice $\langle X, Y, W, I \rangle$ je vícehodnotový kontext, kde $I \subseteq X \times Y \times W$ je ternární operace, u které platí, že pokud $\langle x, y, v \rangle \in I$ a $\langle x, y, w \rangle \in I$, tak potom $v = w$. Škála

pro atribut vícehodnotového kontextu je kontext $S_y = \langle X_y, Y_y, I_y \rangle$, pro který platí $y(X) \subseteq X_y$, kde $y(X) = \{y(x) | x \in X\}$. Poté prvky množin X_y, Y_y tvoří škálové hodnoty a škálové atributy. Potom je-li $\langle X, Y, W, I \rangle$ vícehodnotový kontext a $S_y = (y \in Y)$ škály, tak potom kontext, který je odvozen jednoduchým škálováním je kontext $\langle X, V, K \rangle$, kde:

- $N = \cup_{y \in Y} Y_y (Y_y = \{y\} \times Y_y)$,
- $\langle x, \langle y, v \rangle \rangle \in K$ právě když $y(x) = w$ a $\langle w, v \rangle \in I_Y$.

Prvky množin X, Y, W jsou objekty, vícehodnotové atributy a hodnoty atributů. Zápis $y(x) = w$ znamená, že objekt x má atribut y s hodnotou w, kde $\langle x, y, w \rangle \in I$. Více hodnotové kontext slouží k rozšíření základních kontextů. Tohoto rozšíření je dosaženo za pomoci škálování, kde je vícehodnotový kontext převeden na základní, který je potom již připraven k analýze. Škálou daného atributu vícehodnotového kontextu může být libovolný kontext, který splňuje podmínky definice. Důležité je, aby škála odrážela význam daného atributu. Škál existuje velké množství, ale mezi nejznámější patří nominální, ordinální, interordinální, biordinální nebo dichotomická. Objekty odvozeného kontextu se shodují s objekty vícehodnotového kontextu a množina atributů odvozeného kontextu he disjunktní sjednocení atributů jednotlivých škál. [42]

Příklad 5.2.1. Mějme tedy tabulku s vícehodnotovým kontextem:

G	y_1	y_2	y_3	y_4
x_1	25	4	1	1
x_2	0	17	0	1
x_3	1	0	1	1
x_4	13	23	0	0

Tab. 5: Vícehodnotový kontext

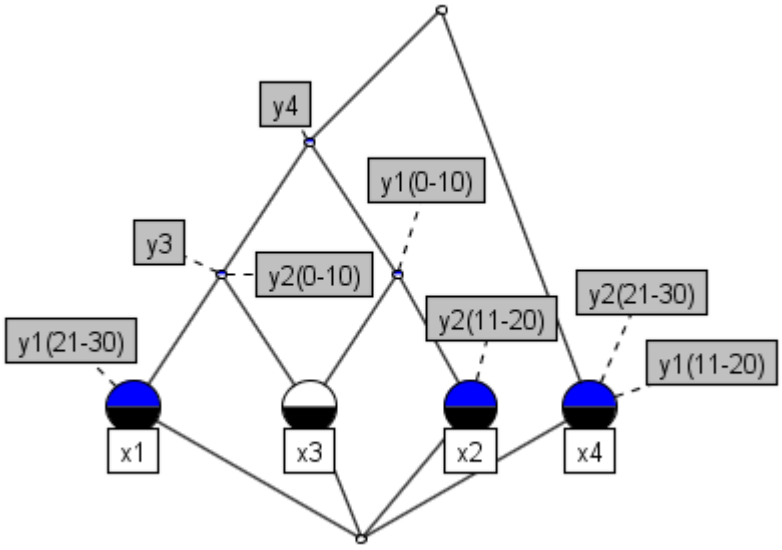
Při tvorbě kontextové tabulky s využitím škálování se na ose objektů nic nemění, ale na ose atributů dojde k vložení $|Y_y|$ sloupců, které jsou označeny atributy z Y_y a každá hodnota

$y(x)$ vícehodnotového kontextu je nahrazena řádkem škály S_y, které patří danému objektu x.

Z předcházející tabulky je patrné, že bivalentních logických hodnot nabývají pouze atributy y_3 a y_4. U ostatních atributů je tedy zapotřebí převedení na základní kontext pomocí škálování. Po použití škálování se tedy tabulky změní třeba takto, záleží na tom, jaké použijeme rozsahy škál.

G	$y_{1(0–10)}$	$y_{1(11–20)}$	$y_{1(21–30)}$	$y_{2(0–10)}$	$y_{2(11–20)}$	$y_{2(21–30)}$	y_3	y_4
x_1	0	0	1	1	0	0	1	1
x_2	1	0	0	0	1	0	0	1
x_3	1	0	0	1	0	0	1	1
x_4	0	1	0	0	0	1	0	0

Tab. 6: Kontextová tabulka s využitím škálování



Obr. 18: Konceptuální svaz vytvořený podle tabulky 6

Na obrázku 18 je vidět vykreslený konceptuální svaz s vyznačenými koncepty.

6 UŽÍTÍ FORMÁLNÍ KONCEPTUÁLNÍ ANALÝZY K ROZBORU KYBERNETICKÝCH ÚTOKŮ

V této kapitole bude prezentována analýza kybernetických útoků popsaných ve druhé kapitole pomocí FKA. Nejprve budou analyzovány DOS útoky jako celek, poté budou analyzovány záplavové útoky DOS, následovat bude analýza útoku využívajících principů Man in the middle, poté budou analyzovány útoky na aplikační úrovni společně s útoky založenými na sociotechnických metodách a také s červy a trojskými koni. Nakonec je prezentována FKA reálných kybernetických útoků detekovaných v první polovině dubna 2014.

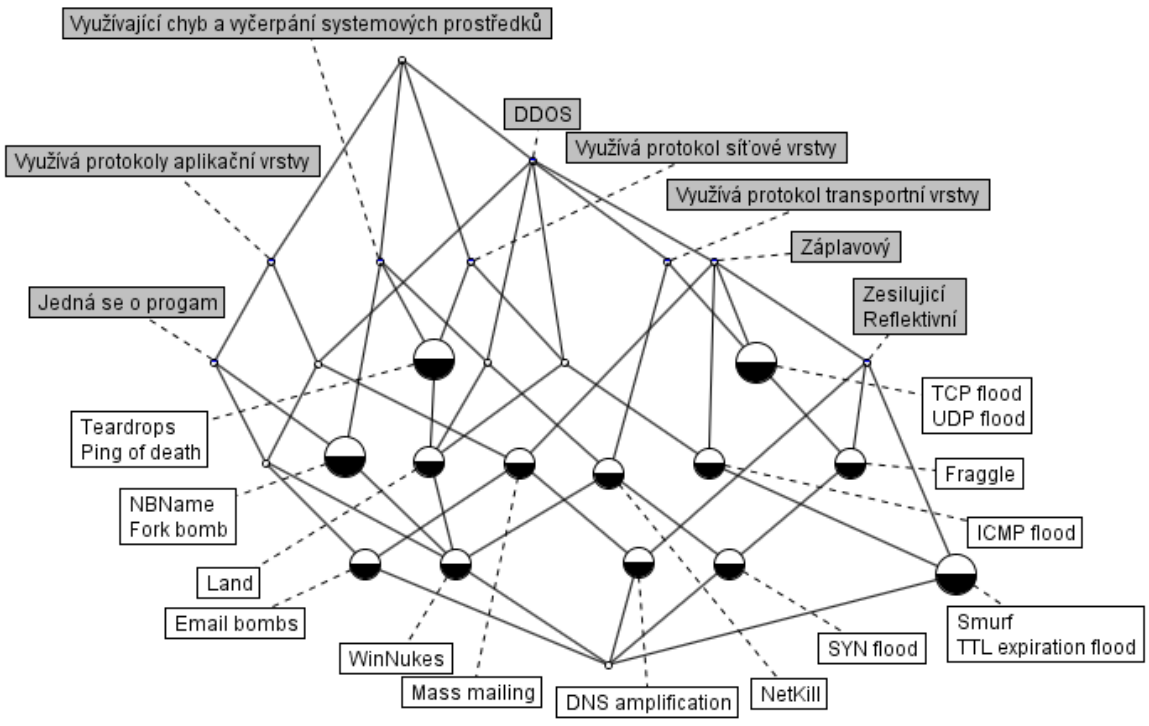
6.1 Analýza všech DOS útoků

Nyní budou analyzovány všechny popsané DOS útoky dohromady podle typu a způsobu použití. U těchto útoku existuje pouze obecné rozdělení do několika skupin, které jsou použity jako atributy, přičemž jednotlivé útoky se dají většinou zařadit do více než jedné skupiny, proto jsou velmi vhodné k analýze pomocí FKA.

	Využívající chyb a vyčerpání systémových prostředků	Záplavový typ	Reflektivní typ	Zesilující typ	DDOS verze	Jedná se o program	Využívá protokol síťové vrstvy	Využívá protokol transportní vrstvy	Využívá protokol aplikační vrstvy
Ping of death	1	0	0	0	0	0	1	0	0
Teardrops	1	0	0	0	0	0	1	0	0
SYN flood	1	1	1	1	1	0	0	1	0
NetKill	1	0	0	0	1	0	0	1	0
Land	1	0	0	0	0	0	1	0	0
IMCP flood	0	1	0	0	1	0	1	0	0
UDP flood	0	1	0	0	1	0	0	1	0

TPC flood	0	1	0	0	1	0	0	1	0
Mass mailing	0	1	0	0	1	0	0	0	1
Email bomb	0	1	0	0	1	1	0	0	1
Fraggle	0	1	1	1	1	0	0	1	0
TTL expiration flood	0	1	1	1	1	0	1	0	0
DNS amplification	0	1	1	1	1	0	0	0	1
Smurf	0	1	1	1	1	0	1	0	0
Fork bomb	1	0	0	0	0	1	0	0	1
NBname	1	0	0	0	0	1	0	0	1
WinNukes	1	0	0	0	1	1	1	1	1

Tab. 7: Kontextová tabulka 6.1



Obr. 19: Konceptuální svaz 6.1

Pro určování jednotlivých konceptů, lze využít konceptuální svaz, tabulku kontextu, ve které se vyhledávají maximální obdélníky, ale i softwarový nástroj FKA extension, který lze doinstalovat do programu Excel z rodiny Microsoft Office.

V kontextové tabulce je možné najít celkem 27 konceptů a jejich seznam je následující:

{Ping of death; Teardrops; SYN flood; NetKill; Land; ICMP flood; UDP flood; TCP flood; Mass mailing; Email bombs; Fraggle; TTL expiration flood; DNS amplification; Smurf; Fork bomb; NBName; WinNukes}	{}
{Mass mailing; Email bombs; DNS amplification; Fork bomb; NBName; WinNukes}	{Využívá protokoly aplikační vrstvy}
{Ping of death; Teardrops; Land; ICMP flood; TTL expiration flood; Smurf; WinNukes}	{Využívá protokol síťové vrstvy}
{Email bombs; Fork bomb; NBName; WinNukes}	{Jedná se o progam; Využívá protokoly aplikační vrstvy}
{SYN flood; NetKill; Land; ICMP flood; UDP flood; TCP flood; Mass mailing; Email bombs; Fraggle; TTL expiration flood; DNS amplification; Smurf; WinNukes}	{DDOS}
{Mass mailing; Email bombs; DNS amplification; WinNukes}	{DDOS; Využívá protokoly aplikační vrstvy}
{SYN flood; NetKill; UDP flood; TCP flood; Fraggle; WinNukes}	{DDOS; Využívá protokol transportní vrstvy}
{Land; ICMP flood; TTL expiration flood; Smurf; WinNukes}	{DDOS; Využívá protokol síťové vrstvy}
{Email bombs; WinNukes}	{DDOS; Jedná se o progam; Využívá protokoly aplikační vrstvy}
{SYN flood; ICMP flood; UDP flood; TCP flood; Mass mailing; Email bombs; Fraggle; TTL expiration flood; DNS amplification; Smurf}	{Záplavový; DDOS}
{Mass mailing; Email bombs; DNS amplification}	{Záplavový; DDOS; Využívá protokoly aplikační vrstvy}
{SYN flood; UDP flood; TCP flood; Fraggle}	{Záplavový; DDOS; Využívá protokol transportní

	vrstvy}
{ICMP flood; TTL expiration flood; Smurf}	{Záplavový; DDOS; Využívá protokol síťové vrstvy}
{Email bombs}	{Záplavový; DDOS; Jedná se o progam; Využívá protokoly aplikační vrstvy}
{SYN flood; Fraggle; TTL expiration flood; DNS amplification; Smurf}	{Záplavový; Reflektivní; Zesilujicí; DDOS}
{DNS amplification}	{Záplavový; Reflektivní; Zesilujicí; DDOS; Využívá protokoly aplikační vrstvy}
{SYN flood; Fraggle}	{Záplavový; Reflektivní; Zesilujicí; DDOS; Využívá protokol transportní vrstvy}
{TTL expiration flood; Smurf}	{Záplavový; Reflektivní; Zesilujicí; DDOS; Využívá protokol síťové vrstvy}
{Ping of death; Teardrops; SYN flood; NetKill; Land; Fork bomb; NBName; WinNukes}	{Využívající chyb a vyčerpání systemových prostředků}
{Ping of death; Teardrops; Land; WinNukes}	{Využívající chyb a vyčerpání systemových prostředků; Využívá protokol síťové vrstvy}
{Fork bomb; NBName; WinNukes}	{Využívající chyb a vyčerpání systemových prostředků; Jedná se o progam; Využívá protokoly aplikační vrstvy}
{SYN flood; NetKill; Land; WinNukes}	{Využívající chyb a vyčerpání systemových prostředků; DDOS}
{SYN flood; NetKill; WinNukes}	{Využívající chyb a vyčerpání systemových prostředků; DDOS; Využívá protokol transportní vrstvy}
{Land; WinNukes}	{Využívající chyb a vyčerpání systemových prostředků; DDOS; Využívá protokol síťové vrstvy}
{WinNukes}	{Využívající chyb a vyčerpání systemových prostředků; DDOS; Jedná se o progam; Využívá protokol síťové vrstvy; Využívá protokol transportní vrstvy; Využívá protokoly aplikační vrstvy}
{SYN flood}	{Využívající chyb a vyčerpání systemových prostředků; Záplavový; Reflektivní; Zesilujicí; DDOS; Využívá protokol transportní vrstvy}

{}	{Využívající chyb a vyčerpání systemových prostředků; Záplavový; Reflektivní; Zesilující; DDOS; Jedná se o progam; Využívá protokol síťové vrstvy; Využívá protokol transportní vrstvy; Využívá protokoly aplikační vrstvy}

Tab. 8: Seznam konceptů z kontextové tabulky 6.1

6.2 Analýza záplavových DOS útoků podle jejich počtu v roce 2013

Záplavové útoky a jejich funkce jsou popsány v druhé kapitole. Další data k analýze jsou pro tento případ použity ze zdroje [45], který se zaobírá statistikou počtu těchto útoků v jejich distribuované verzi.

Po sestavení kontextové tabulky vznikne jeden atribut, který je dále škálován. Pro jeho naškálování jsou zvoleny rozdělení podle procentuálních hodnot 0-10%, 11-20%, 21-30% a 31-40%. Jak je patrné z tabulky 10, tak po naškálování zůstal atribut 21-30% nulový pro všechny typy útoků. Hybridní útok je typ DOS záplavového útoku, který využívá různých kombinací ostatních záplavových útoků.

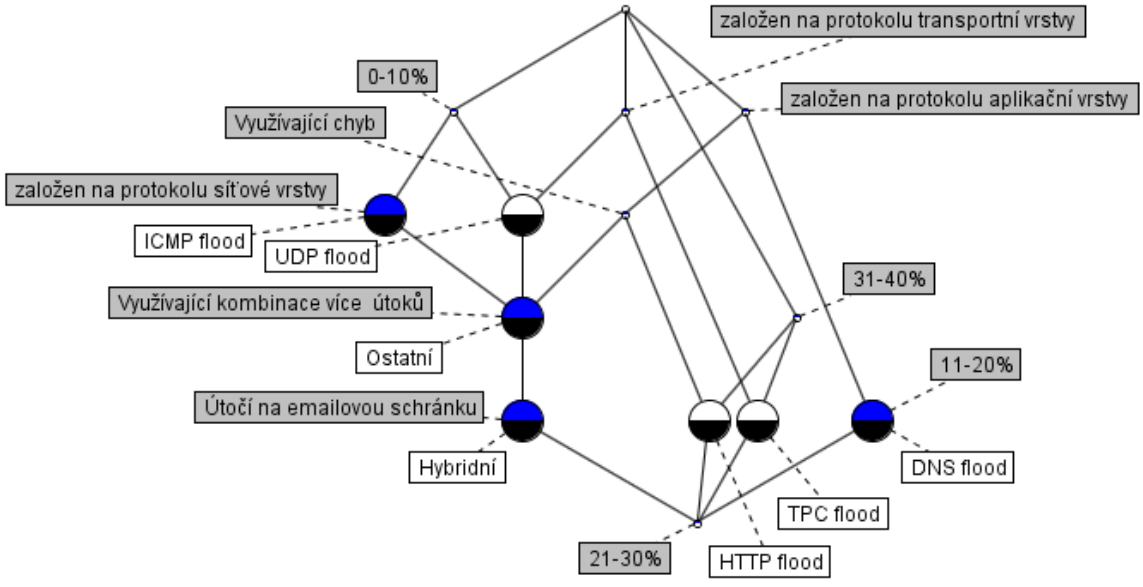
	Procento z celkového počtu útoků	Založen na protokolu síťové vrstvy	Založen na protokolu transportní vrstvy	Založen na protokolu aplikační vrstvy	Využívající chyb	Využívající kombinaci více útoků	Útočí na emailovou schránku
TCP flood	38,7	0	1	0	0	0	0
HTTP flood	37,2	0	0	1	1	0	0
DNS flood	13,1	0	0	1	0	0	0
Hybridní	4,1	1	1	1	1	1	1
UDP flood	3,5	0	1	0	0	0	0
Ostatní	3	1	1	1	1	1	1
ICMP flood	0,3	0	1	0	0	0	0

Tab. 9: Kontextová tabulka 6.2 před škálováním

Nyní je provedeno škálování nebivalentních hodnot.

	Procento z celkového počtu útoků (0-10 %)	Procento z celkového počtu útoků (11-20 %)	Procento z celkového počtu útoků (21-30 %)	Procento z celkového počtu útoků (31-40 %)	Založen na protokolu síťové vrstvy	Založen na protokolu transportní vrstvy	Založen na protokolu aplikační vrstvy	Využívající chyb	Využívající kombinaci více útoků	Útočí na emailovou schránku
TCP flood	0	0	0	1	0	1	0	0	0	0
HTTP flood	0	0	0	1	0	0	1	1	0	0
DNS flood	0	1	0	0	0	0	1	0	0	0
Hybridní	1	0	0	0	1	1	1	1	1	1
UDP flood	1	0	0	0	0	1	0	0	0	0
Ostatní	1	0	0	0	1	1	1	1	0	1
ICMP flood	1	0	0	0	1	0	0	0	0	0

Tab. 10: Kontextová tabulka 6.2 s naškálovaným atributem



Obr. 20: Konceptuální svaz 6.2

V kontextové tabulce je možné najít celkem 14 kontextů a jejich seznam je následující:

{TPC flood; HTTP flood; DNS flood; Hybridní; UDP flood; Ostatní; ICMP flood}	{}
{HTTP flood; DNS flood; Hybridní; Ostatní}	{založen na protokolu aplikační vrstvy}
{HTTP flood; Hybridní; Ostatní}	{založen na protokolu aplikační vrstvy; Využívající chyb}
{TPC flood; Hybridní; UDP flood; Ostatní}	{založen na protokolu transportní vrstvy}
{TPC flood; HTTP flood}	{31-40%}
{HTTP flood}	{31-40%; založen na protokolu aplikační vrstvy; Využívající chyb}
{TPC flood}	{31-40%; založen na protokolu transportní vrstvy}
{DNS flood}	{11-20%; založen na protokolu aplikační vrstvy}
{Hybridní; UDP flood; Ostatní; ICMP flood}	{0-10%}
{Hybridní; UDP flood; Ostatní}	{0-10%; založen na protokolu transportní vrstvy}
{Hybridní; Ostatní; ICMP flood}	{0-10%; založen na protokolu síťové vrstvy}
{Hybridní; Ostatní}	{0-10%; založen na protokolu síťové vrstvy; založen na protokolu transportní vrstvy; založen na protokolu aplikační vrstvy; Využívající chyb; Využívající kombinace více útoků}
{Hybridní}	{0-10%; založen na protokolu síťové vrstvy; založen na protokolu transportní vrstvy; založen na protokolu aplikační vrstvy; Využívající chyb; Využívající kombinace více útoků; Útočí na emailovou schránku}
{}	{0-10%; 11-20%; 21-30%; 31-40%; založen na protokolu síťové vrstvy; založen na protokolu transportní vrstvy; založen na protokolu aplikační vrstvy; Využívající chyb; Využívající kombinace více útoků; Útočí na emailovou schránku}

Tab. 11: Seznam formálních konceptů 6.2

Z analýzy těchto útoku je patrné, že za poslední dobu jsou nejfrekventovanější a tím tedy i nejnebezpečnější TPC a HTPP záplavové útoky. DNS flood pracuje na obdobném principu

jako ostatní záplavové útoky. Funguje tak, že se útočník pokouší zahltit DNS server dotazy na překlad doménového jména.

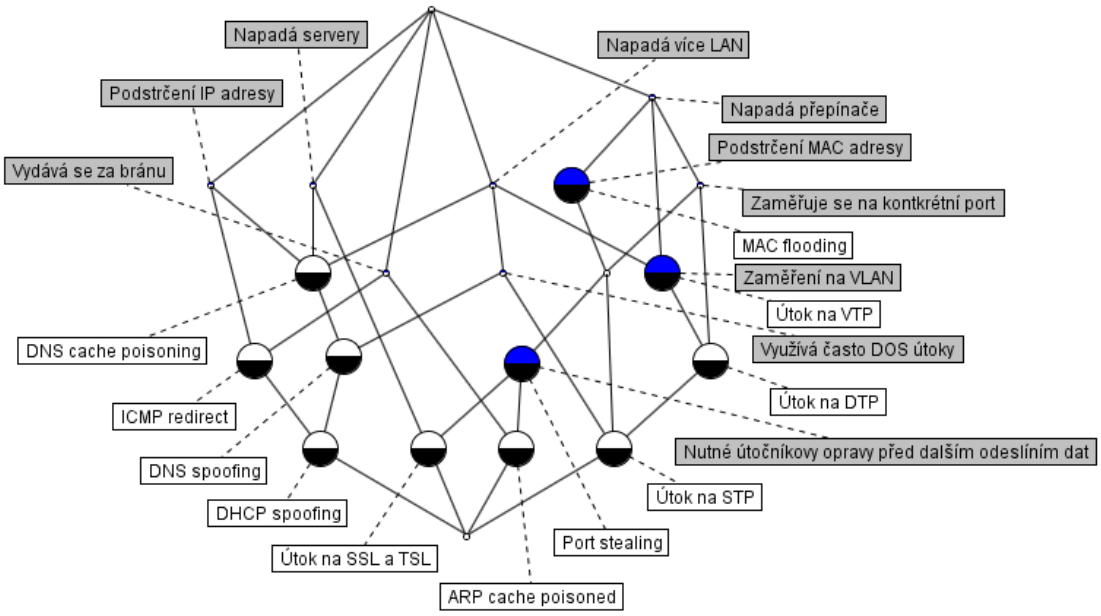
6.3 Analýza útoků využívajících MITM

V této části budou analyzovány útoky, které jsou založeny na principech MITM. Jako atributy objektů jsou voleny vlastnosti, týkající se hlavně toho, na jaké prvky sítě se jednotlivé útoky zaměřují a jaké techniky k tomu využívají.

	Napadá přepínače	Zaměřuje se na konkrétní port	Napadá více LAN	Vydává se za bránu	Napadá servery	Nutné útočníkovy úpravy před dalším odesláním dat	Podstrčení MAC adresy	Podstrčení IP adresy	Využívá často DOS útoky	Zaměření na VLAN
ARP cache poisoned	1	1	0	1	0	1	1	0	0	0
MAC flooding	1	0	0	0	0	0	1	0	0	0
Port stealing	1	1	0	0	0	1	1	0	0	0
DHCP spoofing	0	0	1	1	1	0	0	1	1	0
ICMP redirect	0	0	0	1	0	0	0	1	0	0
DNS spoofing	0	0	1	0	1	0	0	1	1	0
DNS cache poisoning	0	0	1	0	1	0	0	1	0	0
Útok na SSL a TSL	1	1	0	0	0	1	1	0	0	0
Útok na STP	1	1	1	0	0	0	1	0	1	1

Útok na VTP	1	0	1	0	0	0	0	0	0	1
Útok na DTP	1	1	1	0	0	0	0	0	0	1

Tab. 12: Kontextová tabulka 6.3



Obr. 21: Konceptuální svaz 6.3

V kontextové tabulce je možné najít celkem 21 konceptů a jejich seznam je následující:

{ARP cache poisoned; MAC flooding; Port stealing; DHCP spoofing; ICMP redirect; DNS spoofing; DNS cache poisoning; Útok na SSL a TSL; Útok na STP; Útok na VTP; Útok na DTP}	{}
{DHCP spoofing; ICMP redirect; DNS spoofing; DNS cache poisoning}	{Podstrčení IP adresy}
{DHCP spoofing; DNS spoofing; DNS cache poisoning; Útok na SSL a TSL}	{Napadá servery}
{ARP cache poisoned; DHCP spoofing; ICMP redirect}	{Vydává se za bránu}
{DHCP spoofing; ICMP redirect}	{Vydává se za bránu; Podstrčení IP adresy}
{DHCP spoofing; DNS spoofing; DNS cache poisoning; Útok na STP; Útok na VTP; Útok na DTP}	{Napadá více LAN}

{DHCP spoofing; DNS spoofing; Útok na STP}	{Napadá více LAN; Využívá často DOS útoky}
{DHCP spoofing; DNS spoofing; DNS cache poisoning}	{Napadá více LAN; Napadá servery; Podstrčení IP adresy}
{DHCP spoofing; DNS spoofing}	{Napadá více LAN; Napadá servery; Podstrčení IP adresy; Využívá často DOS útoky}
{DHCP spoofing}	{Napadá více LAN; Vydává se za bránu; Napadá servery; Podstrčení IP adresy; Využívá často DOS útoky}
{ARP cache poisoned; MAC flooding; Port stealing; Útok na SSL a TSL; Útok na STP; Útok na VTP; Útok na DTP}	{Napadá přepínače}
{ARP cache poisoned; MAC flooding; Port stealing; Útok na SSL a TSL; Útok na STP}	{Napadá přepínače; Podstrčení MAC adresy}
{Útok na STP; Útok na VTP; Útok na DTP}	{Napadá přepínače; Napadá více LAN; Zaměření na VLAN}
{ARP cache poisoned; Port stealing; Útok na SSL a TSL; Útok na STP; Útok na DTP}	{Napadá přepínače; Zaměřuje se na kontkrétní port}
{ARP cache poisoned; Port stealing; Útok na SSL a TSL; Útok na STP}	{Napadá přepínače; Zaměřuje se na kontkrétní port; Podstrčení MAC adresy}
{ARP cache poisoned; Port stealing; Útok na SSL a TSL}	{Napadá přepínače; Zaměřuje se na kontkrétní port; Nutné útočníkovy opravy před dalším odeslíním dat; Podstrčení MAC adresy}
{Útok na SSL a TSL}	{Napadá přepínače; Zaměřuje se na kontkrétní port; Napadá servery; Nutné útočníkovy opravy před dalším odeslíním dat; Podstrčení MAC adresy}
{ARP cache poisoned}	{Napadá přepínače; Zaměřuje se na kontkrétní port; Vydává se za bránu; Nutné útočníkovy opravy před dalším odeslíním dat; Podstrčení MAC adresy}
{Útok na STP; Útok na DTP}	{Napadá přepínače; Zaměřuje se na kontkrétní port; Napadá více LAN; Zaměření na VLAN}
{Útok na STP}	{Napadá přepínače; Zaměřuje se na kontkrétní port; Napadá více LAN; Podstrčení MAC adresy; Využívá často DOS útoky; Zaměření na VLAN}

{}	{Napadá přepínače; Zaměřuje se na kontkrétní port; Napadá více LAN; Vydává se za bránu; Napadá servery; Nutné útočníkovy opravy před dalším odeslíním dat; Podstrčení MAC adresy; Podstrčení IP adresy; Využívá často DOS útoky; Zaměření na VLAN}

Tab. 13: Seznam formálních konceptů 6.3

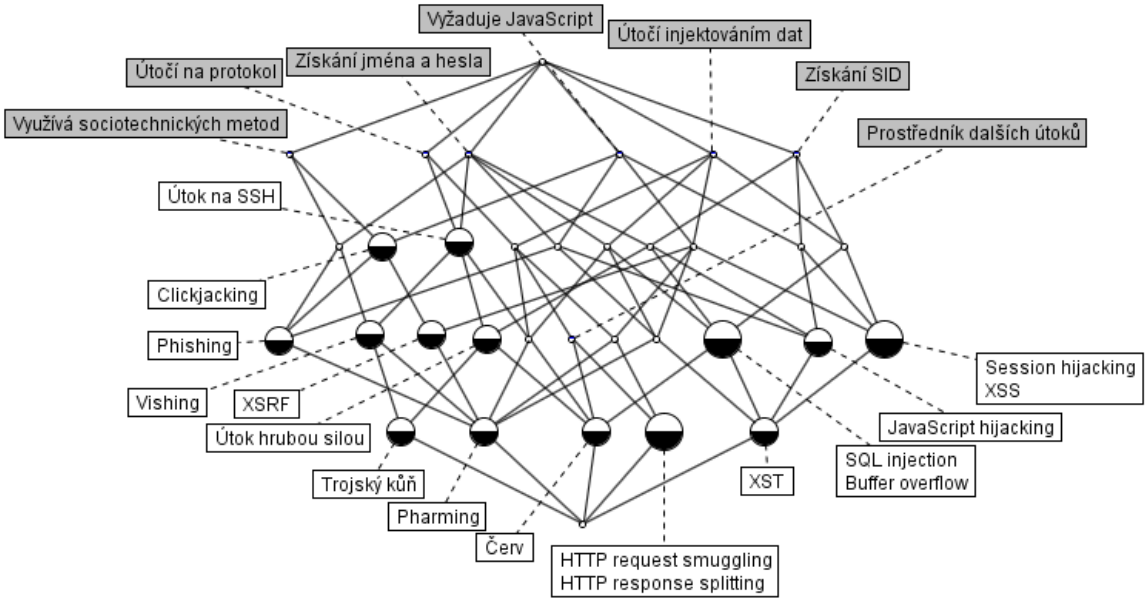
6.4 Analýza útoků na aplikační úrovni

V této části jsou analyzovány útoky na aplikační úrovni. Mezi nimi i útoky využívající sociotechnických metod a také známý škodlivý malware jako je červ nebo trojský kůň. Zde jsou atributy navrženy tak, aby byly co možná nejvíce společné pro tyto typy útoků.

	Vyžaduje JavaScript	Získání jména a hesla	Získání SID	Útočí na protokol	Útočí injektováním dat	Využívá sociotechnických metod	Prostředník dalších útoků
Červ	0	1	1	1	1	0	1
Trojský kůň	0	1	1	1	0	1	0
Útok hrubou silou	0	1	1	1	0	0	0
Buffer overflow	0	1	1	0	1	0	0
SQL Injecton	0	1	1	0	1	0	0
XSS	1	0	1	0	1	0	0
XSRF	1	0	0	0	1	1	0
XST	1	1	1	0	1	0	0
HTTP response splitting	1	0	0	1	1	0	1
HTTP request smuggling	1	0	0	1	1	0	1
Session hijacking	1	0	1	0	1	0	0

JavaScript hijacking	1	1	1	0	0	0	0
Clickjacking	1	0	0	0	0	1	0
Útok na SSH	0	1	0	1	0	0	0
Phishing	1	1	0	0	0	1	0
Pharming	1	1	0	1	1	1	0
Vishing	0	1	0	1	0	1	0

Tab. 14: Kontextová tabulka 6.4



Obr. 22: Konceptuální svaz 6.4

V kontextové tabulce je možné najít celkem 34 konceptů a jejich seznam je následující:

{Červ; Trojský kůň; Útok hrubou silou; Buffer overflow; SQL injection; XSS; XSRF; XST; HTTP response splitting; HTTP request smuggling; Session hijacking; JavaScript hijacking; Clickjacking; Útok na SSH; Phishing; Pharming; Vishing}	{}
{Trojský kůň; XSRF; Clickjacking; Phishing; Pharming; Vishing}	{Využívá sociotechnických metod}
{Červ; Buffer overflow; SQL injection; XSS; XSRF;	{Útočí injektováním dat}

XST; HTTP response splitting; HTTP request smuggling; Session hijacking; Pharming}	
{Červ; Trojský kůň; Útok hrubou silou; HTTP response splitting; HTTP request smuggling; Útok na SSH; Pharming; Vishing}	{Útočí na protokol}
{Červ; HTTP response splitting; HTTP request smuggling; Pharming}	{Útočí na protokol; Útočí injektováním dat}
{Červ; HTTP response splitting; HTTP request smuggling}	{Útočí na protokol; Útočí injektováním dat; Prostředník dalších útoků}
{Červ; Trojský kůň; Útok hrubou silou; Buffer overflow; SQL injection; XSS; XST; Session hijacking; JavaScript hijacking}	{Získání SID}
{Červ; Buffer overflow; SQL injection; XSS; XST; Session hijacking}	{Získání SID; Útočí injektováním dat}
{Červ; Trojský kůň; Útok hrubou silou; Buffer overflow; SQL injection; XST; JavaScript hijacking; Útok na SSH; Phishing; Pharming; Vishing}	{Získání jména a hesla}
{Trojský kůň; Phishing; Pharming; Vishing}	{Získání jména a hesla; Využívá sociotechnických metod}
{Červ; Buffer overflow; SQL injection; XST; Pharming}	{Získání jména a hesla; Útočí injektováním dat}
{Červ; Trojský kůň; Útok hrubou silou; Útok na SSH; Pharming; Vishing}	{Získání jména a hesla; Útočí na protokol}
{Trojský kůň; Pharming; Vishing}	{Získání jména a hesla; Útočí na protokol; Využívá sociotechnických metod}
{Červ; Pharming}	{Získání jména a hesla; Útočí na protokol; Útočí injektováním dat}
{Červ; Trojský kůň; Útok hrubou silou; Buffer overflow; SQL injection; XST; JavaScript hijacking}	{Získání jména a hesla; Získání SID}
{Červ; Buffer overflow; SQL injection; XST}	{Získání jména a hesla; Získání SID; Útočí injektováním dat}
{Červ; Trojský kůň; Útok hrubou silou}	{Získání jména a hesla; Získání SID; Útočí na

	protokol}
{Trojský kůň}	{Získání jména a hesla; Získání SID; Útočí na protokol; Využívá sociotechnických metod}
{Červ}	{Získání jména a hesla; Získání SID; Útočí na protokol; Útočí injektováním dat; Prostředník dalších útoků}
{XSS; XSRF; XST; HTTP response splitting; HTTP request smuggling; Session hijacking; JavaScript hijacking; Clickjacking; Phishing; Pharming}	{Vyžaduje JavaScript}
{XSRF; Clickjacking; Phishing; Pharming}	{Vyžaduje JavaScript; Využívá sociotechnických metod}
{XSS; XSRF; XST; HTTP response splitting; HTTP request smuggling; Session hijacking; Pharming}	{Vyžaduje JavaScript; Útočí injektováním dat}
{XSRF; Pharming}	{Vyžaduje JavaScript; Útočí injektováním dat; Využívá sociotechnických metod}
{HTTP response splitting; HTTP request smuggling; Pharming}	{Vyžaduje JavaScript; Útočí na protokol; Útočí injektováním dat}
{HTTP response splitting; HTTP request smuggling}	{Vyžaduje JavaScript; Útočí na protokol; Útočí injektováním dat; Prostředník dalších útoků}
{XSS; XST; Session hijacking; JavaScript hijacking}	{Vyžaduje JavaScript; Získání SID}
{XSS; XST; Session hijacking}	{Vyžaduje JavaScript; Získání SID; Útočí injektováním dat}
{XST; JavaScript hijacking; Phishing; Pharming}	{Vyžaduje JavaScript; Získání jména a hesla}
{Phishing; Pharming}	{Vyžaduje JavaScript; Získání jména a hesla; Využívá sociotechnických metod}
{XST; Pharming}	{Vyžaduje JavaScript; Získání jména a hesla; Útočí injektováním dat}
{Pharming}	{Vyžaduje JavaScript; Získání jména a hesla; Útočí na protokol; Útočí injektováním dat; Využívá sociotechnických metod}
{XST; JavaScript hijacking}	{Vyžaduje JavaScript; Získání jména a hesla; Získání SID}

{XST}	{Vyžaduje JavaScript; Získání jména a hesla; Získání SID; Útočí injektováním dat}
{}	{Vyžaduje JavaScript; Získání jména a hesla; Získání SID; Útočí na protokol; Útočí injektováním dat; Využívá sociotechnických metod; Prostředník dalších útoků}

Tab. 15: Seznam formálních konceptů 6.4

6.5 Analýza kybernetických útoků detekovaných v první polovině dubna 2014

Na závěr je pomocí FKA proveden rozbor reálných útoků z první poloviny dubna 2014. Jako zdroj informací k této analýze posloužily webové stránky hackmageddon.com [46], které obsahuje popis, historii a statistiku detekovaných kybernetických útoků po celém světě. Tabulka obsahuje hodnoty, které je potřeba naškálovat před dalším zpracováním pomocí FKA. Je patrné, že většina útoků je směřována na průmyslová odvětví.

	Typ útoku	Kategorie oběti	Motivace	Misto
Útok na KLAS Telecom	SQL injection	Průmysl	Hactivismus	USA
Útok na Mad Mini	DDOS	Průmysl	Kybernetická kriminalita	USA
Útok na bigmoneyjobs.com	SQL injection	Průmysl	Kybernetická kriminalita	USA
Útok na Kansas interactive Testing Engine	DDOS	Vzdělávání	Kybernetická kriminalita	USA
Útok na Německé emailové účty	Malware	Ostatní	Kybernetická kriminalita	Evropa
Útok na Kaiser Permanente	Malware	Průmysl	Kybernetická kriminalita	USA

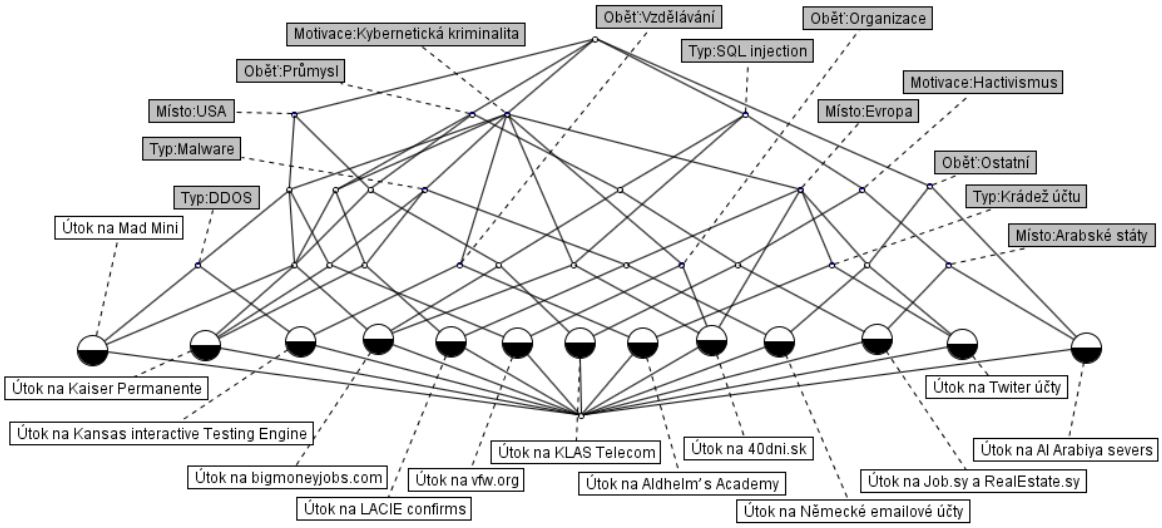
Útok na Al Arabiya severs	SQL injection	Ostatní	Hactivismus	Arabské státy
Útok na Job.sy a RealEstate.sy	SQL injection	Průmysl	Hactivismus	Arabské státy
Útok na vfw.org	Malware	Organizace	Kybernetická kriminalita	USA
Útok na Twiter účty	Krádež účtu	Ostatní	Kybernetická kriminalita	Evropa
Útok na Aldhelm's Academy	Krádež účtu	0	Kybernetická kriminalita	Evropa
Útok na 40dni.sk	SQL injection	0	Kybernetická kriminalita	Evropa
Útok na LACIE confirms	Malware	0	Kybernetická kriminalita	Evropa

Tab. 16: Kontextová tabulka 6.5 před naškálováním

	Typ útoku				Kategorie oběti				Motivace		Místo		
	SQL injection	DDOS	Malware	Krádež účtu	Průmysl	Vzdělávání	Organizace	Ostatní	Hactivismus	Kybernetická kriminalita	Evropa	USA	Arabské stát.
Útok na KLAS Telecom	1	0	0	0	1	0	0	0	1	0	0	1	0
Útok na Mad Mini	0	1	0	0	1	0	0	0	0	1	0	1	0
Útok na bigmoneyjobs.com	1	0	0	0	1	0	0	0	0	1	0	1	0
Útok na Kansas interactive Testing Engine	0	1	0	0	0	1	0	0	0	1	0	1	0
Útok na Německé emailové účty	0	0	1	0	0	0	0	1	0	1	1	0	0
Útok na Kaiser	0	0	1	0	1	0	0	0	0	1	0	1	0

Permanente													
Útok na Al Arabiya severs	1	0	0	0	0	0	0	1	1	0	0	0	1
Útok na Job.sy a RealEstate.sy	1	0	0	0	1	0	0	0	1	0	0	0	1
Útok na vfw.org	0	0	1	0	0	0	1	0	0	1	0	1	0
Útok na Twiter účty	0	0	0	1	0	0	0	1	0	1	1	0	0
Útok na Aldhelm's Academy	0	0	0	1	0	1	0	0	0	1	1	0	0
Útok na 40dni.sk	1	0	0	0	0	0	1	0	0	1	1	0	0
Útok na LACIE confirms	0	0	1	0	1	0	0	0	0	1	1	0	0

Tab. 17: Kontextová tabulka 6.5 po naškálování



Obr. 23: Konceptuální svaz 6.5

Datum útoku	**Popis jednotlivých útoků**
1. dubna	**Útok na KLAS Telecom –** Hackeři ze skupiny NullCrews zaútočili na helpdesk amerického vládního dodavatele KLAS Telecom a došlo k úniku několika účtů a hesel. K útoku využili metodu SQL injection.

1. dubna	**Útok na Mad Mini –** Jedná se o DDOS útok na americký emailový marketingový servis.
2. dubna	**Útok na bigmoneyjobs.com –** Hackeři ze skupiny ProbablyOnion napadli tuto webovou stránku, která slouží k hledání zaměstnání ve Spojených státech. Pomocí metody SQL injection získali přístup k 36 000 online účtům.
2. dubna	**Útok na Kansas Interactive Testing Engine –** Jedná se o DDOS útok na testovací systém studentů ve spojených státech, konkrétně šlo o útok na webovou stránku ksassessments.org.
3. dubna	**Útok na Německé emailové účty –** Tento útok probíhal prostřednictvím botnetů, které využívají malware jako jsou červi. Došlo k němu v Německu, přičemž vyšetřující orgány potvrdily krádež až 18 milionů emailových účtů a hesel, přičemž byli zasaženi všichni významní poskytovatelé Internetu.
3. dubna	**Útok na Kaiser Permanente –** Útok malwarem na americkou společnost zabývající se zdravím, přičemž bylo v ohrožení až 5100 osobních údajů uživatelů.
3. dubna	**Útok na Al Arabiya severs –** Útok na servery ve Spojených arabských emirátech hackerskými týmy NullCrew a TheHorseMenlulz. Došlo k zveřejnění emailových serverů a odkazů na kořenové soubory se zranitelností používanou k průniku do systémů.
4. dubna	**Útok na Job.sy a RealEstate.sy –** Útočník ze skupiny European Cyber Arm napadl dvě syrské webové stránky a získal přístup k 60 000 účtům.
4. dubna	**Útok na vfw.org –** Téměř 55 000 členů spolku amerických armádních veteránů se stalo obětí útoku na jejich webové stránky, přičemž k útoku došlo pomocí malware, a byly odcizeny bezpečnostní kódy a osobní data.
5. dubna	**Útok na Twiter účty –** Při tomto útoku došlo k odcizení účtů k Twitteru ve Velké Británii, kdy útočník použil při útoku falešnou identitu.
8. dubna	**Útok na Aldhelm's Academy –** Při tomto útoku ve Velké Británii došlo k odcizení až 1 700 000 amerických dolarů. Jednalo se útok na banku akademie.
12. dubna	**Útok na 40dni.sk –** Při útoku na tyto slovenské webové stránky s náboženskou tématikou bylo odcizeno na 4800 uživatelských jmen a hesel.

15. dubna	**Útok na LACIE confirms –** Při tomto útoku ve Francii docházelo k přístupu útočníkům k uživatelským citlivým transakcím pomocí malware.

Tab. 18: Popis jednotlivých útoků detekovaných v první polovině dubna 2014

V kontextové tabulce je možné najít celkem 40 konceptů a jejich seznam je následující:

{Útok na KLAS Telecom; Útok na Mad Mini; Útok na bigmoneyjobs.com; Útok na Kansas interactive Testing Engine; Útok na Německé emailové účty; Útok na Kaiser Permanente; Útok na Al Arabiya severs; Útok na Job.sy a RealEstate.sy; Útok na vfw.org; Útok na Twiter účty; Útok na Aldhelm's Academy; Útok na 40dni.sk; Útok na LACIE confirms}	{}
{Útok na KLAS Telecom; Útok na Mad Mini; Útok na bigmoneyjobs.com; Útok na Kansas interactive Testing Engine; Útok na Kaiser Permanente; Útok na vfw.org}	{Místo:USA}
{Útok na Mad Mini; Útok na bigmoneyjobs.com; Útok na Kansas interactive Testing Engine; Útok na Německé emailové účty; Útok na Kaiser Permanente; Útok na vfw.org; Útok na Twiter účty; Útok na Aldhelm's Academy; Útok na 40dni.sk; Útok na LACIE confirms}	{Motivace:Kybernetická kriminalita}
{Útok na Mad Mini; Útok na bigmoneyjobs.com; Útok na Kansas interactive Testing Engine; Útok na Kaiser Permanente; Útok na vfw.org}	{Motivace:Kybernetická kriminalita; Místo:USA}
{Útok na Německé emailové účty; Útok na Twiter účty; Útok na Aldhelm's Academy; Útok na 40dni.sk; Útok na LACIE confirms}	{Motivace:Kybernetická kriminalita; Místo:Evropa}
{Útok na Německé emailové účty; Útok na Al Arabiya severs; Útok na Twiter účty}	{Oběť:Ostatní}
{Útok na Německé emailové účty; Útok na Twiter účty}	{Oběť:Ostatní; Motivace:Kybernetická kriminalita; Místo:Evropa}
{Útok na vfw.org; Útok na 40dni.sk}	{Oběť:Organizace; Motivace:Kybernetická kriminalita}

{Útok na Kansas interactive Testing Engine; Útok na Aldhelm's Academy}	{Oběť:Vzdělávání; Motivace:Kybernetická kriminalita}
{Útok na KLAS Telecom; Útok na Mad Mini; Útok na bigmoneyjobs.com; Útok na Kaiser Permanente; Útok na Job.sy a RealEstate.sy; Útok na LACIE confirms}	{Oběť:Průmysl}
{Útok na KLAS Telecom; Útok na Mad Mini; Útok na bigmoneyjobs.com; Útok na Kaiser Permanente}	{Oběť:Průmysl; Místo:USA}
{Útok na Mad Mini; Útok na bigmoneyjobs.com; Útok na Kaiser Permanente; Útok na LACIE confirms}	{Oběť:Průmysl; Motivace:Kybernetická kriminalita}
{Útok na Mad Mini; Útok na bigmoneyjobs.com; Útok na Kaiser Permanente}	{Oběť:Průmysl; Motivace:Kybernetická kriminalita; Místo:USA}
{Útok na Twiter účty; Útok na Aldhelm's Academy}	{Typ:Krádež účtu; Motivace:Kybernetická kriminalita; Místo:Evropa}
{Útok na Twiter účty}	{Typ:Krádež účtu; Oběť:Ostatní; Motivace:Kybernetická kriminalita; Místo:Evropa}
{Útok na Aldhelm's Academy}	{Typ:Krádež účtu; Oběť:Vzdělávání; Motivace:Kybernetická kriminalita; Místo:Evropa}
{Útok na Německé emailové účty; Útok na Kaiser Permanente; Útok na vfw.org; Útok na LACIE confirms}	{Typ:Malware; Motivace:Kybernetická kriminalita}
{Útok na Kaiser Permanente; Útok na vfw.org}	{Typ:Malware; Motivace:Kybernetická kriminalita; Místo:USA}
{Útok na Německé emailové účty; Útok na LACIE confirms}	{Typ:Malware; Motivace:Kybernetická kriminalita; Místo:Evropa}
{Útok na Německé emailové účty}	{Typ:Malware; Oběť:Ostatní; Motivace:Kybernetická kriminalita; Místo:Evropa}
{Útok na vfw.org}	{Typ:Malware; Oběť:Organizace; Motivace:Kybernetická kriminalita; Místo:USA}
{Útok na Kaiser Permanente; Útok na LACIE confirms}	{Typ:Malware; Oběť:Průmysl; Motivace:Kybernetická kriminalita}
{Útok na Kaiser Permanente}	{Typ:Malware; Oběť:Průmysl;

	Motivace:Kybernetická kriminalita; Místo:USA}
{Útok na LACIE confirms}	{Typ:Malware; Oběť:Průmysl; Motivace:Kybernetická kriminalita; Místo:Evropa}
{Útok na Mad Mini; Útok na Kansas interactive Testing Engine}	{Typ:DDOS; Motivace:Kybernetická kriminalita; Místo:USA}
{Útok na Kansas interactive Testing Engine}	{Typ:DDOS; Oběť:Vzdělávání; Motivace:Kybernetická kriminalita; Místo:USA}
{Útok na Mad Mini}	{Typ:DDOS; Oběť:Průmysl; Motivace:Kybernetická kriminalita; Místo:USA}
{Útok na KLAS Telecom; Útok na bigmoneyjobs.com; Útok na Al Arabiya severs; Útok na Job.sy a RealEstate.sy; Útok na 40dni.sk}	{Typ:SQL injection}
{Útok na bigmoneyjobs.com; Útok na 40dni.sk}	{Typ:SQL injection; Motivace:Kybernetická kriminalita}
{Útok na KLAS Telecom; Útok na Al Arabiya severs; Útok na Job.sy a RealEstate.sy}	{Typ:SQL injection; Motivace:Hactivismus}
{Útok na Al Arabiya severs; Útok na Job.sy a RealEstate.sy}	{Typ:SQL injection; Motivace:Hactivismus; Místo:Arabské státy}
{Útok na Al Arabiya severs}	{Typ:SQL injection; Oběť:Ostatní; Motivace:Hactivismus; Místo:Arabské státy}
{Útok na 40dni.sk}	{Typ:SQL injection; Oběť:Organizace; Motivace:Kybernetická kriminalita; Místo:Evropa}
{Útok na KLAS Telecom; Útok na bigmoneyjobs.com; Útok na Job.sy a RealEstate.sy}	{Typ:SQL injection; Oběť:Průmysl}
{Útok na KLAS Telecom; Útok na bigmoneyjobs.com}	{Typ:SQL injection; Oběť:Průmysl; Místo:USA}
{Útok na bigmoneyjobs.com}	{Typ:SQL injection; Oběť:Průmysl; Motivace:Kybernetická kriminalita; Místo:USA}
{Útok na KLAS Telecom; Útok na Job.sy a RealEstate.sy}	{Typ:SQL injection; Oběť:Průmysl; Motivace:Hactivismus}
{Útok na Job.sy a RealEstate.sy}	{Typ:SQL injection; Oběť:Průmysl; Motivace:Hactivismus; Místo:Arabské státy}
{Útok na KLAS Telecom}	{Typ:SQL injection; Oběť:Průmysl;

	Motivace:Hactivismus; Místo:USA}
{}	{Typ:SQL injection; Typ:DDOS; Typ:Malware; Typ:Krádež účtu; Oběť:Průmysl; Oběť:Vzdělávání; Oběť:Organizace; Oběť:Ostatní; Motivace:Hactivismus; Motivace:Kybernetická kriminalita; Místo:Evropa; Místo:USA; Místo:Arabské státy}

Tab. 19: Seznam formálních konceptů 6.5

ZÁVĚR

Cílem této práce bylo zpracovat poznatky o kybernetických útocích, dále základní pojmy z oblasti teorie svazů, uzávěrových operátorů, věty o pevném bodě a také pojmy z oblasti formální konceptuální analýzy. Aby bylo možné kybernetické útoky kvalitně a srozumitelně popsat, tak bylo zapotřebí nejprve definovat některé ze základních poznatků z oblasti počítačových sítí, zejména modelu ISO/OSI a protokolů na jednotlivých vrstvách. Útočníci často právě těchto protokolů využívají k napadení daného systému. Při popisu samotných útoku v další části práce je nejprve řešena problematika útoků způsobující odepření určité služby. Tyto útoky lze rozdělit na více skupin, z nichž nejzákladnější jsou útoky využívající chyb a vyčerpání systémových prostředků, záplavové typy, reflektivní typy a zesilující typy. Tyto útoky jsou velmi rozšířeny a je možné se s nimi setkat i při dalších typech hrozeb jako je napadení bezdrátové sítě. Útoky způsobující odepření určité služby se velice často vyskytují v distribuované verzi, kde je útok veden z více než jednoho místa. Dalším popsaným typem jsou útoky využívající Man in the middle, tedy útoky, kdy útočník je připojen mezi odesílatelem a příjemcem, přičemž odchytává a případně modifikuje jejich komunikaci. Poté jsou definovány základní typy škodlivého malware, jako je červ nebo trojský kůň. V následující části jsou popsány útoky na protokoly, které slouží k zabezpečení komunikace v bezdrátových sítích, zejména útoky na protokoly WEP, WPA a WPA2. Další část je věnována útokům na aplikační úrovni, které se nejčastěji zaměřují na získání přístupových údajů oběti. V poslední části kapitoly o kybernetických útocích jsou popsány ty, které využívají sociotechnických metod.

Při samotné formální konceptuální analýze kybernetických útoků je využito mnoho poznatků z oblasti teorie svazů, přičemž konceptuální svaz je i jedním z výstupů formální konceptuální analýzy. Při analýze útoků způsobujících odepření služby jsou jako atributy zvoleny typy těchto útoků, možnost výskytu distribuované verze, ale také vrstvy, na jejichž protokolech jsou útoky založeny. Dále při analýze samotných záplavových útoků jsou převzata data o počtu výskytů těchto útoku v roce 2013, z nichž je zřejmé, že se útočníci zaobírali hlavně útoky využívajícími protokoly TPC a HTTP. Útoky na protokoly bezdrátových sítí analyzovány nejsou, jelikož mají velmi podobné vlastnosti. Při analýze útoků MITM byly atributy voleny tak, aby odhalily zejména to, jaké prvky a typy sítí útoky napadají, a které údaje jsou jejich prostřednictvím zfalšovány. Útoky na aplikační úrovni jsou porovnávány společně s útoky využívajícími sociotechnických metod, jelikož spolu

přímo souvisí. Při analýze těchto útoků byly jako atributy zvoleny operace, které se při vytváření útoků provádějí a informace, jenž lze po provedení jednotlivých útoků získat. Na závěr je provedena analýza některých reálných útoků ve světě, z první poloviny dubna 2014. Zde je kladen zřetel zejména na to, na jakých principech jsou útoky založeny a proti komu jsou směřovány. Při tvorbě práce byla vytvořena i většina obrázků, které se v práci vyskytují. Práce nabízí přehledný výpis jednotlivých útoků a jejich rozbor pomocí formální konceptuální analýzy může napomoci k lepšímu zabezpečení počítačových sítí a k vytvoření preventivních opatření.

ZÁVĚR V ANGLIČTINĚ

The aim of this work it was to develop knowledge of cyber attacks, as well as basic concepts of lattice theory, closure operators, fixed point theorems and concepts of formal concept analysis. In order to describe cyber attacks well and clearly, it was necessary to define first some basic knowledge of computer networks, especially the ISO/OSI model and protocols at each layer. The attackers often just use these protocols to attack the system. When describing the attacks themselves in another part of the work is first solved the issue of attacks causing a denial of service. These attacks can be divided into several groups, of which the most basic attacks use mistakes and exhaustion of system resources, flood types, reflective types and reinforcement types. These attacks are widespread and we can meet them during other types of threats such as attack of wireless network. Attacks causing a denial of service very often occur in distributed version where the attack is from more than one location. Another type of attacks is described using Man in the middle, is attacks where the attacker is connected between the sender and the recipient, while he captures and possibly modifies their communication. Afterwards basic types of malicious malware are defined, such as a worm or Trojan horse. Next section describes the attacks on the protocol used to secure communications in wireless networks, especially the attacks on WEP, WPA and WPA2. The following section is devoted to the application on level attacks that are most often focused on obtaining access data victims. In the last part of the chapter about cyber attacks those are descibed that make use of socio-technical methods.

In formal concept analysis of cyber attacksis itself used a lot of knowledge from the field of lattice theory, when the conceptual association is also one of the outputs of formal concept analysis. When analyzing the cause of denial of service attacks are selected as attributes of these types of attacks, the possibility of a distributed version, but also layers on the protocols of which attacks are based. Furthermore, by the analysis of flood attacks themselves are taken data about the number of occurrences of the attacks in 2013, from which it is clear that the attackers were interested mainly in attacks utilizing TPC and HTTP protocols. The attacks on protocols of wireless networks are not analyzed, as they have very similar characteristics. In the analysis of MITM attacks the attributes were chosen so as to reveal particularly, what elements and types of network they attack, and what data are falsified. The attacks on the application level are compared, together with attacks utilizing socio-technical methods, as they are directly related. When analysing these

attacks were as attributes such operations chosen that are carried out by formation of the attacks and information which can be obtained after accomplishing individual attacks. In conclusion, the analysis of some real attacks in the world, from is carried out the first half of April 2014. Attention is placed here in particular to the principles upon which the attacks are based and against whom they are directed. When creating the work most of the images were formed that occur in the work. The work offers a clear listing of individual attacks and their analysis by using formal concept analysis may help to improve the security of computer networks and to develop prevention measures.

SEZNAM POUŽITÉ LITERATURY

[1] JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. 1. vyd. Praha, 2007, 284 s. ISBN 978-80-247-1561-2.

[2] ŠPIDLA, Aleš. KYBERNETICKÉ ÚTOKY: GENEZE ÚTOKŮ – LIFE HACKING. [online]. [cit. 2014-03-10]. Dostupné z: http://www.cybersecurity.cz/data/spidla120404.pdf.

[3] Vstupuje do nové éry kybernetických útoků. Zapálit počítač na dálku? Žádný problém!. In: Electropiknik.cz [online]. 2014-03-08 [cit. 2014-03-10]. Dostupné z: http://www.electropiknik.cz/it-novinky/bezpecnost/vstupuje-do-nove-ery-kybernetickych-utoku-zapalit-pocitac-na-dalku-zadny-problem/2014/03/.

[4] PŘÍHODA, Petr. POČÍTAČOVÉ SÍTĚ [online]. Olomouc, 2007 [cit. 2014-03-10]. Dostupné z: http://phoenix.inf.upol.cz/esf/ucebni/poc_site.pdf.

[5] KLIMEŠ, Cyril. Distribuované systémy: texty pro distanční studium [online]. Ostrava, 2006 [cit. 2014-03-11]. Dostupné z: http://www1.osu.cz/~prochazka/ds/SkriptaKlimes.pdf.

[6] Wi-Fi Wireless LAN - MAC adresa. Wi-fi.unas [online]. 2008 [cit. 2014-04-18]. Dostupné z: http://wi-fi.unas.cz/mac.php.

[7] KABELOVÁ, Alena a Libor DOSTÁLEK. Velký průvodce protokoly TCP/IP a systémem DNS. 5., aktualiz. vyd. Brno: Computer Press, 2008. ISBN 978-80-251-2236-5.

[8] Protokol ARP (Address Resolution Protocol). Technet.microsoft [online]. 2014 [cit. 2014-04-18]. Dostupné z: http://technet.microsoft.com/cs-cz/library/cc758357(v=ws.10).aspx.

[9] DoS a DDoS útoky a ochrana proti nim. Svetsiti.cz [online]. 2008 [cit. 2014-05-18]. Dostupné z: http://www.svetsiti.cz/clanek.asp?cid=DoS-a-DDoS-utoky-a-ochrana-proti-nim-1-742008.

[10] HALLER, Martin. Denial of Service (DoS) útoky. [online]. 2006 [cit. 2014-03-11]. Dostupné z: http://www.lupa.cz/clanky/denial-of-service-dos-utoky-uvod/.

[11] HALLER, Martin. Denial of Service (DoS) útoky: typy využívající chyb a vyčerpání systémových prostředků (1.). Lupa.cz [online]. 2006 [cit. 2014-05-18]. Dostupné z: http://www.lupa.cz/clanky/typy-vyuzivajici-chyb-a-vycerpani-systemovych-prostredku-1/.

[12] HALLER, Martin. Denial of Service (DoS) útoky: typy využívající chyb a vyčerpání systémových prostředků (2.). Lupa.cz [online]. 2006 [cit. 2014-05-18]. Dostupné z: http://www.lupa.cz/clanky/typy-vyuzivajici-chyb-a-vycerpani-systemovych-prostredku-2/#ic=serial-box&icc=text-title.

[13] HALLER, Martin. Denial of Service (DoS) útoky: záplavové typy. Lupa.cz [online]. 2006 [cit. 2014-05-18]. Dostupné z: http://www.lupa.cz/clanky/denial-of-service-dos-utoky-zaplavove-typy/#ic=serial-box&icc=text-title.

[14] HALLER, Martin. Denial of Service útoky: man in the middle, distribuované DoS. Lupa.cz [online]. 2006 [cit. 2014-05-18]. Dostupné z: http://www.lupa.cz/clanky/denial-of-service-utoky-vyuziti-mitm-utoku/#ic=serial-box&icc=text-title.

[15] HALLER, Martin. Denial of Service útoky: reflektivní a zesilující typy. Lupa.cz [online]. 2006 [cit. 2014-05-18]. Dostupné z: http://www.lupa.cz/clanky/denial-of-service-utoky-reflektivni-a-zesilujici-typy/#ic=serial-box&icc=text-title.

[16] BLAŽEK, Zdeněk. Útoky na informační systémy [online]. Praha, 2011 [cit. 2014-03-12]. Dostupné z: BLAŽEK, Zdeněk. Útoky na informa č ní systémy. Praha, 2011. Dostupné z: https://edux.fit.cvut.cz/oppa/MI-KYB/prednasky/kybernalita_-_ii_-_typy_utoku.pdf.

[17] HALLER, Martin. Seriál Odposloucháváme data na přepínaném Ethernetu. Lupa.cz [online]. 2006 [cit. 2014-04-21]. Dostupné z: http://www.lupa.cz/serialy/odposlouchavame-data-na-prepinanem-ethernetu/#ic=serial-box&icc=title.

[18] POSPÍCHAL, Petr. Útoky v počítačových sítích. In: Petr.pospichal.biz [online]. 2008 [cit. 2014-05-06]. Dostupné z: http://petr.pospichal.biz/PDS/utoky-v-pc-sitich.pdf.

[19] What Is the Difference: Viruses, Worms, Trojans, and Bots?. Cisco.com [online]. 2014 [cit. 2014-05-18]. Dostupné z: http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html.

[20] Bezpečnost a Hacking WiFi (802.11) - 3. WEP. Security-Portal.cz [online]. 2009 [cit. 2014-05-14]. Dostupné z: http://www.security-portal.cz/clanky/bezpe%C4%8Dnost-hacking-wifi-80211-3-wep.

[21] Bezpečnost a Hacking WiFi (802.11) - 4. část WPA a WPA2. Security-Portal.cz [online]. 2010 [cit. 2014-05-15]. Dostupné z: http://www.security-portal.cz/clanky/bezpe%C4%8Dnost-hacking-wifi-80211-4-%C4%8D%C3%A1st-wpa-wpa2.

[22] Bezpečnost a Hacking WiFi (802.11) - 5. část Zamietnutie služby (DoS). Security-Portal.cz [online]. 2011 [cit. 2014-05-15]. Dostupné z: http://www.security-portal.cz/clanky/bezpe%C4%8Dnost-hacking-wifi-80211-5-%C4%8D%C3%A1st-zamietnutie-slu%C5%BEby-dos.

[23] Detekce a ochrana před hackerským útoky (2): s jakými typy útoků se lze setkat?. LASEK, Petr. Svetsiti.cz [online]. 2003 [cit. 2014-04-27]. Dostupné z: http://www.svetsiti.cz/clanek.asp?cid=Detekce-a-ochrana-pred-hackerskym-utoky-2-s-jakymi-typy-utoku-se-lze-setkat-2762003.

[24] SQL Injection. Security-Portal.cz [online]. 2005 [cit. 2014-04-14]. Dostupné z: http://www.security-portal.cz/clanky/sql-injection.

[25] Cross-site scripting. TICHÝ, Jan. PHP Guru [online]. 2008 [cit. 2014-04-18]. Dostupné z: http://www.phpguru.cz/clanky/cross-site-scripting.

[26] PEJŠA, Jan. Co je Cross-Site Request Forgery a jak se mu bránit. Zdrojak [online]. 2008 [cit. 2014-04-18]. Dostupné z: http://www.zdrojak.cz/clanky/co-je-cross-site-request-forgery-a-jak-se-branit/.

[27] Cross Site Tracing. Owasp.org [online]. 2013 [cit. 2014-05-03]. Dostupné z: https://www.owasp.org/index.php/Cross_Site_Tracing.

[28] AUGER, Robert. HTTP Response Splitting. Webappsec [online]. 2010 [cit. 2014-04-18]. Dostupné z: http://projects.webappsec.org/w/page/13246931/HTTP%20Response%20Splitting

[29] HTTP Request Smuggling. Owasp.org [online]. 2009 [cit. 2014-05-02]. Dostupné z: https://www.owasp.org/index.php/HTTP_Request_Smuggling.

[30] Session hijacking aneb ukradení session ID. TICHÝ, Jan. Phpguru.cz [online]. 2008 [cit. 2014-05-01]. Dostupné z: http://www.phpguru.cz/clanky/session-hijacking.

[31] XSS + Session hijacking = Hack abclinuxu.cz. Abclinuxu.cz [online]. 2007 [cit. 2014-05-01]. Dostupné z: http://www.abclinuxu.cz/blog/zatial_bez_mena/2007/7/xss-plus-session-hijacking-hack-abclinuxu.cz.

[32] Bezpečnost na webu: přehled útoků na webové aplikace. FERSCHMANN, Petr. Zdrojak.cz [online]. 2008 [cit. 2014-05-01]. Dostupné z: http://www.zdrojak.cz/clanky/prehled-utoku-na-webove-aplikace/.

[33] What is phishing?. Securelist [online]. 2014 [cit. 2014-04-02]. Dostupné z: https://www.securelist.com/en/threats/spam?chapter=85.

[34] Phishing, pharming, vishing, and smishing. Online Security Center [online]. 2014 [cit. 2014-04-03]. Dostupné z: https://security.intuit.com/phishing.html.

[35] HLINĚNÝ, Petr. Uspořádané množiny, Uzávěry. In: [online]. Brno [cit. 2014-04-15]. Dostupné z: http://www.fi.muni.cz/~hlineny/Vyuka/UINF/UInf-lect--5.pdf.

[36] Relace uspořádání. Matematika.cz [online]. 2014 [cit. 2014-04-05]. Dostupné z: http://www.matematika.cz/relace-usporadani.

[37] KUČERA, Radan. *Základy teorie svazů* [online]. [cit. 2014-04-05]. Dostupné z: http://www.math.muni.cz/~kucera/texty/Svazy2003.pdf.

[38] WILLE, R., GANTER, B. *Formal Concept Analysis – Mathematical Foundations*. 1st ed. Springer, 1998. 284 s. ISBN 3-540-62771-5.

[39] KOPKA, Jan. Svazy a booleovy algebry. Ústí nad Labem : Univerzita J. E. Purkyně, 1991. 244 s. ISBN 80-7044-025-2.

[40] SVOZIL, Karl. Quantum logic. Singapore: Springer-Verlag, c1998, xviii, 214 p. ISBN 98-140-2107-5.

[41] BĚLOHLÁVEK, Radim. Konceptuální svazy a formální konceptuální analýza [online]. 2004 [cit. 2014-04-10]. Dostupné z: http://belohlavek.inf.upol.cz/publications/Bel_Ksfka.pdf.

[42] RACHŮNEK, Jiří. Svazy. Olomouc : Univerzita Palackého, 2003. 85 s. ISBN 80-2440-650-0.

[43] KRUPKA, Michal. Formální konceptuální analýza: Metoda zpracování dat s filozofickým pozadím. [online]. 2011 [cit. 2014-04-10]. Dostupné z: http://krupka.inf.upol.cz/seminar/20111006_FCA.pdf.

[44] KÜHR, Tomáš. Formální konceptuální analýza: moderní metoda analýzy dat. [online]. 2011 [cit. 2014-04-10]. Dostupné z: http://www.inf.upol.cz/downloads/ruzne/FCAproSS.pdf.

[45] NSFOCUS: Mid-Year DDOS Thread Report 2013. In: [online]. 2013 [cit. 2014-04-13]. Dostupné z: http://en.nsfocus.com/SecurityReport/2013%20NSFOCUS%20Mid-Year%20DDoS%20Threat%20Report.pdf.

[46] PASSERI, Paolo. 1-15 April 2014 Cyber Attacks Timeline. Hackmageddon.com [online]. 2014 [cit. 2014-05-14]. Dostupné z: http://hackmageddon.com/2014/04/24/1-15-april-2014-cyber-attacks-timeline/#more-9803.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

FKA	Formální Konceptuální Analýza
PAN	Personal Area Network
LAN	Local Area Network
MAN	Metropolian Area Network
WAN	Wide Area Network
CAM	Content Addressable Memory
IP	Internet Protocol
UDP	User Datagram Protocol
TCP	Transmission Control Protocol
HTTP	HyperText Transfer Protocol
FTP	File Transfer Protocol
DNS	Domain Name System
DHCP	Dynamic Host Configuration Protocol
ICMP	Internet Control Message Protocol
ARP	Address Resolution Protocol
DOS	Denial Of Service
PING	Packet InterNet Groper
ISP	Internet Service Provider
DDOS	Distributed Denial Of Service
TTL	Time To Live
MITM	Man In The Middle
SSL	Secure Sockets Layer
TSL	Transport Layer Security
STP	Spanning Tree Protocol

VLAN	Virtual Local Area Network
VTP	Virtual Local Area Network Trunking Protocol
DTP	Dynamic Trunking Protocol
BPDU	Bridge Protocol Data Unit
WEP	Wired Equivalent Privacy
IV	Incialization Vector
ICV	Integrity Check Value
WPA	WiFi Protected Access
TKIP	Temporary Key Integrity Protocol
PTK	Pairwise Transient Key
QOS	Quality Of Service
RTS	Request To Send
CTS	Clear To Send
SQL	Structured Query Langue
XSS	Cross Site Scripting
XSRF	Cross Site Request Forgery
XST	Cross Site Tracing
SID	Session ID
URL	Uniform Resource Locator
JSON	JavaScript Object Notation
SSH	Secure Shell
RAM	Random Access Memory

SEZNAM OBRÁZKŮ

SEZNAM TABULEK