Posudek vedoucího závěrečné práce

Název práce:	IoT bezpečnost - pokus o napadení kamery
Jméno autora:	Martin Kubeša
Typ práce:	bakalářská
Fakulta:	Fakulta elektrotechnická (FEL)
Katedra:	Katedra měření
Vedoucí práce:	Ing. Josef Kokeš
Pracoviště vedoucího práce:	ČVUT FIT, katedra informační bezpečnosti

Zadání: Průměrně náročné

Náročnost zadání spočívá primárně v tom, že řada důležitých informací není dopředu známa a mnohdy je možné je jen odhadovat, ne stoprocentně určit. Student musí k problematice přistupovat kreativně a hledat možnosti, jak překonat bezpečnostní opatření vytvořená výrobcem, aniž by měl od výrobce k tomuto jakoukoliv podporu nebo dokumentaci. V rámci těchto omezení lze však k práci přistupovat různě. Student zvolil přístup spočívající zejména na existujících nástrojů, který hodnotím jako relativně méně náročný, nakonec ale stejně musel pracovat vlastními silami.

Splnění zadání: Splněno

Celkově vzato student zadání splnil. Mohl jít i více do hloubky a zaměřit se na méně přístupné aspekty bezpečnosti, ale z pohledu požadovaných schopností bakalanta je jeho řešení v pořádku.

Aktivita a samostatnost: D - uspokojivě

S aktivitou a samostatností studenta jsem nebyl v průběhu práce příliš spokojen, obě patřily k těm horším a práce vznikala pomalu a ve velkých bolestech. Studentův výkon byl v průběhu času značně nevyrovnaný, střídala se období aktivity a období, kdy zřejmě žádná činnost neprobíhala. Zejména zpočátku jsem také pozoroval nadprůměrnou nejistotu studenta v tom, co vlastně chce dělat a jak toho chce dosáhnout. Je však třeba upozornit na to, že na tom mají podíl (možná značný podíl) objektivní zdravotní důvody. Také koronavirová situace nenabízela zrovna příznivé podmínky. V průběhu posledních 3 měsíců se však celá situace významně zlepšila.

Odborná úroveň: C - dobře

Student v zásadě postupoval tak, jak se při obdobných analýzách běžně postupuje, v tomto směru nemám připomínky. Na snížené známce za tuto kategorii se podepisuje zejména kapitola 2, jak po obsahové stránce, tak po stránce použitých zdrojů, a také volba studenta jít spíše už vyzkoušenými cestami než hledat nové. Výsledkem je práce, která neurazí, ale také neohromí.

Podrobnější výhrady:

Kapitola "Základní pojmy" působí poněkud rozpačitě. V první řadě není jasné, jestli je vůbec v bakalářské práci potřeba, aspoň ve své stávající podobě. Volba pojmů a jejich posloupnost není ani

po přečtení práce vždy srozumitelná. Běžně je popsána jen velmi omezená část dané problematiky bez vysvětlení, proč zrovna tato část (např. u OSI modelu je volba vysvětlena, u TLS protokolu ne). Popisy samotné jsou v řadě případů osekané až do takové míry, že už ani nejsou správné (např. popis reverse shellu úplně pomíjí "reverse" část a fakticky odpovídá spíše "remote shellu"). Zcela nesrozumitelné pak je, proč některé pojmy jsou vysvětleny pouze citací z Wikipedie, když ostatní student popsal vlastními slovy. Za krajně nevhodné považuji vysvětlit pojem "salted hash" pouze odkazem do dosti vzdálené části textu - buď nejde o základní pojem a pak v této kapitole nemá co dělat, nebo měl být aspoň stručně vysvětlen už zde. Celkově bych považoval za vhodnější kapitolu úplně vynechat, v ní definované pojmy definovat až v místě, kde jsou skutečně použity, a nahradit ji kapitolou obecně popisující postupy bezpečnostních analýz.

Tvrzení z kapitoly 4.5, že TLS certifikáty "nejsou zásadní pro důvěrnost přenosu ale jsou důležité pro ověření důvěryhodnosti serveru", je hodně zavádějící a snadno ve čtenáři vyvolá mylný dojem o bezpečnosti. Certifikát slouží k ověření identity serveru, tedy zejména toho, zda se uživatel nepřipojuje k falešnému serveru, který se jenom tváří jako pravý. V tomto smyslu je ovšem správná práce s certifikátem pro zajištění důvěrnosti nezbytná, byť nepřímo.

Z metodologického hlediska považuji za nedostatečně prověřený myšlenkový skok z bodu A "ke kameře existují volně dostupné zdrojové kódy" do bodu B "kamera skutečně tyto volně dostupné zdrojové kódy používá, a to právě v té dostupné verzi". Závěry odvozené z předpokladu, že B platí, tak nejsou spolehlivé (kapitola 5.2.2).

Doporučení na opravu nalezených zranitelností cílí výhradně na možnosti výrobce kamery. Chybí mi aspoň stručné doporučení pro uživatele, co má dělat, aby rizika zmenšil - uživatel své chování změnit může hned, reakce výrobce může zabrat delší čas, přijde-li vůbec. Doporučení pro výrobce jsou v některých případech zbytečně přísná (není důvod pro *asymetrické* šifrování obsahu paměťové karty, kap. 5.2.1, slabá politika hesel je poměrně dobře kompenzována omezením počtu pokusů o přihlášení za jednotku času, kap. 5.2.10, slabý RSA klíč nemusí vadit, protože jde jen o doplněk k ochraně přenášených dat protokolem TLS, kap. 5.2.11).

Formální a jazyková úroveň: B - velmi dobře

Nalezl jsem několik překlepů (viditelná je zvlášť copy&paste chyba ve všech kapitolách 5.2.x), chybných čárek, u některých cizích pojmů bych osobně volil jiný rod než student. Text často používá cizí výrazy i v situacích, kdy by nemusel a neměl (výrazy jako "fixní", "zafixovat" v kapitole 3 apod.). Netěší mě použití budoucího času pro odkazování na pozdější části práce. Slovo "nejideálnější" neexistuje. Celkově ale nejde o větší výskyt jazykových nedostatků než na jaké jsme u podobných prací zvyklí.

Kapitoly jsou organizovány tak, že mezi částí a podčástí není žádný spojovací text, např. kapitola 2 a 2.1 nebo 2.1 a 2.1.1. Kapitola 7 měla být spíše přílohou.

Na straně 55 dole je dvakrát bod 2 a ani jednou bod 1. Na straně 55 nahoře je bod "1, 2" (to je jeden bod) a v posloupnosti chybí body 3 a 4.

Organizace přiloženého média mi připadá podivná.

Výběr zdrojů, korektnost citací: C - dobře

Zdrojů student používá hodně, většinou ale vzhledem k předmětné problematice spíš okrajových (nicméně, když už se do daných oblastí pustil, tak nutných). Očekával bych větší zaměření na literaturu k penetračnímu testování, řada možných zdrojů byla uvedena už v zadání.

Citace samotné jsou vesměs v pořádku, bylo by dobré si více pohlídat umístění před nebo za tečku. Cizí obrázky by měly být citovány i přímo v popisu obrázku, nikoliv pouze v textu (obrázek 1.1 a 1.2).

Celkové hodnocení:

I když výhrady uvedené výše mohou působit hrozivě, není práce vůbec špatná. Student si zvolil black-box bezpečnostní analýzu, což je skoro vždy těžké a nikdy není dopředu známo, co se podaří nebo nepodaří zjistit. Navíc nejde o oblast, kde by se dal jednoduše převzít a aplikovat nějaký standardní postup, vždy je zde velký vliv osobní zkušenosti a schopnosti odhadu, na co se zaměřit. V tomto smyslu je to, že student práci dotáhl až do konce, důkazem, že tyto zkušenosti a schopnosti získal. Co se týče konkrétních výsledků, mohu mít výhrady k dílčím aspektům jeho postupu, ale nelze upřít, že požadované cíle splnil způsobem, který odpovídá úrovni kladené na bakalářské práce. Že se nepodařilo nalézt žádnou katastrofální zranitelnost, to není jeho chyba, naopak je to spíš uklidňující pro uživatele kamery.

Práci doporučuji k obhajobě a hodnotím stupněm C - dobře.