1.OllyDebug sazlaýjynyň mümkinçilikleri.
2.OllyDebug sazlaýjyny programmalaryň goragyny döwmekde ulanmagyň esaslary.
3.Debaggerleri ulanman maşyn kodundaky gizlin maglumatlary kesgitlemek.
4.OllyDebug programmasynda programmalaryň seljerilmesiniň mysallary.
5.Maşyn koduny debaggerlerden we beýleki hüjümlerden goramak:

–Ýaşyrmaly maglumatlary reýestrde ýerleşdirmek we olary faýlyň programmanyň maşyn kodunyň içindäki maglumat-lar bilen baglaşdyrmak;–Olara bolan ýollary maşyn kodunda şifrlemek;
–Programmada şertli geçişleri ýaşyrmak;
–Boş geçişleri guramak;
–Debagger arkaly goýberilendigi barada habar berýän programma koduny düzmek.

Mundan öňki bölümlerde biz maglumat goragynyň birnäçe usullaryna seredip geçdik. Olaryň her biriniň artykmaçlygy bar hem bolsa, ýetmezçilikleri hem az däl. Bu ýetmezçilikler şol gorag usullaryň her biri üçin aýratyn hem bolsa, olary birleşdirýän ýetmezçilik hem bardyr. Bu debagger arkaly hüjümdir.

Mundan öňki bölümlerde biz maglumat goragynyň birnäçe usullaryna seredip geçdik. Olaryň her biriniň artykmaçlygy bar hem bolsa, ýetmezçilikleri hem az däl. Bu ýetmezçilikler şol gorag usullaryň her biri üçin aýratyn hem bolsa, olary birleşdirýän ýetmezçilik hem bardyr. Bu debagger arkaly hüjümdir.

Sazlaýjylaryň köp dürli görnüşleri bar: SoftICE, OllyDebug, IDA we ş.m. Windows-platformalar üçin bar bolanlaryň hemmesiniň arasynda has meşhur bolup Numega firmasynyň SoftICE önümi çykyş edýär. Onuň iň esasy aýratynlygy bolup, goragyň 0njy halkasynda işlemeklik çykyş edýär. Gorag halkalary Intel firmasynyň 32derejeli prosessorlaryň gurluşlarynda ýerine ýetirilýän programmalaryň özara we amallar ulgamy bilen baglaşmagyny çäklendirmek üçin ulanylýar. Adatça, amallar ulgamy hemme beýleki ýerine ýetirilýän program-malara bolan doly elýeterlilik hukugyna eýe, sebäbi ol goragyň 0-njy halkasynda işleýär, ulgamlaýyn meseleler 1nji we 2nji halkalarda, goşundylar 3nji halkada işleýär. Goýberilen goşundylary bölekleýin dolandyrmagy goragyň 1nji we 2nji halkalaryndan amala aşyrmak mümkin. Hut şeýle ýagdaýda sazlaýjylaryň köpüsi işleýär. SoftICE amallar ulgamynyň özeni ýüklenmezden öň ýüklenýär we diňe ulgam tarapyndan ýerine ýetirilýän hemme meseleleri gözegçilikde sakla-man, eýsem amallar ulgamynyň özüni hem gözegçilikde saklamagy mümkin edýär.

Kitabyň bu bölüminde esasy maksat – debaggerler arkaly programmalaryň goragynyň döwülmegini amala aşyrmak dälde, ony seljermek, seljermegiň esasynda oňa garşy

programma kodlary işläp düzmek. Munuň üçin ýönekeý hasaplanylýan, emma şol bir wagtda öndürijilikli bolan debaggersazlaýjy – OllyDebug programmasynyň işine serediler.

Didar BAÝRAMOW
Türkmenistanyň Telekommunikasiýalar
we Informatika institutynyň talyby