Posudek disertační práce Ing. Mateje Kačice “Analýza útoků na bezdrátové sítě“

Tématem práce, jak již plyne z názvu, byla analýza útoků na bezdrátové počítačové sítě, konkrétně na WiFi sítě. Text se skládá z osmi kapitol a má celkem sto deset stran včetně úvodu a závěru, na kterých doktorand představuje svoji práci a dosažené výsledky. Cílem měl být, jak je deklarováno v úvodu, návrh systému pro analýzu útoků na bezdrátové sítě zahrnující podsystém pro generování takovýchto útoků.

První polovina textu se věnuje počítačovým bezdrátovým sítím, souvisejícím standardům protokolů a zabezpečení komunikace v těchto sítích. Na to navazuje část, která popisuje známé útoky na bezdrátové WiFi sítě, zejména útoky na dostupnost služeb v nich, a jsou uvedeny mechanismy, kterými se lze těmto útokům bránit. Dále je představen nový, doktorandem nalezený útok, využívající zranitelnost známou jako Hole196. Poté následuje popis navrženého a vyvinutého nástroje pro generování útoků. Předpokládá se, že bude využit při analýze možných nových protiopatření na tyto útoky. Text pokračuje popisem nedostatků, které mají nebo mohou mít zmíněná protiopatření a na základě toho je navržen systém pro jejich odstranění. Doktorand zvolil využití reputačních systémů, které by zlepšily schopnost detekce nežádoucího chování na základě zkušeností s jednotlivými prvky systému v minulosti. Navržený reputační systém je popsán tentokrát i formálně. V poslední části textu se doktorand věnuje analýze metrik, které jsou běžně používány pro detekci útoků a ověřuje jejich použitelnost v navrženém reputačním systému. Ukazuje, že některé z nich zde nejsou vhodné a jiné naopak vhodné jsou. V závěru navrhuje některé nové metriky pro tyto účely.

Práce na tématu dala vzniknout celkem třinácti publikacím. Jedná se většinou o příspěvky na mezinárodních odborných konferencích, ale je zde uvedena i jedna časopisecká publikace. Zaměření konferencí i onoho časopisu odpovídají tématu práce. Uvedené publikace pokrývají dosažené výsledky a odborná veřejnost tedy s nimi byla seznámena.

K některým aspektům předloženého textu se vyjádřím spíše kriticky na následujících řádcích. Jádro práce, nebo spíše výsledky, kterými se doktorand prezentuje, je rozprostřeno na různých místech textu. Očekával bych, jak je dle mého názoru obvyklé, že výsledky budou odděleny výrazněji v druhé části textu po shrnutí současného stavu. V disertaci by také měl být vlastní přínos popsán pečlivěji a formálněji, než jak jej představuje doktorand. Například nástroj pro generování útoků, který je jedním z výsledků doktorandova snažení, je popsán spíše vágně. Za stěžejní část práce považuji tu o použití principů důvěry a reputace pro zkvalitnění identifikace útoků. Zde se objevují na několika stranách jisté matematické definice, kterými je uvedeno fungování navrženého reputačního systému, ale i zde budu mít několik připomínek.

V následujících bodech zmíním některé otázky a nedostatky konkrétněji.

- Práce s literaturou a její citace je vesměs v pořádku, ale například na straně 51 uvádíte, že ‘Z několika článků plyne, že …’ bez dalšího citování.
- Reputační systémy byly hojně zkoumány v minulých letech a desetiletích a proto bych očekával pozornější rozbor dosaženého stavu v této oblasti. To, co bylo doktorandem vytvořeno, lze dle mého názoru za reputační systém považovat, ale patří spíš k jednodušším.
- Důvěra je na straně 79 definována jako symetrická a reflexivní. Platí toto ale vždy? Musí mít vždy prvek systému důvěru ve své schopnosti a musí být vždy důvěra opětována?

K formálnímu modelu mám následující poznámky.

- V definici 6.2 na stran 77 je uvedena posloupnost, která je zapsána tak, jak obvykle zapisujeme množiny.
- Definice důvěry na straně 84 je podivná. Jednak píšete, že riziko události je interval, ale zde má být asi prvkem z intervalu, a dále mi není jasné, jak je hodnota Rs, která vystupuje ve vztahu 6.9 definována. Je to hodnota z intervalu <-1,1>? Navíc je otázkou, co tedy reprezentuje riziko, Rs, nebo re? Také by bylo vhodné představit, o pravděpodobnost jakého jevu se jedná. Co znamená, že pravděpodobnost vyjádřená hodnotou re je například 0.3?
- Senzitivita systému je na straně 85 definována jako exponenciální funkce a později se uvádí, že se tato citlivost jednou za den upravuje. Pravděpodobně se tedy mění základ této funkce, ale v textu není zmíněno jak. Jelikož se jedná o jeden z důležitých parametrů pro fungování reputačního systému, navrhuji toto jako téma k diskusi.

Vzhledem k tomu, že Ing. Kačic během zpracovávání tématu disertační práce prezentoval novou zranitelnost a dále díky tomu, že prezentovaný systém využívající reputaci systém byl experimentálně ověřen a bylo potvrzeno, že přináší zlepšení, doporučuji tuto práci k obhajobě s tím, že přepokládám, že doktorand se vyjádří k mnou uvedeným připomínkám.

V Brně dne 18.8.2018 doc. Ing. František Zbořil Ph.D.