FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Ing. Josef Kokeš
Student:	Martin Šutovský
Název práce:	Bezpečnostní analýza bezklíčového vstupu Tesla Model 3
Obor / specializace:	Bezpečnost a informační technologie
Vytvořeno dne:	26. května 2021

Hodnotící kritéria

1. Splnění zadání

[1] zadání splněno
▸ **[2] zadání splněno s menšími výhradami**
[3] zadání splněno s většími výhradami
[4] zadání nesplněno

Zadání práce je splněno, ale samotný text je velmi zmatečný. Jen na jeho základě se nedá spolehlivě určit, do jaké míry zadání splněno bylo, ale s dodatečnými informacemi, které mi byly prezentovány, jsem o splnění přesvědčen. Chápu důvody, které k té zmatečnosti vedly, ale je to škoda - domnívám se, že i tak bylo možné text práce formulovat tak, aby z něj lépe vyplynulo, co vlastně student udělal.

2. Písemná část práce

40 / 100 (F)

Textová stránka práce je bohužel dosti slabá. Podílí se na tom několik faktorů, z toho dva velmi výrazně - použití anglického jazyka a snaha o zodpovědnou práci s nalezenými zranitelnostmi, včetně nutnosti dodržet NDA.

Po jazykové stránce není práce dobrá. Vedle běžných chyb, jako je nevhodná práce s členy a předložkami nebo špatné tvary sloves, jde zejména o celkovou velmi nízkou srozumitelnost. Částečně je daná českou/slovenskou stavbou pro anglické věty, ale mnohdy je text nesrozumitelný i po otrockém překladu. Například v kapitole 4.4 student píše, že komunikace s vozidlem není šifrovaná a zachycené packety se zdají toto podporovat. Zároveň se ale v posledním odstavci na str. 34 dočteme, že probíhá výměna dat za účelem vytvoření šifrované komunikace. Kapitola 6.2.1 v první větě hovoří o tom, že komunikace je nešifrovaná, ve třetí, že je šifrovaná. Kapitola 6.1 říká, že pro provedení více než jen replay útoku by útočník musel zvrátit šifrovací proces. Jak to tedy je? Kapitole 6.2.5 vůbec nerozumím, text při nejlepší vůli chápu jako "Náhodné adresy mohou zlepšit bezpečnost, protože je Man-in-the-Middle (MITM) nemůže zkopírovat. Protože Tesla nepoužívá statické adresy, může útočník adresu Tesly zkopírovat a vydávat se za ni," což mi nedává žádný smysl.

Dále je v textu řada tvrzení, která mi připadají přinejmenším neúplná, ne-li úplně nesprávná. Několikrát se například opakuje, že MITM může způsobit odepření služby tím, že zahodí packety uživatele. Není však vůbec jasné, jak to prakticky udělá - jak zabrání tomu, aby packety kromě útočníka nedostalo také samotné vozidlo? Tvrzení v kapitole 7.1 ve smyslu, že "útočníkovi stačí prolomit šifrování a potom má volný přístup", je platné vždy a všude. Některé kapitoly (2.4, 5, 6, 7, 8) jsou stručné na hranici únosnosti a pod hranicí srozumitelnosti, z části kvůli potřebě část zjištění utajit. Což samo o sobě chápu, ale toto utajení se nesmí udělat tak brutálně, že zbylý text ztratí smysl!

Ve srovnání s výše uvedeným jsou drobností nedostatky technického rázu, jako že abstrakt je rozpadlý na dvě stránky, že často neexistuje spojovací text mezi kapitolou a její první podkapitolou, že se v textu běžně používají mínusy na místě pomlček, že seznam použitých zkratek měl být seřazen nebo že popsat soubor GATT.json na přiloženém médiu jako "the file with JSON file" opravdu nic nevysvětluje.

3. Nepísemná část, přílohy 30/100 (F)

Nepísemná část práce prakticky neexistuje. K textu je přiložen soubor GATT.json, o kterém není k dispozici žádná použitelná informace, a dva soubory se zachycenými packety, o kterých sice víme, kterými příkazy byly získány, ale nic o jejich obsahu nebo o kontextu, ve kterém vznikly. Tím pádem ovšem není jasné, co z nich máme vyčíst nebo k čemu je použít.

4. Hodnocení výsledků, jejich využitelnost 100/100 (A)

Výsledky práce je velmi obtížné hodnotit, protože je tu obrovský nepoměr mezi tím, čeho student skutečně dosáhl, a tím, co do práce zařadil.

Pokud bych měl hodnotit výsledky podle toho, co je veřejně prezentováno, nepovažoval bych je za dostatečné. Samotná zjištění mi připadají zajímavá a potenciálně i velmi závažná, takže pokud je výrobce vozu opraví, bude to jen dobře. Jsou ale tak nedostatečně a zmatečně popsána, že je obtížné k nim hledat důvěru - a i kdyby čtenář tu důvěru mít chtěl, stejně nebude vědět, čemu vlastně chce důvěřovat. Chybí také jakékoliv doporučení pro uživatele vozidla, na co by si měl dávat pozor nebo co by měl pro zmírnění rizika dělat.

Na druhé straně stojí to, co student dokázal a do práce neuvedl. Tyto výsledky mi byly prezentovány a na tomto základě mohu prohlásit, že s jejich nezveřejněním souhlasím,

protože i kdyby nebylo NDA, jsou jejich potenciální důsledky natolik závažné, že se prostě nemohou zveřejnit dříve, než výrobce chyby opraví. Nebylo by správné studenta penalizovat za to, že tyto velmi závažné chyby nalezl a pak je v rámci responsible disclosure neuvedl přímo v práci.

Celkové hodnocení 75 /100 (C)

Celkové hodnocení práce je v tomto případě velkým oříškem. Odevzdaná podoba práce není dobrá, ani po textové stránce, ani po stránce dosažených výsledků. Na druhou stranu je třeba mít na vědomí, že ty skutečně významné výsledky jsou takového charakteru, že by bylo extrémně nebezpečné je publikovat předtím, než budou opraveny a oprava distribuována. Tomu bylo podřízeno i brutální zmasakrování značné části textu, který je kvůli tomu v kapitolách 5-8 hluboko pod úrovní, kterou mají jiné práce. To ale do hodnocení nezařazuji, není chybou studenta, že výsledky analýzy jsou tak zničující, že je nejde zveřejnit. Naproti tomu ale nemohu zavírat oči nad celkově špatnou kvalitou textu (rozebráno výše) a velmi slabou odevzdanou netextovou částí práce - zvlášť s ohledem na to, že právě to budou mít k dispozici další čtenáři. Po zhodnocení všech těchto faktorů se přikláním k známce C-dobře, ovšem s poznámkou, že samotnou odvedenou práci považuji za výbornou.

Otázky k obhajobě

1) Máte nějaká doporučení pro majitele vozu, co by měl dělat, aby rizika plynoucí z vámi nalezených hrozeb omezil?

Instrukce

Splnění zadání

Posuďte, zda předložená ZP dostatečně a v souladu se zadáním obsahově vymezuje cíle, správně je formuluje a v dostatečné kvalitě naplňuje. V komentáři uveďte body zadání, které nebyly splněny, posuďte závažnost, dopady a případně i příčiny jednotlivých nedostatků. Pokud zadání svou náročností vybočuje ze standardů pro daný typ práce nebo student případně vypracoval ZP nad rámec zadání, popište, jak se to projevilo na požadované kvalitě splnění zadání a jakým způsobem toto ovlivnilo výsledné hodnocení.

Písemná část práce

Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Dále posuďte, zda předložená ZP je po věcné stránce v pořádku, případně vyskytují-li se v práci věcné chyby nebo nepřesnosti.

Zhodnoťte dále logickou strukturu ZP, návaznosti jednotlivých kapitol a pochopitelnost textu pro čtenáře. Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 26/2017, článek 3.

Posuďte, zda student využil a správně citoval relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami. Zhodnoťte, zda převzatý software a jiná autorská díla, byly v ZP použity v souladu s licenčními podmínkami.

Nepísemná část, přílohy

Dle charakteru práce se případně vyjádřete k nepísemné části ZP. Například: SW dílo – kvalita vytvořeného programu a vhodnost a přiměřenost technologií, které byly využité od vývoje až po nasazení. HW – funkční vzorek – použité technologie a nástroje, Výzkumná a experimentální práce – opakovatelnost experimentů.

Hodnocení výsledků, jejich využitelnost

Dle charakteru práce zhodnoťte možnosti nasazení výsledků práce v praxi nebo uveďte, zda výsledky ZP rozšiřují již publikované známé výsledky nebo přinášející zcela nové poznatky.

Celkové hodnocení

Shrňte stránky ZP, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení nemusí být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích. Obecně platí, že bezvadně splněné zadání je hodnoceno klasifikačním stupněm A.