후킹(HOOKING)을 이용한 프로그램 해킹

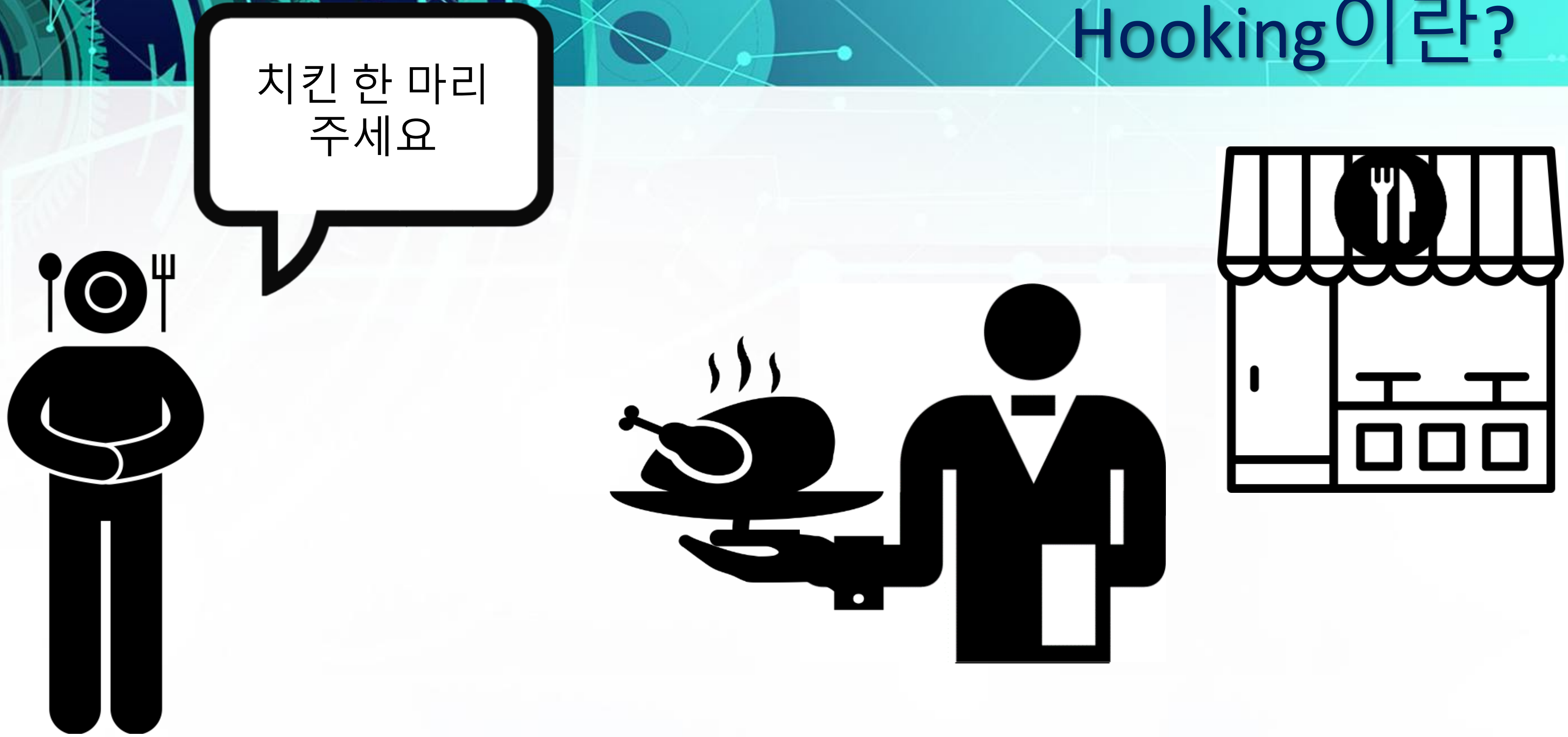
AGENDA

- Hooking이란?
- 기본지식?
- KeyLogging이란?
- KeyLogging 시연

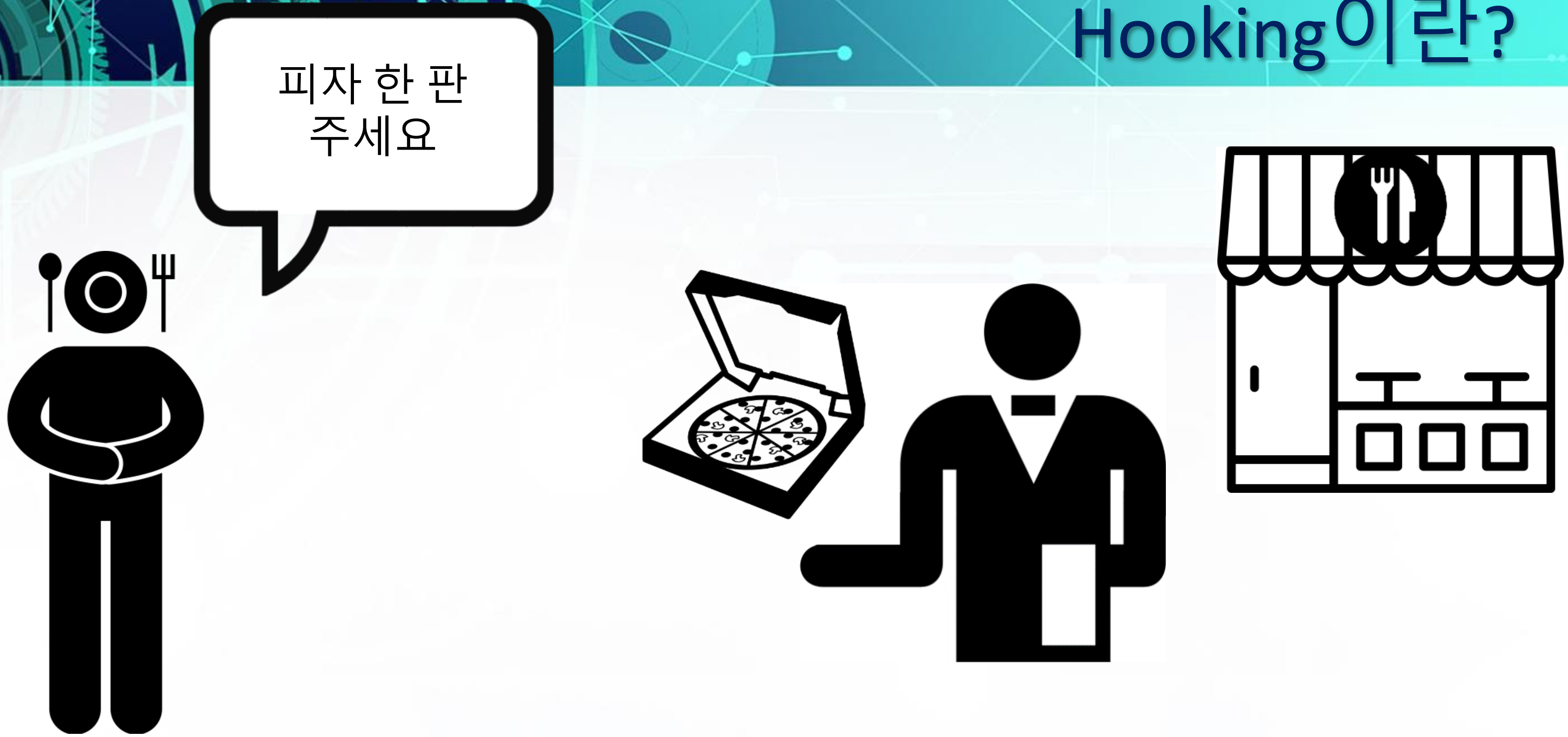
Hooking이란?

Hooking

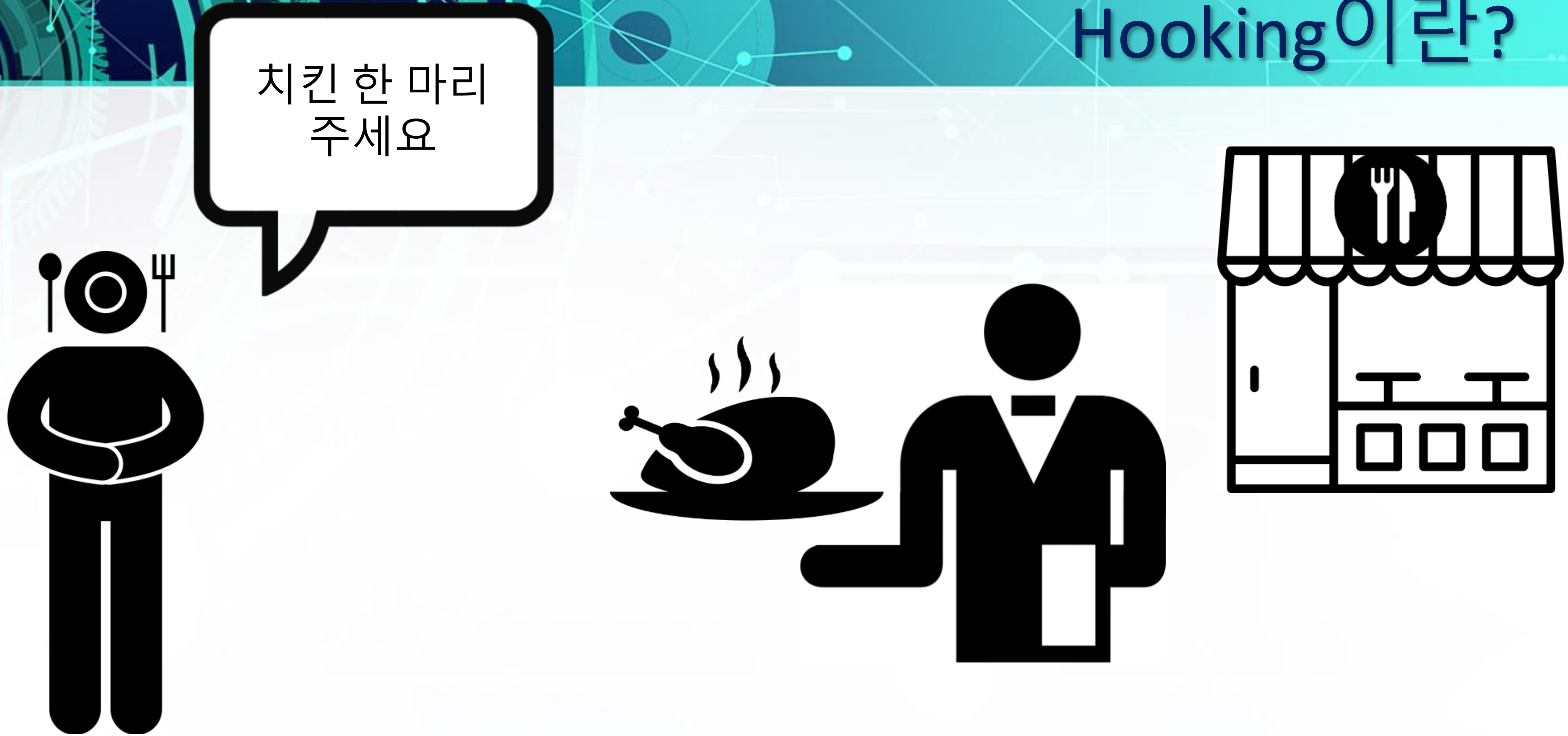
Hooking이란?



Hooking이란?

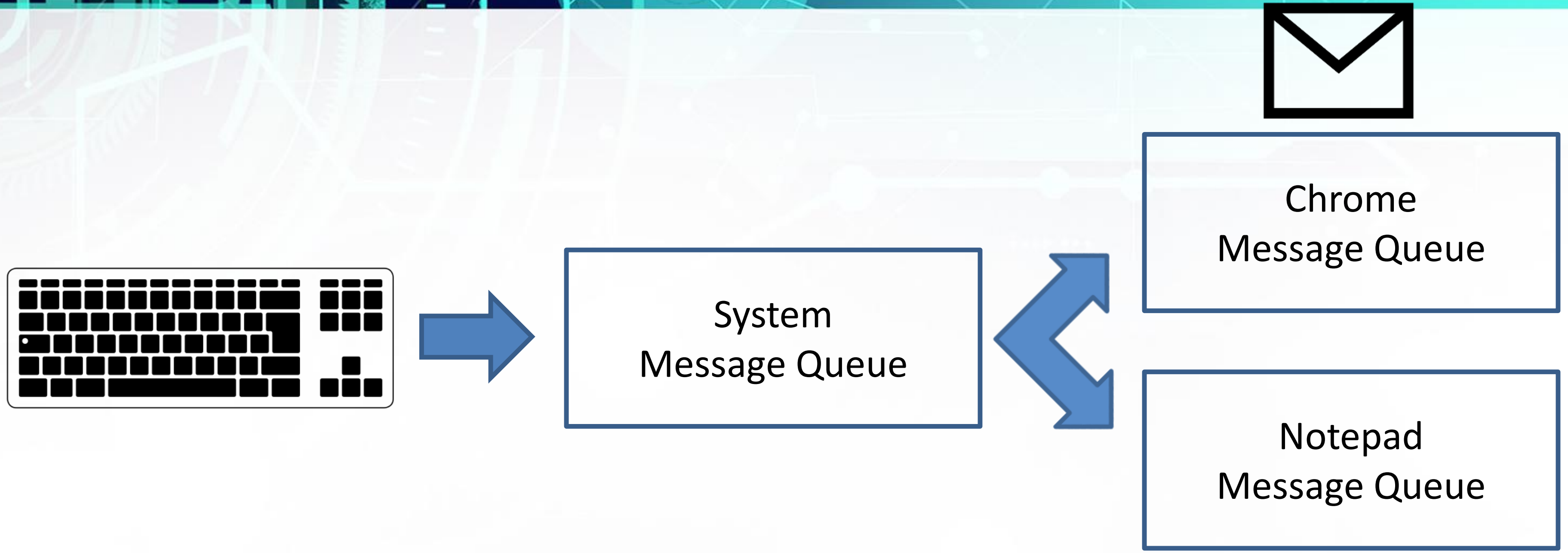


Hooking이란?



Hooking이란?

Key input



System
Message Queue

Chrome
Message Queue

Notepad
Message Queue

Message Queue

Message **Q**ueue

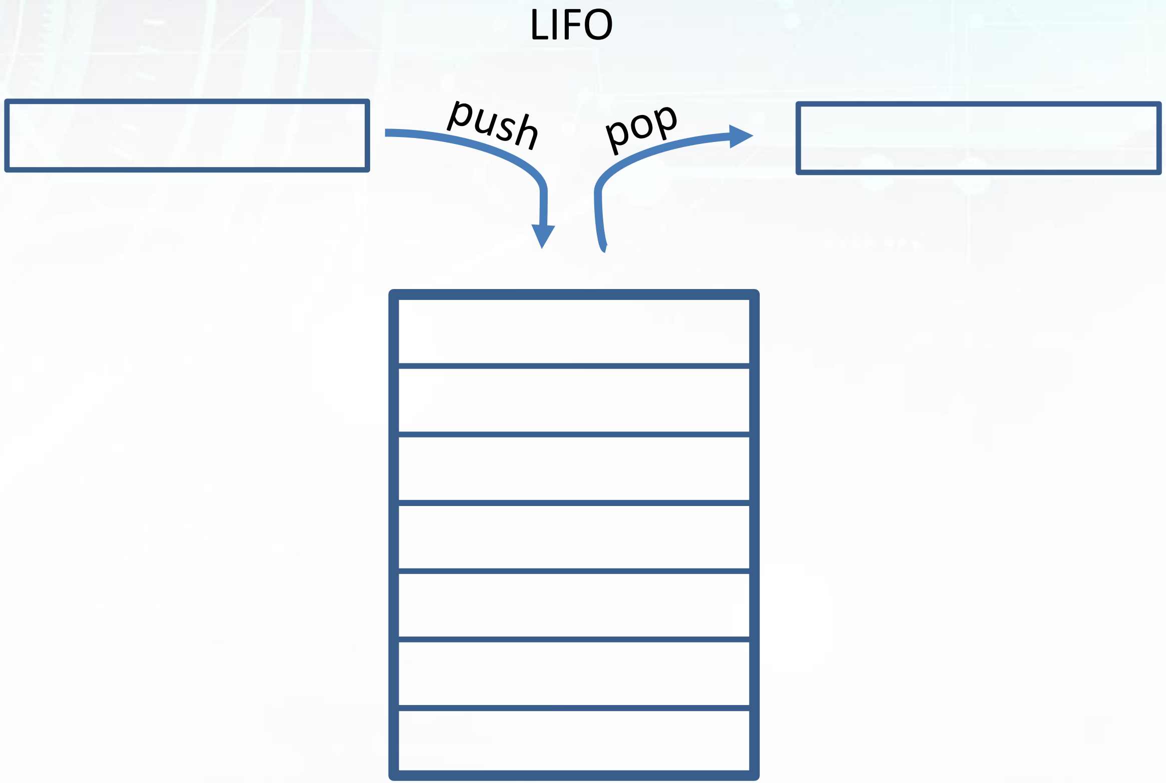
Message Queue

Queue

Stack

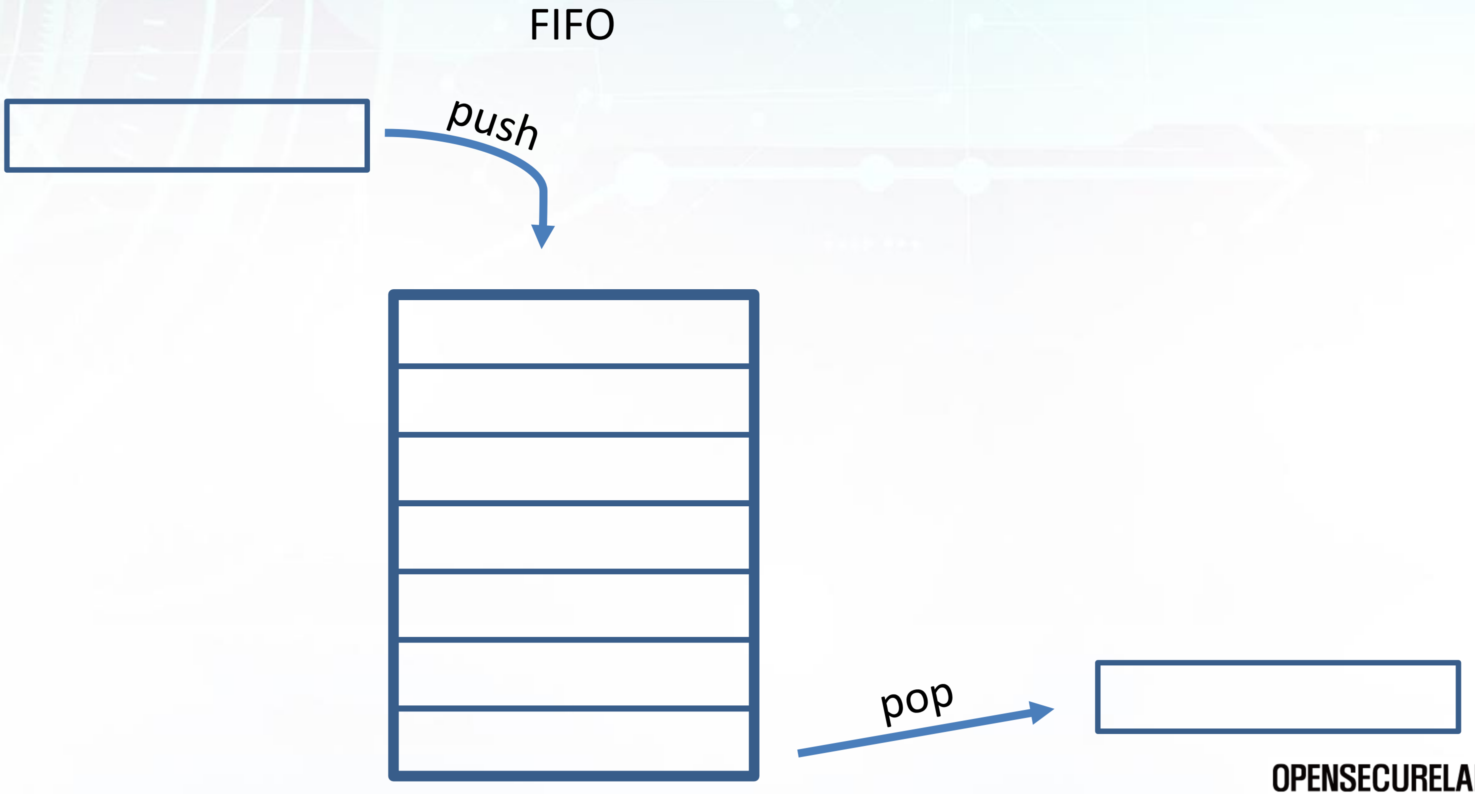
Message Queue

- Stack



Message Queue

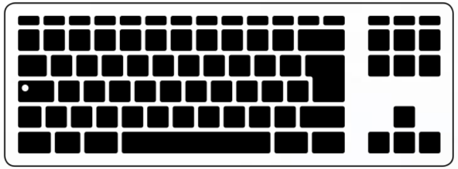
- Queue



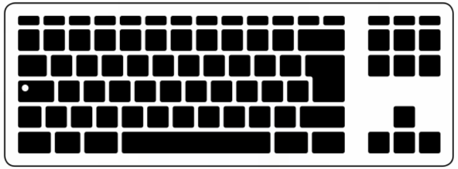
OPENSECURELAB
Information Security : Community·Consulting

Message Queue

Hle olrl!Wdo



Hello World!



SetWindowsHookEx

Set**W**indows**H**ook**E**x

```
HHOOK WINAPI SetWindowsHookEx(
 _In_ int        idHook,
 _In_ HOOKPROC   lpfn,
 _In_ HINSTANCE hMod,
 _In_ DWORD      dwThreadId
);
```

```
HHOOK WINAPI SetWindowsHookEx(
 _In_ int        WH_KEYBOARD,
 _In_ HOOKPROC   keylog,
 _In_ HINSTANCE hIns,
 _In_ DWORD      0
);
```

SetWindowsHookEx

Set**W**indows**H**ook**E**x

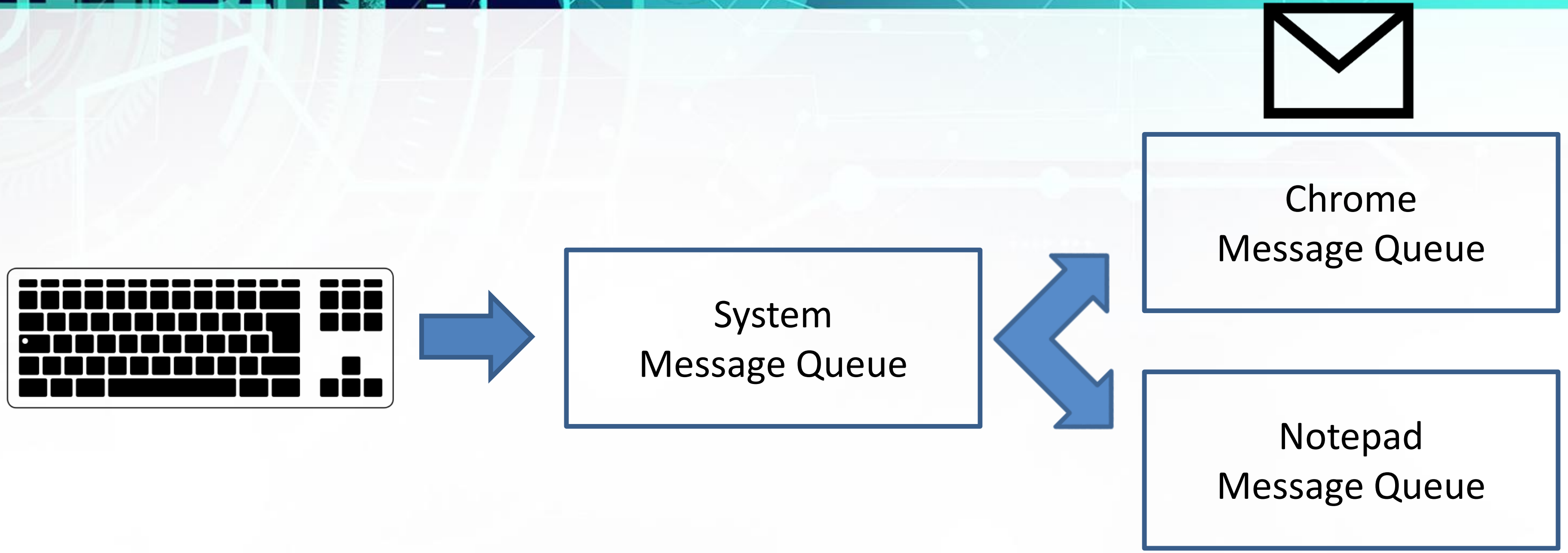
Main Program

```
 int main(void){
   LoadLibraryA(DLL);
   DLL.Hooking();
   DLL.UnHooking();
   FreeLibrary(DLL);
   return 0;
}
```

DLL

```
LRESULT CALLBACK keylog(…){…}
extern void Hooking(void){
  SetWindowsHookEx();
}
extern void UnHooking(void){
  UnHookWindowsHookEx();
}
```

KeyLogging 시연

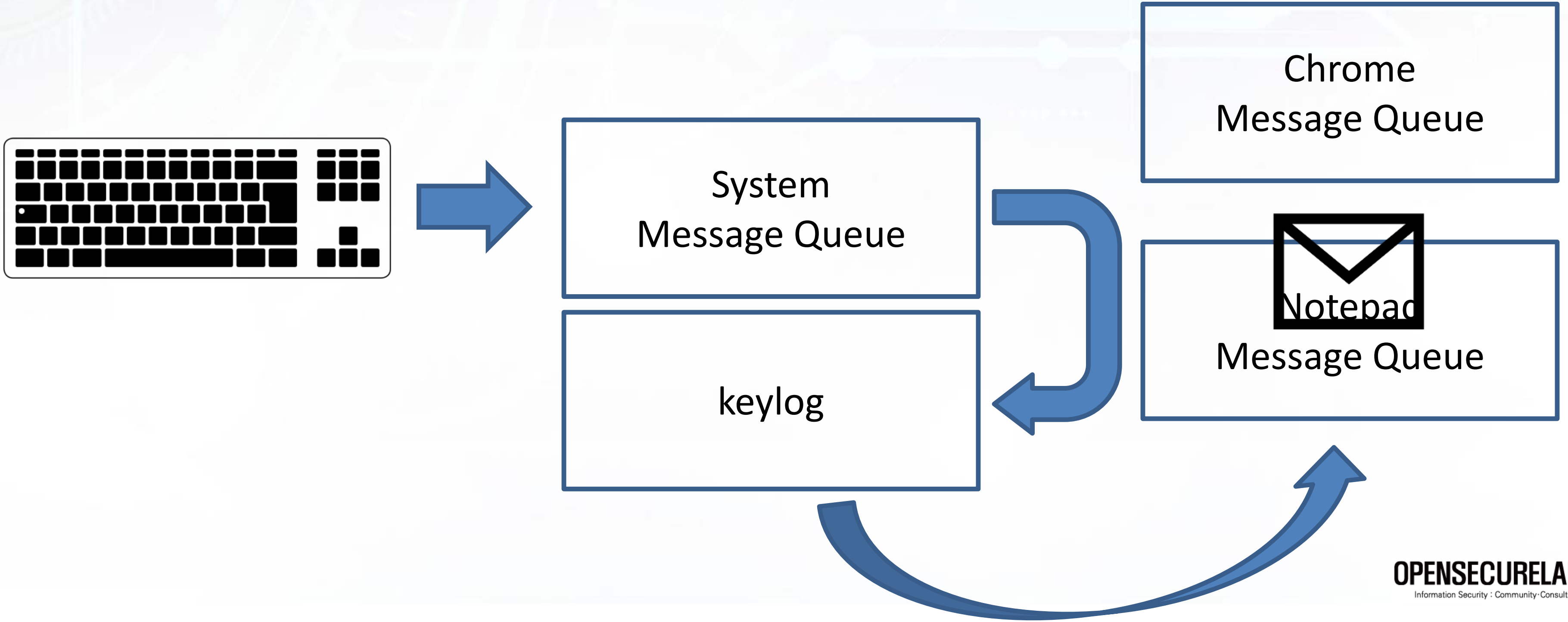


System
Message Queue

Chrome
Message Queue

Notepad
Message Queue

KeyLogging 시연



System
Message Queue

keylog

Chrome
Message Queue

Notepad
Message Queue

OPENSECURELAB
Information Security : Community·Consulting

KeyLogging 시연

감사합니다

MINJK1213