Overview of the following windows security related topics

- Quick windows security aspects (pros&contras)
- overview of security mechanisms
- two visual versions of stacks
- in-depth ASLR and DEP

Quick windows security aspects (Pros)

Good:

- User privileges
- Automated windows security updates
- Windows recovery
- Windows Defender
- Fingerprint login
- Security mechanisms in programs

Quick windows security aspects (Contras)

Bad:

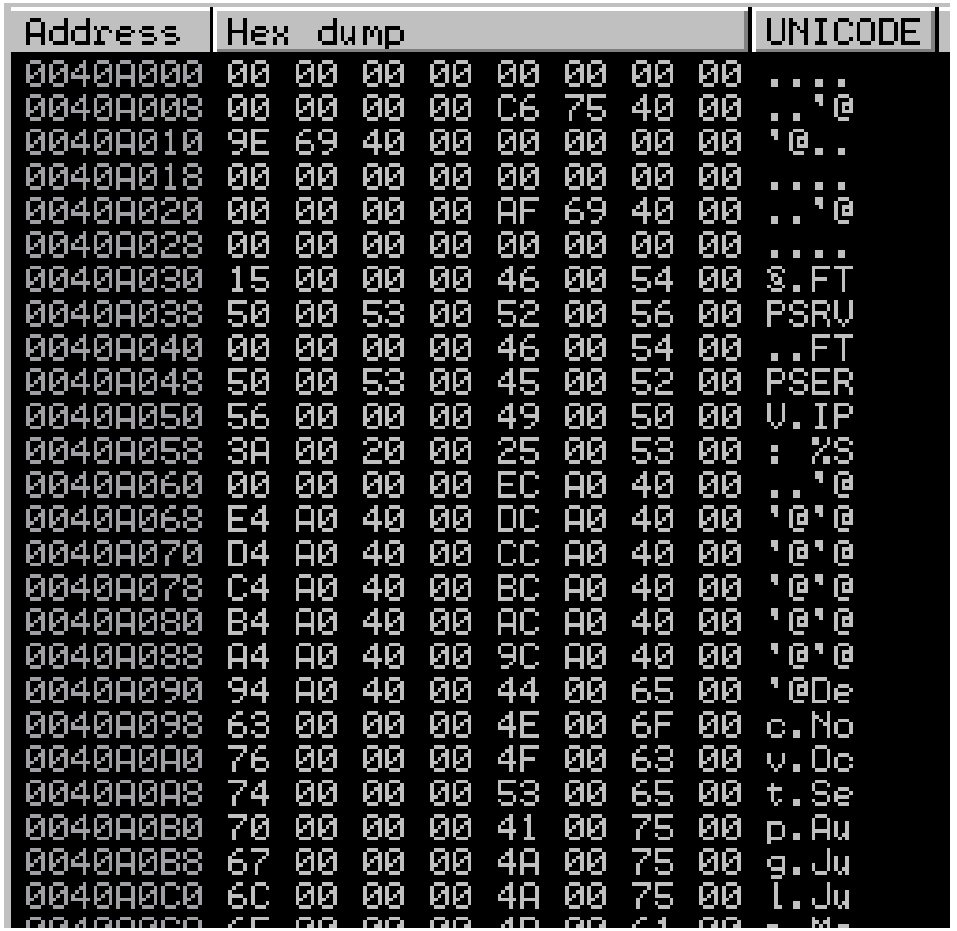
- Windows != open-source
- Windows is part of the PRISM project
- Windows used to use autorun for USB devices for win7 and below.

Overview of security mechanisms

- GS Stack buffer overrun detection.
- SafeSEH exception handling protection.
- Structured Exception Handler Overwrite Protection (SEHOP).
- Data Execution Prevention (DEP) / No eXecute (NX).
- **Address space layout randomization (ASLR).**
- Pointer Encoding.
- Heap corruption detection.
- Migration of buffer-overrun prone functions to safer versions.

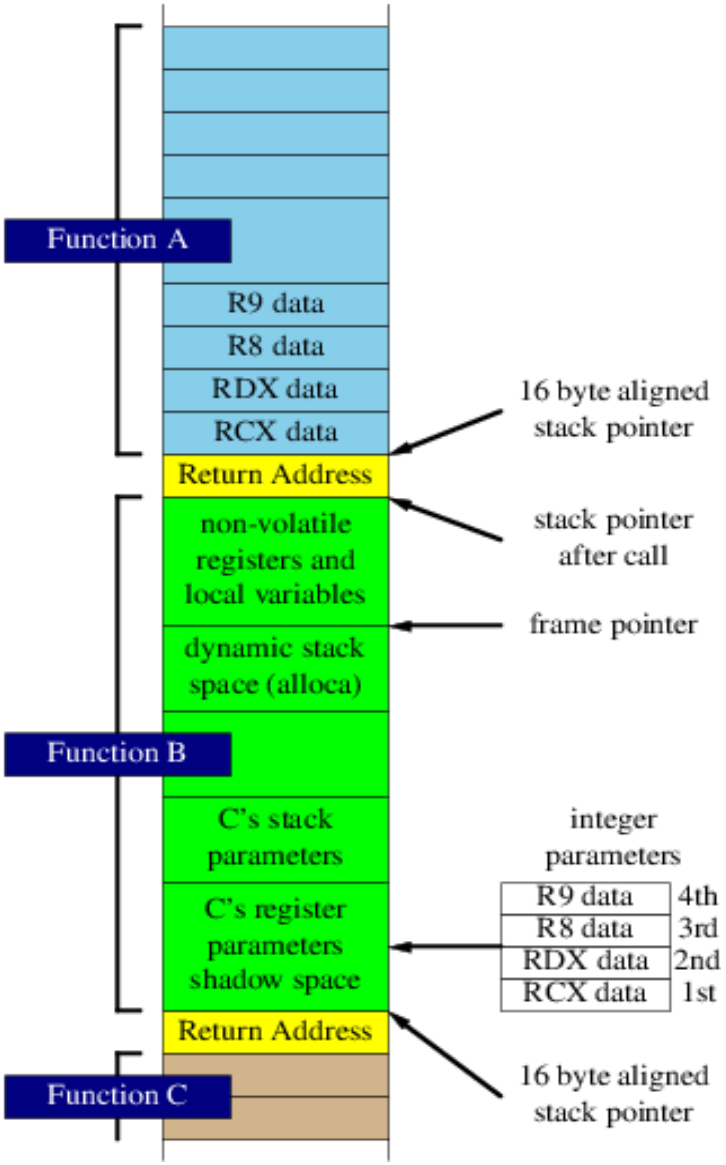
Before we jump into it...

- This is how a hex stack looks like...



Address	Hex dump	UNICODE
0040A000	00 00 00 00 00 00 00 00	....
0040A008	00 00 00 00 C6 75 40 00	..'@
0040A010	9E 69 40 00 00 00 00 00	'@..
0040A018	00 00 00 00 00 00 00 00	....
0040A020	00 00 00 00 AF 69 40 00	..'@
0040A028	00 00 00 00 00 00 00 00	....
0040A030	15 00 00 00 46 00 54 00	§.FT
0040A038	50 00 53 00 52 00 56 00	PSRV
0040A040	00 00 00 00 46 00 54 00	..FT
0040A048	50 00 53 00 45 00 52 00	PSER
0040A050	56 00 00 00 49 00 50 00	V.IP
0040A058	3A 00 20 00 25 00 53 00	: %S
0040A060	00 00 00 00 EC A0 40 00	..'@
0040A068	E4 A0 40 00 DC A0 40 00	'@'@
0040A070	D4 A0 40 00 CC A0 40 00	'@'@
0040A078	C4 A0 40 00 BC A0 40 00	'@'@
0040A080	B4 A0 40 00 AC A0 40 00	'@'@
0040A088	A4 A0 40 00 9C A0 40 00	'@'@
0040A090	94 A0 40 00 44 00 65 00	'@De
0040A098	63 00 00 00 4E 00 6F 00	c.No
0040A0A0	76 00 00 00 4F 00 63 00	v.Oc
0040A0A8	74 00 00 00 53 00 65 00	t.Se
0040A0B0	70 00 00 00 41 00 75 00	p.Au
0040A0B8	67 00 00 00 4A 00 75 00	g.Ju
0040A0C0	6C 00 00 00 4A 00 75 00	l.Ju

This is how a real stack looks like...



In-depth ASLR and DEP

- DEP makes data non-executable

  BUT we can bypass that...
- ASLR randomizes addresses

  This is also bypassable, but...