ハニーポット生成の基盤となる車載機器の発見方法

2022/10/12

松本　勉

横浜国立大学

- This presentation is based on the joint research with Takahiro Ueda, Takayuki Sasaki, and Katsunari Yoshioka.
- This research was conducted under a contract of "Automated Driving for Universal Services" among Cross-ministerial Strategic Innovation Promotion Program (SIP), which was supported by the Cabinet Office, Japan.
- A part of this research was conducted in "MITIGATE" project among "Research and Development for Expansion of Radio Wave Resources (JPJ000254)", supported by the Ministry of Internal Affairs and Communications, Japan.

◆ コネクティッドカーに対するブラックハット攻撃が増加傾向にある

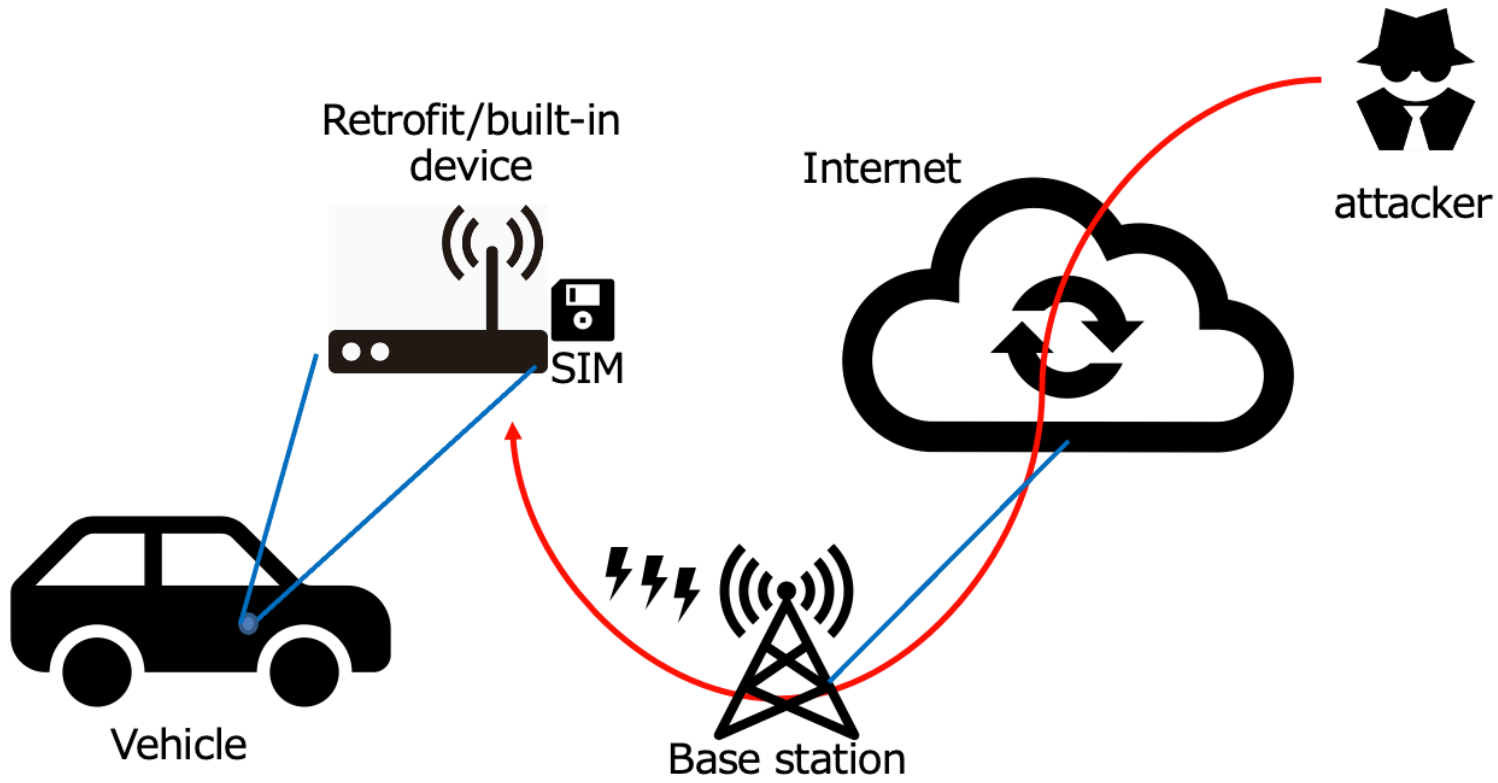
- Attacks on connected cars are increasing.
- For example, Upstream reports that the percentage of black-hat attacks went up to 56.9% in 2021.
- There are many communication channels to access connected cars.
- The same report says that remote attacks greatly outnumbered physical attacks in 2021.

Upstream, 2022 Global Automotive Cybersecurity Report, https://upstream.auto/2022report/

https://www.researchgate.net/publication/333132722_A_strategy_for_vehicular_honeypots

◆主としてコネクティッドデバイスへの直接攻撃に着目

We focus on the case where a device inside a car is directly accessible from the Internet (via mobile network) as it can be an immediate threat.



具体例: Telematics Gateway - C4max

- C4max, a telematics gateway unit (TGU), was assigned global IP addresses with several services open including telnet without authentication.
- It also connects to the internal vehicular network.


```
22/tcp OpenSSH5.1
23/tcp telnet
80/tcp http
```

No-authentication

WebUI(80/tcp)

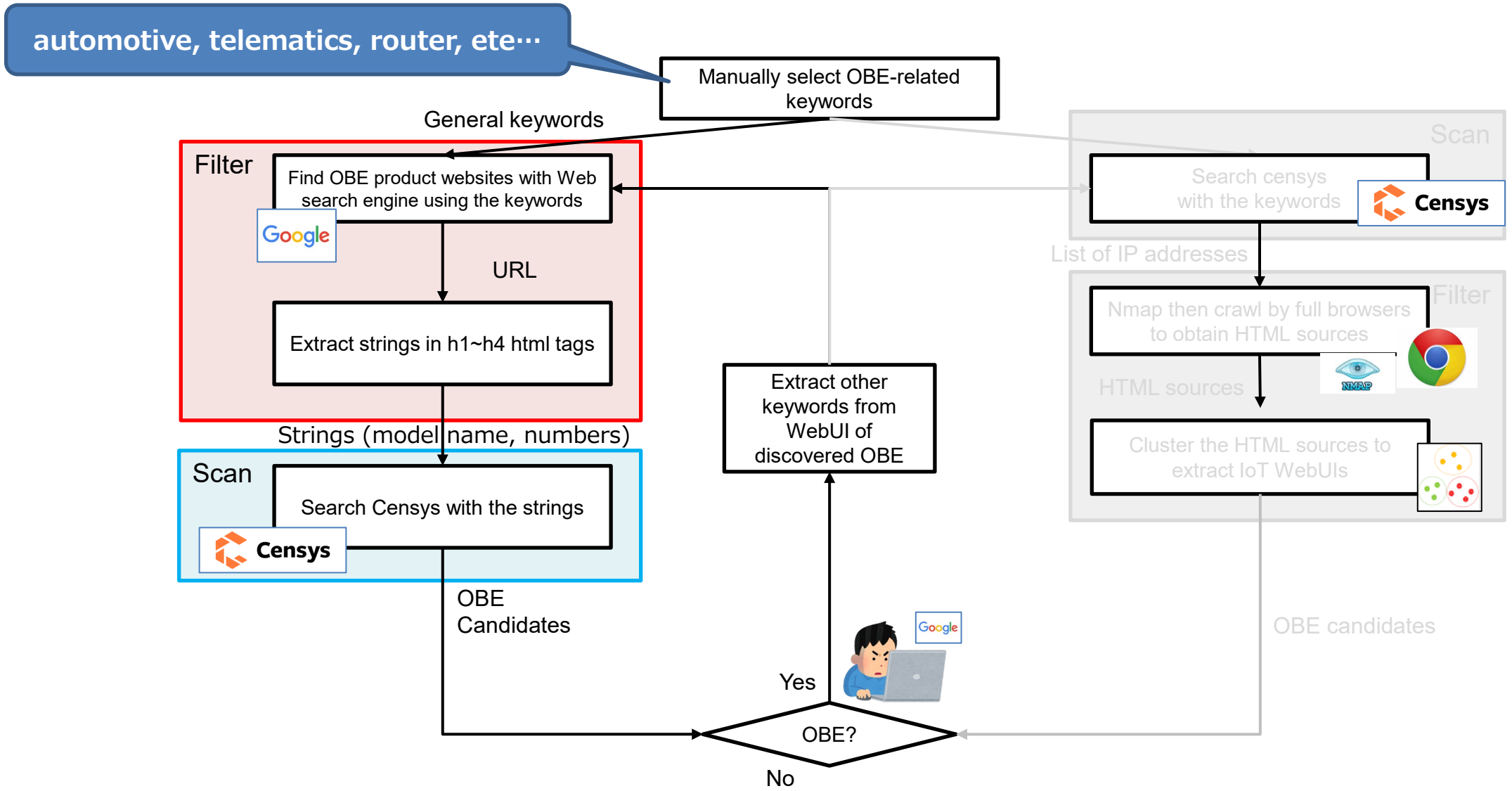
```
Connected

Builtins
cversion Console version
lang Set the console language
reboot Reboot

Basics
1wire Display 1wire information
iostate Display input/output state
modem Display modem state
gpspos Retrieve last GPS position
list List available modules.\n[all] List all available modu
Download result.
g Get module parameter value
s Set module parameter value
listdb List available DB parameters
gdb Get a DB parameter
sdb Set a DB parameter
logdump Display all logs
```

Jose Carlos Norte. Hacking industrial vehicles from the internet: http://jcarlosnorte.com/security/2016/03/06/hacking-tachographs-from-the-internets.html

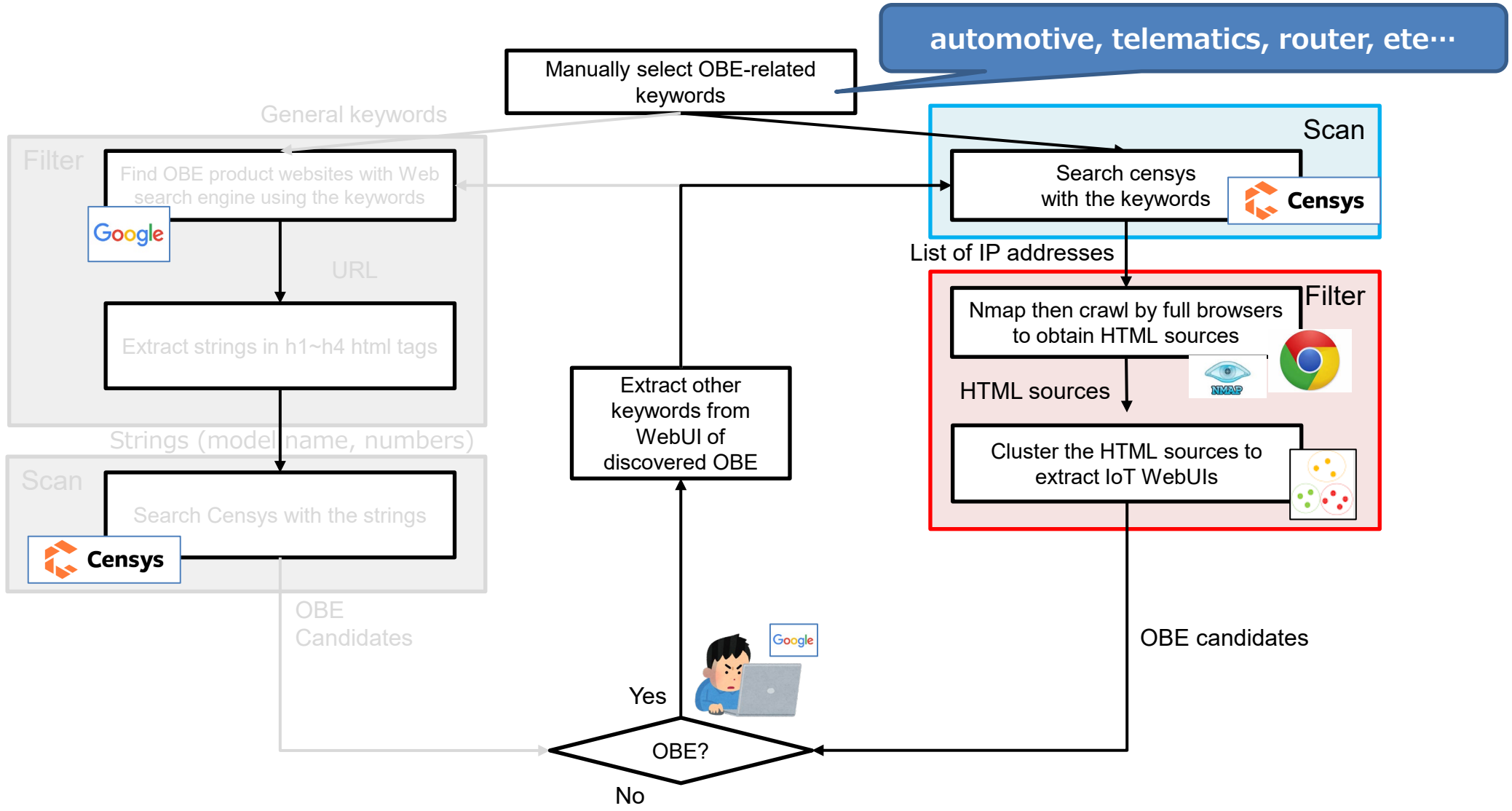
◆ 研究上の関心事項

1. How many and what kind of OBE (On-board Equipment) products can be discovered on the Internet?
   >>> Internet-wide scan for discovery
2. What is the likelihood that the exposed OBE products could be compromised and become an entry point for further attacks against the in-vehicle network?
   >>> Surface security investigation on discovered devices
3. Is any of the discovered devices attacked? If so, is it targeted?
   >>> We have started development of a honeypot imitating discovered devices and analyze observed attacks

車載機器発見方法（その１）



車載機器発見方法（その２）

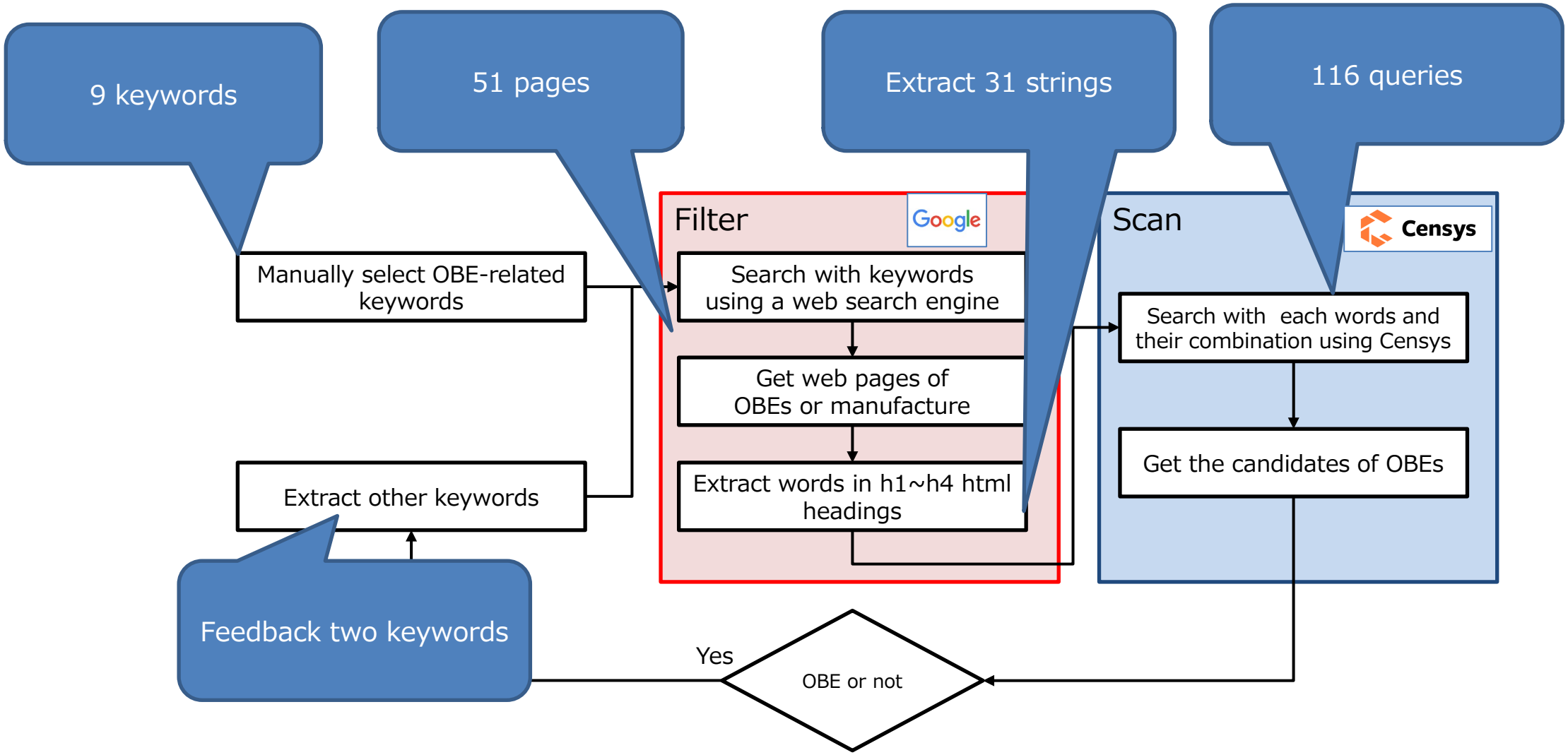


結果の概要

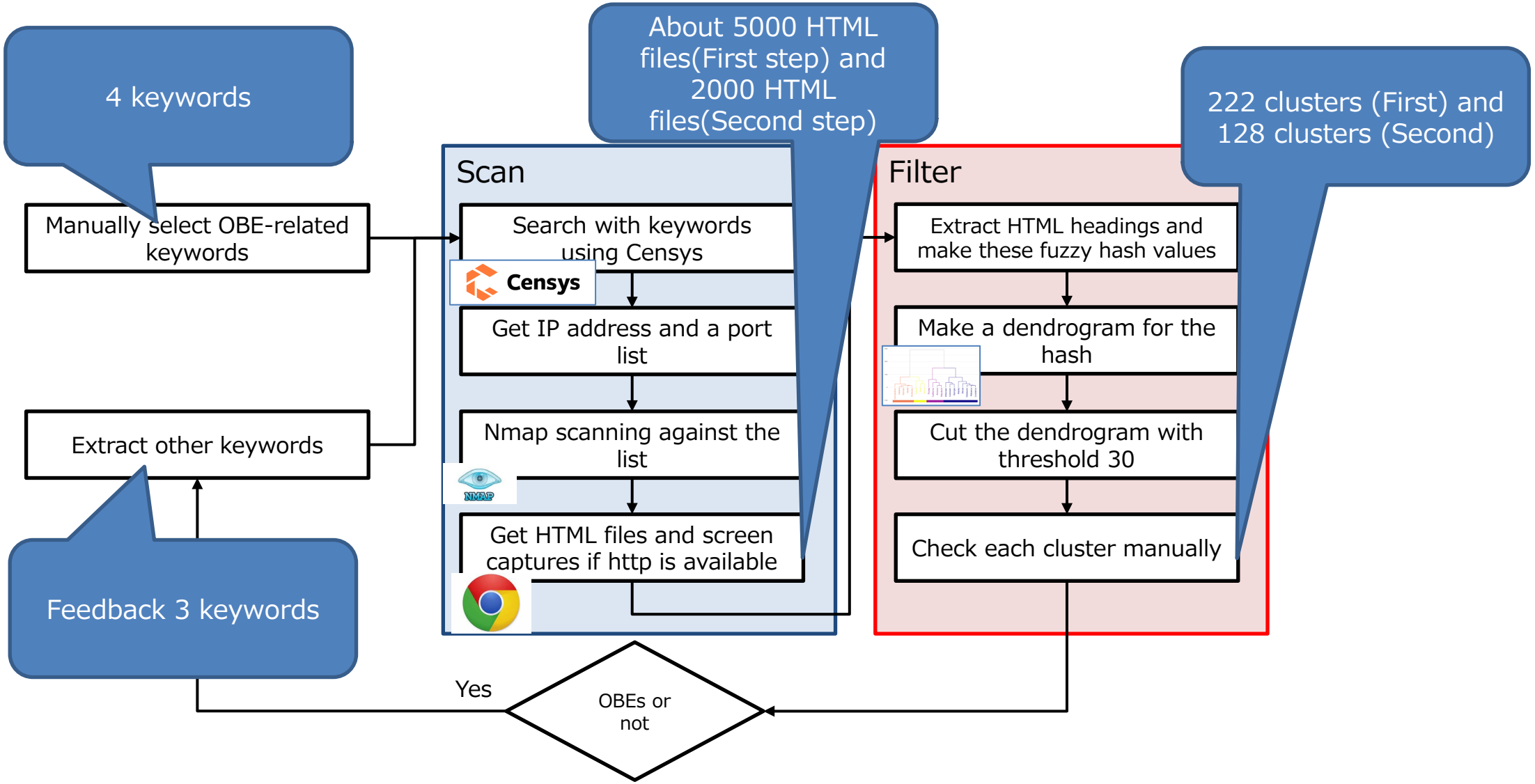
- How many?
  - 12 OBE models
  - 2,532 devices
- What kind?
  - All devices are vehicle routers or gateways
- Where?
  - Mobile networks
  - Europe, US, Asia, South America

device name	Web-base/Cluster-base	#devices	Discovered countries	AS
A	Clustering-based	278	NL 26.0% SE 18.9% US 16.3%	DTAG internet service / KPN KPN network
B	Clustering-based	391	ES 59% MA 20.3% DE 11.9%	VODAPONE_ES / DTAG ineternet service
C	Web-search-engine-based	821	US 96.5% BR 2.2%	CELLCO-PART
D	Web-search-engine-based	186	IT 59.1% DE 40.0%	VODAPONE_IT ASN
E	Web-search-engine-based	88	DE 95.6%	DTAG internet service
F	Both	104	US 60.0% ES 11.8% AU 10.0%	CELLCO-PART / TELEPONICA_DE_ESPANA
G	Web-search-engine-based	5	TW 100.0%	HINET Data Communication
H	Web-search-engine-based	360	ES99.4%	VODAPONE_ES / TELEPONICA_DE_ESPANA
I	Web-search-engine-based	3	DE 100%	INTERNETX_AS / DTAG internet service
J	Web-search-engine-based	67	US 51.5% FR 19.6% CN9.6%	CELLCO-PART / CELLCO
K	Web-search-engine-based	144	ES 99.9%	VODAPONE_ES / TELEPONICA_DE_ESPANA
L	Web-search-engine-based	85	us 84.3%	CELLCO-PART / CELLCO

実験の詳細 (web検索)


9 keywords
51 pages
Extract 31 strings
116 queries
Manually select OBE-related keywords
Filter
Google
Search with keywords using a web search engine
Get web pages of OBEs or manufacture
Extract words in h1~h4 html headings
Extract other keywords
Feedback two keywords
Yes
OBE or not
Scan
Censys
Search with each words and their combination using Censys
Get the candidates of OBEs

実験の詳細 (クラスタリング)



発見した車載機器の例 1/2

- Device F
  - Description
    - Multi-Port LTE-A Pro Rugged Vehicle Router for Public Safety Fleets and Industrial IoT.
  - Interfaces
    - Gigabit Ethernet ports (4), RS-232, USB 2.0, Configurable I/O and analog inputs

発見した車載機器の例 2/2

- Device G
  - Description of the manual
    - This device enables WAN connectivity for moving vehicles and contribute a reliable bi-directional communication for other on-board electronic devices.
  - Interfaces
    - 3-port gigabit Ethernet, digital IO, and RS232 serial.
    - A communication hub for other on-board electronic devices

発見した車載機器のセキュリティ

We investigated device security from network observations and online manuals.

7 out of 12 products run telnet/FTP

8 out of 12 products run outdated software

9 out of 12 products are confirmed/capable to connect to in-vehicle NW

4 out of 12 products expose sensitive information (e.g. location)

device name	Build-in/Retrofit	Manufacture country	Telnet/FTP	Weak default password	Outdated software	Telnet without Authentication	Connect to in-vehicle network	Information disclosure
A	Retrofit	US	-	-	Tildeslash monit 5.0	-	Confirmed by WebUI	Running process
B	Retrofit	FR	Telnet	-	OpenSSH 5.1	Possible	Confirmed by telnet	Location, ignition, and more…
C	?	US	-	Exists	Anonymized server name 1	-	-	-
D	?	DE	FTP, Telnet	-	OpenSSH 6.0p1 light httpd 1.4.26 PHP 5.2.6 Debian 7.0	-	Possible according to manual	-
E	?	DE	Telnet	-	Dropbear SSH 2017.75 light httpd 1.4.53 PHP 5.6.31	-	Possible according to manual	-
F	Retrofit	CA	Telnet	-	-	-	Possible according to manual	Location
G	Built-in	TW	-	-	-	-	Possible according to manual	-
H	Retrofit	FR	-	-	PHP 5.3.10	-	Possible according to manual	-
I	Built-in	SK	FTP	-	CrushFTP	-	-	-
J	Retrofit	CA	Telnet	-	-	-	Possible according to manual	Location
K	Built-in	ES	FTP	-	-	-	Possible according to manual	-
L	?	US	-	Exists	Anonymized server name 2	-	-	-

発見した車載機器のセキュリティ

We investigated device security from network observations and online manuals.

7 out of 12 products run telnet/FTP

8 out of 12 products run outdated software

9 out of 12 products are confirmed/capable to connect to in-vehicle NW

4 out of 12 products expose sensitive information (e.g. location)

device name	Build-in/Retrofit	Manufacture country	Telnet/FTP	Weak default password	Outdated software	Telnet without Authentication	Connect to in-vehicle network	Information disclosure
A	Retrofit	US	-	-	Tildeslash monit 5.0	-	Confirmed by WebUI	Running process
B	Retrofit	FR	Telnet	-	OpenSSH 5.1	Possible	Confirmed by telnet	Location, ignition, and more…
C	?	US	-	Exists	Anonymized server name 1	-	-	-
D	?	DE	FTP, Telnet	-	OpenSSH 6.0p1 light httpd 1.4.26 PHP 5.2.6 Debian 7.0	-	Possible according to manual	-
E	?	DE	Telnet	-	Dropbear SSH 2017.75 light httpd 1.4.53 PHP 5.6.31	-	Possible according to manual	-
F	Retrofit	CA	Telnet	-	-	-	Possible according to manual	Location
G	Built-in	TW	-	-	-	-	Possible according to manual	-
H	Retrofit	FR	-	-	PHP 5.3.10	-	Possible according to manual	-
I	Built-in	SK	FTP	-	CrushFTP	-	-	-
J	Retrofit	CA	Telnet	-	-	-	Possible according to manual	Location
K	Built-in	ES	FTP	-	-	-	Possible according to manual	-
L	?	US	-	Exists	Anonymized server name 2	-	-	-

発見した車載機器のセキュリティ

We investigated device security from network observations and online manuals.

7 out of 12 products run telnet/FTP

8 out of 12 products run outdated software

9 out of 12 products are confirmed/capable to connect to in-vehicle NW

4 out of 12 products expose sensitive information (e.g. location)

device name	Build-in/Retrofit	Manufacture country	Telnet/FTP	Weak default password	Outdated software	Telnet without Authentication	Connect to in-vehicle network	Information disclosure
A	Retrofit	US	-	-	Tildeslash monit 5.0	-	Confirmed by WebUI	Running process
B	Retrofit	FR	Telnet	-	OpenSSH 5.1	Possible	Confirmed by telnet	Location, ignition, and more…
C	?	US	-	Exists	Anonymized server name 1	-	-	-
D	?	DE	FTP, Telnet	-	OpenSSH 6.0p1 light httpd 1.4.26 PHP 5.2.6 Debian 7.0	-	Possible according to manual	-
E	?	DE	Telnet	-	Dropbear SSH 2017.75 light httpd 1.4.53 PHP 5.6.31	-	Possible according to manual	-
F	Retrofit	CA	Telnet	-	-	-	Possible according to manual	Location
G	Built-in	TW	-	-	-	-	Possible according to manual	-
H	Retrofit	FR	-	-	PHP 5.3.10	-	Possible according to manual	-
I	Built-in	SK	FTP	-	CrushFTP	-	-	-
J	Retrofit	CA	Telnet	-	-	-	Possible according to manual	Location
K	Built-in	ES	FTP	-	-	-	Possible according to manual	-
L	?	US	-	Exists	Anonymized server name 2	-	-	-

発見した車載機器のセキュリティ

We investigated device security from network observations and online manuals.

7 out of 12 products run telnet/FTP

8 out of 12 products run outdated software

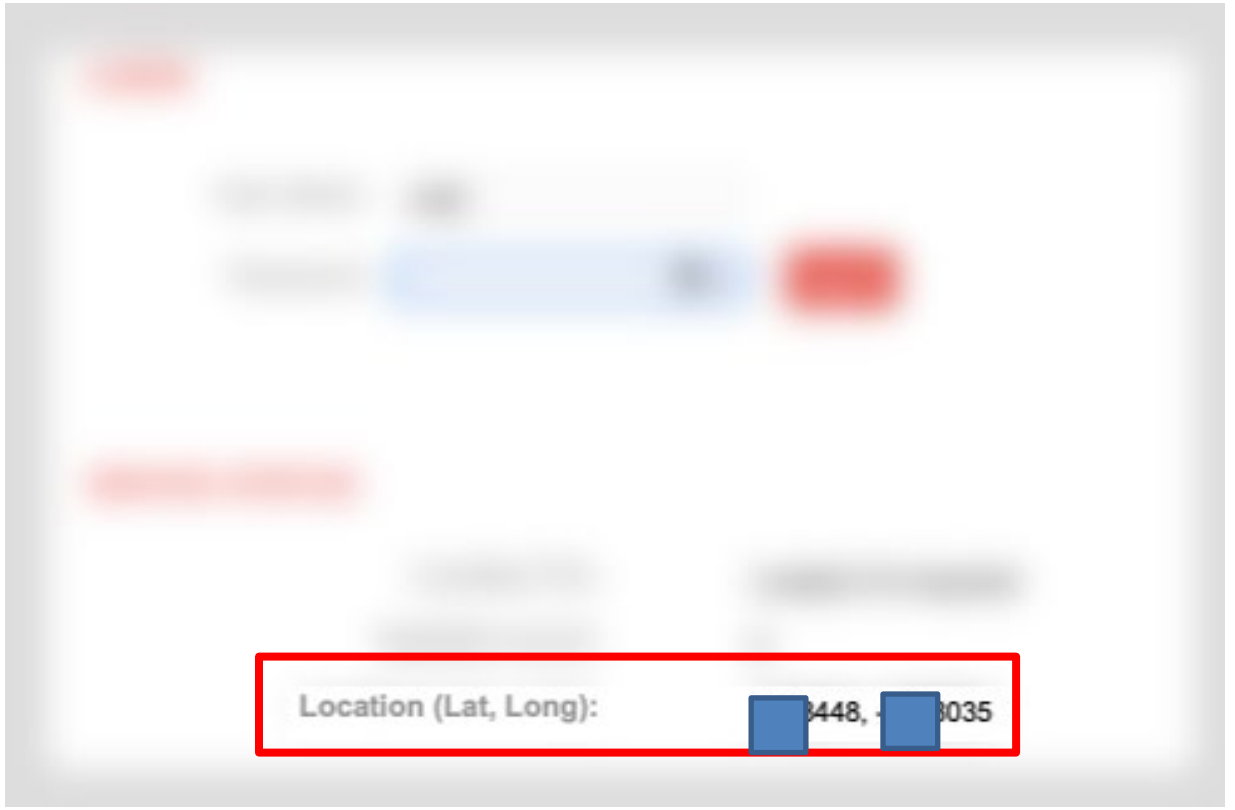
9 out of 12 products are confirmed/capable to connect to in-vehicle NW

4 out of 12 products expose sensitive information (e.g. location)

device name	Build-in/Retrofit	Manufacture country	Telnet/FTP	Weak default password	Outdated software	Telnet without Authentication	Connect to in-vehicle network	Information disclosure
A	Retrofit	US	-	-	Tildeslash monit 5.0	-	Confirmed by WebUI	Running process
B	Retrofit	FR	Telnet	-	OpenSSH 5.1	Possible	Confirmed by telnet	Location, ignition, and more…
C	?	US	-	Exists	Anonymized server name 1	-	-	-
D	?	DE	FTP, Telnet	-	OpenSSH 6.0p1 light httpd 1.4.26 PHP 5.2.6 Debian 7.0	-	Possible according to manual	-
E	?	DE	Telnet	-	Dropbear SSH 2017.75 light httpd 1.4.53 PHP 5.6.31	-	Possible according to manual	-
F	Retrofit	CA	Telnet	-	-	-	Possible according to manual	Location
G	Built-in	TW	-	-	-	-	Possible according to manual	-
H	Retrofit	FR	-	-	PHP 5.3.10	-	Possible according to manual	-
I	Built-in	SK	FTP	-	CrushFTP	-	-	-
J	Retrofit	CA	Telnet	-	-	-	Possible according to manual	Location
K	Built-in	ES	FTP	-	-	-	Possible according to manual	-
L	?	US	-	Exists	Anonymized server name 2	-	-	-

例：位置情報プライバシーの問題

- Device G opens 80/tcp and has a login console. The console discloses GPS location.



製造者への通知

- As a result of the security investigation, we identified that most devices have security concerns.

- From the viewpoint of responsible disclosure, we notified 11 manufacturers of the devices with security concerns.

製造者への質問

- With the notification document, we sent the following questions to OBE manufacturers.
  - Q1. Is the Web UI image from your product [product name]?
  - Q2. Were you aware of any security concerns?
  - Q3. Would you consider taking any mitigating actions regarding this security notification and what is it?
- 7 out of 11 manufacturers responded to our notification, and one manufacturer answered to our questionnaire.

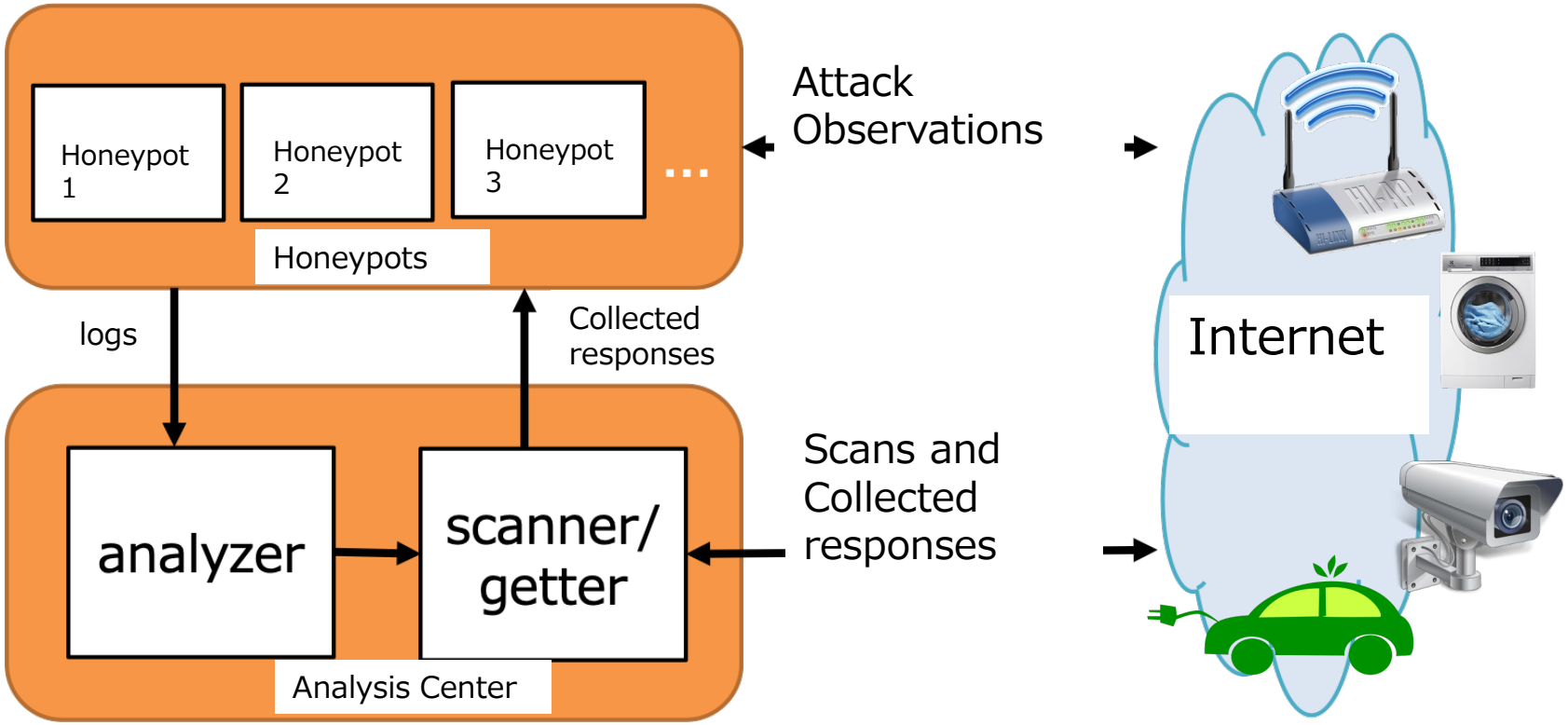
製造者からの回答状況

Manufacturer	Device	Our notification	Our questionnaire	Response from Manufacturers
1	A	Responded	Unanswered	It's a specification, not a vulnerability
2	B	Responded	Answered	Will remind clients to apply the available update with correct configuration for the affected devices
3	C	Responded	Unanswered	It's a specification, not a vulnerability
3	D	Responded	Unanswered	It's a specification, not a vulnerability
4	E	Acknowledgement	Unanswered	
4	F	Acknowledgement	Unanswered	
5	G	Ignored	Ignored	
7	I	Acknowledgement	Unanswered	It is great to hear from you that our product, device I is listed at your survey for vehicle solutions. Could you share the report for our reference? Thank you.
8	J	Ignored	Ignored	
5	K	Ignored	Ignored	
9	L	Ignored	Ignored	

For those manufacturers who did not respond at all, we also sent notification to the corresponding national CERT to inform the issue.

発見した車載機器を模擬するハニーポットの生成（実施中）

X-pot, our adaptive IoT honeypot, uses collected responses from Internet-wide scans as responses of honeypots.



We utilize this concept for vehicular honeypot.

まとめ

- We focused on the case that On Board Equipment directly connects to the Internet.
- We proposed a discovery method of connected OBE and found 12 OBE models (2,532 devices). They were routers or gateways for vehicles.
- We have started preliminary observations by our honeypots imitating discovered devices.

関連発表論文

Takahiro Ueda, Takayuki Sasaki, Katsunari Yoshioka, and Tsutomu Matsumoto, "An Internet-wide View of Connected Cars: Discovery of Exposed Automotive Devices," Proc. The 2nd International Workshop on Security and Privacy in Intelligent Infrastructures (SP2I 2022), 2022.

Takayuki Sasaki, Akira Fujita, Carlos Hernandez Ganan, Michel van Eeten, Katsunari Yoshioka, Tsutomu Matsumoto, "Exposed Infrastructures: Discovery, Attacks and Remediation of Insecure ICS Remote Management Devices," Proc. 43rd IEEE Symposium on Security and Privacy (IEEE S&P), 2022.

Seiya Kato, Rui Tanabe, Katsunari Yoshioka, Tsutomu Matsumoto, "Adaptive Observation of Emerging Cyber Attacks targeting Various IoT Devices," IFIP/IEEE International Symposium on Integrated Network Management (IM), 2021.