Pokročilé asemblery

Cvičení 1, 2017

Organizace

Cvičení

- Cvičení budou probíhat skoro každý týden (celkem 8)
- Cvičení jsou hodnocená 0-2 body, celkem je možné získat za cvičení 16 bodů

Projekty

- Cvičení a projekty budou částečně propojené.
- První kontrolní bod: 4 bodů
- Druhý kontrolní bod: 8 bodů
- Dořešení projektu (doladěni kódu, dokumentace, prezentace): 12 bodů
- Týmy napříč zadáními

Konzultace

- cvičení, projekty (Ing. Tomáš Goldmann, igoldmann@fit.vutbr.cz nebo osobně po domluvě e-mailem)
- projekty, organizační záležitosti (Ing. Filip Orság Ph.D., orsag@fit.vutbr.cz)

Knihovny

Statické

- Linkují se při překladu
- Funkce ze statické knihovny jsou linkovány do přeloženého souboru (součást výsledného binárního souboru)
- Rychlejší spouštění programu, nemusí se provádět *loading*
- Přípony: .a, .lib

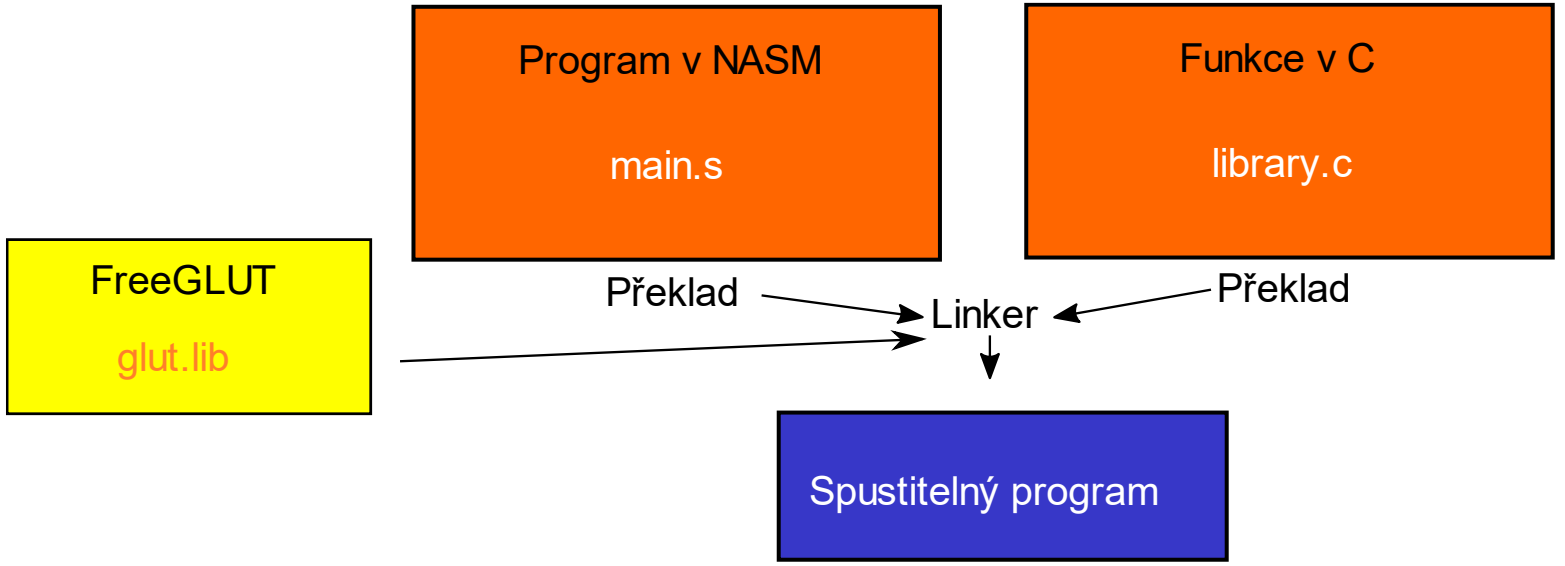
Dynamické

- Načítají se za běhu, jedna načtená knihovna může být sdílena mezi více procesů
- Menší velikost výsledného programu
- Přípony: .dll, .so

Pro gcc:
gcc -fPIC -c ipa.c
gcc -shared ipa.o -o ipa.so

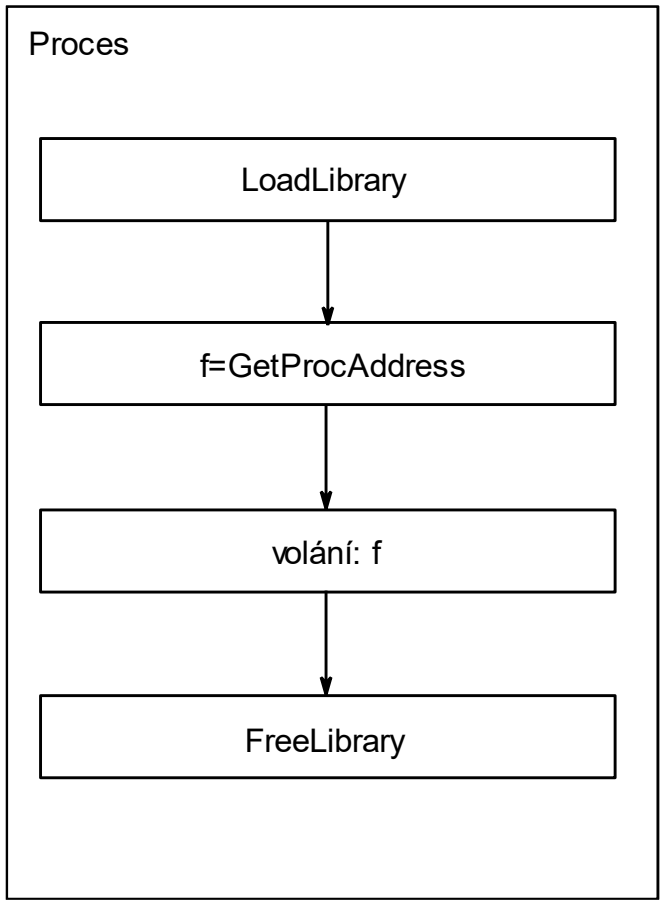
Překlad – statická knihovna

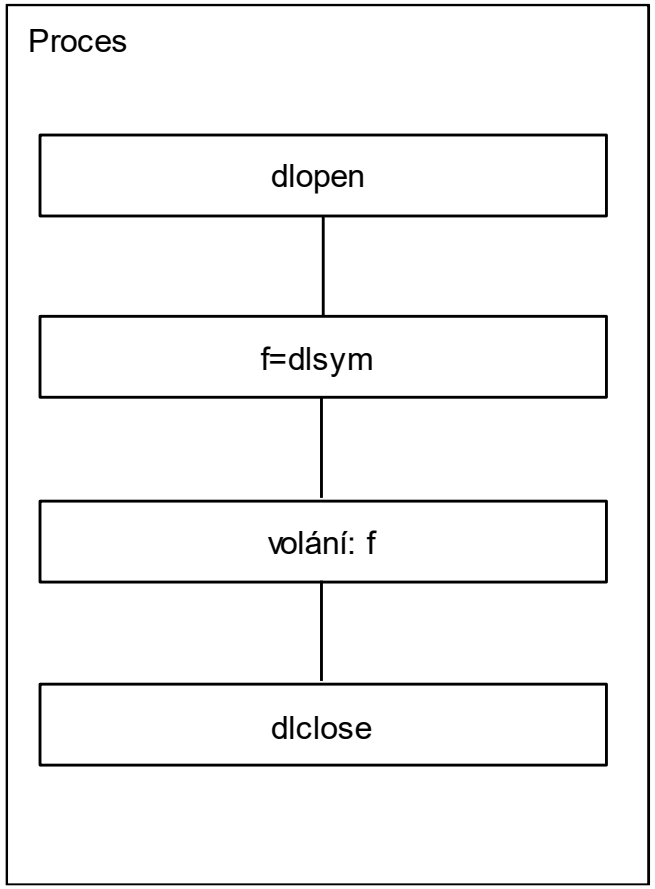
- Diagram překladu



- Překladače: GCC, Visual C++,…

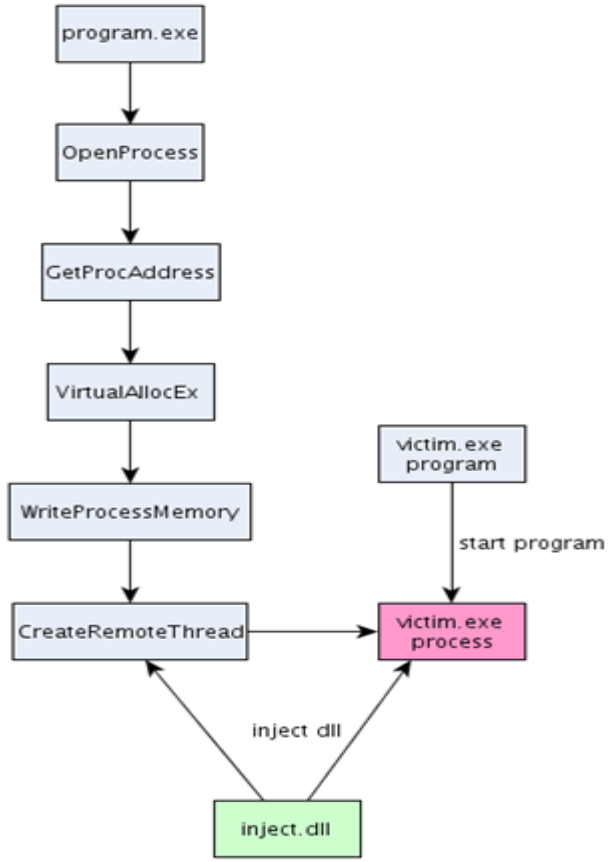
Volání DLL knihovny – Windows, Linux





DLL injection

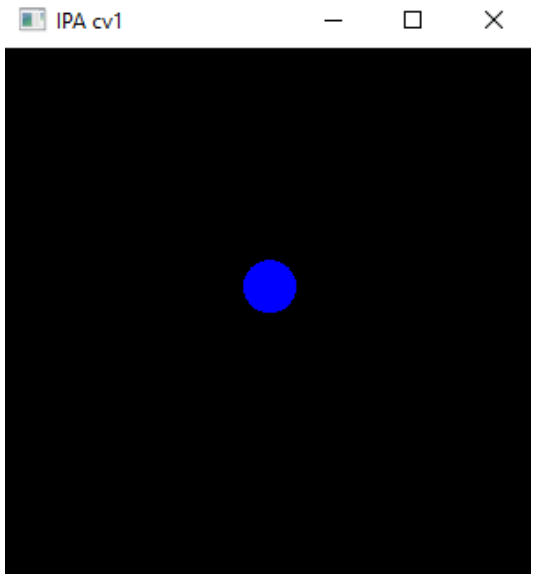
- DLL injection je typ útoku při kterém útočník prostřednictvím programu zavede do procesu (oběti) DLL knihovnu se škodlivým kódem



http://resources.infosecinstitute.com/using-createremotethread-for-dll-injection-on-windows/#gref

Nástroje

- Stáhněte si balík s nástroji z odkazu www.fit.vutbr.cz/~igoldmann/ipa1.zip (nebo wiki), tyto nástroje rozbalte do adresáře P:.
- V adresáři najdete NASM + knihovny pro práci s OpenGL.
- Ve složce ipa_cv1 naleznete solution se dvěma projekty (jeden dll knihovna + aplikace v C, která načítá DLL a vykresluje kolečko.



Vytvořeni DLL knihovny

- Cílem tohoto cvičení je vytvořit DLL knihovnu, která bude obsahovat minimálně dvě funkce pro ovládání pohybu balónku:

Funkce:

- **getY** – Tato funkce vrátí aktuální souřadnici y polohy míčku, při každém zavolání této funkce dojde k inkrementaci/dekrementaci souřadnice. Po každé inkrementaci a dekrementaci ověřte, zda balónek není mimo hranice plochy.
- **update** – Tato funkce nastaví hranice plochy pro pohyb

Nápověda:

- Pracujte s koprocesorem v 32bitovém režimu

Další úkoly:

- Vyzkoušejte v DLL knihovně funkci WriteFile z Win32API (stdcall)