Phase 2. Code Review Report

Team 5verFlow

23 Jun

CDR-001	23 Jun	
Speaker	SW Cha	
Reviewer	DH Han, YK Choi, WL Cha, SJ Lee, YJ Lee	
Objective	File Management	
Defects	Defect001-01	App::App() at client/src/app.cpp:233
		filename is hardcoded !!! it can make harder to maintain code -> use const variable
	Defect001-02	App::App() at client/src/app.cpp:238 ~ 244
		Validate uploaded files are the expected type by checking file headers. Checking for file type by extension alone is not sufficient !!! it can make fault when file contains binary data which has not NULL character -> need to restrict the max file size
	Defect001-03	App::App() at client/src/app.cpp:233
		ip configuration file is not secured !!! User may connect with fake server when configuration file is replaced by attacker
Action Item		it could be vulnerability point

```cpp
if (!g_file_get_contents("./remote.config", &this->remote_ip, &len, NULL)) {
    LOG_WARNING("cannot read remote.config file");
    exit(-1);
}

if (len < 7) {
    LOG_WARNING("not enough contents length in remote.config file");
    g_free(this->remote_ip);
    exit(-1);
}

g_strstrip(this->remote_ip);
```

CDR-002	23 Jun	
Speaker	SW Cha	
Reviewer	DH Han, YK Choi, WL Cha, SJ Lee, YJ Lee	
Objective	Input Validation	
Defects	Defect002-01	App::on_button_login() at client/src/app.cpp:547~548
		regular expression is hardcoded !!! it can make harder to maintain code -> use const variable
	Defect002-02	main() at server/src/main.cpp:461
		there is not new name validation !!! user name can be duplicated or multiple face is registered as one name. so user cannot distinguish people correctly
Action Item		looks good

```cpp
if (check_valid_input("^[a-zA-Z0-9]+$", m_Entry_Id.get_text().c_str()) &&
    check_valid_input("^(?=.*[A-Za-z])(?=.*\\d)(?=.*[\\^@$!%*#?&])[A-Za-z\\d\\^@$!%*#?&]{8,}$", m_Entry_Password.
    get text().c str())) {
```

```cpp
faceNet.addNewFace_name(frame, outputBbox, (gchar *)req_parsed_data);
```

CDR-003	23 Jun		
Speaker	SW Cha		
Reviewer	DH Han, YK Choi, WL Cha, SJ Lee, YJ Lee		
Objective	Authentication and Password Management		
Defects	Defect003-01	App::connect_server() at app.cpp:349	```if (0 != check_client_cert()) { LOG_WARNING("Certificate Error"); show_dialog("Certificate Error"); goto exit;}```
		Enforce account disabling after an established number of invalid login attempts (e.g., five attempts is common). The account must be disabled for a period of time sufficient to discourage brute force guessing of credentials, but not so long as to allow for a denial-of-service attack to be performed !!! it can be target of brute force attack -> insert some time delay when failure or follow the guidance.	
	Defect003-02	App::connect_server() at app.cpp:355~357	
		if certi files are replace then always fail to log in !!! it can be target of DoS attack	```ca = getFilepath_ca_cert();crt = getFilepath_client_cert();key = getFilepath_client_key();```
Action Item		it could be target of fuzz testing	

CDR-004	23 Jun	
Speaker	SW Cha	
Reviewer	DH Han, YK Choi, WL Cha, SJ Lee, YJ Lee	
Objective	Session Management	
Defects	Defect004-01	App::connect_server() at app.cpp:388, 638, 653
		There are no return value check !!! User may confused although request was failed
	Defect004-02	App::connect_server() at app.cpp:418, 426, 434
		There are no authentication for additional connection after login !!! it can be session hijacking
Action Item		need further investigation

```cpp
TcpSendLoginData(this->port_control, m_Entry_Id.get_text().c_str(), m_Entry_Password.get_text().c_str()),
show_dialog("Show your face on camera within 5sec");
```

```cpp
if ((this->port_secure = OpenTcpConnection(this->remote_ip, "5000", ca, crt, key)) == NULL) // Open
{
    LOG_WARNING("error open port_secure");
    disconnect_server();
    show_dialog("Connection Fail");
    goto exit;
}

if ((this->port_nonsecure = OpenTcpConnection(this->remote_ip, "5000", NULL, NULL, NULL)) == NULL) ,
non secure mode
```

CDR-005	23 Jun		
Speaker	SW Cha		
Reviewer	DH Han, YK Choi, WL Cha, SJ Lee, YJ Lee		
Objective	Error Handling and Logging		
Defects	Defect005-01	ReadDataTcp() at common/NetworkTCP.cpp:796	

		when using ssl_read() with select(), it must be check the return value with ssl_get_error() because return behavior is a little different with normal read() or recv() in case of SSL library (ex. affected by ssl control frame)
		!!! it could be lost connection unexpectedely
			``c++
			if (bytes == 0) { // recv error
			    LOG_WARNING("peer is disconnected");
			    return TCP_RECV_PEER_DISCONNECTED;
			}
			``

	Defect005-02	FaceAuthencticate() at server/src/main.cpp:82	

		it could fall into infinite loop when frame is empty because endtime is not updated.
		!!! it could not provide service properly
			``c++
			videoStreamer->getFrame(frame);
			if (frame.empty())
			    continue;
			``

	Defect005-03	TcpRecvLoginData() at common/TcpSendRecv.cpp:194	

		user login data is dynamically constructed so if attacker inject below data instead real user data then it could make heap overflow
		ex) 0x00, 0xFF, 0xXX....
		g_strndup() source add 1 bytes regardless of input string length
		   new_str = g_new (gchar, n + 1);
		!!! it could make abnormal termination
			``c++
			*userid = g_strndup (req->data + 1, userid_len);
			if (*userid == NULL) {
			    LOG_WARNING("memory allocation fail");
			    goto exit;
			}
			
			*userpw = g_strndup (req->data + 1 + userid_len + 1, userpw_len);
			``

	Defect005-04	TcpRecvImageAsJpeg() at common/TcpSendRecv.cpp:54	

		it doesn't check imagesize length
		!!! it could make abnormal termination
			``c++
			imagesize = ntohl(imagesize); // convert image size to host format
			buff = (guchar*)g_malloc(imagesize);
			``

	Defect005-05	AcceptTcpConnection() at common/Network.cpp:237	

		it doesn't return without dismiss ConnectedPort
		!!! it could make memory leak
			``c++
			if (!(TcpConnectedPort->ctx = get_server_context(ca_pem, cert
			    LOG_WARNING("get_server_context failed");
			    return(NULL);
			}
			``

	Defect005-06	AcceptTcpConnection() at common/Network.cpp:309	

		it doesn't return without dismiss TcpConnectedPort->ssl
		!!! it could make memory leak
			``c++
			if (client_cert == NULL) {
			    // The handshake was succe
			    // Most likely using an in
			    LOG_WARNING("SSL_get_peer_
			    goto ssl_exit;
			}
			``

	Defect005-07	AcceptTcpConnection() at common/Network.cpp:327	

		it doesn't return without dismiss TcpConnectedPort->ssl and TcpConnectedPort
		!!! it could make memory leak
			``c++
			error_verify_hostname:
			    if (client_cert) {
			        X509_free(client_cert)
			    }
			``

	Defect005-08	main() at server/src/main.cpp	

		if getFrame() cannot retrieve valid frame then following functions could not work properly
		!!! it could not provide service properly
			``c++
			videoStreamer->getFrame(frame);
			// Create a destination to paint the source in
			dst_img.create(frame.size(), frame.type());
			``

	Defect005-09	VideoStreamer::VideoStreamer() at server/src/videoStreamer.cpp:35	

		there is no NULL check
		!!! it could make abnormal termination
			``c++
			m_capture = new cv::VideoCapture(filename);
			if (!m_capture->isOpened()){
			``

	Defect005-10	baseEngine::caffeToGIEModel() at server/src/baseEngine.cpp:75	

		there is no NULL check
		!!! it could make abnormal termination
			``c++
			IBuilder *builder = createInferBuilder(gLogger);
			``

	Defect005-10	baseEngine::caffeToGIEModel() at server/src/baseEngine.cpp:86	

		there is no NULL check
		!!! it could make abnormal termination
			``c++
			const IBlobNameToTensor *blobNameToTensor = parser->parse(deployFile.c_str(),
			    modelFile.c_str(),
			``

Action Item		need further investigation	

CDR-005	23 Jun	
Speaker	SW Cha	
Reviewer	DH Han, YK Choi, WL Cha, SJ Lee, YJ Lee	
Objective	Communication Security	
Defects		
Action Item		great