OEM Finder

Hunting Vulnerable OEM IoT Devices at Scale

Asuka Nakajima
NTT Secure Platform Laboratories

# whoami

Asuka Nakajima

@AsuNa_jp

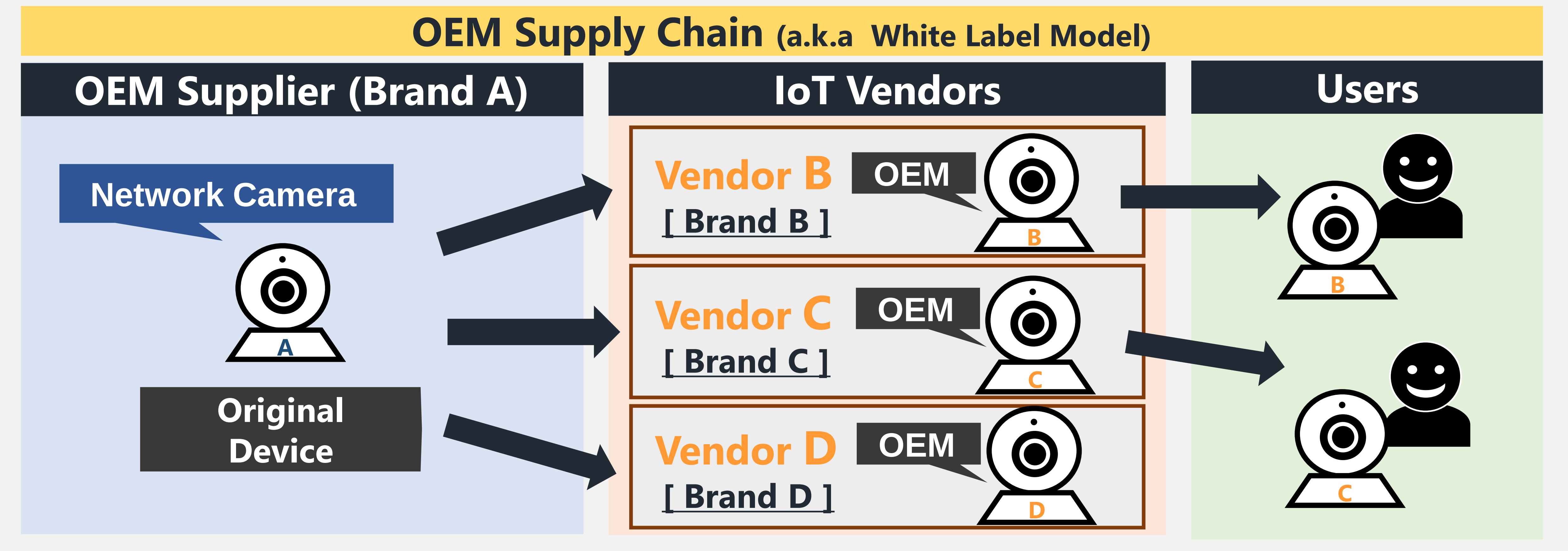
http://kun0ichi.net

- **Security Researcher @ NTT**
  - Vulnerability Discovery, Reverse Engineering, and IoT Security
    - Speaker: BlackHatUSA 2019, AsiaCCS 2019, ROOTCON 2019, PHDays 2016
- **Black Hat Asia Review Board**
  - From 2018 – 2020
- **Founder of CTF for GIRLS**
  - First Female InfoSec Community in Japan
    - Est. **2014.06**

CTF for GIRLS

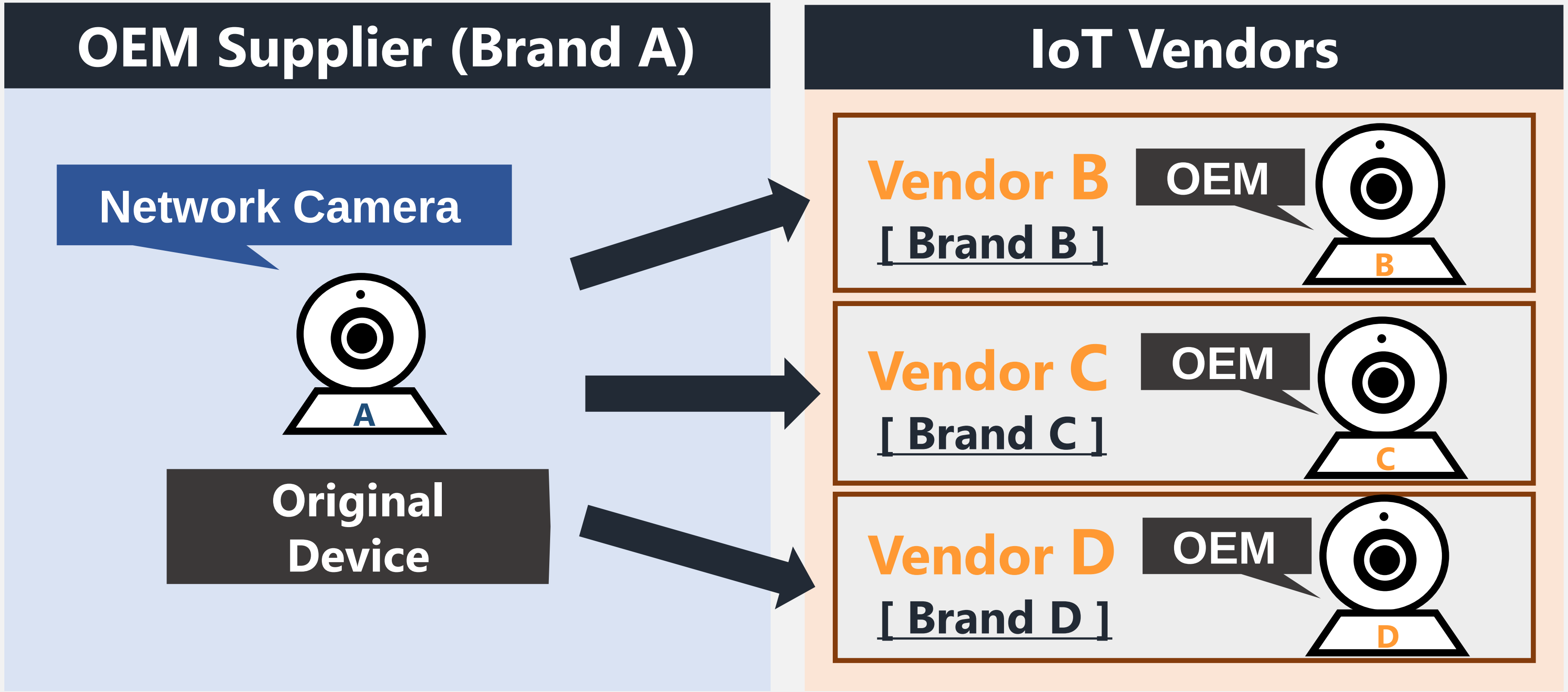
Background [1/4]

Many Consumer IoT Vendors Employ an OEM *(Original Equipment Manufacture)* Production Model



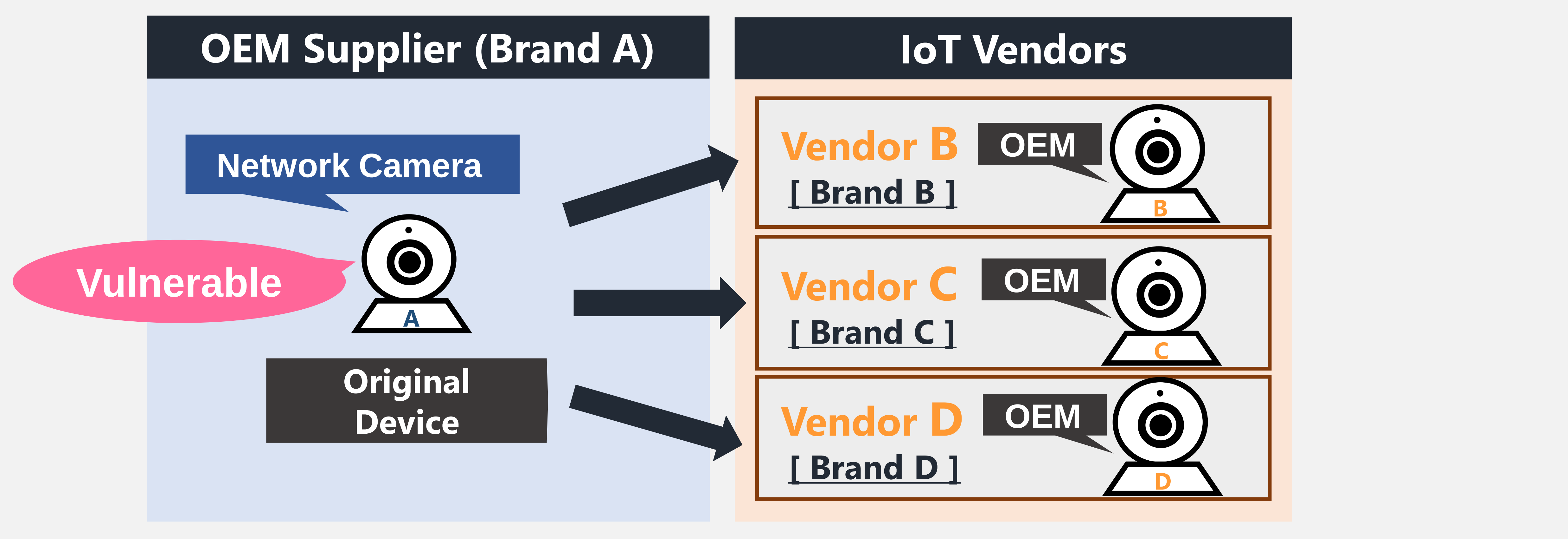
Background [2/4]

While OEM Production Model Can Reduce the Device Manufacturing Costs, It Could Lead to a High-Security Risk



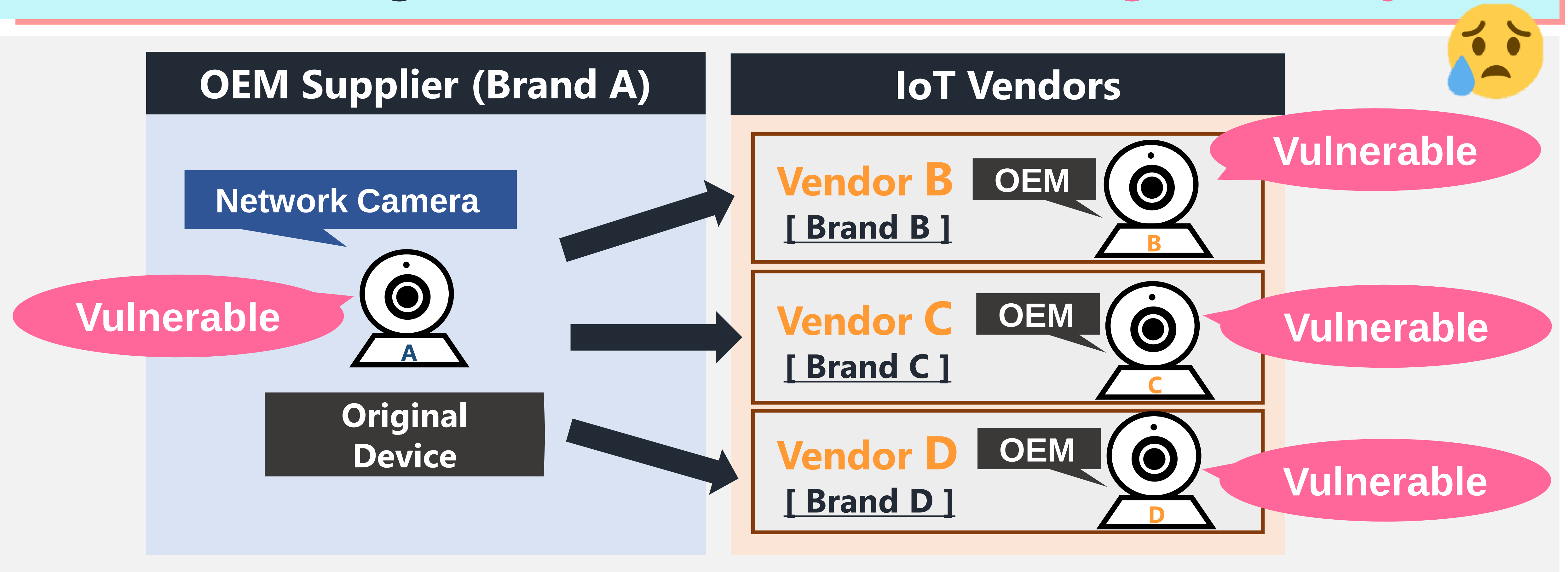
Background [2/4]

While OEM Production Model Can Reduce the Device Manufacturing Costs, It Could Lead to a High-Security Risk



Background [2/4]

While OEM Production Model Can Reduce the Device Manufacturing Costs, It Could Lead to a High-Security Risk

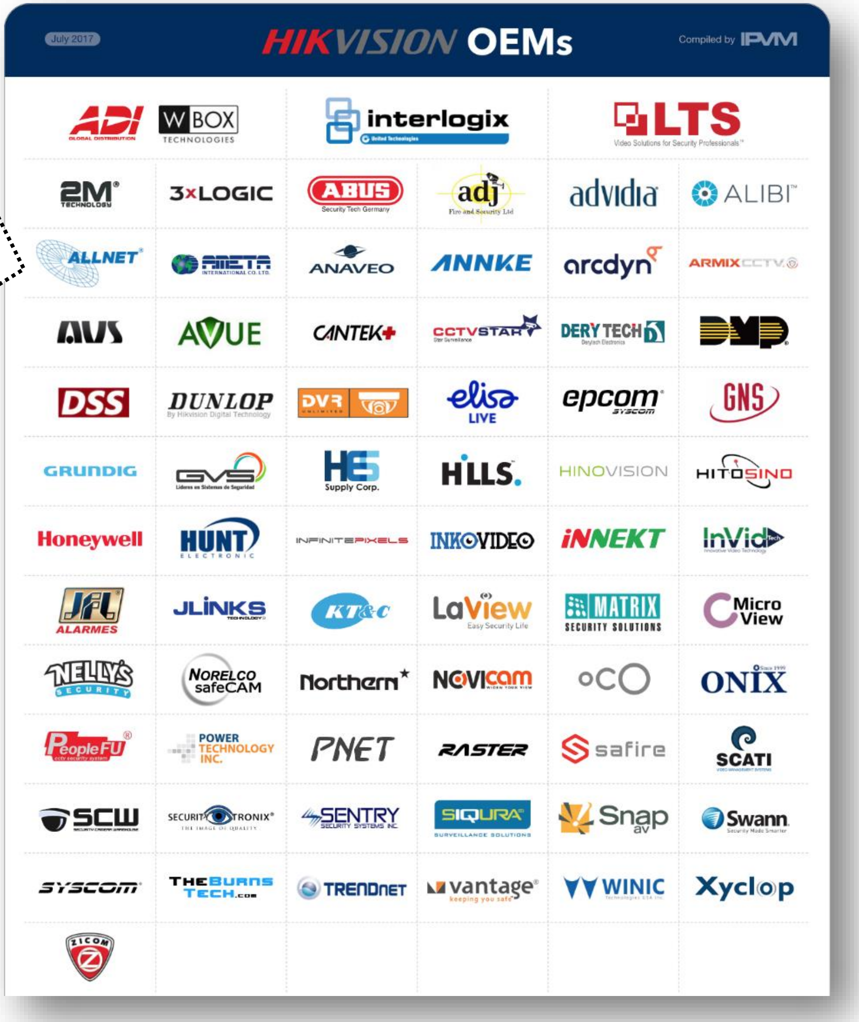


Background [3/4]

2017

CVE-2017-7921

Vulnerability found in the Hikvision's (OEM Supplier's) network camera was propagated to its various OEM devices which are sold by over 80 vendors[1]



[1] 80+ OEMs Verified Vulnerable To Hikvision Backdoor, IPVM, Sep 22, 2017, https://ipvm.com/reports/hik-oem-vuln

Background [4/4]

e.g.) NVD, CVE

Vulnerability Databases Do <u>NOT</u> Include and Announce Vulnerable OEM Devices as One of the Affected Products

Preliminary Survey

- ✓ Investigated CVEs which are related to IoT Devices from 2002 - mid 2018 by using NVD data feeds[2].
  1. Searched CVE which include "firmware" or "camera" or "router" or "modem" or router's name listed in [3] in the affected product/software name
  2. Filtered out the CVEs which affects only one vendor, and then manually investigated all the CVEs

nearly 2000 CVEs

- ✓ Only <u>6</u> CVEs list the OEM devices as one of the affected products

CVE-ID	Affected Vendors	
	OEM Supplier	Vendor which sells the OEM Product
CVE-2010-4230	Camtron	Tecvoz
CVE-2010-4231		
CVE-2010-4232		
CVE-2010-4233		
CVE-2010-4234		
CVE-2017-3216	Zyxel	Huawei, Zteo, Mada, Greenpacket,

[2] NVD Data Feeds, https://nvd.nist.gov/vuln/data-feeds

[3] Router Check Support, http://support.routercheck.com/

Background [4/4]

e.g.) NVD, CVE

Vulnerability Databases Do NOT Include and Announce Vulnerable OEM Devices as One of the Affected Products

One of the Probable Causes

Still No Means to Find the OEM Devices!

other than asking the OEM suppliers or inspecting each device manually

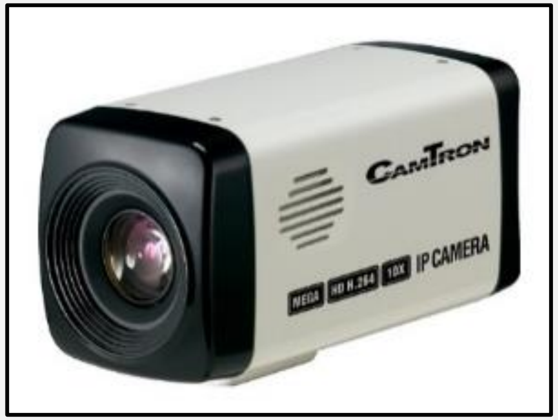
😥

[5] Router Check Support, http://support.routercheck.com/

How to Find OEM Devices

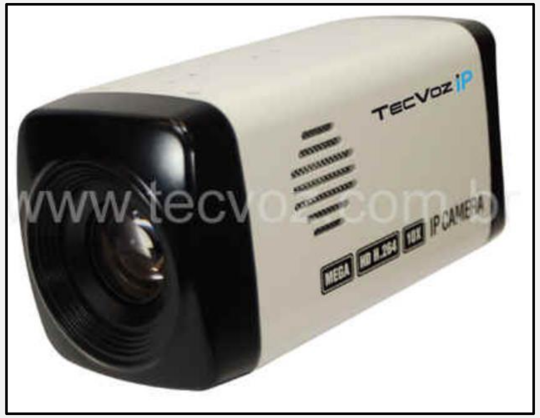
OEM Devices Share a Similar Appearance to the Original Device

CVE-2010-4230



Original Device

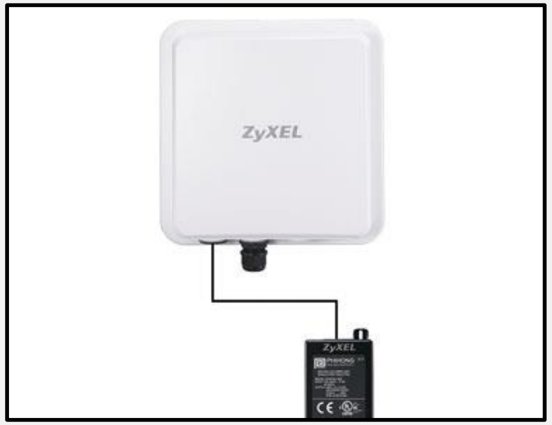
Vendor: Camtron
Model: CMNC-200



OEM Device

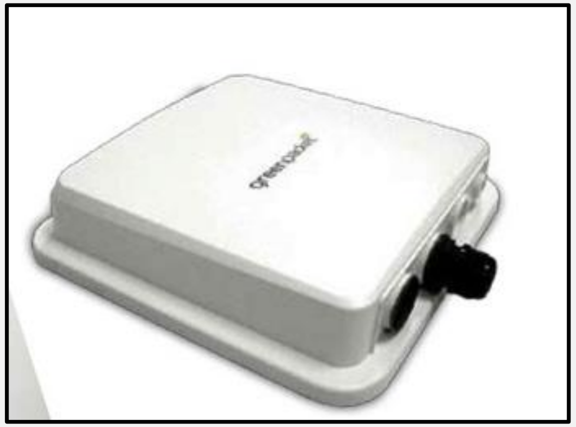
Vendor: Tecvoz
Model: CMNC-200

CVE-2017-3216



Original Device

Vendor: ZyXEL
Model: max308m



OEM Device

Vendor: Greenpacket
Model: ox350

Challenges

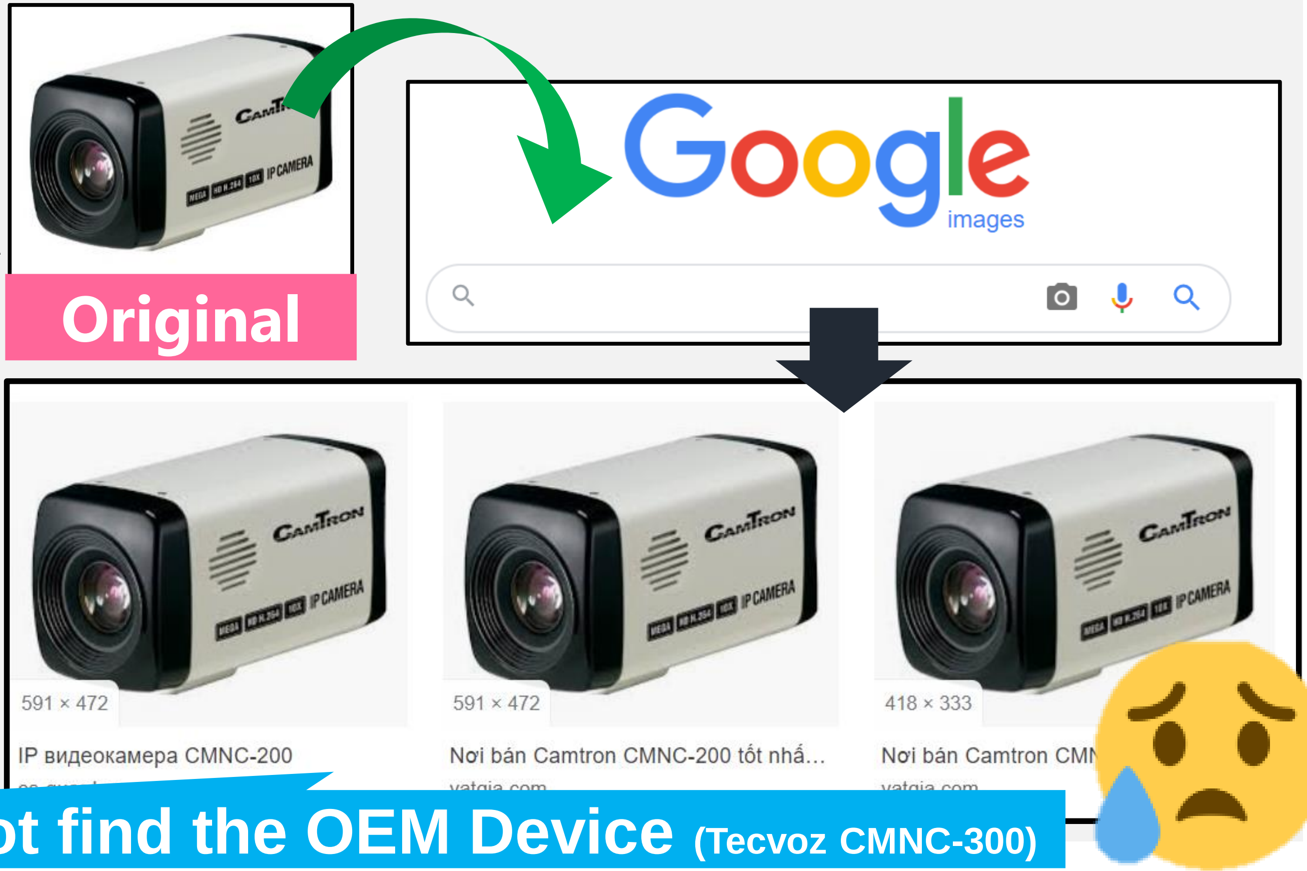
Typical Image Comparison Algorithms Do Not Work For Our Purpose

Challenges

1. **OEM devices are sometimes customized**
   - e.g.,) Additional antenna, Different lens

2. **Photo of OEM devices is sometimes taken in a completely different way than the original device**
   - e.g.) Different angle, Different light sources

Google Image Search



Can not find the OEM Device (Tecvoz CMNC-300)

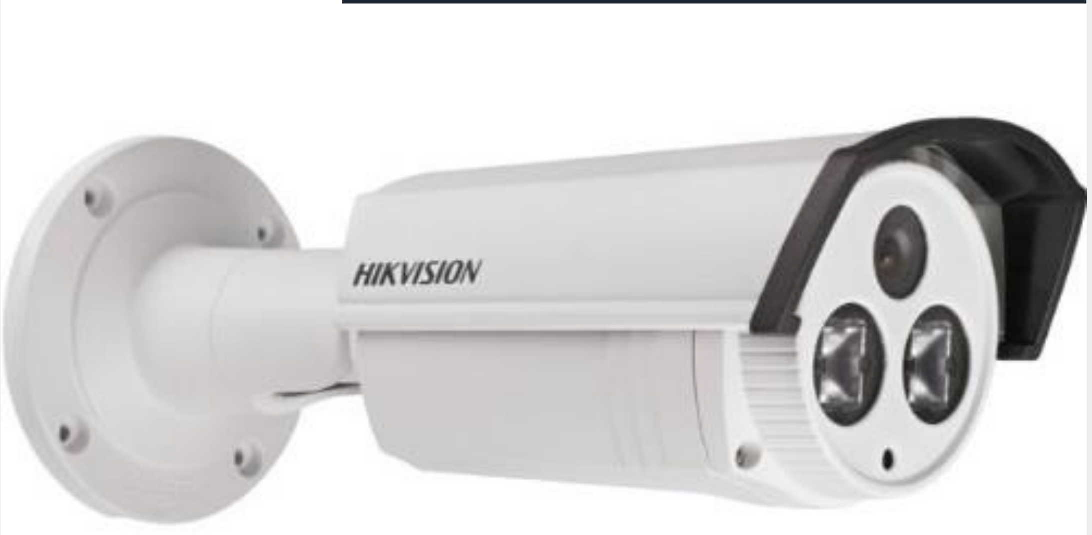
Approach

STEP1 | STEP 2 | STEP 3 | STEP 4

Use Specific Object Recognition Algorithm (KAZE[4]) to Extract the Object Features (Keypoints)

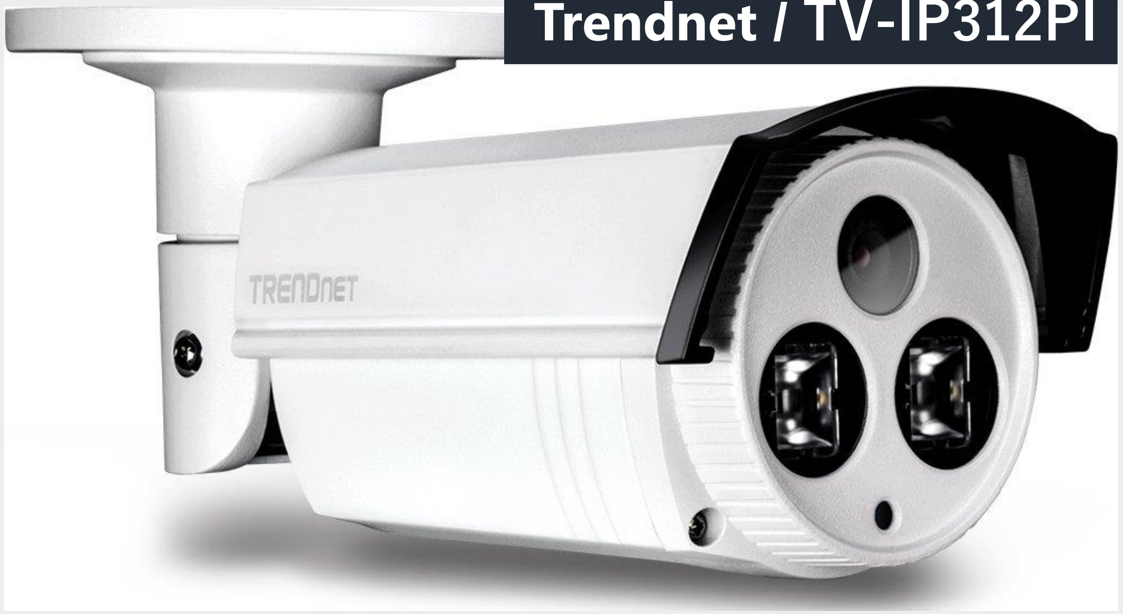
Original Device Image

Hikvision / DS-2CD2232-I5



Target Device (OEM Device) Image

Trendnet / TV-IP312PI



[4] Alcantarilla, P.F., A. Bartoli, and A.J. Davison. "KAZE Features." *ECCV 2012, Part VI, LNCS 7577.* 2012, p. 214

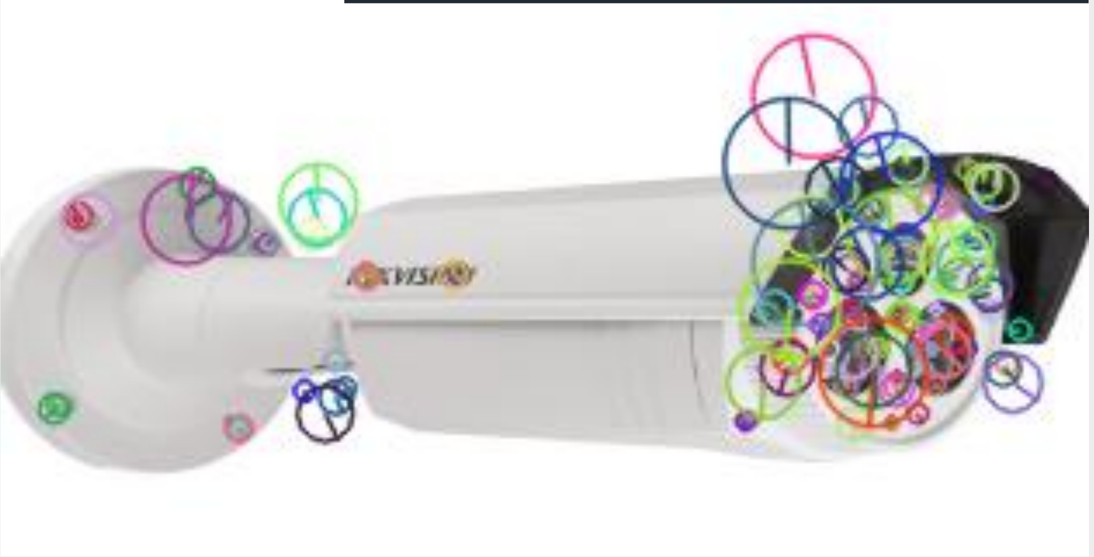
Approach

STEP1 | STEP 2 | STEP 3 | STEP 4

Use Specific Object Recognition Algorithm (KAZE[4]) to Extract the Object Features (Keypoints)

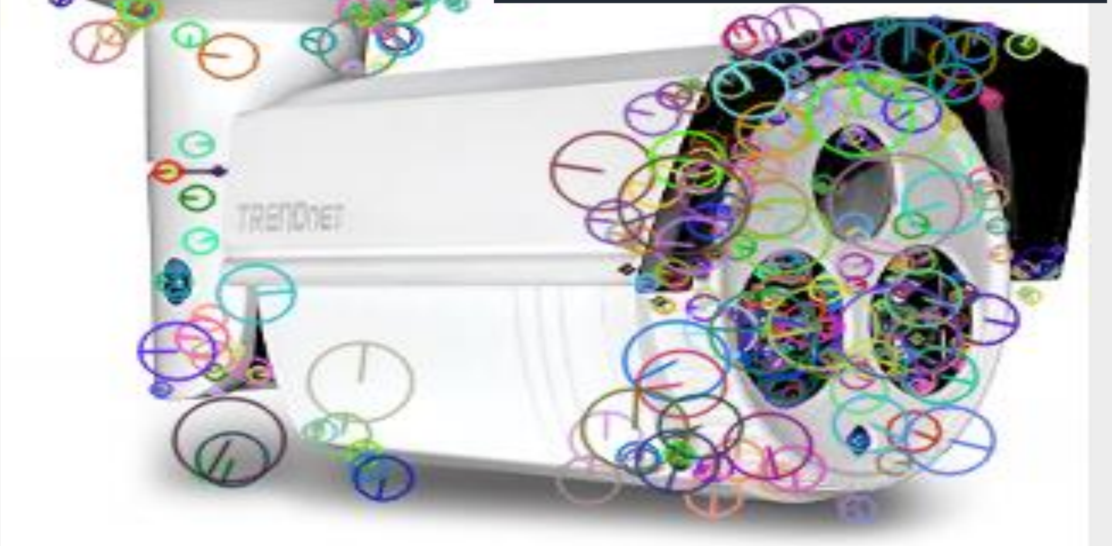
Original Device Image

Hikvision / DS-2CD2232-I5



Target Device (OEM Device) Image

Trendnet / TV-IP312PI

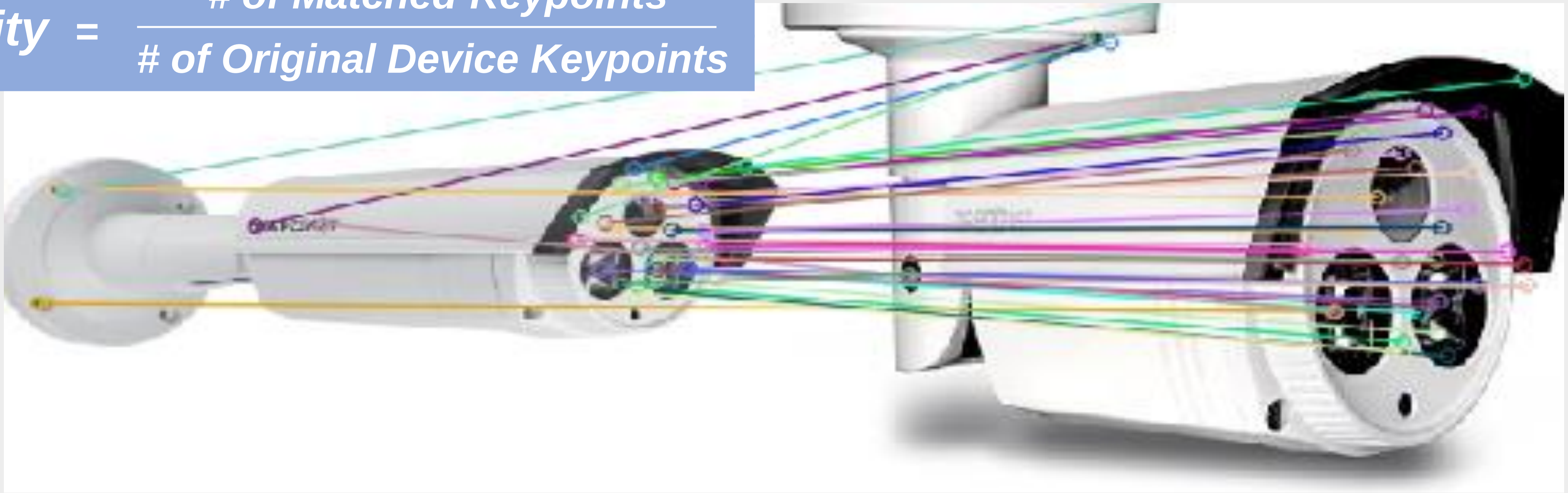


Approach

STEP1 | **STEP 2** | STEP 3 | STEP 4

Search & Match the Similar Keypoints by Using Manhattan Distance (L1 norm)

$$\text{Similarity} = \frac{\text{\# of Matched Keypoints}}{\text{\# of Original Device Keypoints}}$$

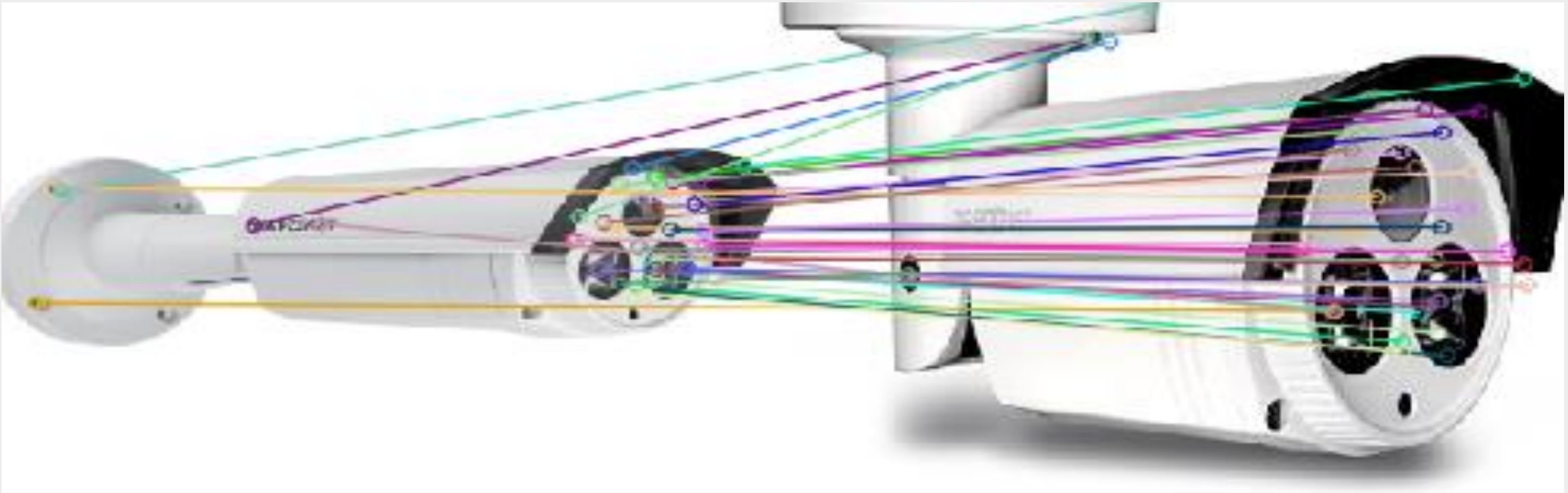


If Similarity < Threshold, move to the next image

Approach

STEP1 | STEP 2 | **STEP 3** | STEP 4

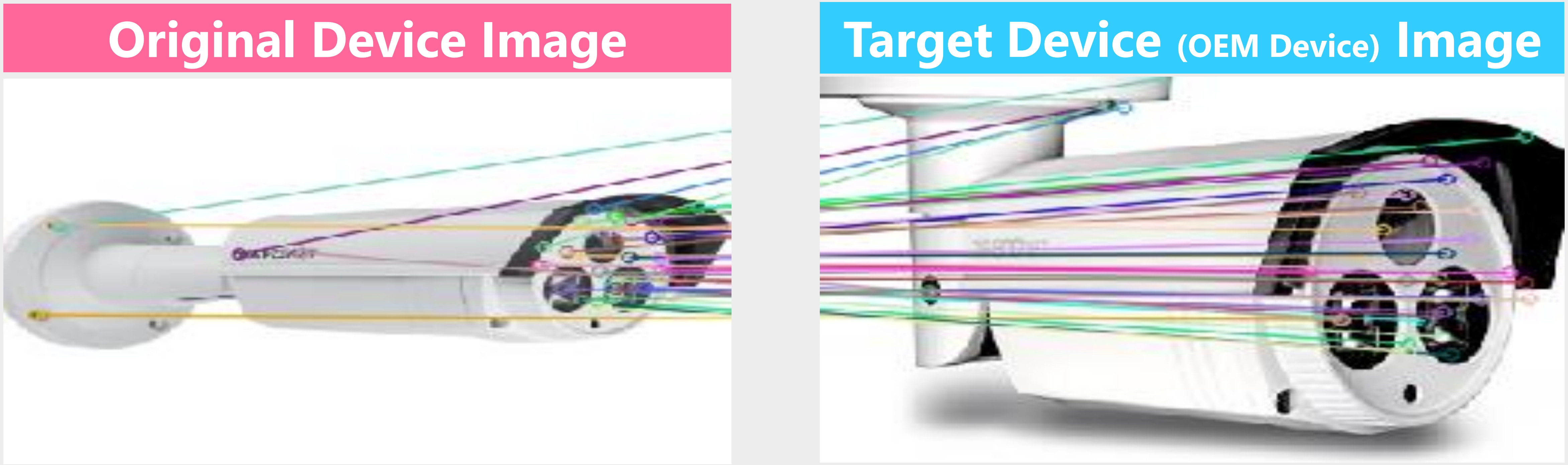
Construct a Relative Neighborhood Graph Based on the Matched Keypoints



Approach

STEP1 → STEP 2 → **STEP 3** → STEP 4

Construct a Relative Neighborhood Graph Based on the Matched Keypoints



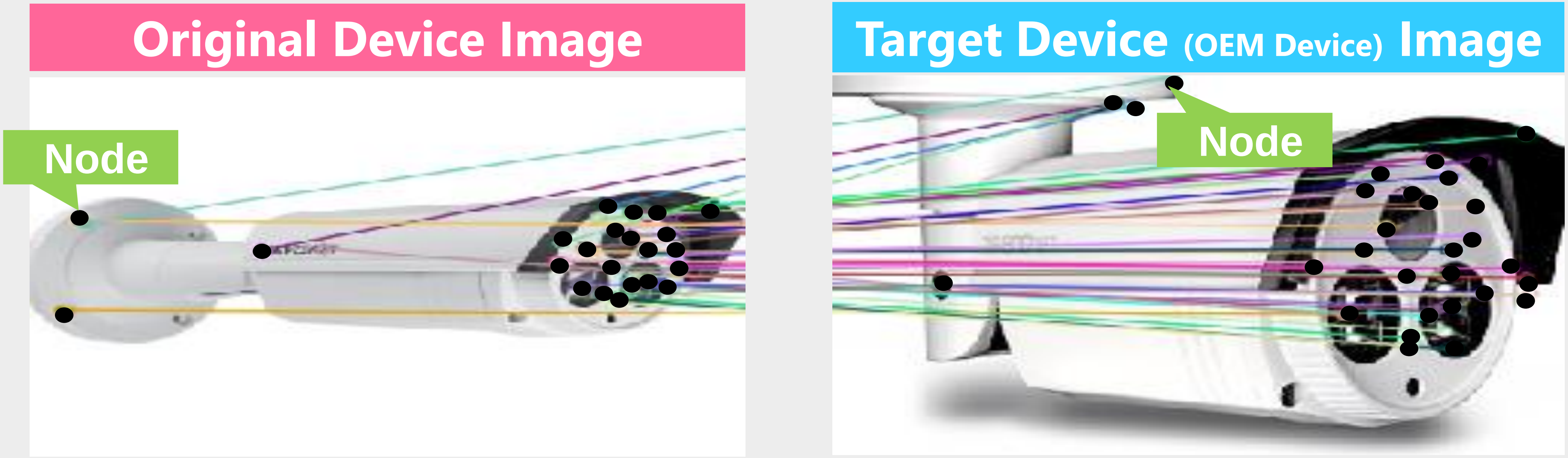
Original Device Image

Target Device (OEM Device) Image

Approach

STEP1 | STEP 2 | **STEP 3** | STEP 4

Construct a Relative Neighborhood Graph Based on the Matched Keypoints

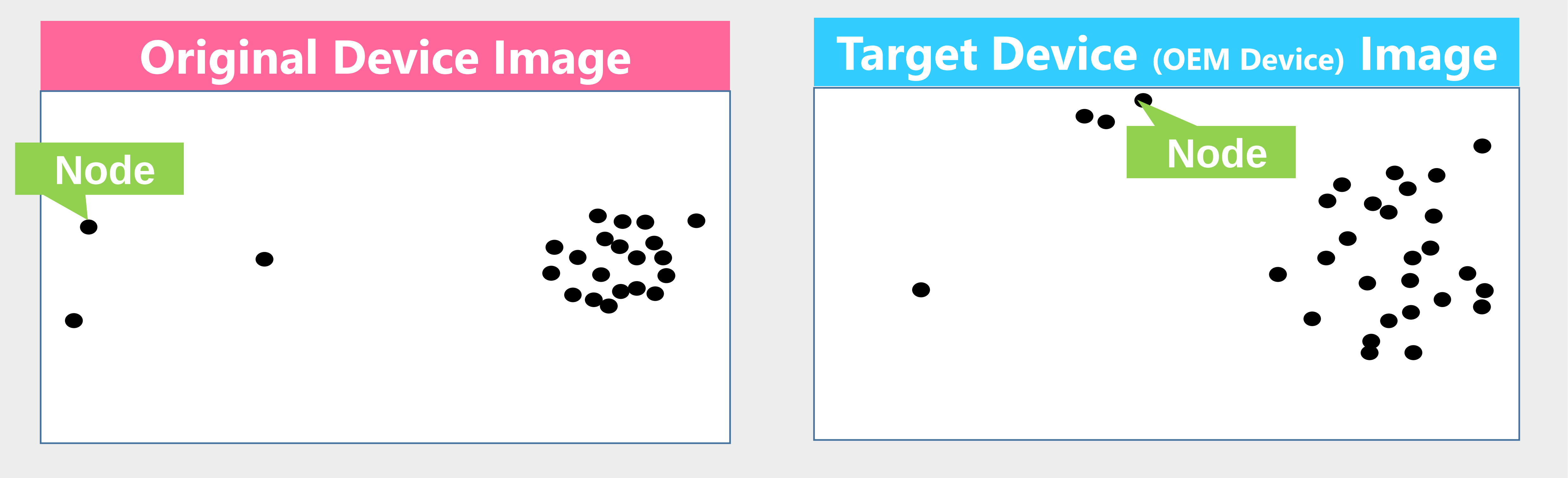


* Labeled each matched keypoint as same label

Approach

STEP1 | STEP 2 | **STEP 3** | STEP 4

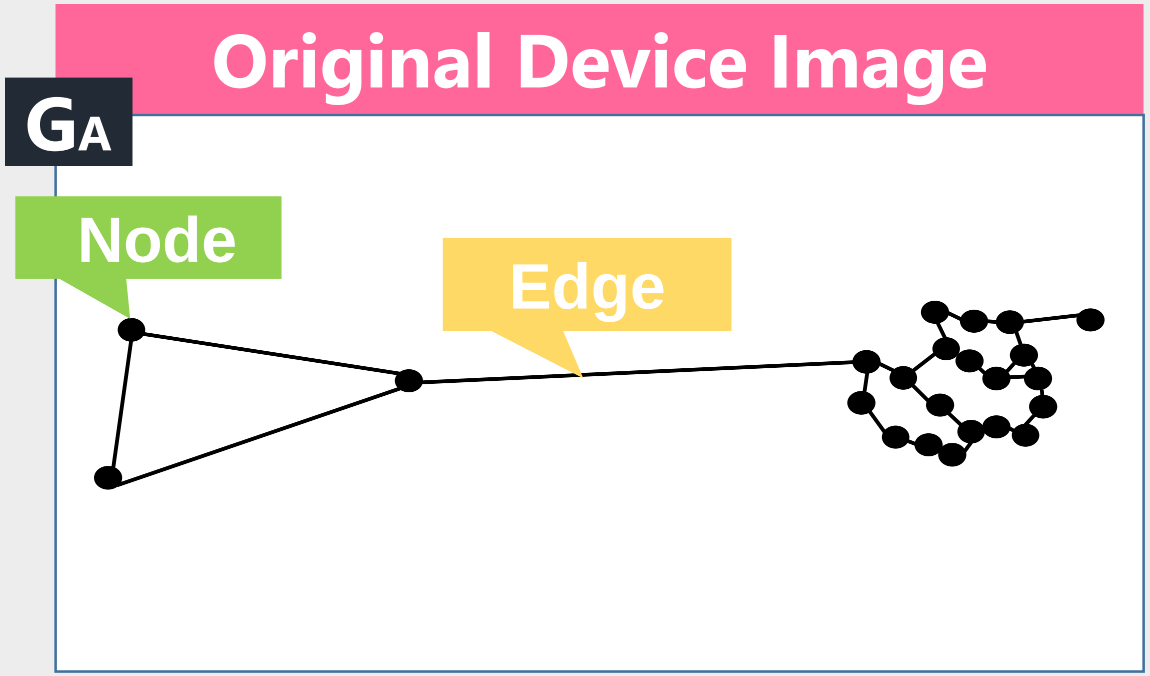
Construct a Relative Neighborhood Graph Based on the Matched Keypoints

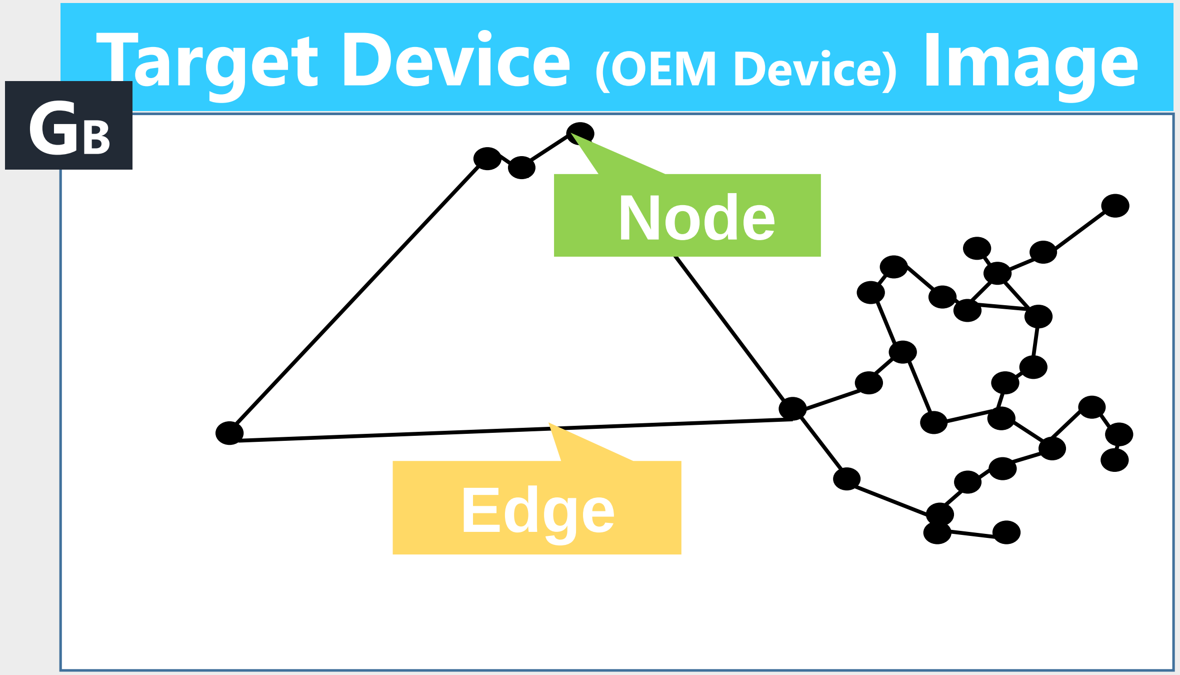


Approach

STEP1 | STEP 2 | **STEP 3** | STEP 4

Construct a Relative Neighborhood Graph Based on the Matched Keypoints



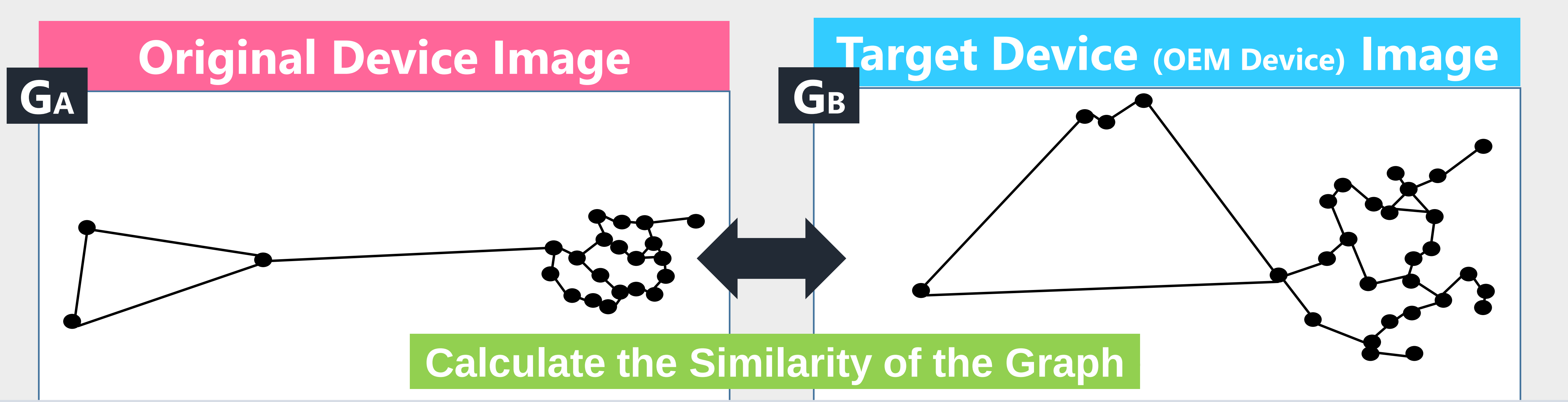


* Above is just a sample image of the relative neighborhood graph. Not the actual example.

Approach

STEP1 | STEP 2 | STEP 3 | STEP 4

Calculate the Structure Similarity
By Using Shortest Path Graph Kernel



Original Device Image

G_A

Target Device (OEM Device) Image

G_B

Calculate the Similarity of the Graph

$$\mathrm{sim}(G_A, G_B) = \Sigma\ \mathrm{sim}(\text{ all-shortest-path}(G_A), \text{all-shortest-path}(G_B))$$

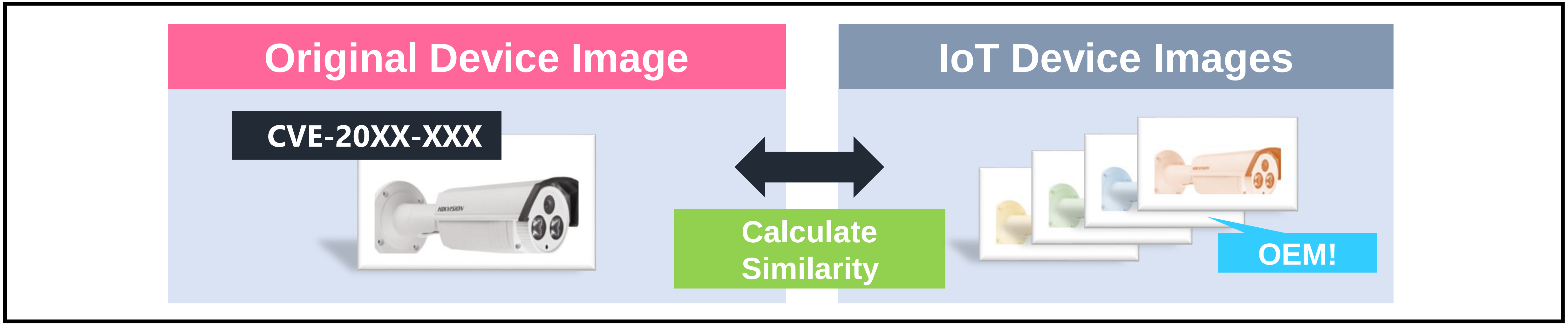
Experiment Overview

GOAL

Verify That This Approach Can Find OEM Devices

❖ Dataset

- IoT Device Image Dataset
- Original Device Image Dataset
  - Image of IoT Devices which OEM supplier sells



Dataset [1/2]

IoT Device Image Dataset

- Collected more than **54,000** network camera images from **Amazon** & **Walmart**

EC Website	Region	API	Target Category	# of Collected Images
Amazon	Amazon.com	Product Advertising API	Dome Camera	13433
			Bullet Camera	7410
			Web Camera	2114
	Amazon.jp	Product Advertising API	Dome Camera	541
			Bullet Camera*	1000
			Web Camera	3277
Walmart	walmart.com	Open API	Indoor Camera	23159
			Outdoor Camera	3651
			Wireless Camera	247
			Web Camera	3
TOTAL				54835

*Bullet Camera category is called “Standard Camera” in amazon.jp, but the category number is the same as Bullet Camera in amazon.com

Dataset [2/2]

Original Device Image Dataset

- Collected more than **120** images of network cameras (from amazon.com) in which vulnerabilities were discovered in this past two years from the four representative OEM supplier vendors

Vendor name	# of CVEs	# of Products	# of Collected Images
Hikvision	3	20	21
Dahua	5	75	80
Foscam	24	21	21
Wanscam	1	1	3
TOTAL	33	117	125

Experiment Result

Summary

- ✓ **Found more than 180 unique vulnerable OEM device candidates which are sold by over 25 vendors**
- ✓ **Analyzed the latest firmware images of some of the OEM device candidates**
  - Confirmed that the detected devices are **indeed OEM devices**
  - Found that some of the OEM firmware images are **still vulnerable**

Case Study 1: Hikvision

CVE-2017-7921 & CVE-2017-7923

Original

Model: ds-2cd2312-i

OEM Device Candidates

Vendor: KT & C
Model:KNC-P3TR6XIR

Vendor: PNET
Model: PN-402EX

Vendor: PWS Security
Model: Unknonwn

Vendor: LTS
Model: CMIP3032-28

Vendor:
Orange Sources
Model: Unknown

Vendor: P2P Security
Model: Unknown

Vendor: HDView
Model: Unknown

Vendor: AVUE
Model:AV50HTWX

Vendor: CMPLE
Model:1287-N

Vendor:
Securtiy Camera King
Model:IPOD-PR2EXIRE28

Case Study 1: Hikvision

CVE-2017-7921 & CVE-2017-7923

Original Device

Model: ds-2cd4132fwd-i(z)

OEM Device Candidate

Vendor: Panasonic
(brand name: advidia)
Model:A-44-IR-V2

Case Study 1: Hikvision

Candidate Vendors Name	Listed on IPVM?	Possible to Collect Firmware from the official website?
SPT Security	No	X
Xinnrray (Xinray)	No	X
Security Camera King	No	X
HDView	No	X
CMPLE	No	X
Orange Sources	No	X
Urban Security Group	No	○
PWS Security	No	No Web site
CONDORD	No	No Web site
P2P Security	No	No Web site
KT&C	Yes	X
AVUE	Yes	○
ANNKE	Yes	○
CCTV Star	Yes	X
Pnet	Yes	X
Panasonic(advidia)	Yes	○

July 2017
HIKVISION OEMs
Compiled by IPVM
ADI
W BOX
interlogix
LTS
2M
3xLOGIC
ABUS
adj
advidia
ALIBI
ALLNET
AMETA
ANAVEO
ANNKE
arcdyn
ARMIX CCTV
AVUS
AVUE
CANTEK
CCTVSTAR
DERY TECH
DMP
DSS
DUNLOP
DVR
elisa LIVE
epcom
GNS
GRUNDIG
GVS
HES
HILLS
HINOVISION
HITOSINO
Honeywell
HUNT
INFINITEPIXELS
INKOVIDEO
iNNEKT
InVid
JFL ALARMES
JLINKS
KT&C
LaView
MATRIX
Micro View
NELLY'S
NORELCO safeCAM
Northern
NOVICAM
OCO
ONIX
PeopleFu
POWER TECHNOLOGY INC.
PNET
RASTER
safire
SCATI
SCW
SECURITYTRONIX
SENTRY
SIQURA
Snap av
Swann
SYSCOM
THE BURNS TECH
TRENDnet
vantage
WINIC
Xyclop
ZICOM

Case Study 2 : Dahua

CVE-2017-9317 & CVE-2917-9315

Original Device

Model
IPC-HDBW4831E-ASE

OEM Device Candidates

Vendor: iMaxCamPro
Model:WEC-IP9-WiFi

Vendor:PWS Security
Model: Unknown

Vendor: Night King
Model:NK-6030G-4K

Vendor:
Urban Security Group
Model: USGDK8W405GAHBB56A

Case Study 3: Foscam

black hat EUROPE 2019

CVE-2018-6830

Original Device

Model: FI9805W

OEM Candidate

Vendor: Skyreo
Model:
SR8905W-SLUS

Original Device

Model: FI9900EP

OEM Candidate

Vendor: Ambient Weather
Model: AMBIENTCAMHDA

Case Study 3: Foscam

CVE-2018-6830

Original Device

Model:
FI9816P

OEM Device Candidates

Vendor: Vstarcam
Model: C37A

Vendor: Escam
Model: QF001

Vendor: Sricam
Model: Unknown

Vendor: EVAKION
Model: EV130

Detailed Analysis

CVE-2017-9315

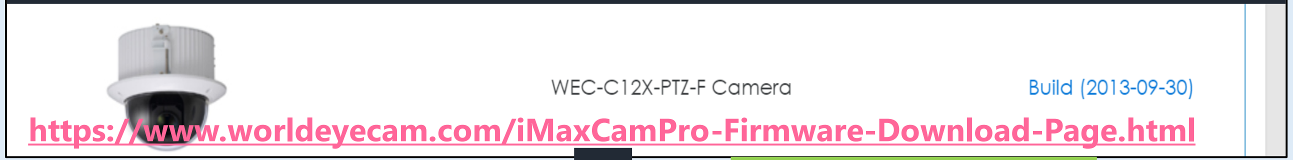
Original

Vendor:Dahua
Model:
SD52C430U-HNI

OEM Candidate

Vendor: iMaxCamPro
Model:
IMAX-CVI720P12X-PTZ-FM

Download Firmware (IMAX Cam Pro)

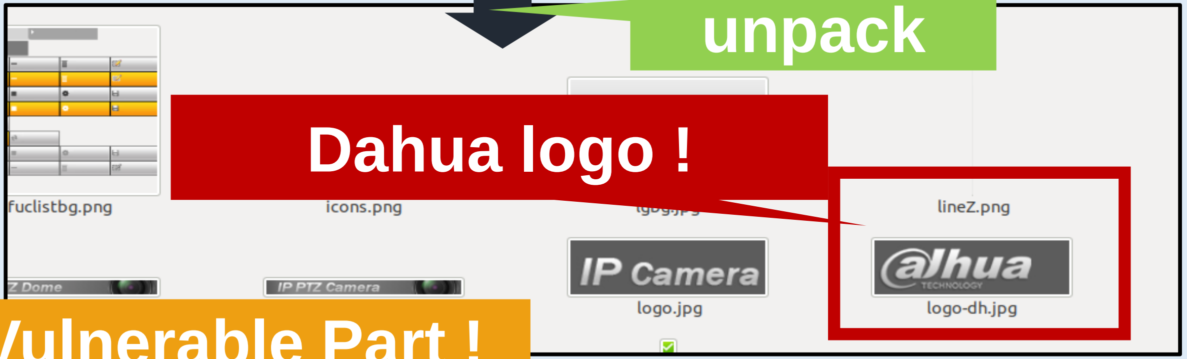


WEC-C12X-PTZ-F Camera Build (2013-09-30)

https://www.worldeyecam.com/iMaxCamPro-Firmware-Download-Page.html

unpack

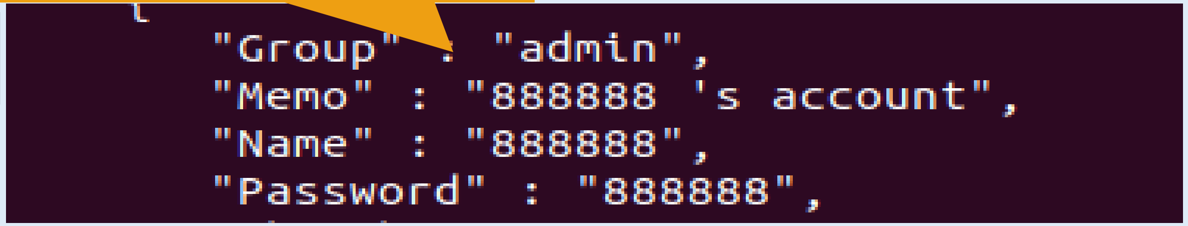
A



Dahua logo !

Vulnerable Part !

B



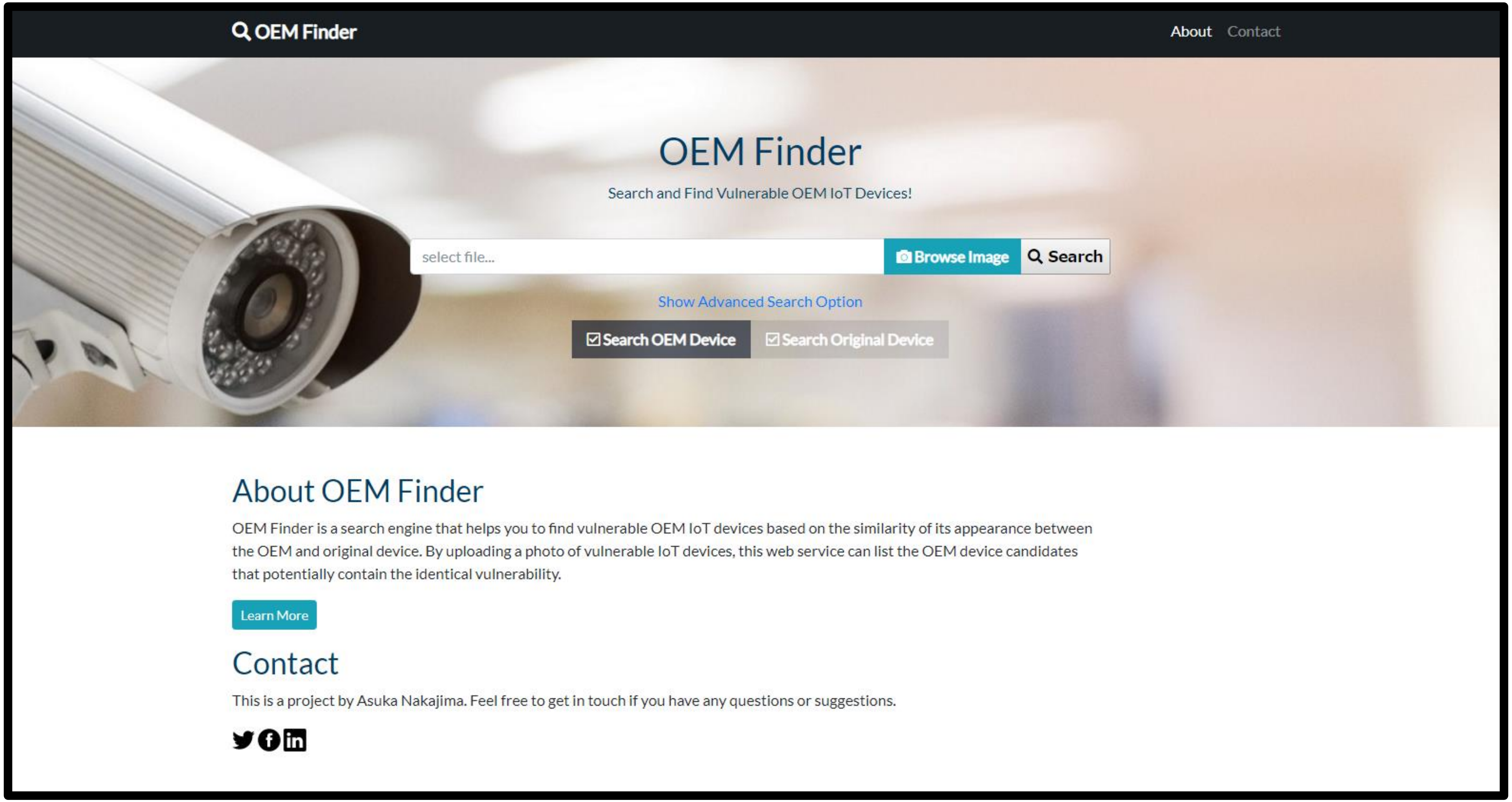
```
{
        "Group" : "admin",
        "Memo" : "888888 's account",
        "Name" : "888888",
        "Password" : "888888",
```

Summary

- ✓ Confirmed that the OEM candidate devices are indeed OEM devices (A)
- ✓ Found that the OEM firmware images are still vulnerable (B)

DEMO Time!

OEM Finder



OEM Finder

Search and Find Vulnerable OEM IoT Devices!

About OEM Finder

OEM Finder is a search engine that helps you to find vulnerable OEM IoT devices based on the similarity of its appearance between the OEM and original device. By uploading a photo of vulnerable IoT devices, this web service can list the OEM device candidates that potentially contain the identical vulnerability.

Contact

This is a project by Asuka Nakajima. Feel free to get in touch if you have any questions or suggestions.

DEMO

Find and show vulnerable OEM device candidates by using the OEM Finder

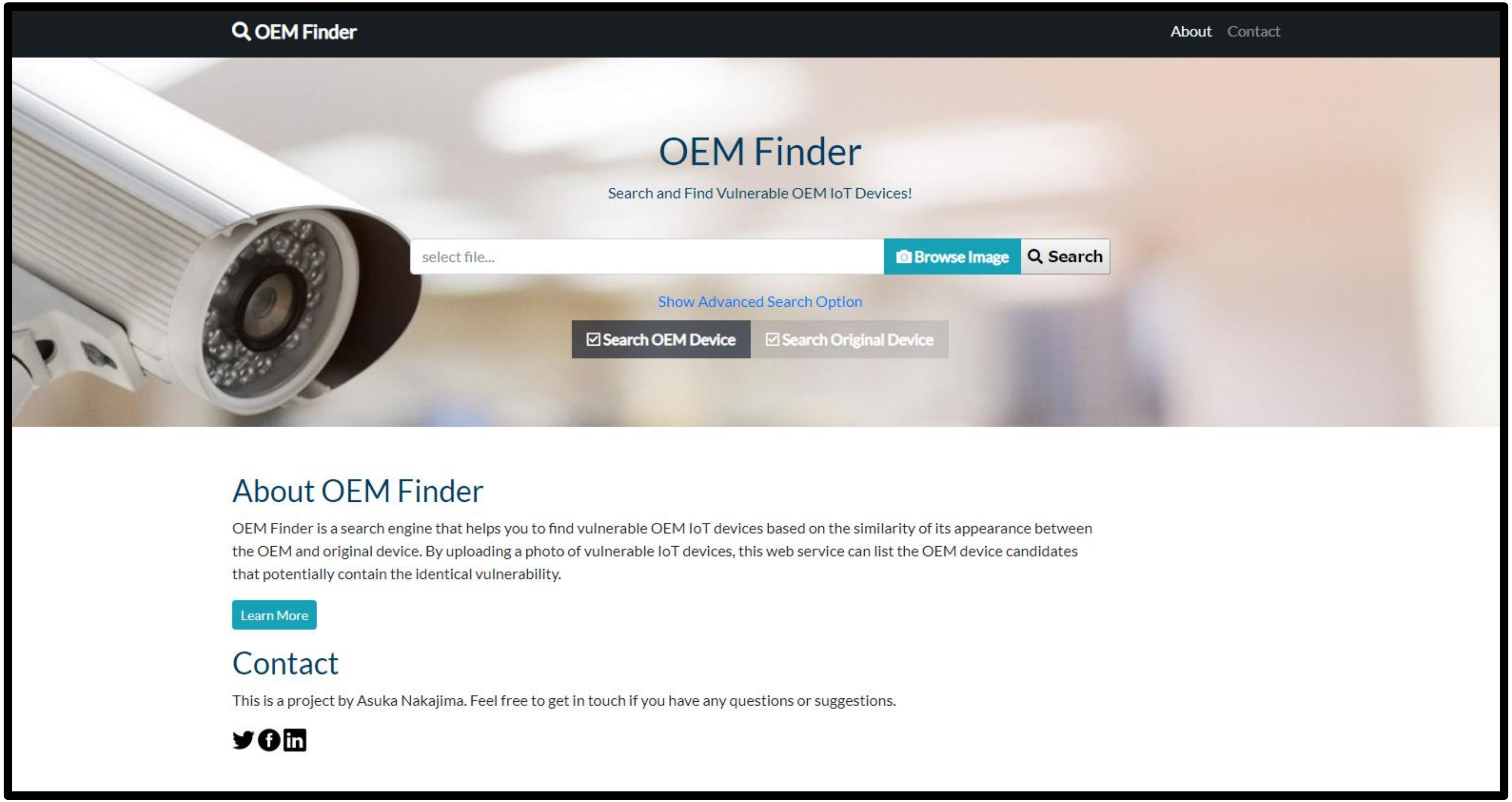
[Vendor]
+ Hikvision

[Model]
+ DS-2CD2232-I5

[CVE-ID]
+ CVE-2017-7923 / CVE-2017-7921

OEM Finder

http://oemfinder.ilab.ntt.co.jp



OEM Finder

Search and Find Vulnerable OEM IoT Devices!

About OEM Finder

OEM Finder is a search engine that helps you to find vulnerable OEM IoT devices based on the similarity of its appearance between the OEM and original device. By uploading a photo of vulnerable IoT devices, this web service can list the OEM device candidates that potentially contain the identical vulnerability.

Contact

This is a project by Asuka Nakajima. Feel free to get in touch if you have any questions or suggestions.

About Other Consumer IoT Devices

Smart Speaker

Original ?

Vendor: COWIN
Model: Dida

OEM ?

Vendor: ELEPAWL
Model: Dida

Black Hat Sound Bytes

Take Aways

Black Hat Sound Bytes

☑ **Explained About Security risk of consumer OEM IoT devices**

1. When the original IoT device is vulnerable, the OEM device is also vulnerable
2. Vulnerability databases do not include the vulnerable OEM device as one of the affected products

☑ **Developed a new tool called OEM Finder, which can automatically detect OEM device candidates based on the similarity of its appearance between the OEM and original device**

- Adopt an object recognition algorithm, and employ a graph kernel algorithm

☑ **Published OEM Finder as an online search engine**

- **http://oemfinder.ilab.ntt.co.jp**

Acknowledgement

Acknowledgment

- **<u>Team Members</u>**
  - Takuya Watanabe, Eitaro Shioji, Mitsuaki Akiyama
    - For insightful discussion
- **<u>Special Thanks</u>**
  - **<u>Toshiki Shibahara</u>**
    - For insightful discussion and his suggestion about employing graph kernel algorithm

Questions?

E-Mail	asuka.nakajima.db@hco.ntt.co.jp
Twitter	@AsuNa_jp