F-Prot Management Console

Miðstýring öryggishugbúnaðar í fyrirtækjum

Anton Stefánsson
Kristján Pálmi Gunnarsson
Magni R. Sigurðsson

Tölvunarfræðideild
Vor 2011

Lokaverkefni Tölvunarfræðideild 2011

Miðstýring öryggishugbúnaðar í fyrirtækjum

Lokaskýrsla

Nemendur:

Anton Stefánsson

Kt: 131283-2969

Kristján Pálmi Gunnarsson

Kt: 140586-2189

Magni R. Sigurðsson

Kt: 241085-2959

Leiðbeinandi:

Bjarki Guðlaugsson

Prófdómari:

Stefán Freyr Stefánsson

Efnisyfirlit

Inngangur

Verkefnið fólst í því að smíða hugbúnað fyrir Friðrik Skúlason ehf., sem hjálpar kerfisstjóra að hafa yfirsýn yfir tölvur á neti innan fyrirtækis. Tilgangurinn með hugbúnaðinum er að veita kerfisstjóra mikilvægar upplýsingar um þær tölvur sem eru á neti innan fyrirtækis og hvort öll öryggismál séu í lagi. Hugbúnaðurinn hefur allar nýjustu upplýsingar hvað varðar vírusvörn notanda sem og alla þá sögu sem henni fylgir.

Markmið verkefnisins var að smíða notendavænan hugbúnað sem gæti birt þessi gögn á mjög aðgengilegan hátt. Það sem var einnig mjög mikilvægt, var að kerfisstjóri gæti haft sem besta yfirsýn yfir þær tölvur sem eru á hans neti og gæti flokkað tölvur eftir því sem honum hentar.

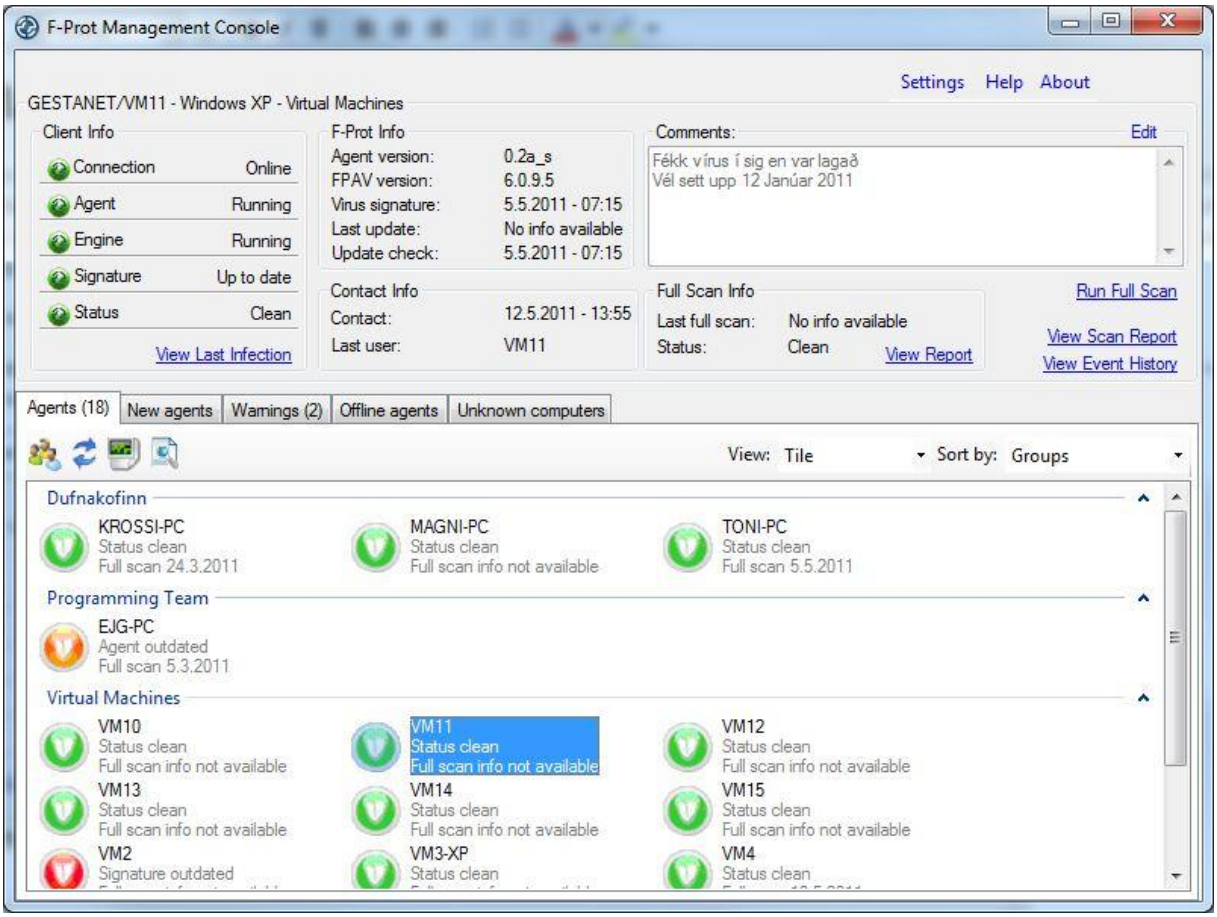
Hugbúnaðurinn er viðbót við vírusvörn Friðriks Skúlasonar ehf., F-Prot Antivirus.

Lýsing verkefnis

F-Prot Antivirus er vírusvarnarhugbúnaður fyrir Windows smíðaður af fyrirtækinu Friðrik Skúlason ehf. F-Prot er íslensk vírusvörn sem byggir á margra ára rannsóknar- og þróunarvinnu helstu veiruvarnasérfræðinga hér á landi og erlendis. Það sem hefur vantað er hugbúnaður fyrir kerfisstjóra sem getur fylgst með F-Prot vírusvörninni á tölvum notenda innan nets fyrirtækis.

Hugbúnaðurinn sem nemendur tóku að sér að smíða heitir F-Prot Management Console (hér eftir kallað: F-Prot MC) og er Windows gluggaforrit. F-Prot MC les upplýsingar úr gagnagrunni um stöðu notenda á neti innan fyrirtækis, skóla eða annarrar stofnunar. Upplýsingarnar sem F-Prot MC les upp úr gagnagrunninum eru skrifaðar af svokölluðum „Agent" með nokkurra mínútna millibili í gagnagrunn. „Agent-inn" sem er lítil þjónusta inn á tölvu notanda les upplýsingar frá bæði stýrikerfinu og vírusvörninni F-Prot Antivirus. „Agent-inn" var smíðaður af starfsmönnum Friðriks Skúlasonar og var því ekki hluti af lokaverkefni nemenda. Gagnagrunnurinn sem F-Prot MC les upp úr og „Agent-inn" skrifar í var hannaður af starfsmönnum Friðriks Skúlasonar í samstarfi við nemendur.

Með F-Prot MC er hægt að sjá nokkurra sekúndna gamlar upplýsingar um notendur sem eru tengdir gagnagrunninum ásamt þeim notendum sem ekki hafa „Agent" en eru inn á neti fyrirtækisins. Það er gert með því að nota WMI tengingu (sjá blaðsíðu 8). Hugbúnaðinum er skipt upp í tvo glugga innan þess ramma sem það er í. Efri ramminn birtir stöður og upplýsingar um hvern notanda fyrir sig ásamt aðgerðum sem tengjast þeim notanda sem er valinn í neðri glugganum. Neðri glugginn birtir notendur á neti fyrirtækisins. Ýtarlegri upplýsingar um stöður og aðrar upplýsingar sem birtast í efri glugganum er hægt að sjá á blaðsíðu þrjú í Notendahandbók. Mikilvægur þáttur í verkefninu var að kerfisstjórinn gæti flokkað tölvur í hópa svo hann hafi sem besta yfirsýn yfir þær tölvur sem eru á hans neti.



F-Prot Management Console

Ýtarlegri upplýsingar og útskýringar um virkni kerfisins má sjá í Notendaleiðbeiningar.pdf á meðfylgjandi geisladiski.

Skipulag

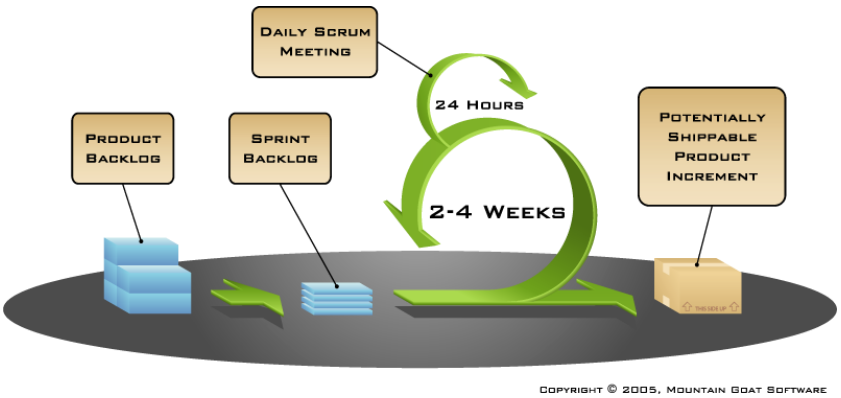
Aðferðarfræði

Eftir að hafa rætt við leiðbeinanda ákváðu nemendur að nota SCRUM aðferðafræðina til að vinna verkefnið. Nemendur hópsins þekktu Scrum og var því auðvelt fyrir þá að koma sér strax að verki. Eftir að nemendur höfðu fundað með verkkaupa (*e. product owner*) og komið sér vel inn í hver tilgangur verkefnisins væri, var farið í að búa til kröfulista (*e. product backlog*). Fyrstu drög að honum voru búin til út frá hugkorti sem nemendur fengu frá verkkaupa á áður nefndum fundi.

Því næst var búin til verkáætlun þar sem verkinu var skipt upp í sjö, tveggja vikna spretti (*e. sprints*). Kröfum var svo raðað niður á sprettina. Fyrir hvern sprett voru kröfur brotnar upp og skipt niður í verkliði (*e. sprint backlog*) og hjálpuðust nemendur að við að brjóta upp kröfur og áætla tíma á þær.

Á hverjum morgni áður en nemendur byrjuðu að vinna í verkefninu var haldinn stuttur stöðufundur (*e. daily standup meeting*) þar sem farið var yfir hvað hver hefði gert daginn áður, hvað þeir ætluðu að gera í dag og hvort það væri eitthvað sem stæði í vegi fyrir þeim.

Eftir hvern sprett var haldin lítil kynning (*e. sprint review*) þar sem að nemendur kynntu fyrir verkkaupa hvað hefði verið gert í sprettinum og hvað ætti að gera í þeim næsta. Að lokum var svo farið yfir hvað hefði verið gott og hvað hefði mátt gera betur (*e. retrospective*).



Yfirlitsmynd af SCRUM[1]

[1] Yfirlitsmynd af SCRUM, http://www.mountaingoatsoftware.com/scrum/overview

Hlutverk

Verkkaupi (*e. product owner*)	Kristmundur Jón Hjaltason
Verkefnastjóri (*e. scrum master*)	Kristján Pálmi Gunnarsson
Teymið	Anton Stefánsson Kristján Pálmi Gunnarsson Magni R. Sigurðsson

Hlutverk verkkaupa var að skilgreina kröfur og að sjá til þess að þeim væri rétt forgangsraðað. Verkkaupi sat einnig kynningar eftir spretti (*e. sprint review*) og var alltaf til taks til að svara spurningum.

Hlutverk verkefnastjóra var að halda utan um alla tíma sem unnir voru í hverjum spretti og passa upp á að það stæði ekkert í vegi fyrir því að teymið gæti unnið í verkefninu.

Teymið ásamt verkkaupa vann saman að hönnun hugbúnaðarins og hönnun gagnagrunns. Teymið vann svo saman að forritun, skýrslugerð og að framkvæmd prófana.

Greining

Greining á hugbúnaðinum var framkvæmd í samvinnu við verkkaupa. Strax í upphafi fór verkkaupi yfir það hvernig hann hafði hugsað sér að uppsetning og önnur atriði skildu vera í hugbúnaðinum. Eftir að hafa fengið grófa útskýringu á því hvernig hugbúnaðurinn ætti að lýta út var farið í að gera frumgerð sem var gerð í spretti 1. Verkkaupi var búinn að teikna upp viðmót fyrir nemendur, sem var eins og hann vildi að hugbúnaðurinn myndi líta út. Nemendur smíðuðu viðmótið í Microsoft Visual Studio 2010 í C# og báru það undir verkkaupa sem samþykkti.

Þarfagreining

Þarfagreining var gerð út frá hugkorti sem verkkaupi lét nemendur hafa í upphafi verkefnisins. Eftir að hafa búið til kröfur og forgangsraðað þeim voru þær bornar undir verkkaupa sem samþykkti þær. Kröfurnar voru svo brotnar upp í verkliði fyrir hvern sprett og áætlaður tími á þá. Hægt er að sjá kröfulistann í heild sinni þar sem er búið að

skipta niður kröfunum og brjóta þær upp í verkliði fyrir hvern sprett í Kröfulisti-FPROT.xlsx á meðfylgjandi geisladiski.

Áhættugreining

Í töflunni hér að neðan er listi yfir áhættur sem þótti líklegt að kæmu upp á meðan á verkefninu stóð. Áhættunum var gefin númer til að greina þær í sundur. Í dálkinum *líkur* eru stuðlar sem gefa til kynna hversu miklar líkur séu á því að ákveðinn áhættuþáttur muni eiga sér stað, þar sem 5 merkir að mjög líklegt sé að áhættuþátturinn eigi sér stað og 1 að mjög litlar líkur séu á því. *Alvarleiki* fær einnig ákveðinn stuðul frá 1 og upp í 5, þar sem 5 merkir að afleiðingar áhættunnar geti haft mjög slæm áhrif og 1 að afleiðingarnar séu litlar sem engar. *Áhættustuðullinn* er svo líkur margfaldaðar með alvarleika.

Nr.	Nafn	Líkur	Alvarleiki	Áhættu-stuðull	Afgreitt	Ábyrgðarmaður
1.	Óþekkt tækni (WMI)	5	4	20	24.02.11	Magni
2.	Leita/tengjast client	5	4	20	24.02.11	Anton, Kristján
3.	Álag í öðrum kúrsum	5	4	20	30.04.11	Allir
4.	Tenging við gagnagrunn	5	3	15	16.2.11	Anton
5.	Veikindi	3	3	9	16.5.11	Allir
6.	Umfang verkefnis	3	3	9	15.03.11	Kristmundur/Finnbogi
7.	Samstæðustjórnunarkerfi	1	5	5	01.02.11	Finnbogi
8.	Óljósar kröfur	2	2	4	15.03.11	Kristmundur

Tafla 1

Hægt er að sjá áhættugreininguna í heild sinni með útskýringum á hverju atriði fyrir sig í skjalinu Áhættugreining.pdf sem er á meðfylgjandi geisladiski.

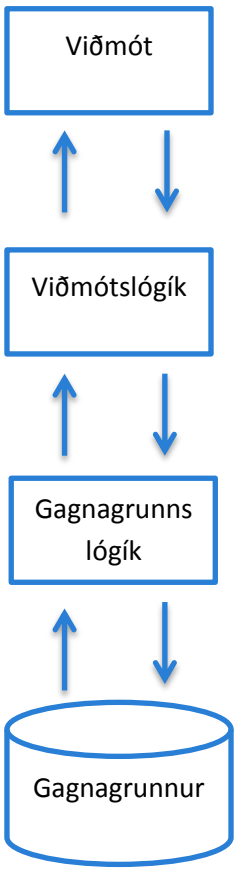
Forritun

Verkefnið unnu nemendur í Microsoft Visual Studio 2010 og var það forritað í C# .NET 4.0. Hugbúnaðurinn var smíðaður út frá Windows Form Application. Verkkaupi óskaði þess að sá ritstíll (*e. coding standard*) sem nemendur notuðu væri All-In-One Code Framework Coding Standards.[2]

Windows Management Instrumentation (WMI)[3] var notað til að ná tengingu við tölvur inn á sama neti (*e. network domain*) og kerfisstjóri. Með WMI tengingu var hægt að fá tengingu við WIN_32[4] klasasafnið sem gefur aðgang að stóru upplýsingasafni. Upplýsingarnar sem nemendur sóttu í gegnum WIN_32 kalsasafnið voru upplýsingar um tölvu notanda á netinu sem hefur ekki Agent. WMI var einnig notað til að skoða lista yfir þjónustur sem voru keyrandi á tölvu notanda til að sjá hvort Agent væri keyrandi og hvort vírusvörn væri virk. Hægt er að sjá ýtarlegri upplýsingar um WMI í Rekstrarhandbók og á heimasíðu Microsoft[3].

Þriggja laga hönnun

Við forritun hugbúnaðarins fannst bæði nemendum og verkkaupa mjög mikilvægt að kerfið yrði smíðað eftir þriggja laga arkitektúr.



Nemendur aðskildu viðmót frá allri lógík og öll lógík var aðskilin frá allri gagnagrunnsvinnslu. *GUILogic* er einn af aðal klösum hugbúnaðarins. Hans hlutverk er að tala við bæði viðmótið og gagnagrunns klasann DBLogic, sem er hinn aðal klasi hugbúnaðarins. Þegar smellt er á takka eða tengil í viðmóti hugbúnaðarins um að sækja nýjar upplýsingar er sent *CallBack* frá viðmóti niður í GUILogic. GUILogic kallar niður í DBLogic eftir nýjum upplýsingum. DBLogic sendir nýjar upplýsingar upp í GUILogic og sér GUILogic um að skila upplýsingunum á réttan stað í viðmóti.

Klasarit og gagnagrunnsskema er hægt að sjá á meðfylgjandi geisladiski.

[2] All-In-One Code Framework Coding Standards: http://1code.codeplex.com/releases/view/50431
[3] Windows Management Instrumentation: http://msdn.microsoft.com/en-us/library/aa394582(v=vs.85).aspx
[4] Win 32 klasasafn: http://msdn.microsoft.com/en-us/library/aa394084(v=vs.85).aspx

Prófanir

Framkvæmdar voru kerfis- og notendaprófanir á hugbúnaðinum. Notendaprófið var þó frekar óformlegt, en þar var fengið starfsfólk Friðriks Skúlasonar ehf. til að prufa hugbúnaðinn. Það var í flestum tilfellum mjög ánægt með hugbúnaðinn og gat leiðbeint nemendum um hvað betur mætti fara.

Útbúið var kerfispróf af nemendum þar sem prófunaraðili var fenginn til fara í gegnum prófið. Lýsing var á því hvað prófunaraðilinn ætti að gera og svo hver útkoman ætti að vera. Prófið var í 30 liðum og var prófunaraðili beðinn um að skrá allar athugasemdir sem hann hafði varðandi kerfið. Í spretti 6 og 7 var kerfið prófað ýtarlega af nemendum.

Prófanirnar sem gerðar voru á kerfinu í spretti 6 og 7 leiddu í ljós margar smávægilegar villur sem reyndist frekar auðvelt að lagfæra. Það voru þó nokkrar villur sem tóku lengri tíma að lagfæra. Hægt er að sjá kerfisprófið í heild sinni á meðfylgjandi geisladisk, Kerfispróf.pdf.

Þróunartól og tækniumhverfi

Eins og fram kom í kaflanum hér á undan var verkefnið forritað í tungumálinu C# og unnu nemendur verkefnið í Microsoft Visual Studio 2010.

Microsoft SQL Server 2008 R2 var notað til vinnslu við gagnagrunna.

Við tengingu milli hugbúnaðar og gagnagrunns var notast við LINQ to SQL sem er hluti af .NET Framework 3,5 útgáfunni.

Nemendur notuðust við samstæðustjórnunarkerfið TortoiseSVN 1.6.9 og var einnig notast við viðbót í Microsoft Visual Studio 2010, AnkhSVN sem gerði nemendum kleyft að senda inn og sækja kóða beint í gegnum Microsoft Visual Studio 2010.

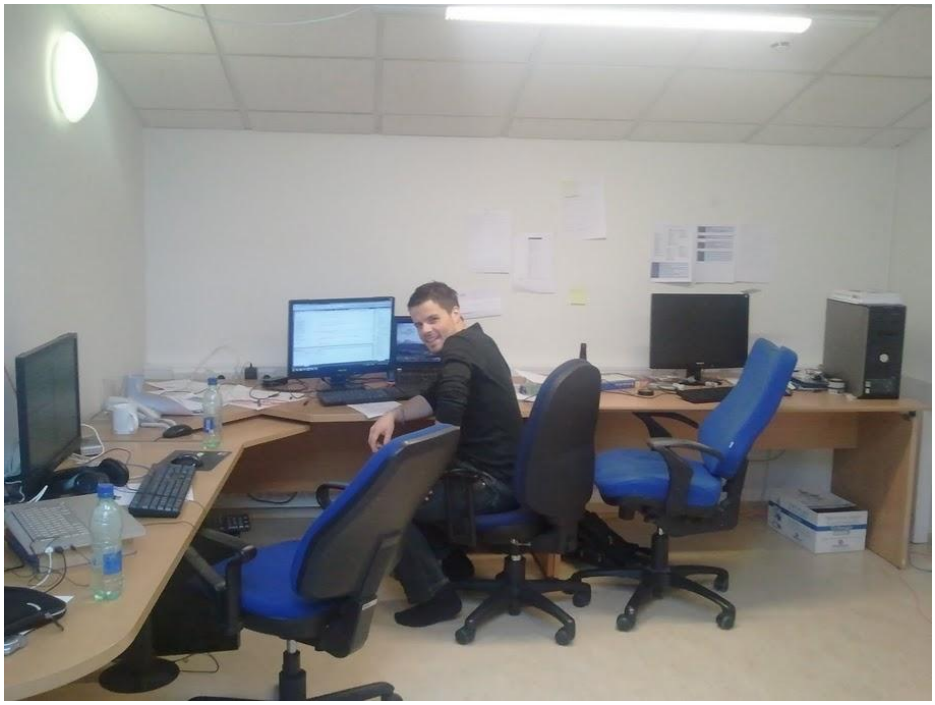
Nemendur fengu tvær tölvur sem ætlaðar voru til prófana. Sú fyrri sem nemendur fengu var með Microsoft Server 2008 og var gerð að „domain controler“ og sá hún að stjórna netinu. Seinni tölvan sem nemendur fengu var mjög öflugur turn sem notaður var til að keyra sýndarvélar (*e. virtual machines*). Settar voru upp 15 Microsoft Windows XP og 2 Microsoft Windows Vista vélar. Hugbúnaðurinn sem notaður var til að keyra þær var VMWare Workstation 7.1. Allar sýndarvélarnar nema ein höfðu uppsetta vírusvörn Friðriks Skúlasonar ehf., F-Prot Antivirus og Agent. Önnur af Microsoft Windows Vista vélunum hafði hvorki F-Prot Antivirus né Agent. Vélin hafði vírusvörn frá Avast og var það gert til að prufa hvort hægt væri að sækja upplýsingar um vírusvörnina með WMI.

Kröfulistar og aðrar áætlanir voru unnar í Microsoft Excel. Skjöl og kynningar voru unnar í Microsoft Word og Microsoft Powerpoint.

Öll skjölun var geymd í sameiginlegri möppu og var þar notast við Dropbox.

Aðstaða

Aðstaðan sem nemendur fengu innan fyrirtækisins var frábær. Nemendum var komið fyrir í stóru og góðu herbergi þar sem þeir fengu stóra skjái til að vinna á. Ef það var eitthvað sem nemendum vantaði þá voru starfsmenn Friðriks Skúlasonar ehf. alltaf til í að hjálpa. Nemendur unnu verkefnið eingöngu í húsakynnum Friðriks Skúlasonar ehf.



Aðstaða nemenda hjá Friðriki Skúlasyni ehf.

Dagbók

Nemendur héldu utan um dagbók þar sem allir tímar sem fóru í að vinna lokaverkefnið voru skráðir í. Dagbókin var einfalt *Excel* skjal sem geymt var inn á *Google Docs* og hafði leiðbeinandi hópsins aðgang að því þar. Dagbókina er hægt að skoða á meðfylgjandi geisladisk, Dagbok.pdf.

Framvinda

Eins og fram kom ofar í skýrslunni var verkefninu skipt upp í sjö spretti. Hér fyrir neðan er stutt samantekt á framvindu verkefnisins. Ýtarlegri framvinduyfirlit fyrir hvern sprett fyrir sig má sjá í Framvinduskyrsla.pdf á meðfylgjandi geisladiski.

Nemandi	Tímar
Anton	409
Kristján	376,5
Magni	387
Samtals	1172,5

Tafla 2

Í upphafi hvers spretts áætluðu nemendur tíma á hverja kröfu í viðkomandi spretti. Við lok hvers dags var farið yfir hvað hver og einn aðili innan hópsins gerði og skráð í verkefnisskjal fyrir viðkomandi sprett (*e. sprint backlog*).

Ef að unnið var í kröfu sem þótti óraunhæft að klára á þeim tíma sem hafði verið áætlaður í upphafi, var gerð enduráætlun á þá kröfu.

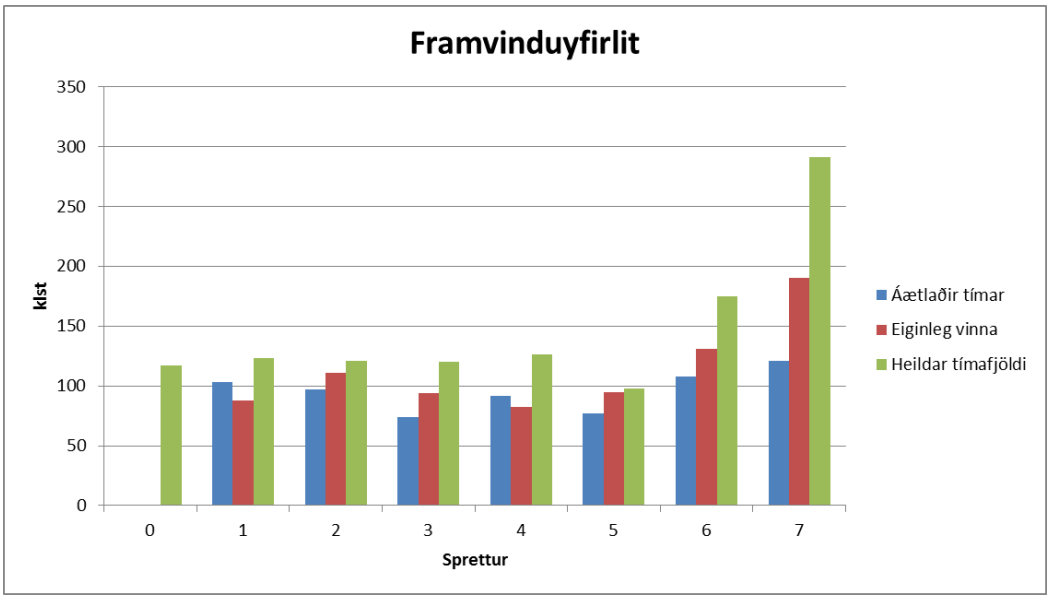
Tafla 2 er sundurliðun á hvað hver nemandi vann margar klukkustundir í verkefninu.

Sprettir	Áætlaður tímafjöldi	Eiginleg vinna	Heildar tímafjöldi
Sprettur 0		81,5	117
Sprettur 1	103	88	123,5
Sprettur 2	97	111	121
Sprettur 3	74	94	120
Sprettur 4	92	82	126,5
Sprettur 5	77	95	98
Sprettur 6	108	131	175
Sprettur 7	121	190	291,5

Tafla 3

Tafla 3 sýnir tíma sem áætlaður var á hvern sprett fyrir sig í upphafi, eiginlega vinnu sem lýsir þeim fjölda klukkustunda sem fór í kröfur úr kröfulista. Heildar tímafjöldi er sá tími sem nemendur unnu að verkefninu, þar er meðtalin eiginlega vinnan.

Súluritið hér að neðan endurspeglar gögnin í töflu 3.



Lokaorð

Nemendur voru almennt sáttir með útkomu verksins og hvernig til tókst. Með því að klára allar A kröfur töldu nemendur sig hafa náð markmiðinu sem þeir settu sér í upphafi. Nemendur lærðu ýmislegt á meðan á verkefninu stóð. Að vinna saman sem ein heild og halda skipulagi var eitt af því sem skipti miklu máli og gekk það mjög vel. Eins og fram kemur ofar í skýrslunni þurftu nemendur að vinna eftir reglum sem verkkaupi setti, þ.e. að vinna eftir ákveðnum forritunarstíl. Nemendur voru kunnugir Scrum, en höfðu allir litla reynslu af því að vinna eftir aðferðafræðinni. Báðir þessir liðir voru mjög krefjandi fyrir nemendur en nemendur voru þó ekki í neinum vandræðum með að tileinka sér þessa nýju siði.

Það sem nemendur áttu hvað erfiðast með að temja sér var að skrá niður alla tíma sem þeir unnu, enda óvanir að þurfa að skrá niður hvað þeir eru að gera, a.mk. í tölvu geiranum. Suma daga gleymdist að skrifa í dagbók en það kom þó ekki að sök þar sem alltaf var hægt að rifja upp hvað verið var að gera þá daga sem skráning gleymdist. Hægt er að sjá allar tímaskráningar í dagbók hópsins, Dagbok.pdf á meðfylgjandi geisladisk.

Erfiðasta verkefnið forritunarlega séð sem nemendur þurftu að glíma við var WMI tenging við mismunandi Windows stýrikerfi. Til að geta talað við vírusvörn notanda þarf að fara í gegnum *Windows Security center.* Til eru tvær útgáfur af *Windows Security Center* og er misjafnt hvort „center-ið“ á að tala við og fer það eftir stýrikerfi notanda. Það reyndist erfitt að geta sannreynt hvort allt væri að virka rétt þar sem að nemendur fengu ekki tölvur með öllum stýrikerfum fyrr en undir lok verkefnisins til að prufa virkni.

Þegar á heildina er litið gekk verkefnið mjög vel og voru nemendur virkilega ánægðir með þá vinnu sem þeir lögðu í verkefnið. Nemendur náðu líka einstaklega vel saman og komu engin ósætti upp í hópnum á meðan á verkefninu stóð.

Framtíðarsýn

Margar breytingar eiga eftir að eiga sér stað áður en hugbúnaðurinn verður að fullu tilbúinn til að fara á markað. Þær endurbætur sem nemendur sjá fyrir sér ásamt verkkaupa að hægt sé að gera í hugbúnaðinum í framtíðinni eru:

- Að geta sett upp Agent á útistandandi tölvur þar sem að hann hefur ekki verið settur upp.
- Að geta einangrað tölvur frá neti sem hafa fengið smit.
- Að geta ræst bæði vírusvörn og Agent á tölvum þar sem er slökkt hefur verið á þeim þjónustum.
- Að geta búið til yfirlits mynd af til dæmis hæð í byggingu og dregið þar inn þær tölvur sem eru á þeirri hæð.
- Að geta leitað eftir vírusum á tölvum.

Umsögn tengiliðs

Ástæða þess að við ákváðum að leita að nemendahópi til að vinna að gerð "Management Console" fyrir F-PROT, er í stuttu máli sú að slíkt forrit vantaði í okkar vörulínu og er okkur í raun nauðsynlegt til að vera samkeppnishæf við okkar helstu keppinauta.

Verkefnið var í upphafi afmarkað við þriðjung þeirrar vöru sem til stendur að þróa og markmiðið var að klára þann hluta kerfisins sem snýr að kerfisstjóranum hvað upplýsingaöflun varðar, þannig að hann gæti haft yfirlit yfir tölvur í hans umsjón, flokkað þær og séð stöðu þeirra.

Niðurstaðan nú við lok verkefnis er að ofangreint markmið hefur náðst - þótt enn sé mikið verk óunnið uns fullbúin vara verður tilbúin, þá er þetta verkefni nokkuð sem hægt er að byggja framtíðarþróun á, en ætlunin er að ráðast núna í beinu framhaldi í þróun á öðrum hlutum kerfisins.

Við höfum einstaka sinnum á undanförnum árum fengið nemendahópa til að vinna svipuð verkefni, en í sumum þeirra tilvika hefur afraksturinn verið frekar fátæklegur og verkefnin hafa oftast reynst fyrirtækinu gagnslítil til lengri tíma litið. Við væntum þess hins vegar að þetta verkefni muni nýtast okkur mun betur.

- *Friðrik Skúlason, eigandi Friðriks Skúlasonar ehf.*