

# GYMNASIUM JANA KEPLERA

Parléřova 2/118, 169 00 Praha 6



## Bezpečnostní kamera

Maturitní práce

Autor: Vítek Peterka

Třída: 4.A

Školní rok: 2022/2023

Předmět: Informatika

Vedoucí práce: Bc. Emil Miler

Praha, 2023





**GYMNASIUM JANA KEPLERA**  
*Kabinet informatiky*

## **ZADÁNÍ MATURITNÍ PRÁCE**

*Student:* Robot Karel  
*Třída:* 4.Z  
*Školní rok:* 2020/2021  
*Platnost zadání:* 30. 9. 2021  
*Vedoucí práce:* Šimon Schierreich

*Název práce:* **Název maturitního projektu.**

*Pokyny pro vypracování:*

**Zde popište, čeho se chystáte v práci dosáhnout.**

*Doporučená literatura:*

**Zde bude vedoucím práce doplněna doporučená literatura.**

*URL repozitáře:*

**<https://gitlab.com/gjk/maturitni-projekt>**

---

*vedoucí práce*

---

*student*

*V Praze dne 10. 3. 2021*



## **Prohlášení**

Prohlašuji, že jsem svou práci vypracoval samostatně a použil jsem pouze prameny a literaturu uvedené v seznamu bibliografických záznamů. Nemám žádné námitky proti zpřístupňování této práce v souladu se zákonem č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších předpisů.

V Praze dne 22. března 2023

Vítek Peterka



## **Poděkování**

Děkuji především svému vedoucímu Bc. Emilu Milerovi za podporu a cenné rady při zpracování této práce, především pak za jeho trpělivost a ochotu.

Dále musím poděkovat Vlastimilovi Čejpovi za jeho technickou asistenci a za rady se sázením samotné práce.





## **Abstrakt**

Maturitní práce pojednává o problematice bezpečnostních kamer, nahrávacích zařízení a jejich zabezpečení. Popisuje úskalí běžně dostupných komerčních řešení a navrhuje alternativu v podobě DIY kamery založené na jednodeskovém počítači a vlastním softwaru. Ten umožňuje end-to-end šifrované zálohování videozáznamu na vzdálený server, jakož i živý přenos.

## **Klíčová slova**

bezpečnostní kamera, end-to-end šifrování, nahrávací zařízení, jednodeskový počítač

## **Abstract**

The thesis deals with the issue of security cameras, video recorders and their security. It describes the pitfalls of commonly available commercial solutions and proposes an alternative in the form of a DIY camera based on a single-board computer and custom software. The latter allows end-to-end encrypted backup of video footage on a remote server as well as live streaming.

## **Keywords**

security camera, end-to-end encryption, video recorder, single-board computer



# Obsah

<b>1</b>	<b>Teoretická část</b>	<b>3</b>
1.1	Výrobci bezpečnostních kamer . . . . .	3
1.2	Nejznámější bezpečnostní problémy . . . . .	3
1.2.1	ICSA-17-124-01 . . . . .	3
1.2.2	CVE-2021-36260 . . . . .	3
1.2.3	CVE-2021-33044 . . . . .	4
<b>2</b>	<b>Implementace</b>	<b>5</b>
2.1	Ukázka sekce . . . . .	5
<b>3</b>	<b>Technická dokumentace</b>	<b>7</b>
3.1	Vygenerování klíčů . . . . .	7
3.2	Nastavení serveru . . . . .	7
3.3	Nastavení kamery . . . . .	8
3.4	Sledování živého přenosu . . . . .	8
3.5	Dešifrování a přehrání uložených nahrávek . . . . .	9
	<b>Závěr</b>	<b>11</b>
	<b>Seznam použité literatury</b>	<b>13</b>
	<b>Seznam obrázků</b>	<b>15</b>
	<b>Seznam tabulek</b>	<b>16</b>



# 1. Teoretická část

Bezpečnostní kamery a nahrávací zařízení jsou pro svou povahu častým cílem internetových útočníků. Navzdory tomu jsou běžně komerčně dostupná řešení v odborné komunitě notoricky známá svým špatným zabezpečením. Kromě zpřístupnění samotného obrazu, který kamera vidí, může kompromitované zařízení posloužit útočnickovi i jako vstupní vektor pro další průnik do počítačové sítě. Výrobci často bezpečnostní rizika přehlíží a raději se soustředí na vývoj chytrých funkcí, jako jsou detekce osob a rozpoznání obličejů.

## 1.1 Výrobci bezpečnostních kamer

Podle některých odhadů může svět sledovat až jedna miliarda bezpečnostních kamer. [3] Největšími světovými výrobci jsou pak společnosti Hikvision a Dahua, přičemž dohromady ovládají asi 60 % světového trhu s kamerami. [9] Ve Spojených státech amerických byl oběma firmám z důvodu potenciálních bezpečnostních rizik zakázán prodej nových produktů – obě společnosti jsou státní, vlastněny zcela, respektive z části, Komunistickou stranou Číny. [7] Mezi další významné výrobce patří firmy Bosch, Axis a Uniview. [8]

## 1.2 Nejznámější bezpečnostní problémy

Čínští výrobci jsou nechvalně proslulí bezpečnostními problémy jejich zařízení. Společným jmenovatelem chyb bývá zanedbání běžných bezpečnostních praktik, jako je hashování hesel nebo sanitace vstupu od uživatele.

### 1.2.1 ICSA-17-124-01

Nejznámější bezpečnostní chybou v Hikvision produktech je takzvaný backdoor. Jedná se o chybu vedenou pod označením ICSA-17-124-01. Po zadání speciální hodnoty parametru do URL adresy bylo možné v některých verzích firmwaru zcela obejít autorizační mechanismus a rovnou přistupovat k citlivým datům, jako je například konfigurační soubor obsahující heslo do uživatelského rozhraní. [2] Ačkoliv výrobce uvádí, že se jednalo o přebytek z testovací fáze vývoje, toto vysvětlení není experty považováno za pravděpodobné a jedná se tak spíše o záměrně umístěná zadní vrátka. [5]

### 1.2.2 CVE-2021-36260

Další ze známých chyb v kamerách a nahrávacích zařízeních Hikvision je CVE-2021-36260. Nedostatečná validace vstupu vede v některých verzích firmwaru ke spuštění kódu přímo na daném zařízení. Tato chyba může postihovat až více než 100 milionů produktů. [6] Jedná se o zvlášť závažný problém, neboť útočník může díky této chybě zcela převzít kontrolu nad chováním systému. [4]

### **1.2.3 CVE-2021-33044**

Bezpečností problémy se nevyhly ani firmě Dahua. Chyba vedená jako CVE-2021-33044 způsobuje, podobně jako ICSA-17-124-01, možnost kompletně obejít mechanismus přihlašování uživatelů a přistupovat ke kameře s plným oprávněním. Je tedy možné bez znalosti platných přihlašovacích údajů sledovat záznam kamery a měnit její nastavení. [1]

## 2. Implementace

Druhá kapitola obsahuje detailní informace o tom, jak probíhala implementace. Zde se objeví zdůvodnění výběru technologií, řešení problémů, na které jste narazili, informace o použitých knihovnách apod. Pochvalte se, nikdo to za Vás neudělá. Přiznejte chyby, není to ostuda.

### 2.1 Ukázka sekce

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetur id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetur adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

Fusce mauris. Vestibulum luctus nibh at lectus. Sed bibendum, nulla a faucibus semper, leo velit ultricies tellus, ac venenatis arcu wisi vel nisl. Vestibulum diam. Aliquam pellentesque, augue quis sagittis posuere, turpis lacus congue quam, in hendrerit risus eros eget felis. Maecenas eget erat in sapien mattis porttitor. Vestibulum porttitor. Nulla facilisi. Sed a turpis eu lacus commodo facilisis. Morbi fringilla, wisi in dignissim interdum, justo lectus sagittis dui, et vehicula libero dui cursus dui. Mauris tempor ligula sed lacus. Duis cursus enim ut augue. Cras ac magna. Cras nulla. Nulla

egestas. Curabitur a leo. Quisque egestas wisi eget nunc. Nam feugiat lacus vel est. Curabitur consetetur.

Suspendisse vel felis. Ut lorem lorem, interdum eu, tincidunt sit amet, laoreet vitae, arcu. Aenean faucibus pede eu ante. Praesent enim elit, rutrum at, molestie non, nonummy vel, nisl. Ut lectus eros, malesuada sit amet, fermentum eu, sodales cursus, magna. Donec eu purus. Quisque vehicula, urna sed ultricies auctor, pede lorem egestas dui, et convallis elit erat sed nulla. Donec luctus. Curabitur et nunc. Aliquam dolor odio, commodo pretium, ultricies non, pharetra in, velit. Integer arcu est, nonummy in, fermentum faucibus, egestas vel, odio.

Sed commodo posuere pede. Mauris ut est. Ut quis purus. Sed ac odio. Sed vehicula hendrerit sem. Duis non odio. Morbi ut dui. Sed accumsan risus eget odio. In hac habitasse platea dictumst. Pellentesque non elit. Fusce sed justo eu urna porta tincidunt. Mauris felis odio, sollicitudin sed, volutpat a, ornare ac, erat. Morbi quis dolor. Donec pellentesque, erat ac sagittis semper, nunc dui lobortis purus, quis congue purus metus ultricies tellus. Proin et quam. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent sapien turpis, fermentum vel, eleifend faucibus, vehicula eu, lacus.



## 3. Technická dokumentace

Projekt je rozdělen na tři části: kamera, server a prohlížečová aplikace pro živý přenos.

### 3.1 Vygenerování klíčů

Kód pro generování klíčů se nachází v adresáři `utils`. Následující ukázky předpokládají, že se v tomto adresáři nacházíte i vy.

Klíče lze vygenerovat jednoduše za použití scriptu, takto: `python generate_keys.py`.

Klíče jsou čtyři, dva (privátní a veřejný) pro kameru a dva pro příjemce obrazu z kamery. Uloží se do souborů `camera_private.key`, `camera_public.key`, `receiver_private.key` a `receiver_public.key`.

Aby šifrování bylo smysluplné, privátní klíče musí být uchovávány na bezpečném místě (tedy určitě ne na stejném zařízení, jako na kterém poběží server).

### 3.2 Nastavení serveru

Kód pro server se nachází v adresáři `server`. Následující ukázky předpokládají, že se v tomto adresáři nacházíte i vy.

Před spuštěním je nejprve potřeba vytvořit konfigurační soubor `server_config.json`. V něm musí být definovány tyto hodnoty:

- `max_recording_file_size`: Maximální velikost jednoho souboru se záznamem z kamery v bytech
- `max_recording_files`: Maximální počet souborů se záznamem, které budou najednou uloženy na disku
- `records_directory`: Adresář, do kterého se budou průběžně ukládat soubory se záznamem
- `server_port`: Port, na kterém bude server poslouchat

Konfigurační soubor může vypadat například takto:

```
{
  "max_recording_file_size": 20000000,
  "max_recording_files": 5,
  "records_directory": "records",
  "server_port": 8765
}
```

S takovýmto konfiguračním souborem tedy bude server poslouchat na portu 8765 a záznam z kamery ukládat do adresáře `records`. Jeden soubor bude mít maximálně 20 Mb a zároveň bude uloženo maximálně 5 souborů. Velikost adresáře `records` tedy nikdy nepřesáhne  $5 * 20 \text{ Mb} = 100 \text{ Mb}$ .

Server lze spustit takto: `python receiver_server.py`.

### 3.3 Nastavení kamery

Kód pro kameru se nachází v adresáři `camera`. Následující ukázky předpokládají, že se v tomto adresáři nacházíte i vy.

Před spuštěním je nejprve potřeba vytvořit konfigurační soubor `camera_config.json`. V něm musí být definovány tyto hodnoty:

- `receiver_public_key_hex`: Veřejný klíč příjemce obrazu z kamery (zkopírováno z `receiver_public.key`)
- `camera_private_key_hex`: Privátní klíč kamery (zkopírováno z `camera_private.key`)
- `video_height`: Výška přenášeného obrazu v pixelech
- `video_width`: Šířka přenášeného obrazu v pixelech. Kombinace výšky a šířky musí být podporována hardwarem připojeného kamerového modulu
- `video_quality`: Číslo od 0 do 4, čím vyšší, tím nižší úroveň komprese
- `server_address`: Adresa serveru

Konfigurační soubor může vypadat například takto:

```
{
  "receiver_public_key_hex": "abc123",
  "camera_private_key_hex": "cba321",
  "video_height": 972,
  "video_width": 1296,
  "video_quality": 4,
  "server_address": "ws://192.168.0.88:8765"
}
```

S takovýmto konfiguračním souborem tedy bude kamera posílat obraz nejvyšší kvality o rozlišení 972 x 1296 na server na adrese `ws://192.168.0.88:8765`. Obraz bude šifrován zadanými klíči.

Odesílání obrazu lze spustit takto: `python camera_client.py`.

### 3.4 Sledování živého přenosu

Kód prohlížečové aplikace pro živé sledování se nachází v adresáři `viewer-live`. Následující ukázky předpokládají, že se v tomto adresáři nacházíte i vy.

Aplikaci lze spustit příkazem `npm run dev`. Po spuštění bude vyžadovat zadání tří hodnot:

- Camera public key (hex): Veřejný klíč kamery (zkopírováno z `camera_public.key`)
- Viewer private key (hex): Privátní klíč příjemce obrazu z kamery (zkopírováno z `receiver_private.key`)
- Server address: Adresa serveru, na který kamera posílá obraz

Po zadání hodnot a kliknutí na tlačítko Start stream začne živý přenos.

### 3.5 Dešifrování a přehrání uložených nahrávek

Šifrované nahrávky ze serveru nejprve přeneste na zařízení, na kterém jsou uloženy privátní klíče, abyste je mohli dešifrovat.

Kód pro dešifrování nahrávek se nachází v adresáři `utils`. Následující ukázky předpokládají, že se v tomto adresáři nacházíte i vy.

Dešifrování lze provést za pomoci scriptu, takto: `python decryptor.py nahravka.h264.enc`. Script načte soubory `camera_public.key` a `receiver_private.key` a dešifruje nahrávku `nahravka.h264.enc`. Výsledek uloží do souboru `nahravka.h264` (odstraní příponu `.enc`).

Dešifrovaná nahrávka je stream H.264 framů. Lze ji přehrát například pomocí programu `ffplay`: `ffplay nahravka.h264`.

Pro přehrání v běžných přehrávačích (VLC, apod.) je třeba stream zabalit do nějakého kontejneru. To lze udělat například pomocí programu `ffmpeg`: `ffmpeg -i nahravka.h264 -c copy nahravka.mp4`

Před zabalením do kontejneru je také možné několik nahrávek spojit do jedné: `cat nahravka1.h264 nahravka2.h264 nahravka3.h264 > spojena.h264`



# Závěr

Závěr obsahuje shrnutí práce a vyjadřuje se k míře splnění jejího zadání. Dále by se zde mělo objevit sebehodnocení studenta a informace o tom, co nového se naučil a jak vnímal svou práci na projektu.



# Seznam použité literatury

- [ ] NVD - CVE-2021-33044. URL: <https://nvd.nist.gov/vuln/detail/CVE-2021-33044>.
- [23] *Hikvision cameras: CISA*. Břez. 2023. URL: <https://www.cisa.gov/news-events/ics-advisories/icsa-17-124-01>.
- [Cos19] Elly Cosgrove. *One billion surveillance cameras will be watching around the world in 2021, a new study says*. Pros. 2019. URL: <https://www.cnbc.com/2019/12/06/one-billion-surveillance-cameras-will-be-watching-globally-in-2021.html>.
- [IP21] Watchful IP. *Unauthenticated Remote Code Execution (RCE) vulnerability in Hikvision IP camera/NVR firmware (CVE-2021-36260)*. Zář. 2021. URL: <https://watchfulip.github.io/2021/09/18/Hikvision-IP-Camera-Unauthenticated-RCE.html>.
- [Ipv17] Ipvideomarket. *Hikvision Backdoor exploit*. Zář. 2017. URL: <https://ipvm.com/reports/hik-exploit>.
- [Ipv21] Ipvideomarket. *Hikvision has "highest level of critical vulnerability," impacting 100+ million devices*. Zář. 2021. URL: <https://ipvm.com/reports/hikvision-36260>.
- [Pag22] Carly Page. *US government bans Huawei, ZTE and hikvision tech over 'unacceptable' spying fears*. Lis. 2022. URL: <https://techcrunch.com/2022/11/28/fcc-huawei-zte-hikvision-hytera-dahua-ban>.
- [Pao20] William Pao. *The top 10 biggest companies in video surveillance*. Lis. 2020. URL: <https://www.asmag.com/showpost/31985.aspx>.
- [RM22] Research a Markets. *Global surveillance camera market to 2027 with Chinese companies such as Hikvision and dahua dominating the market*. Zář. 2022. URL: <https://www.globenewswire.com/news-release/2022/09/29/2524920/28124/en/Global-Surveillance-Camera-Market-to-2027-with-Chinese-Companies-Such-as-Hikvision-and-Dahua-Dominating-the-Market.html>.





# Seznam obrázků

# Seznam tabulek