

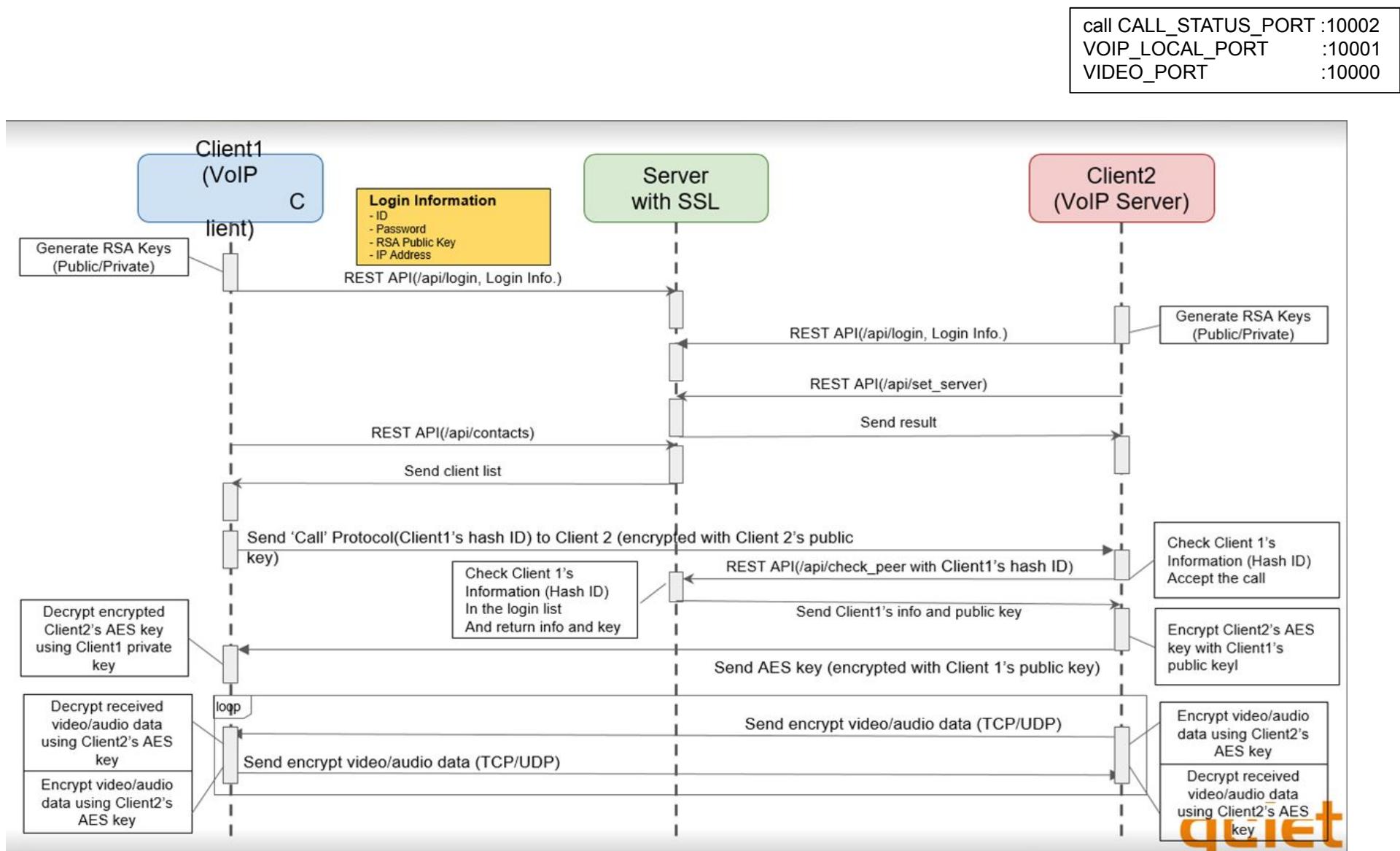
# VideoChat

3조 보안연대  
Team David  
Belasco

**team**  
**DB**



# Architecture(team1 project)



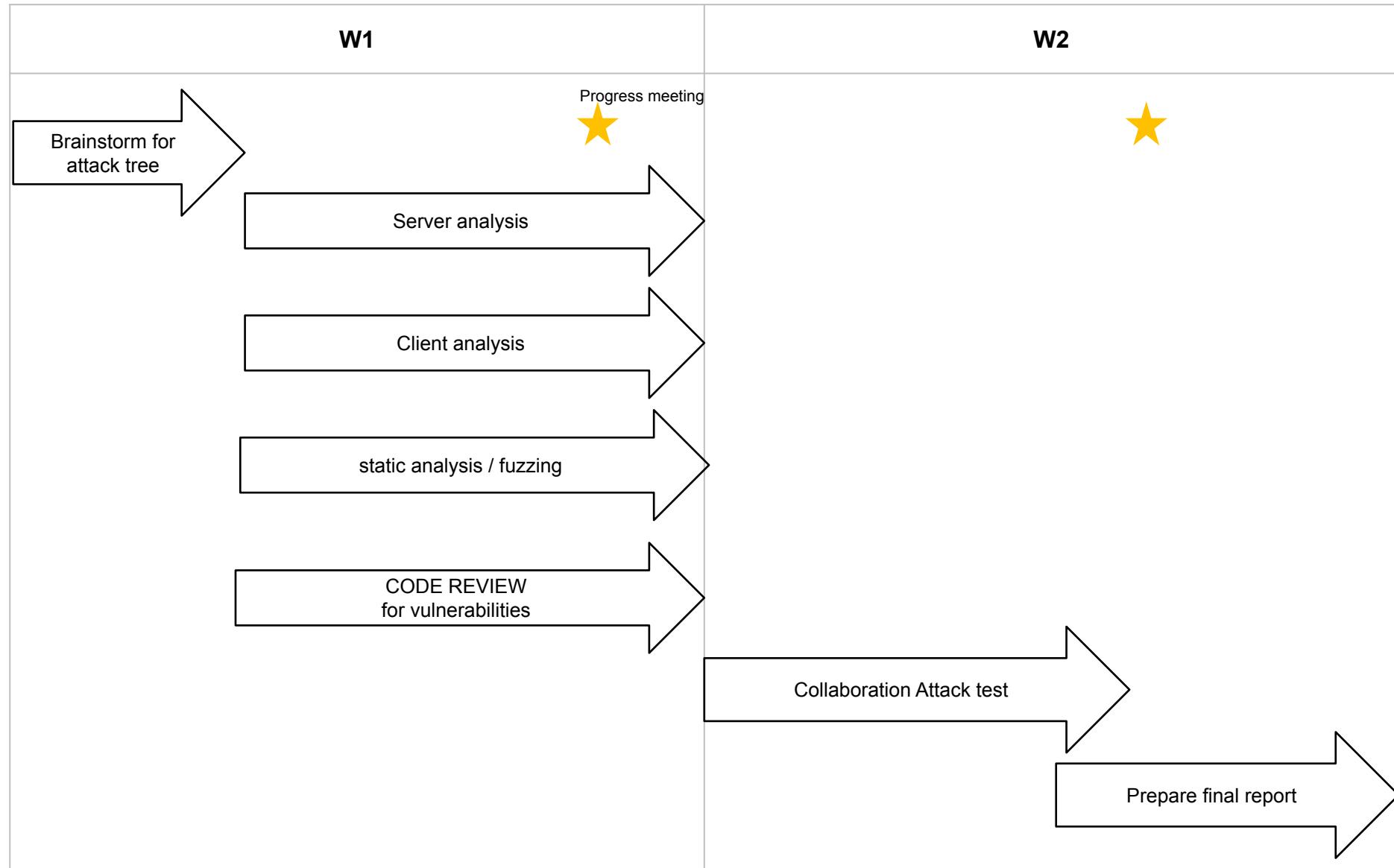
# Demo

# Project Members and Role

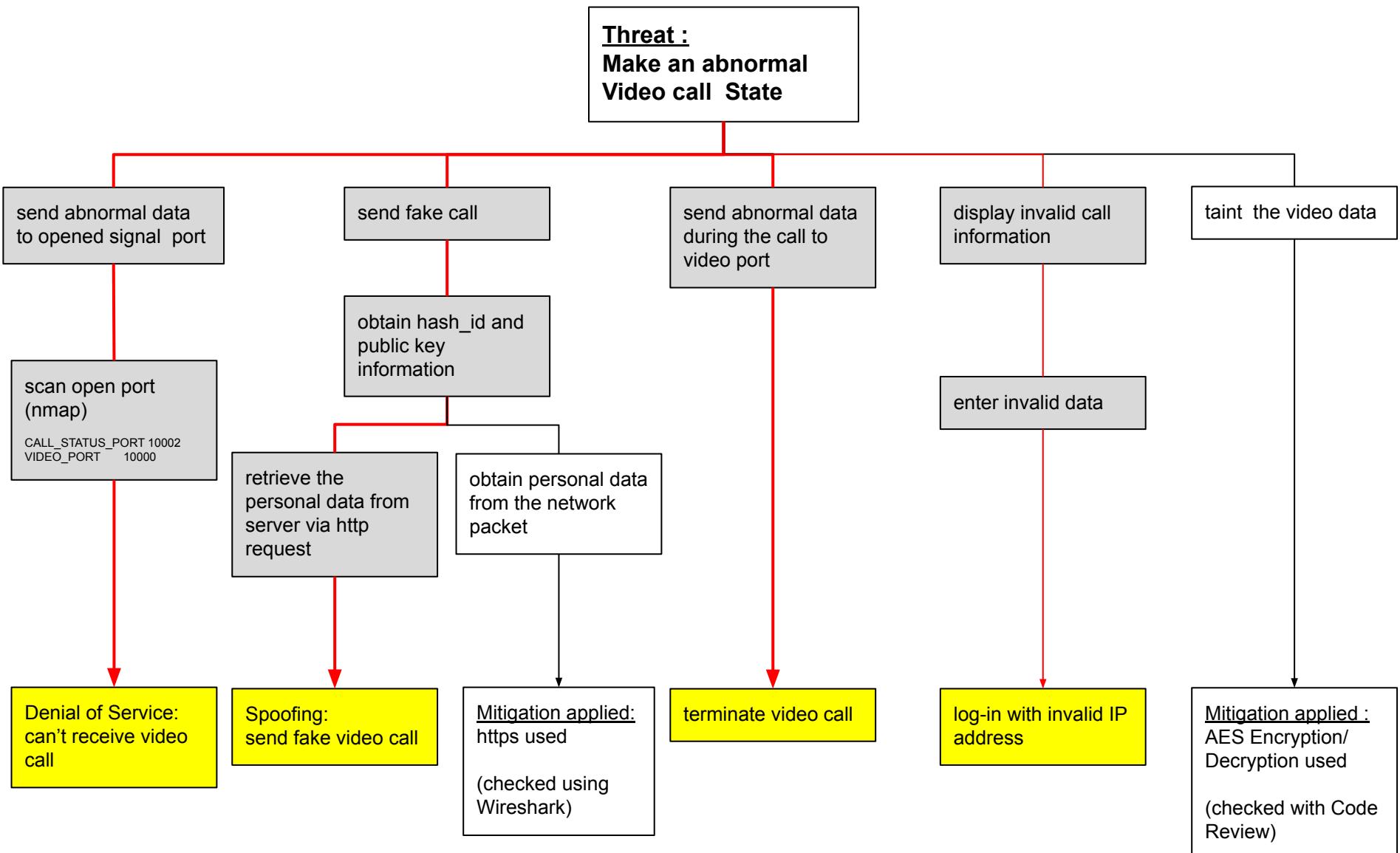
---

- Server vulnerability analysis  
Robin Kim(김성준), SeKi Park(박세기)
- Client vulnerability analysis  
SungMin Kim(김성민), DongHoon Shin(신동훈)
- Static analysis and fuzzing  
JiYoung Yoon(윤지영)
- Mentor / Support  
David Belasco

# Schedule



# Attack Tree



# Executive Summary

- Top 5 vulnerabilities listed out of 12

Priority	Vulnerability	Impact	Recommendation
High (CVSS 7.5) <b>Appendix-22</b>	If hash_id and public key is known, it is possible to make fake call. <b>(Spoofing)</b>	Attacker can <a href="#">make a fake call with hash_id and public_key</a> .	- Check and validate the caller's IP address. - Compare real IP and IP registered in server
High (CVSS 7.5)	Any call request can be allowed. <b>(Denial of Service)</b>	Attacker can <a href="#">make a fake call infinitely</a>	- Check and validate the caller's IP address - Limit request count within some duration
High (CVSS 7.5)	Anyone can send the call end request. <b>(Denial of Service)</b>	Attacker can <a href="#">make a request call end infinitely</a> Attacker can make <a href="#">call end during a call</a>	- Open video port only call is received
Mid (CVSS 5.4)	All REST api is exposed. <b>(Information disclosure)</b>	An attacker can <a href="#">retrieve the personal data via http request</a>	Remove REST api document page
Low (CVSS 3.1)	Need <a href="#">IP address sanitizer</a>	Possible to log-in with invalid IP address	IP address input validation

# Evaluation Constraints - Mitigating Factors

Mitigating Factors	Descriptions
Data Encryption	Video call data should be secured in transit.
	Sensitive data should be stored securely.
Authentication / Authorization	All users should be authenticated correctly and securely.
	Network communications should use TLS or an equivalent encryption protocol.
	Each user should only have the capabilities they are explicitly granted permitted to use
Secure Coding	Secure coding practices are applied to avoid common security flaws like SQL injection and buffer overflow.

# Evaluation Constraints - Assumptions

Assumptions	Descriptions
Cryptography	Crypto APIs used are assumed to be secure. ex) RAND_bytes()
	Crypto library providing APIs is assumed to be safe. ex) OpenSSL
Storage Security	Due to hardware constraints, credentials are assumed to be securely stored in trusted location.
	Credentials are not left in system memory.
	The inherent stability and security specific to currently used database are not taken into consideration.

# Evaluation Narrative

Analysis Technique	Using Tool	Result	Vulnerability
Static Analysis X Code Review O	SonarCloud, Cppcheck	No meaningful issue	Vul-5 <a href="#">Appendix-11~13</a>
Web Fuzzing O	DirBuster, DIRB	Detected critical page (docs, redoc) REST api is exposed and possible to get user data.	Vul-1 <a href="#">Appendix-1~4</a>
Client Fuzzing X	SPIKE	Run a fuzzing test on the socket communication and found no issues.	None <a href="#">Appendix-23</a>
Input Validation O	Code Review	Need IP address validation. (Any data is acceptable in IP addr)	Vul-5 <a href="#">Appendix-10</a>
Use Exploit Tools O	Postman, Wireshark, nmap, Kali, scapy, checksec	Postman - http request Kali - ARP spoofing checksec - CFG,RFG not present User info. is exposed with REST api.	Vul-2, Vul-3, Vul-4 Vul-6 <a href="#">Appendix-5~9</a> <a href="#">Appendix-17~21</a>
Research Vulnerability DB X	<a href="https://www.cvedetails.com">https://www.cvedetails.com</a>	No issue : There's no vulnerabilities. (openssl 3.1.1, opus 1.3.1)	None <a href="#">Appendix-14</a>
Dependency check X	Owasp dependency-check	No meaningful issue	None <a href="#">Appendix-15</a>

\*\* Vul : It's defined vulnerability issue.

# Vulnerability Reporting(1)

Num.	Summary	Location	Consequences/ Impact	CVSS Score	Proof of Concept(POC)
Vul-1	REST api is exposed. <b>/ Network Attack</b>	FastAPI expose REST api in docs, redoc	Attacker can retrieve user information / <b>Information disclosure</b>	CVSS 5.4	<a href="https://ip:8000/docs">https://ip:8000/docs</a> <a href="https://ip:8000/redoc">https://ip:8000/redoc</a>
Vul-2	Make fake call <b>/ Client exploit</b>	If hash_id, public_key and IP is known, it is possible to make fake call	Attacker can make the fake call / <b>Spoofing</b>	CVSS 7.5	C++/Python exploit code can be made
Vul-3	Make fake call infinitely <b>/ Client exploit</b>	same as Vul-2	Attacker can make the fake call infinitely / <b>Denial of Service</b>	CVSS 7.5	C++/Python exploit code can be made

```
peer_hash_id = 'WOYXCNFRXYCVFO66'  
rsa_key = 'LS0tLS1CRUdJTiBQVUJMSUMgS0VZLS0 ... <snippet>'  
  
my_socket.connect(host, port)  
encrypt_msg = my_socket.encrypt_message(rsa_key, peer_hash_id)  
my_socket.send(encrypt_msg)
```

# Vulnerability Reporting(2)

Num.	Summary	Location	Consequences/ Impact	CVSS Score	Proof of Concept(POC)
Vul-4	Make fake call end infinitely <b>/ Client exploit</b>	video port 10000 is always ready	Attacker can make the fake call end infinitely / <b>Denial of Service</b>	CVSS 7.5	C++/Python exploit code can be made
Vul-5	IP address input validation <b>/ Client attack</b>	No IP address validation check	Can not use video call if invalid IP address entered /	CVSS 3.1	Executable with invalid IP address
Vul-6	Spoof Voip Server <b>/ MITM, Network Attack</b>  <u>* Exploit not complete</u>	Voip client does not have the process of authenticating Voip server.	Attacker can send AES keys Voip client/ Incorrect call connection or exposure of image data	CVSS 5.4	ARP Spoofing IP Spoofing

# Weakness Reporting(1) - Client

Num.	Summary	Location	Consequences/ Impact	CWE number	Proof of Concept(POC)
Weak-1	Unchecked Return Value	LgVideoChatDemo\LgVideoChat Demo\AecKsBinder.cpp line 202,203 LgVideoChatDemo\LgVideoChat Demo.cpp line 175,705, 713	N/A	CWE-252	If error returns, malfunction
Weak-2	Indicator of Poor Code Quality	LgVideoChatDemo\LgVideoChat Demo\FixedSizeQueue.h line 18  LgVideoChatDemo\LgVideoChat Demo\mediabuf.h line 20	N/A	CWE-398	N/A
Weak-3	Missing Release of File Descriptor Handle after Effective Lifetime	LgVideoChatDemo\LgVideoChat Demo.cpp line 925	N/A	CWE-775	Memory leak

verbose	sinceDate	cwe	file0
Return value of function StringCchCopy() is not used.	M/d/yyyy	252	C:/hacking/LG_Security_Team1/LgVideoChatDemo/LgVideoChatDemo/AeksBin
Return value of function StringCchCopy0 is not used.	M/d/yyyy	252	C:/hacking/LG_Security_Team1/LgVideoChatDemo/LgVideoChatDemo/LgVideoChatDemo/AeksBin
Return value of function freopen_s0 is not used.	M/d/yyyy	252	C:/hacking/LG_Security_Team1/LgVideoChatDemo/LgVideoChatDemo/LgVideoChatDemo/LgVideoChatDemo/AeksBin
Return value of function CreateWindow() is not used.	M/d/yyyy	252	C:/hacking/LG_Security_Team1/LgVideoChatDemo/LgVideoChatDemo/LgVideoChatDemo/LgVideoChatDemo/LgVideoChatDemo/AeksBin
Return value of function CreateWindow() is not used.	M/d/yyyy	252	C:/hacking/LG_Security_Team1/LgVideoChatDemo/LgVideoChatDemo/LgVideoChatDemo/LgVideoChatDemo/LgVideoChatDemo/LgVideoChatDemo/AeksBin
Return value of function CreateWindow() is not used.	M/d/yyyy	252	C:/hacking/LG_Security_Team1/LgVideoChatDemo/LgVideoChatDemo/LgVideoChatDemo/LgVideoChatDemo/LgVideoChatDemo/LgVideoChatDemo/AeksBin
Return value of function CreateWindowEx0 is not used.	M/d/yyyy	252	C:/hacking/LG_Security_Team1/LgVideoChatDemo/LgVideoChatDemo/LgVideoChatDemo/LgVideoChatDemo/LgVideoChatDemo/LgVideoChatDemo/AeksBin
Return value of function CreateWindow() is not used.	M/d/yyyy	252	C:/hacking/LG_Security_Team1/LgVideoChatDemo/LgVideoChatDemo/LgVideoChatDemo/LgVideoChatDemo/LgVideoChatDemo/LgVideoChatDemo/AeksBin
Return value of function CreateWindow() is not used.	M/d/yyyy	252	C:/hacking/LG_Security_Team1/LgVideoChatDemo/LgVideoChatDemo/LgVideoChatDemo/LgVideoChatDemo/LgVideoChatDemo/LgVideoChatDemo/AeksBin
Resource leak: m_singleInstanceMutex	M/d/yyyy	775	C:/hacking/LG_Security_Team1/LgVideoChatDemo/LgVideoChatDemo/LgVideoChatDemo/LgVideoChatDemo/LgVideoChatDemo/LgVideoChatDemo/AeksBin
#error Please add support for your architecture in typedefs.h	M/d/yyyy		
Class &#039;FixedSizeQueue&#039; does not have a copy constructor which is recommended since it has no operator=.	M/d/yyyy	398	C:/hacking/LG_Security_Team1/LgVideoChatDemo/LgVideoChatDemo/VoipNetw
Class &#039;FixedSizeQueue&#039; does not have a copy constructor which is recommended since it has no operator=.	M/d/yyyy	398	C:/hacking/LG_Security_Team1/LgVideoChatDemo/LgVideoChatDemo/VoipNetw
Class &#039;FixedSizeQueue &lt; voipbuffer &gt;&#039; does not have a copy constructor which is recommended since it has no operator=.	M/d/yyyy	398	C:/hacking/LG_Security_Team1/LgVideoChatDemo/LgVideoChatDemo/VoipVoic
Class &#039;FixedSizeQueue &lt; voipbuffer &gt;&#039; does not have a copy constructor which is recommended since it has no operator=.	M/d/yyyy	398	C:/hacking/LG_Security_Team1/LgVideoChatDemo/LgVideoChatDemo/VoipVoic
Member variable &#039;CBaseMediaBuffer::m_pData&#039; is not initialized in the constructor.	M/d/yyyy	398	C:/hacking/LG_Security_Team1/LgVideoChatDemo/LgVideoChatDemo/VoipVoic
Member variable &#039;CBaseMediaBuffer::m_ulSize&#039; is not initialized in the constructor.	M/d/yyyy	398	C:/hacking/LG_Security_Team1/LgVideoChatDemo/LgVideoChatDemo/VoipVoic
Member variable &#039;CBaseMediaBuffer::m_cRef&#039; is not initialized in the constructor.	M/d/yyyy	398	C:/hacking/LG_Security_Team1/LgVideoChatDemo/LgVideoChatDemo/VoipVoic
Member variable &#039;CBaseMediaBuffer::m_ulData&#039; is not initialized in the constructor.	M/d/yyyy	398	C:/hacking/LG_Security_Team1/LgVideoChatDemo/LgVideoChatDemo/VoipVoic

# Weakness Reporting(2) - OpenCV

OpenCV has 8 CWEs, Major 3 are below

## CWE - 190 : Integer Overflow or Wraparound

CWE Definition	<a href="http://cwe.mitre.org/data/definitions/190.html">http://cwe.mitre.org/data/definitions/190.html</a>
Number of vulnerabilities:	<a href="#">1879</a>
Description	The software performs a calculation that can produce an integer overflow or wraparound, when the logic assumes that the resulting value will always be larger than the original value. This can introduce other weaknesses when the calculation is used for resource management or execution control. An integer overflow or wraparound occurs when an integer value is incremented to a value that is too large to store in the associated representation. When this occurs, the value may wrap to become a very small or negative number. While this may be intended behavior in circumstances that rely on wrapping, it can have security consequences if the wrap is unexpected. This is especially the case if the integer overflow can be triggered using user-supplied inputs. This becomes security-critical when the result is used to control looping, make a security decision, or determine the offset or size in behaviors such as memory allocation, copying, concatenation, etc.

## CWE - 476 : NULL Pointer Dereference

CWE Definition	<a href="http://cwe.mitre.org/data/definitions/476.html">http://cwe.mitre.org/data/definitions/476.html</a>
Number of vulnerabilities:	<a href="#">2131</a>
Description	A NULL pointer dereference occurs when the application dereferences a pointer that it expects to be valid, but is NULL, typically causing a crash or exit.
Background Details	
Other Notes	

## CWE - 457 : Use of Uninitialized Variable

CWE Definition	<a href="http://cwe.mitre.org/data/definitions/457.html">http://cwe.mitre.org/data/definitions/457.html</a>
Number of vulnerabilities:	<a href="#">10</a>
Description	The code uses a variable that has not been initialized, leading to unpredictable or unintended results. In some languages, such as C, an uninitialized variable contains contents of previously-used memory. An attacker can sometimes control or read these contents.
Background Details	
Other Notes	Before variables are initialized, they generally contain junk data of what was left in the memory that the variable takes up. This data is very rarely useful, and it is generally advised to pre-initialize variables or set them to their first values early. If one forgets -- in the C language -- to initialize, for example a char *, many of the simple string libraries may often return incorrect results as they expect the null termination to be at the end of a string.

# Conclusions and Recommendations

---

- REST API document page must be \*NOT\* exposed publicly.
- Authenticate and validate all requests on server-side (eg. IP check)
- Rate Limiting
  - Set limits on number of requests per user or IP in certain time
- Recommend implementing logging system
- IP Reputation Lists : Blocking known malicious IPs
- Least Privilege Principle to SQLite db
  - No password and no setting of privilege in SQLite db
- Setup IDS(Intrusion Detection Systems)
  - monitor and alert system to detect any unusual activities

# Reflection and Lessons Learned

---

- Gained critical insights into security vulnerabilities, types of attacks, and the potential for exploitation
- Required more experience to apply the attack techniques we have practiced in the course

## What Worked Well?

- All requirements are satisfied in time
- Collaborated very well with each other during the project

## What Didn't Work Well?

- Does NOT execute GUI based Client Fuzzing (winAFL...)

# Appendix

# Appendix-1) DirBuster

## Web Fuzzing Tool (DirBuster)

OWASP DirBuster 0.12 - Web Application Brute Forcing

File Options About Help

https://localhost:8000/

List View Tree View

Type	Found	Res...	Size	Include	Status
Dir	/home/	405	187	<input checked="" type="checkbox"/>	Waiting
Error	/login/		69	<input type="checkbox"/>	Return code for first HEAD, is different to the second GET: 405 - 200
Dir	/login/	405	1268	<input checked="" type="checkbox"/>	Waiting
Dir	/docs/	307	147	<input checked="" type="checkbox"/>	Waiting
Error	/signup/		69	<input type="checkbox"/>	Return code for first HEAD, is different to the second GET: 405 - 200
Dir	/signup/	405	1530	<input checked="" type="checkbox"/>	Waiting
Dir	/contacts/	307	151	<input checked="" type="checkbox"/>	Waiting
Error	/		39	<input type="checkbox"/>	IOException Connection refused: connect
Error	/forgetpw		39	<input type="checkbox"/>	IOException Connection refused: connect
Error	/resetpw		39	<input type="checkbox"/>	IOException Connection refused: connect
Error	/logout/		69	<input type="checkbox"/>	Return code for first HEAD, is different to the second GET: 405 - 307
Dir	/logout/	405	126	<input checked="" type="checkbox"/>	Waiting
Dir	/redoc/	307	148	<input checked="" type="checkbox"/>	Waiting

Current speed: 216 requests/sec (Select and right click for more options)  
Average speed: (T) 213, (C) 214 requests/sec  
Parse Queue Size: 0 Current number of running threads: 10  
Total Requests: 97180/18963863 Change  
Time To Finish: 24:29:22

Back Pause Stop Report

Brute forcing dirs in / /webattackgold/

# Appendix-2) DIRB(1)

---

```
$ dirb https://127.0.0.1:8000
```

```
-----  
DIRB v2.22
```

```
By The Dark Raver
```

```
-----  
START_TIME: Tue Jun 27 22:31:01 2023
```

```
URL_BASE: https://127.0.0.1:8000/
```

```
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
```

```
-----  
GENERATED WORDS: 4612
```

```
---- Scanning URL: https://127.0.0.1:8000/ ----
```

```
+ https://127.0.0.1:8000/contacts (CODE:422|SIZE:175)  
+ https://127.0.0.1:8000/docs (CODE:200|SIZE:953)  
+ https://127.0.0.1:8000/home (CODE:307|SIZE:0)  
+ https://127.0.0.1:8000/login (CODE:307|SIZE:0)  
+ https://127.0.0.1:8000/logout (CODE:307|SIZE:0)  
+ https://127.0.0.1:8000/signup (CODE:307|SIZE:0)  
+ https://127.0.0.1:8000/static (CODE:307|SIZE:0)
```

```
-----  
END_TIME: Tue Jun 27 22:31:08 2023
```

```
DOWNLOADED: 4612 - FOUND: 7
```

# Appendix-3) DIRB(2)

<https://localhost:8000/redoc>

The screenshot shows a web browser window with the URL <https://localhost:8000/redoc>. The title bar says "주의 요함 | https://localhost:8000/redoc". The page content is titled "LG Secu Team 1 - Login Server (1.0.0)". On the left, there are two sections: "users-webapp" and "auth-webapp", each with a right-pointing arrow. Below these, under "auth-webapp", is the text "Download OpenAPI specification: [Download](#)". A red rectangular box highlights the "Download" button.

## openapi.json

```
{"openapi": "3.0.2", "info": {"title": "LG Secu Team 1 - Login Server", "version": "1.0.0"}, "paths": {"/signup": {"get": {"tags": ["users-webapp"], "summary": "Register", "operationId": "register_signup_get", "responses": {"200": {"description": "Successful Response", "content": {"application/json": {"schema": {}}}}, "post": {"tags": ["users-webapp"], "summary": "Register", "operationId": "register_signup_post", "responses": {"200": {"description": "Successful Response", "content": {"application/json": {"schema": {}}}}, "422": {"description": "Validation Error", "content": {"application/json": {"schema": {"$ref": "#/components/schemas/HTTPValidationError"}}}}}}, "/login": {"get": {"tags": ["auth-webapp"], "summary": "Login", "operationId": "login_login_get", "responses": {"200": {"description": "Successful Response", "content": {"application/json": {"schema": {}}}}, "post": {"tags": ["auth-webapp"], "summary": "Login", "operationId": "login_login_post", "responses": {"200": {"description": "Successful Response", "content": {"application/json": {"schema": {}}}}, "422": {"description": "Validation Error", "content": {"application/json": {"schema": {"$ref": "#/components/schemas/HTTPValidationError"}}}}}}, "/login_from_app": {"post": {"tags": ["auth-webapp"], "summary": "Login From App", "operationId": "login_from_app_login_from_app_post", "requestBody": {"content": {"application/json": {"schema": {"$ref": "#/components/schemas/AppLoginData"}}}, "required": true}, "responses": {"200": {"description": "Successful Response", "content": {"application/json": {"schema": {}}}}, "422": {"description": "Validation Error", "content": {"application/json": {"schema": {"$ref": "#/components/schemas/HTTPValidationError"}}}}}}, "/get_contacts": {"get": {"tags": ["auth-webapp"], "summary": "Get Contacts", "operationId": "get_contacts_contacts_get", "parameters": [{"required": true, "schema": {"title": "Hash Id", "name": "hash_id", "in": "query"}}, {"required": true, "schema": {"title": "Session Id", "name": "session_id", "in": "query"}]}, "responses": {"200": {"description": "Successful Response", "content": {"application/json": {"schema": {}}}}, "422": {"description": "Validation Error", "content": {"application/json": {"schema": {"$ref": "#/components/schemas/HTTPValidationError"}}}}}, "/set_server": {"post": {"tags": ["auth-webapp"], "summary": "Turn On Server", "operationId": "set_server_set_server_post", "requestBody": {"content": {"application/json": {"schema": {"$ref": "#/components/schemas/AppSessionData"}}}, "required": true}, "responses": {"200": {"description": "Successful Response", "content": {"application/json": {"schema": {}}}}, "422": {"description": "Validation Error", "content": {"application/json": {"schema": {"$ref": "#/components/schemas/HTTPValidationError"}}}}}}}}
```

# Appendix-4) DIRB(3)

The screenshot shows a web-based API documentation interface, likely from a tool like Swagger or Postman. The top navigation bar includes icons for back, forward, search, and various system links related to LG SOLAR, t-enervu, ESSSWELL, and other internal systems.

The main title is "LG Secu Team 1 - Login Server" with version "1.0.0" and "OAS3". Below the title is a link to "/openapi.json".

The interface is organized into sections:

- users-webapp**:
  - GET /signup/ Register
  - POST /signup/ Register
  - GET /qrcode Register
- auth-webapp**:
  - GET /login/ Login
  - POST /login/ Login
  - POST /login\_from\_app Login From App
  - GET /contacts Get Contacts
  - POST /contacts Get Contacts

# Appendix-5) Information Disclosure(Postman) - Exploit

POST https://localhost:8000/login\_from\_app...

Params Authorization Headers (10) Body Pre-request

none form-data x-www-form-urlencoded raw

```
1 {"email": "seongjun@andrew.cmu.edu",
2 "password": "Lge1234!@#$",
3 "token": "775733",
4 "ip_address": "127.0.0.1",
5 "rsa_public_key": "LS0tLS1CRUdJTiBQVUJMSUMgS0VZLS0tLS0KTUlJQk1q
mttRGluc0s5TjgwQXovCkVYcFlHYVdqawJXOHftT0VyRj
pVApVNFFTRs9PNStyVmhp0VQ3S3hQbWZudlI3bTRLMmpF
S0tLS1FTkQgUFVCTElDIEtFWS0tLS0tCg=="
6
7 }
```

Body Cookies Headers (4) Test Results

Pretty Raw Preview Visualize JSON

```
1 {"errorCode": 0,
2 "msg": "Success",
3 "session_id": "3Z5SNUTM7JFFUQEG",
4 "hash_id": "WOYXCNFRXYCVF066"
5
6 }
```

POST https://localhost:8000/contacts

Params Authorization Headers (10) Body Pre-request Script Tests Set

none form-data x-www-form-urlencoded raw binary GraphQL

```
1 {"session": "3Z5SNUTM7JFFUQEG",
2 "hash_id": "WOYXCNFRXYCVF066"
3
4 }
```

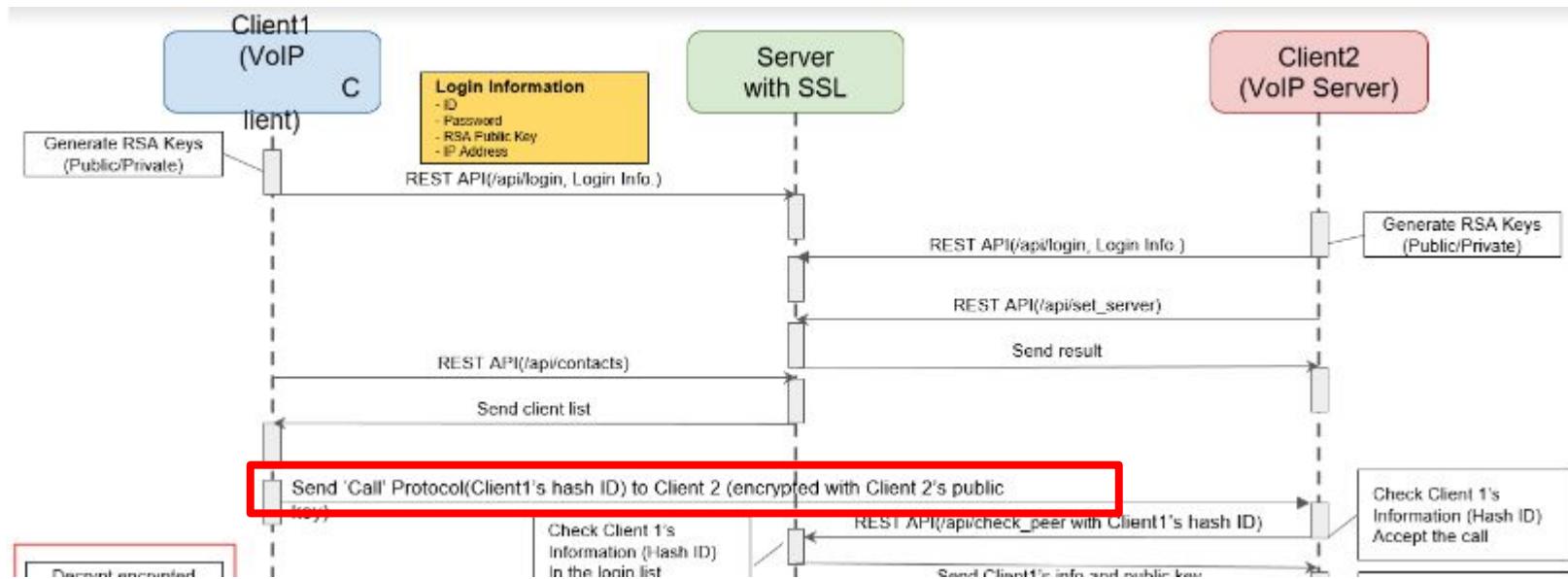
Body Cookies Headers (4) Test Results

Pretty Raw Preview Visualize JSON

```
1 {"errorCode": 0,
2 "msg": [
3     {
4         "email": "shindh84@gmail.com",
5         "hash_id": "6NSPYQESY2RT3AFJ",
6         "ip_address": "192.168.219.111",
7         "rsa_public_key": "LS0tLS1CRUdJTiBQVUJMSUMgS0VZLS0tLS0KTUlJQk1qQU5CZ
UtHTE1GL2d6YWFOVf1MaxNLRGQ4ZHNCkKN5eW1Z0GZ0aGFh1LZ
0N2tpL0NOQ2hUS3Z5ZE1IUFhNTAp4WVBmNLz1Ri9DRktoS0VXbr
XhGeURNUFN5RTZYc3JjbVIKQ1FJREFRQUIKLS0tLS1FTkQgUFV
8
9         "first_name": "Donghoon",
10        "last_name": "Shin",
11        "is_server": true
12    },
13    {
14        "email": "seongjun@andrew.cmu.edu",
15        "hash_id": "WOYXCNFRXYCVF066",
16        "ip_address": "127.0.0.1",
17        "rsa_public_key": "LS0tLS1CRUdJTiBQVUJMSUMgS0VZLS0tLS0KTUlJQk1qQU5CZ
2M4dFU0bkNkYmttRGluc0s5TjgwQXovCkVYcFlHYVdqawJXOHft
aSHz1UVZCMitsVWFpcUhjalRpVApVNFFTRs9PNStyVmhp0VQ3S
1N5Y0EzZ3pwK1Q5N0l0MHcKRXdJREFRQUIKLS0tLS1FTkQgUFV
18        "first_name": "Robin",
19        "last_name": "Kim",
20        "is_server": false
21    }
22 ]}
```

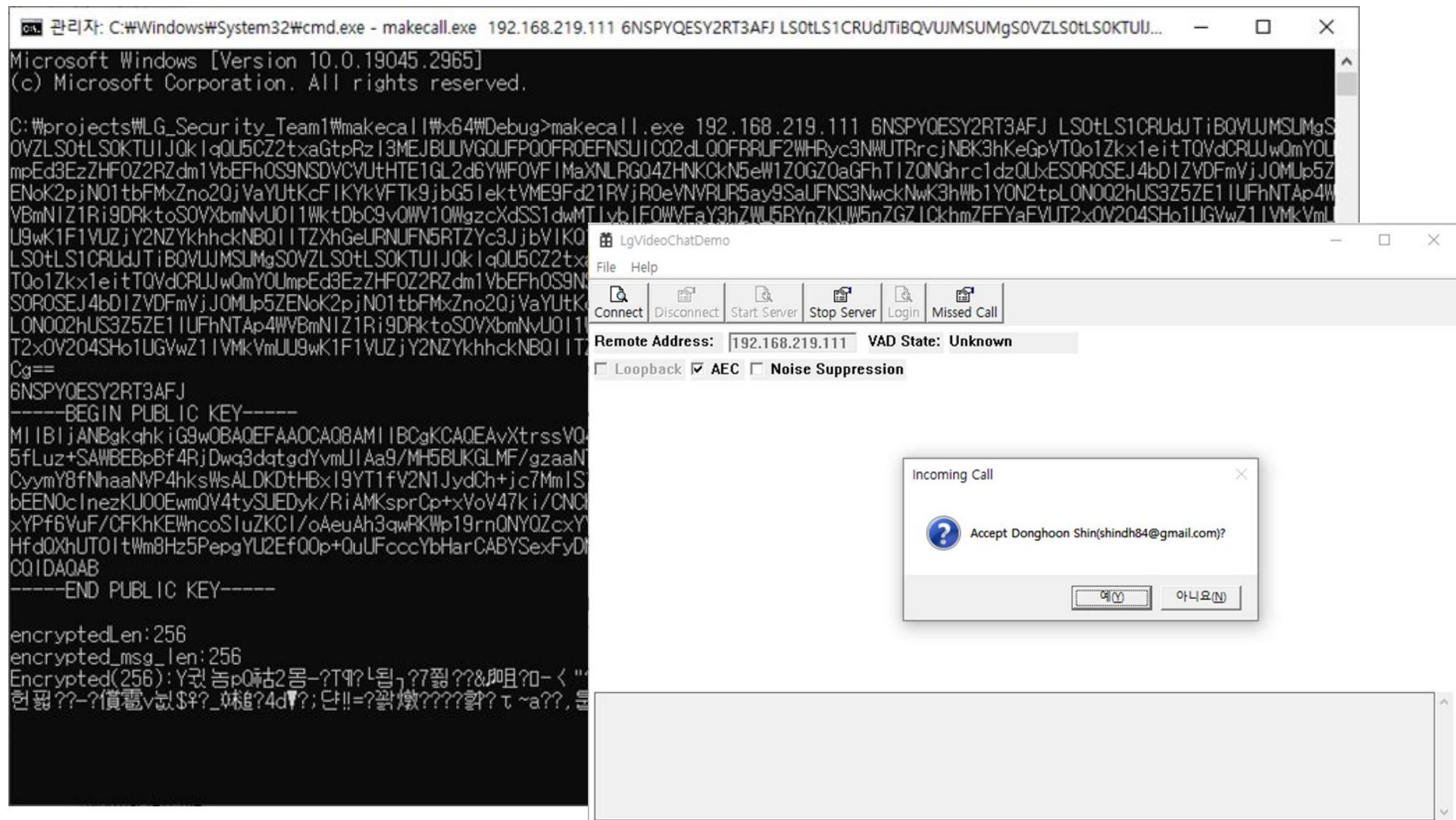
# Appendix-6) Spoofing - Vulnerability

We can pretend to be someone else on the contact list with hash\_id and rsa\_public\_key and make a call



# Appendix-7) Spoofing - Exploit

Exploit with hash\_id and rsa\_public\_key for making a call



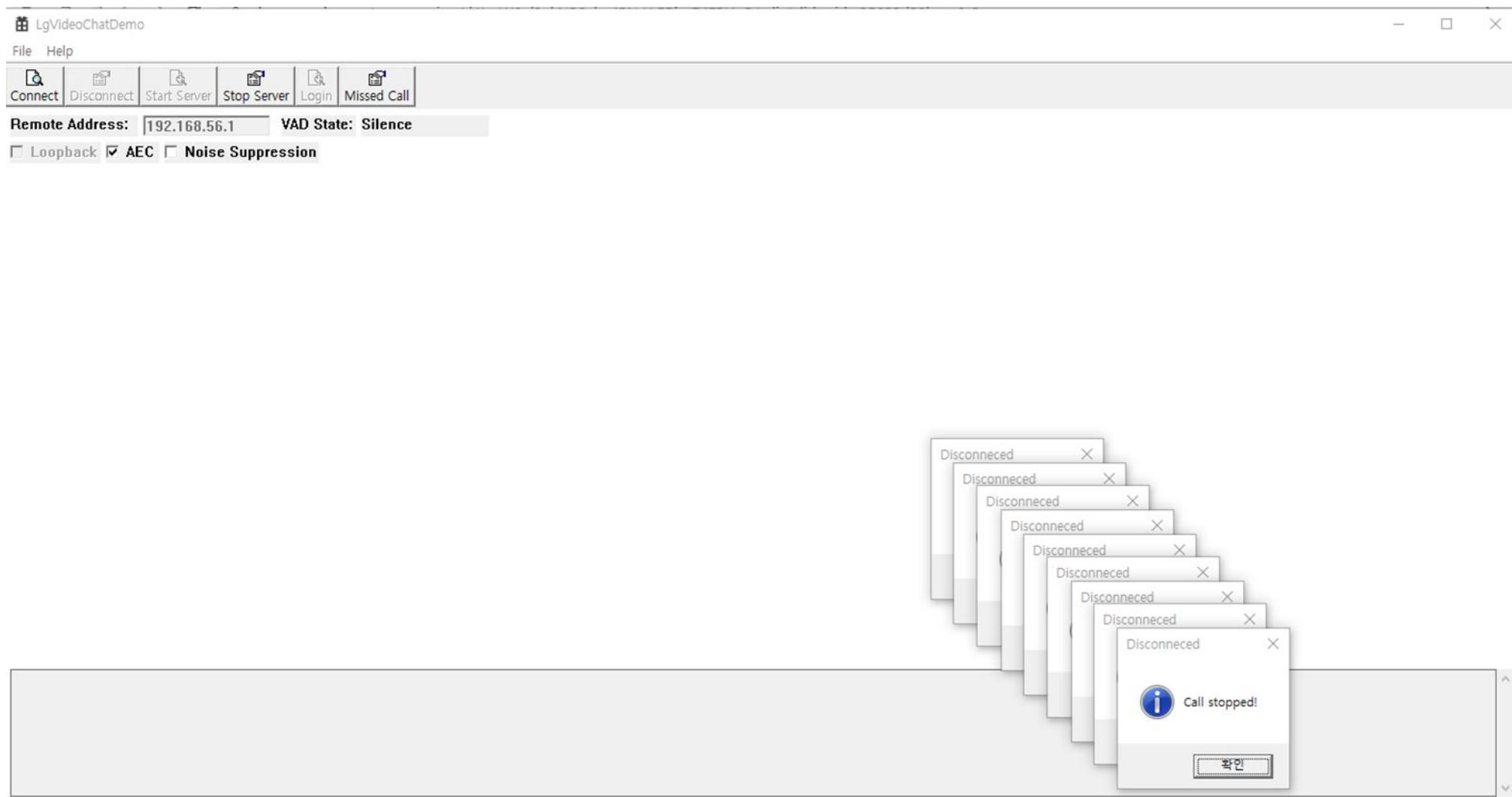
# Appendix-8) Denial of Service - Vulnerability

Exploit with hash\_id and rsa\_public\_key for making a call

Last option is count and if we keep make a call, app invoke notice popup infinitely

```
C:\projects\LG_Security_Team1\makecall\Debug>makecall.exe 192.168.219.111 6NSPYQESY2RT3AFJ LS0tLS1CRUdJTiBQVUJMSUMgS0VZLS0tLS0KU1JQkIqQU5CZ2txaGtpRzI3MEJBUIUVGQULFPQ0FROEFNSU1CQ2dLQ0FRRLUF2WHRyc3NWUTRrcjNBK3hKeGpVTQo1Zkx1eitTQVdCRUJwQmYOUmpEd3EzZHF0Z2RZdm1YbEFh0S9NSDVCVUtHTE1GL2d6YWF0VFIMaXNLRGQ4ZHNKckN5eW1ZOGZ0aGFhTIZQNghrc1dzQUxES0ROSEJ4bDIZVDFmVjJOMUp5ZENoK2pjN01tbFMxZno2QjVaYUjtKcFIKYkVFTk9jbG5IektVME9Fd21RVjRoEVNVRUR5ay9SaUFNS3NwckNwK3hWb1YON2tpLON0Q2hUS3Z5ZE1IUFhNTAp4WVBmN1Z1Ri9DRktoS0VXbmNvU011WktDbC9vQWV1QWgzcXdSS1dwMTIybIF0WVFaY3hZWU5RYnZKUW5nZGZ1CkhmZFFYaFVUT2x0V204SHo1UGVwZ1IVMkVmLU9wK1F1VUZjY2NZYkhckNBQ1ITZXhGeURNUFN5RTZYc3JjbVIKQ1FJREFRQIJKLS0tLS1FTkQgUFVCTEIDIEtFWS0tLS0tCg== 10
```

# Appendix-9) Denial of Service - Exploit



# Appendix-10) Input Validation

The image displays three windows illustrating a login process and its interaction with a video chat application.

**Left Window (Login Form):** A "Login" dialog box with fields for URI, Email, Password, Authentication Code, and IP Address. The IP Address field contains the value "hello! myname is robin". A large red arrow points from this field to the "Remote Address" field in the video chat application below.

**Middle Window (Postman API Request):** A POST request to "https://localhost:8000/login\_from\_app". The "Body" tab shows JSON data:

```
1: { "email": "seongjun@andrew.cmu.edu",  
2: "password": "Lge1234!@#$",  
3: "token": "05267",  
4: "ip_address": "abdbadsadfsadfd",  
5: "rsa_public": "...",  
6: "rsa_private": ""}
```

The response body is:

```
1: { "errorCode": 0,  
2: "msg": "Success",  
3: "session_id": "VGQQVJWLM2UXTPJW",  
4: "hash_id": "WOYXCNFRXYCVF066"}
```

**Bottom Window (Video Chat Application):** The "LgVideoChatDemo" application window. It shows a toolbar with "Connect", "Disconnect", "Start Server", "Stop Server", "Login", and "Missed Call" buttons. The "Remote Address" field at the top contains "hello! myname is VAD State: Unknown". Below it, a text area shows "Remote Address: hello! myname is robin Loopback False".

# Appendix-11) Code Review- Server

Last analysis 3 days ago [a3c78993](#) sonar-project.properties

The Quality Gate helps you see if your New Code is deployable or not.

**Not computed**

**Reliability** D 23 Bugs

**Maintainability** A 36 Code Smells

**Security** A 0 Vulnerabilities

**Security Review** E 2 Security Hotspots 0.0% Reviewed

**Coverage** O 0.0% Coverage

**Duplications** 0.0% Duplications

**Filters** [Clear All Filters](#)

Type

- Bug 2
- Vulnerability 0
- Code Smell 9

Add to selection [Ctrl + click](#)

Severity

- Blocker 0 Minor 10
- Critical 2 Info 0
- Major 11

Add to selection [Ctrl + click](#)

LgVideoChatDemo/opus-1.3.1/doc

[Add to selection Ctrl + click](#)

[Unexpected nonstandard directive](#)

Bug Open Critical

Severity

- Blocker 0 Minor 7
- Critical 9 Info 0
- Major 20

[Add to selection Ctrl + click](#)

[Resolution](#)

[Status](#)

[Security Category](#)

[Define a constant instead of duplicating this literal "home/index.html" 3 times.](#)

Code Smell Open Critical Not assigned

[TOTP Demo/routers/home/route\\_home.py](#)

[Define a constant instead of duplicating this literal "login/login.html" 5 times.](#)

Code Smell Open Critical Not assigned

[TOTP Demo/routers/login/route\\_login.py](#)

[Refactor this function to reduce its Cognitive Complexity from 28 to the 15 allowed.](#)

Code Smell Open Critical Not assigned

[Refactor this function to reduce its Cognitive Complexity from 23 to the 15 allowed.](#)

Code Smell Open Critical Not assigned

[TOTP Demo/routers/resetpw/route\\_resetpw.py](#)

[Define a constant instead of duplicating this literal "resetpw/resetpw.html" 5 times.](#)

Code Smell Open Critical Not assigned

[Define a constant instead of duplicating this literal "Don't mess with us buddy" 5 times.](#)

Code Smell Open Critical Not assigned

[Define a constant instead of duplicating this literal "resetpw/forgetpw.html" 4 times.](#)

Code Smell Open Critical Not assigned

# Appendix-12) Code Review- Client

Cppcheck 2.11 - Project: cmu\_phase2\_static\_analysis.cppcheck

File Edit View Analyze Help

Quick Filter:

File	Severity	Line	Id	Inconclusive	Summary
C:\hacking\LG_Security_Team1\LgVideoChatDemo\LgVideoChatDemo\LgVideoChatDemo.cpp	warning	170	ignoredReturnValue	<input type="checkbox"/>	Return value of function freopen_s() is not used.
C:\hacking\LG_Security_Team1\LgVideoChatDemo\LgVideoChatDemo\LgVideoChatDemo.cpp	warning	705	ignoredReturnValue	<input type="checkbox"/>	Return value of function CreateWindow() is not used.
C:\hacking\LG_Security_Team1\LgVideoChatDemo\LgVideoChatDemo\LgVideoChatDemo.cpp	warning	713	ignoredReturnValue	<input type="checkbox"/>	Return value of function CreateWindow() is not used.
C:\hacking\LG_Security_Team1\LgVideoChatDemo\LgVideoChatDemo\LgVideoChatDemo.cpp	warning	721	ignoredReturnValue	<input type="checkbox"/>	Return value of function CreateWindow() is not used.
C:\hacking\LG_Security_Team1\LgVideoChatDemo\LgVideoChatDemo\LgVideoChatDemo.cpp	warning	729	ignoredReturnValue	<input type="checkbox"/>	Return value of function CreateWindowExA() is not used.
C:\hacking\LG_Security_Team1\LgVideoChatDemo\LgVideoChatDemo\LgVideoChatDemo.cpp	warning	740	ignoredReturnValue	<input type="checkbox"/>	Return value of function CreateWindow() is not used.
C:\hacking\LG_Security_Team1\LgVideoChatDemo\LgVideoChatDemo\LgVideoChatDemo.cpp	warning	749	ignoredReturnValue	<input type="checkbox"/>	Return value of function CreateWindow() is not used.
C:\hacking\LG_Security_Team1\LgVideoChatDemo\LgVideoChatDemo\LgVideoChatDemo.cpp	warning	758	ignoredReturnValue	<input type="checkbox"/>	Return value of function CreateWindow() is not used.
C:\hacking\LG_Security_Team1\LgVideoChatDemo\LgVideoChatDemo\LgVideoChatDemo.cpp	error	925	resourceLeak	<input type="checkbox"/>	Resource leak: m_singleInstanceMutex

File: C:\hacking\LG\_Security\_Team1\LgVideoChatDemo\webrtc\ADI\webrtc\ADI\webrtc\clnctypesdefs.h

Line: 10

Severity: warning

Id: CWE-398

Summary: Member variable 'CBaseMediaBuffer::m\_pData' is not initialized in the constructor.

First included by C:\hacking\LG\_Security\_Team1\LgVideoChatDemo\LgVideoChatDemo\voip\voice.cpp

```
9 // PARTICULAR PURPOSE.  
10 //  
11 // Copyright (c) 1999-2001, Microsoft Corporation. All rights reserved.  
12 //--  
13  
14  
15 #ifndef __MEDIABUF_H__  
16 #define __MEDIABUF_H__  
17  
18 class CBaseMediaBuffer : public IMediaBuffer {  
19 public:  
20     CBaseMediaBuffer() {}  
21     CBaseMediaBuffer(BYTE *pData, ULONG ulSize, ULONG ulData) :  
22         m_pData(pData), m_ulSize(ulSize), m_ulData(ulData), m_cRef(1) {}  
23     STDMETHODIMP_(ULONG) AddRef() {  
24         return InterlockedIncrement((long*)&m_cRef);  
25     }  
26     STDMETHODIMP_(ULONG) Release() {  
27         long l = InterlockedDecrement((long*)&m_cRef);  
28         if (l == 0)
```

Analysis Log Warning Details

# Appendix-13) Code Review(OpenCV - CWEs)

## 8 CWEs

id	severity	msg	verbose	sinceDate	cwe	file0
integerOverflow	error	Signed integer overflow for expression &#039;Signed integer overflow for expression &#039;(M/d/yyyy			190	C:/hacking/LG_Security_Team1/LgVideo
integerOverflow	error	Signed integer overflow for expression &#039;Signed integer overflow for expression &#039;(M/d/yyyy			190	C:/hacking/LG_Security_Team1/LgVideo
nullPointer	error	Null pointer dereference: reinterpret_cast<&lt; Null pointer dereference: reinterpret_cast<&lt; T> M/d/yyyy			476	C:/hacking/LG_Security_Team1/LgVideo
uninitMemberVar	warning	Member variable &#039;UntypedMatrix::type&gt; Member variable &#039;UntypedMatrix::type&gt; M/d/yyyy			398	C:/hacking/LG_Security_Team1/LgVideo
uninitMemberVar	warning	Member variable &#039;KNNSimpleResultSet:: Member variable &#039;KNNSimpleResultSet::i M/d/yyyy			398	C:/hacking/LG_Security_Team1/LgVideo
uninitMemberVar	warning	Member variable &#039;KNNSimpleResultSet:: Member variable &#039;KNNSimpleResultSet::i M/d/yyyy			398	C:/hacking/LG_Security_Team1/LgVideo
duplInheritedMember	warning	The class &#039;KNNRadiusUniqueResultSet:: The class &#039;KNNRadiusUniqueResultSet:: M/d/yyyy			398	C:/hacking/LG_Security_Team1/LgVideo
duplInheritedMember	warning	The class &#039;KNNRadiusUniqueResultSet:: The class &#039;KNNRadiusUniqueResultSet:: M/d/yyyy			398	C:/hacking/LG_Security_Team1/LgVideo
uninitvar	warning	Uninitialized variable: topind	Uninitialized variable: topind	M/d/yyyy	457	C:/hacking/LG_Security_Team1/LgVideo
uninitvar	warning	Uninitialized variable: topind	Uninitialized variable: topind	M/d/yyyy	457	C:/hacking/LG_Security_Team1/LgVideo
incorrectStringBooleanError	warning	Conversion of string literal &quot;vectors size Conversion of string literal &quot;vectors size n M/d/yyyy			571	C:/hacking/LG_Security_Team1/LgVideo
incorrectStringBooleanError	warning	Conversion of string literal &quot;vectors size Conversion of string literal &quot;vectors size n M/d/yyyy			571	C:/hacking/LG_Security_Team1/LgVideo
incorrectStringBooleanError	warning	Conversion of string literal &quot;vectors size Conversion of string literal &quot;vectors size n M/d/yyyy			571	C:/hacking/LG_Security_Team1/LgVideo
incorrectStringBooleanError	warning	Conversion of string literal &quot;vectors size Conversion of string literal &quot;vectors size n M/d/yyyy			571	C:/hacking/LG_Security_Team1/LgVideo
operatorEqVarError	warning	Member variable &#039;KMeansDistanceCo Member variable &#039;KMeansDistanceComp M/d/yyyy			398	C:/hacking/LG_Security_Team1/LgVideo
operatorEqVarError	warning	Member variable &#039;KMeansDistanceCo Member variable &#039;KMeansDistanceComp M/d/yyyy			398	C:/hacking/LG_Security_Team1/LgVideo
operatorEqVarError	warning	Member variable &#039;KMeansDistanceCo Member variable &#039;KMeansDistanceComp M/d/yyyy			398	C:/hacking/LG_Security_Team1/LgVideo
operatorEqVarError	warning	Member variable &#039;KMeansDistanceCo Member variable &#039;KMeansDistanceComp M/d/yyyy			398	C:/hacking/LG_Security_Team1/LgVideo
uninitvar	error	Uninitialized variable: centers_length	Uninitialized variable: centers_length	M/d/yyyy	457	C:/hacking/LG_Security_Team1/LgVideo
uninitvar	error	Uninitialized variable: centers_length	Uninitialized variable: centers_length	M/d/yyyy	457	C:/hacking/LG_Security_Team1/LgVideo
uninitMemberVar	warning	Member variable &#039;LshTable &lt; unsigned Member variable &#039;LshTable &lt; unsigned M/d/yyyy			398	C:/hacking/LG_Security_Team1/LgVideo
uninitMemberVar	warning	Member variable &#039;LshTable &lt; unsigned Member variable &#039;LshTable &lt; unsigned M/d/yyyy			398	C:/hacking/LG_Security_Team1/LgVideo
uninitvar	error	Uninitialized variable: state_bucket_size std:: Uninitialized variable: state_bucket_size std:: day M/d/yyyy			457	C:/hacking/LG_Security_Team1/LgVideo

2150개 중 68개의 레코드가 있습니다.

평균: 371.5223881 개수: 68 합계: 24892

# Appendix-14) Research Vulnerability DB

<https://www.cvedetails.com>

There's no vulnerability

## CVE Details

The ultimate security vulnerability datasource

[Log In](#) [Register](#)

[Switch to https://](#)

[Home](#)

**Browse :**

[Vendors](#)

[Products](#)

[Vulnerabilities By Date](#)

[Vulnerabilities By Type](#)

**Reports :**

[CVSS Score Report](#)

[CVSS Score Distribution](#)

**Search :**

[Vendor Search](#)

### Vendor, Product and Version Search

#	Vendor	Product	Version	Language	Update	Edition	Number of Vulnerabilities
---	--------	---------	---------	----------	--------	---------	---------------------------

No matches

**Vendor Name:**

**Product Name:**

**Version:**

## CVE Details

The ultimate security vulnerability datasource

[Log In](#) [Register](#)

[Switch to https://](#)

[Home](#)

**Browse :**

[Vendors](#)

[Products](#)

[Vulnerabilities By Date](#)

[Vulnerabilities By Type](#)

**Reports :**

[CVSS Score Report](#)

[CVSS Score Distribution](#)

**Search :**

[Vendor Search](#)

### Vendor, Product and Version Search

#	Vendor	Product	Version	Language	Update	Edition	Number of Vulnerabilities
---	--------	---------	---------	----------	--------	---------	---------------------------

No matches

**Vendor Name:**

**Product Name:**

**Version:**

# Appendix-15) Dependency-check

There's no vulnerability



Dependency-Check is an open source tool performing a best effort analysis of 3rd party dependencies; false positives and false negatives may exist in the analysis performed by the tool. Use of the tool and the reporting provided constitutes an analysis or its use. Any use of the tool and the reporting provided is at the user's risk. In no event shall the copyright holder or OWASP be held liable for any damages whatsoever arising out of or in connection with the use of this tool, the ana

[How to read the report](#) | [Suppressing false positives](#) | [Getting Help: github issues](#)

[Sponsor](#)

**Project:** .

Scan Information ([show less](#)):

- dependency-check version: 8.2.1
- Report Generated On: Tue, 4 Jul 2023 10:18:18 +0900
- Dependencies Scanned: 54 (44 unique)
- Vulnerable Dependencies: 0
- Vulnerabilities Found: 0
- Vulnerabilities Suppressed: 0
- NVD CVE Checked: 2023-07-04T10:17:59
- NVD CVE Modified: 2023-07-04T09:00:02
- VersionCheckOn: 2023-06-12T15:21:01
- kev.checked: 1688397902

## Summary

Display: [Showing Vulnerable Dependencies \(click to show all\)](#)

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count
------------	-------------------	---------	------------------	-----------	------------	----------------

## Dependencies

# **Attack Scenario (idea)**

# Appendix-16) Attack scenario

Login success with blank rsa\_public\_key -> Bob can send not encrypted AES key(?)  
Not sure if we can get AES key which is not encrypted

The screenshot shows a Postman interface for testing an API endpoint. The URL is `https://localhost:8000/login_from_app`. The request method is POST. The body is set to JSON and contains the following data:

```
1 "email": "seongjun@andrew.cmu.edu",
2 "password": "Lge1234!@#$",
3 "token": "902573",
4 "ip_address": "ahdhsadfsadf!d",
5 "rsa_public_key": ""
```

The field for "rsa\_public\_key": "" is highlighted with a red box. The response status is 200 OK, with a message "Success".

Body	Cookies	Headers (4)	Test Results	Save Response
Pretty	Raw	Preview	Visualize	JSON

```
1
2     "errorCode": 0,
3     "msg": "Success",
4     "session_id": "QDQELW7AR6VOISOD",
5     "hash_id": "WOYXCNFRXYCVF066"
```

# Appendix-17) Client Side attack

test checksec : CFG/RFG disable → ROP Possibile (???)

```
D:\WpgWc++>winchecksec.exe LgVideoChatDemo.exe C:\Windows\Notepad.exe
Warn: large load config, probably contains undocumented fields
Results for: LgVideoChatDemo.exe
Dynamic Base       : "Present"
ASLR              : "Present"
High Entropy VA   : "Present"
Force Integrity   : "NotPresent"
Isolation         : "Present"
NX                : "Present"
SEH               : "Present"
CFG               : "NotPresent"
RFG               : "NotPresent"
SafeSEH           : "NotApplicable"
GS                : "Present"
Authenticode      : "NotPresent"
.NET              : "NotPresent"
CET Compatible    : "NotPresent"
```

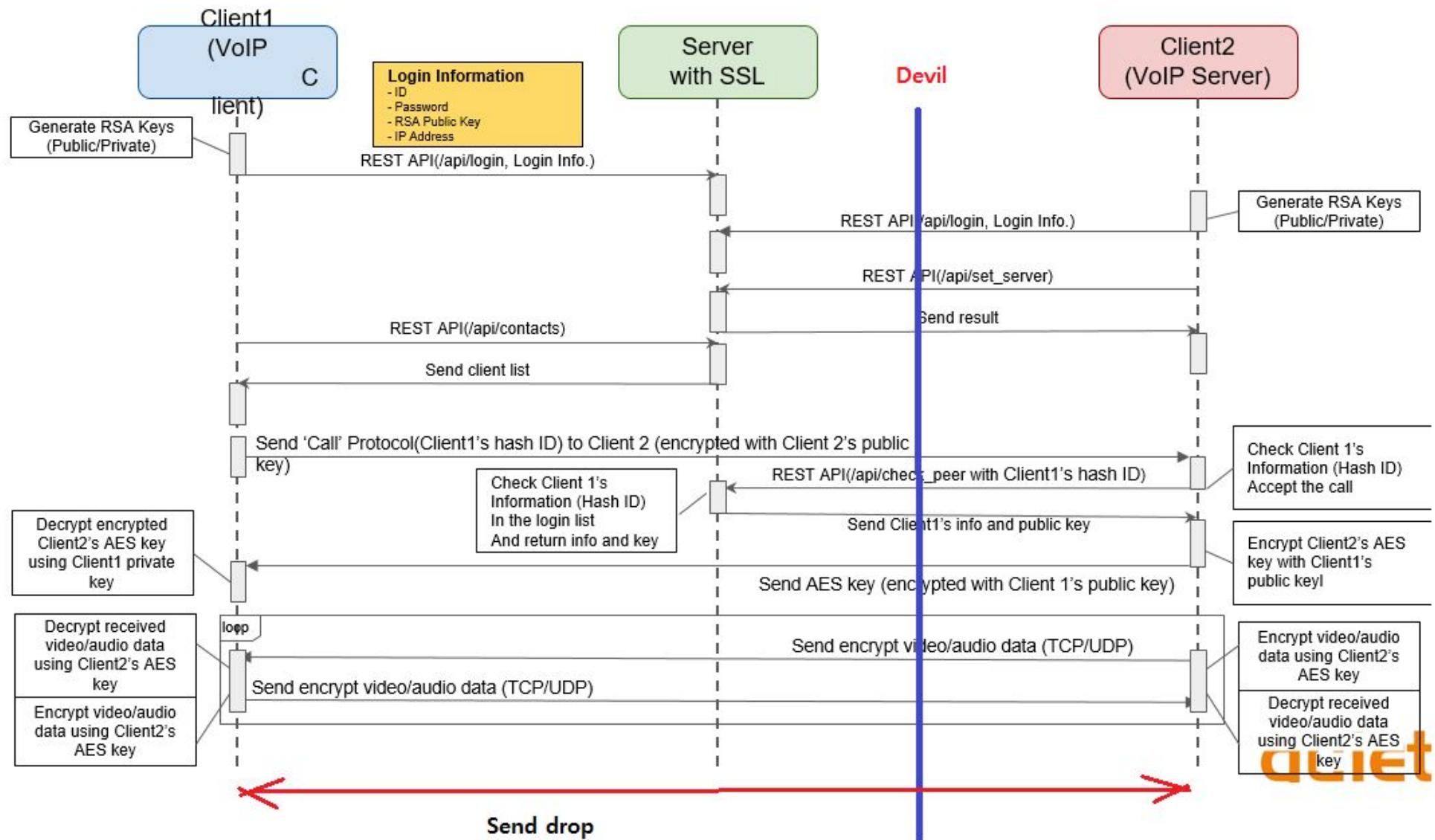
## Scenario 1 :

1. OpenCV within project source has some critical vulnerabilities ( integer overflow, NULL dereference, use of uninitialized variable)
2. code injection using step1's vulnerability
3. the shell code is to send private key or AES to attacker's server.
4. the attacker be able to sniff Video call using the victim's AES key

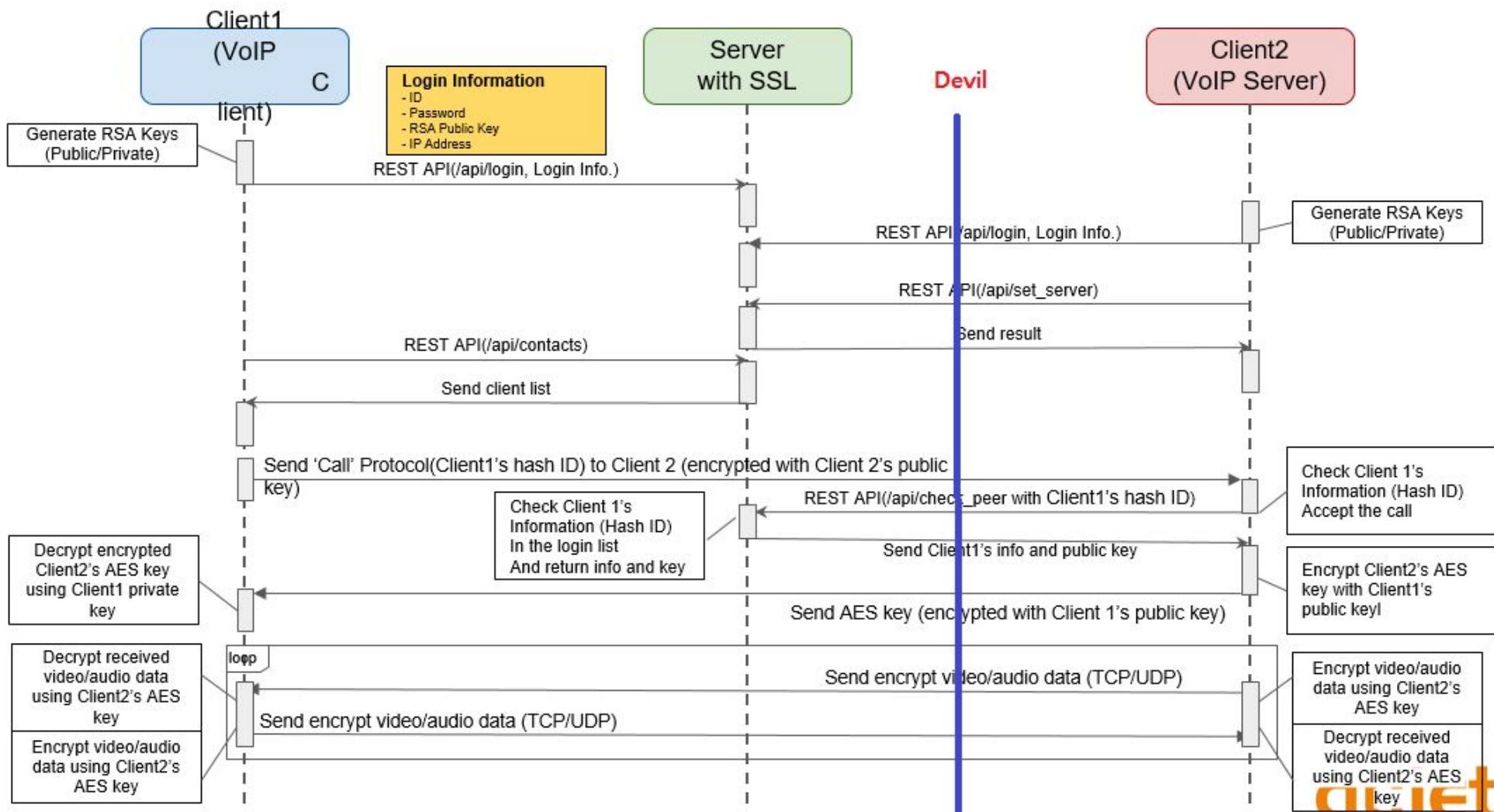
## Scenario 2:

1. OpenCV within project source has some critical vulnerabilities ( integer overflow, NULL dereference, use of uninitialized variable)
2. code injection using step1's vulnerability
3. the shell code is to exploit the client's host system (ex.. to execute powershell with privilege mode)

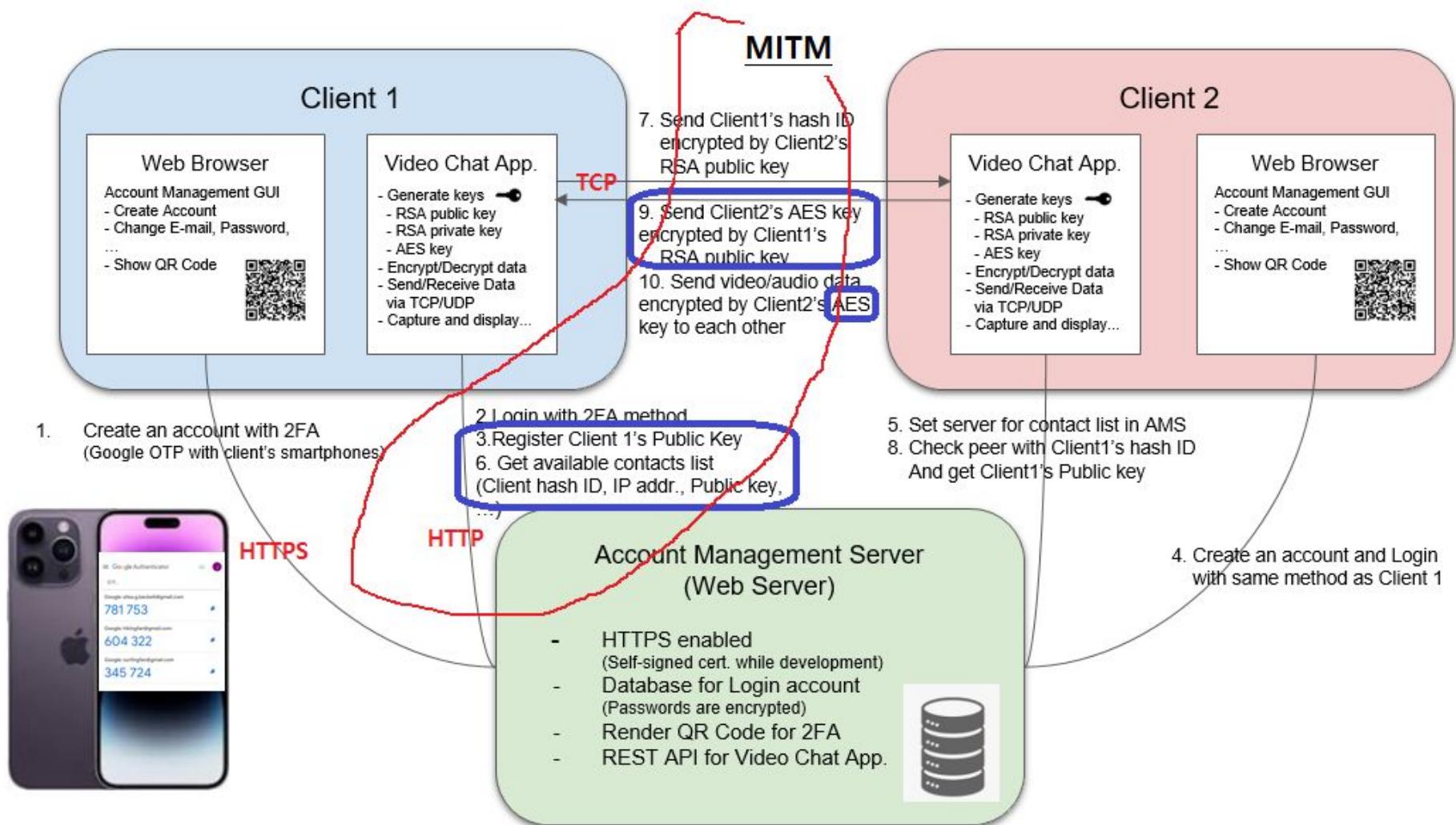
# Appendix-18) Unwanted Call Drop via MITM or spoofing



# Appendix-19) Sniffing video call via MITM(1)



# Appendix-20) Sniffing video call via MITM(2)



**IF Protocol HTTPS, HTTP, TCP more check needed!!**

# Appendix-21) ARP Spoofing

## Attacker changed target's arp table

- Attacker : 192.168.0.242
- Target 1: 192.168.0.153
- Target 2: 192.168.0.216

인터페이스: 192.168.0.153 --- 0xf	인터넷 주소	물리적 주소	유형
	192.168.0.1	98-da-c4:77-4b-f2	동적
	192.168.0.144	8c-17-59-f3-54-12	동적
192.168.0.216	08-00-27-76-cd-18	동적	동적
192.168.0.242	08-00-27-76-cd-18	동적	동적
192.168.0.255	ff-ff-ff-ff-ff-ff	정적	정적
224.0.0.2	01-00-5e-00-00-02	정적	정적
224.0.0.22	01-00-5e-00-00-16	정적	정적
224.0.0.251	01-00-5e-00-00-fb	정적	정적
224.0.0.252	01-00-5e-00-00-fc	정적	정적
239.255.255.250	01-00-5e-7f-f-f-fa	정적	정적
255.255.255.255	ff-ff-ff-ff-ff-ff	정적	정적

## Attacker try to sniff packets

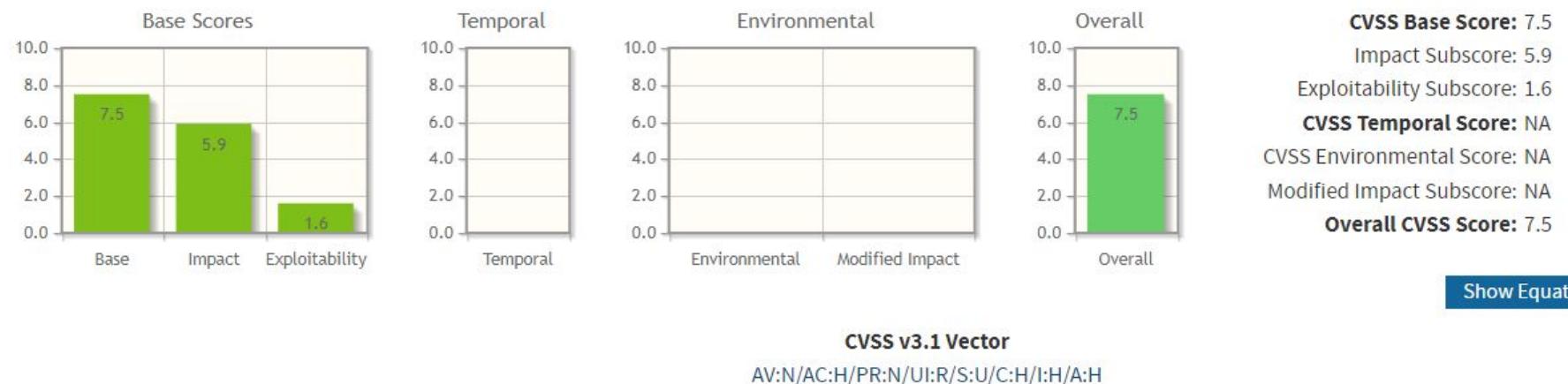
- Target 1: 192.168.0.153 <-> Target 2: 192.168.0.216

The screenshot shows a Kali Linux desktop environment with several windows open:

- Ettercap 0.8.3.1 (EB)**: A network traffic analysis tool. The MAC Address list shows:
  - 98:DA:C4:77:4B:F2 (selected)
  - B4:A9:FC:CC:EA:43
  - 7:4bf2 98:DA:C4:77:4B:F2
  - 00:E0:4C:36:02:5E
- File**: A terminal window showing system logs and configuration.
- Wireshark**: A packet capture tool. The list of captured frames shows traffic between 192.168.0.153 and 192.168.0.216. Frame 3258 is selected, showing details:
  - No. 3258... Time 214.681775704 Source 192.168.0.153 Destination 192.168.0.216 Protocol TCP Length 60 Info 60 60347 → 10000 [ACK] Seq=62776585 Ack=52657701 Win=262656 Len=1514 [TCP Fast Retransmission]
- Frame Details**: A detailed view of frame 325848, showing its structure and contents.
- Hex Editor**: A window showing the raw hex and ASCII representation of the captured frames.

# Appendix-22) Common Vulnerability Scoring System

**Vulnerability :** If hash\_id and public key is known, it is possible to make fake call.



## Base Score Metrics

### Exploitability Metrics

Attack Vector (AV)\*

Network (AV:N)  Adjacent Network (AV:A)  Local (AV:L)  Physical (AV:P)

Attack Complexity (AC)\*

Low (AC:L)  High (AC:H)

Privileges Required (PR)\*

None (PR:N)  Low (PR:L)  High (PR:H)

User Interaction (UI)\*

None (UI:N)  Required (UI:R)

Scope (S)\*

Unchanged (S:U)  Changed (S:C)

### Impact Metrics

Confidentiality Impact (C)\*

None (C:N)  Low (C:L)  High (C:H)

Integrity Impact (I)\*

None (I:N)  Low (I:L)  High (I:H)

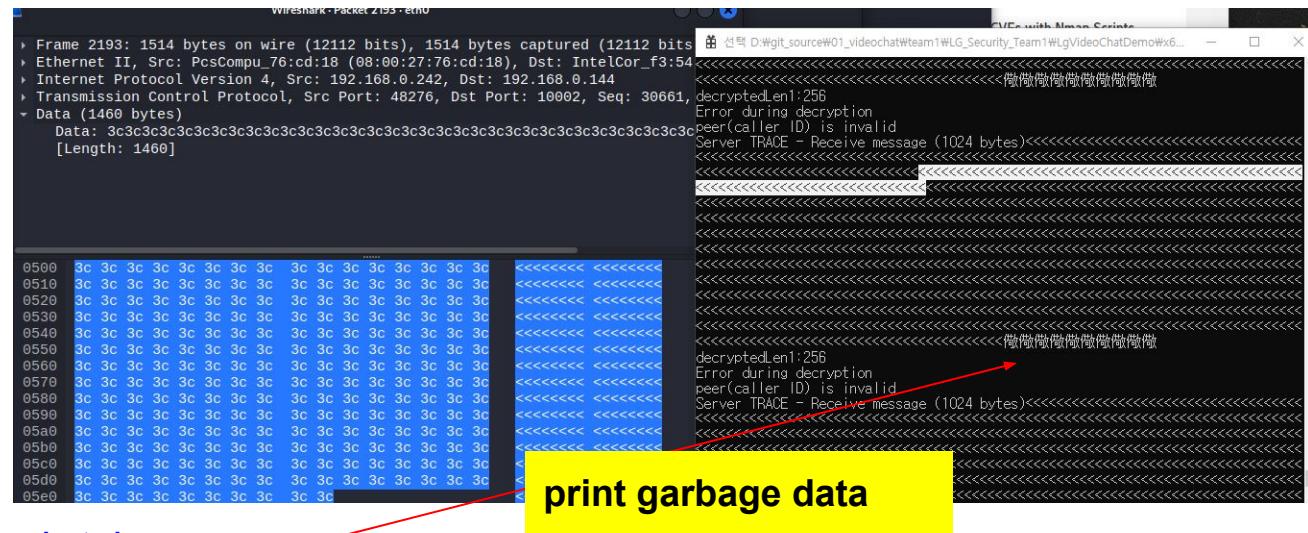
Availability Impact (A)\*

None (A:N)  Low (A:L)  High (A:H)

- <https://www.first.org/cvss/specification-document>
- <https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator>

# Appendix-23) SPIKE Fuzzing

```
—(kali㉿kali)-[~]
$ generic_send_tcp 192.168.0.144 10002 /usr/share/spike/audits/RealServer/stream1.spk 0 0
```



**messageBuffer is not NULL terminated**

## print garbage data

```
static DWORD WINAPI MakeThread(void* data)
{
    int call_status = 0;
    unsigned int timeout_count = 0;
    unsigned char decrypted_data[MAX_BUFFER] = { 0 };
    unsigned char encrypted_data[MAX_BUFFER] = { 0 };
    size_t decrypted_data_size = 0;
    size_t encrypted_data_size = 0;
    SOCKET socket = (SOCKET)data;

    char messageBuffer[MAX_BUFFER] = { 0 };
    int receiveBytes;
    int err = errno;
    while (receiveBytes = recv(socket, messageBuffer, MAX_BUFFER-1, 0))
    {
        if (receiveBytes > 0)
        {
            printf("Server TRACE - Receive message (%d bytes)%s\n", receiveBytes, messageBuffer);
            /* If the received message is longer than the buffer size, we need to read it in parts */
            /* We can do this by setting the timeout to 0 and then reading until the timeout occurs */
            /* This will cause the read function to return -1 with the error code WSAEWOULDBLOCK */
            /* We can then check for this error and read again until the timeout occurs again */
            /* We can do this until we have read all of the data */
            /* We can then free the memory allocated for the buffer */
            /* We can then close the socket */
            /* We can then return the status code */
        }
    }
}
```

A large, solid gray arrow pointing to the right, indicating the direction of the next section.

**Recommend:**  
messageBuffer initialization  
Change receive size

```
static DWORD WINAPI MakeThread(void* data)
{
    int call_status = 0;
    unsigned int timeout_count = 0;
    unsigned char decrypted_data[MAX_BUFFER] = { 0 };
    unsigned char encrypted_data[MAX_BUFFER] = { 0 };
    size_t decrypted_data_size = 0;
    size_t encrypted_data_size = 0;
    SOCKET socket = (SOCKET)data;

    char messageBuffer[MAX_BUFFER] = { 0 };
    int receiveBytes;
    int err = errno;
    while (receiveBytes = recv(socket, messageBuffer, MAX_BUFFER-1, 0))
    {
        if (receiveBytes > 0)
        {
            printf("Server TRACE - Receive message (%d bytes)%s\n", receiveBytes, messageBuffer);
        }
    }
}
```