Security and Advanced DevelopmentMinor

**BEZIGHEDEN**

S. van Staden - Studentnummer : 0883388

S. Prins - Studentnummer : 0882342

Klas : DINF3

Module : MINCMISAD01-1516

Datum : maandag 2 november 2015

Inhoud

[1. Inleiding 3](#_Toc434217880)

[2. BEZIGHEDEN 4](#_Toc434217881)

[Week 1 – S. van Staden 4](#_Toc434217882)

[Week 1 – S. Prins 4](#_Toc434217883)

[Week 2 – S. van Staden 5](#_Toc434217884)

[Week 2 – Sidney Prins 6](#_Toc434217885)

[Week 3 – S. van Staden 6](#_Toc434217886)

[Week 3 – Sidney Prins 6](#_Toc434217887)

[Week 4 – Sidney Prins 6](#_Toc434217888)

[Week 4 – S. van Staden 7](#_Toc434217889)

[Week 5 – S. van Staden 7](#_Toc434217890)

[Week 5 – Sidney Prins 8](#_Toc434217891)

[Week 6 – S. van Staden 8](#_Toc434217892)

[Week 6 – Sidney Prins 8](#_Toc434217893)

[Week 7 – S. van Staden 8](#_Toc434217894)

[Week 7 – Sidney Prins 9](#_Toc434217895)

[Week 8 – S. van Staden 9](#_Toc434217896)

# 1. Inleiding

Dit document is bedoeld om alle werkzaamheden vast te leggen die betrekking hebben op de minor.

# 2. BEZIGHEDEN

## Week 1 – S. van Staden

|  |  |  |
| --- | --- | --- |
| Naam: S. van Staden | | |
| Omschrijving | tijd | Datum |
| Vaste contacturen - Les | 7 uur | 7-9-2015 |
| Instaleren visual studio en code inlezen boek  [http://fsharpgamedev.codeplex.com/SourceControl/latest#](http://fsharpgamedev.codeplex.com/SourceControl/latest) | 2 uur | 7-9-2015 |
| Doorlezen eerste twee hoofdstukken  Boek: Friendly F# (Fun with game programming Book 1) | 2 uur | 8-9-2015 |
| Documentatie doorgenomen  <https://msdn.microsoft.com/en-us/library/vstudio/hh297109%28v=vs.100%29.aspx#sdfsdf> | 2 uur | 8-9-2015 |
| Onderzoek how to write reactive user-interfaces in F# using Silverlight.  <http://www.getcodesamples.com/src/44289F13> | 4 uur | 9-9-2015 |
| Skype call voor project | 2 uur | 9-9-2015 |
| Doorlezen chapter 1 t/m 4, proberen tutorials  <https://www.math.ku.edu/~kangas/Fsharply.pdf> | 4 uur | 10-9-2015 |
| Learning fsharp  <http://www.tryfsharp.org/Learn/getting-started>  instaleren Xamarin for f# | 4 uur | 11-9-2015 |
| Web apps for F#  <http://fsharp.org/guides/web/> | 6 uur | 12-9-2015 |
| Proberen webserver met https op te zetten in fsharp  <http://suave.io/paket.html> | 5 uur | 13-9-2015 |

## Week 1 – S. Prins

|  |  |  |
| --- | --- | --- |
| Naam: Sidney Prins | | |
| Omschrijving | tijd | Datum |
| Vaste contacturen - Les | 7 uur | 7-9-2015 |
| Skype call project | 2 uur | 9-9-2015 |
| Visual Studio installeren | 2 uur | 12-9-2015 |
| F# project werkend krijgen in Visual Studio | 1 uur | 12-9-2015 |
| Chapter 1 doorlezen & kijken naar code | 2 uur | 12-9-2015 |
| Chapter 2 doorlezen & kijken naar code | 2 uur | 13-9-2015 |
| Chapter 1 & 2 code wijzigen | 1 uur | 13-9-2015 |

## Week 2 – S. van Staden

|  |  |  |
| --- | --- | --- |
| Naam: S. van Staden | | |
| Omschrijving | tijd | Datum |
| Vaste contacturen – Les – server aanvragen en configureren | 9 uur | 14-9-2015 |
| AES dEncrypt in F#  <https://nl.wikipedia.org/wiki/Rijndael_%28cryptografie%29>  <https://msdn.microsoft.com/en-us/library/system.security.cryptography.icryptotransform%28v=vs.110%29.aspx>  <https://msdn.microsoft.com/en-us/library/system.security.cryptography.cryptostream.cryptostream%28v=vs.110%29.aspx>  <https://msdn.microsoft.com/en-us/library/system.security.cryptography.rijndaelmanaged%28v=vs.110%29.aspx> | 4 uur | 15-9-2015 |
| AES dEncrypt in F# verder maken, Cryptocat onderzoeken en IV  <http://stackoverflow.com/questions/8041451/good-aes-initialization-vector-practice>  //Password derived  //Derives a key from a password using an extension of the PBKDF1 //algorithm, Na onderzoek is eigenlijk PBKDF2  <https://msdn.microsoft.com/en-us/library/system.security.cryptography.passwordderivebytes%28v=vs.110%29.aspx>  <http://blogs.msdn.com/b/shawnfa/archive/2004/04/14/generating-a-key-from-a-password.aspx>  //Update TLS 1.2 op server was TLS 1.0  //TLS1.0 is niet veilig voor Beast attack  <https://wiki.mozilla.org/Security/Server_Side_TLS#BEAST_.28CVE-2011-3389.29>  <https://support.quovadisglobal.com/KB/a433/how-to-enable-tls-12-on-windows-server-2008-r2.aspx> | 6 uur | 16-9-2015 |
| Skype call en test Suave  <http://suave.io/> | 6 uur | 17-9-2015 |
| Versie control op server voor project en in visual studio  <https://www.visualsvn.com/visualsvn/download/>  MySql op server maak connectie met fsharp  Nuget MySql  PM> Install-Package MySql.Data  Mailboxprocessor <https://en.wikibooks.org/wiki/F_Sharp_Programming/MailboxProcessor> | 6 uur | 18-9-2015 |
| Websockets en skype call | 6 uur | 19-9-2015 |
| Websockets en unmask socket stream  <http://lucumr.pocoo.org/2012/9/24/websockets-101/> | 6 uur | 20-09-2015 |

## Week 2 – Sidney Prins

|  |  |  |
| --- | --- | --- |
| Naam: Sidney Prins | | |
| Omschrijving | tijd | Datum |
| Vaste contacturen – Les – server aanvragen en configureren | 9 uur | 14-9-2015 |
| OTR en OpenSSL uitzoeken | 2 uur | 15-9-2015 |
| Kijken welke libraries we gebruiken | 2 uur | 16-9-2015 |
| Met zijn tween naar document kijken | 2 uur | 17-9-2015 |
| Skype call + naar code kijken | 6 uur | 19-9-2015 |
| Skype call + naar code kijken | 3 uur | 20-09-2015 |

## Week 3 – S. van Staden

|  |  |  |
| --- | --- | --- |
| Naam: S. van Staden | | |
| Omschrijving | tijd | Datum |
| Vaste contacturen – Les – visual studio instaleren en OTRLib c# verkennen  <http://www.codeproject.com/Articles/644318/Off-The-Record-OTR-Security-Protocol> | 9 uur | 21-9-2015 |
| Skype gesprek en security vragen behandelen en opzet applicatie | 4 uur | 22-9-2015 |
| Activity Diagram UML gemaakt met Visual Studio  [Save UML Diagram To Image File 2015](https://visualstudiogallery.msdn.microsoft.com/ac24086a-96dd-45ae-ad38-324c3f0233c3) | 4 uur | 23-9-2015 |
| Inlezen MPOTR  <https://github.com/DrWhax/mpOTR> | 2 uur | 25-9-2015 |
| Skype gesprek en behandelen MPOTR | 4 uur | 27-9-2015 |

## Week 3 – Sidney Prins

|  |  |  |
| --- | --- | --- |
| Naam: Sidney Prins | | |
| Omschrijving | tijd | Datum |
| Vaste contacturen | 9 uur | 21-9-2015 |
| Skype gesprek en security vragen behandelen en opzet applicatie | 4 uur | 22-9-2015 |
| Inlezen MPOTR  <https://github.com/DrWhax/mpOTR> | 3 uur | 24-9-2015 |
| Inlezen MPOTR  <https://github.com/DrWhax/mpOTR> | 3 uur | 25-9-2015 |
| Skype gesprek en behandelen MPOTR | 4 uur | 27-9-2015 |

## Week 4 – Sidney Prins

|  |  |  |
| --- | --- | --- |
| Naam: Sidney Prins | | |
| Omschrijving | tijd | Datum |
| Vaste contacturen | 9 uur | 28-9-2015 |
| Skype call en werken aan chatapplicatie | 2,5 uur | 29-9-2015 |
| Skype call en werken aan chatapplicatie | 2.5 uur | 30-9-2015 |
| Skype call en werken aan chatapplicatie | 2.5 uur | 1-10-2015 |
| Skype call en werken aan chatapplicatie | 2.5 uur | 2-10-2015 |
| Skype call en chatapplicatie | 4 uur | 4-10-2015 |

## Week 4 – S. van Staden

|  |  |  |
| --- | --- | --- |
| Naam: S. van Staden | | |
| Omschrijving | tijd | Datum |
| Vaste contacturen – Netframework 4.5.2 geinstalleerd voor websocket voor Windows server 2008 | 9 uur | 28-9-2015 |
| TLS support ingesteld/gemaakt voor websocket update naar 1.2  <https://en.wikipedia.org/wiki/Galois/Counter_Mode>  Geen AES GMC mogelijk op windows server 2008 gebruik nu CBC | 4 uur | 29-9-2015 |
| Skype call | 2 uur | 30-9-2015 |
| OTRLIB gedeeltelijk geïmplementeerd en skype call | 4 uur | 1-10-2015 |
| Window forms and websocket server aangepast en skype gesprek | 4 uur | 2-10-2015 |
| Maak een exe incl dll files  <http://www.microsoft.com/en-us/download/details.aspx?id=17630>  [http://installforge.net/download/#](http://installforge.net/download/)  NETSH ipsec protocols om windows server 2008 beter te beveiligen  <https://technet.microsoft.com/en-us/library/cc725926%28v=ws.10%29.aspx> | 4 uur | 3-10-2015 |
| Chat synchronisatie en errors in OTR onderzocht en skype call | 2 uur | 4-10-2015 |

## Week 5 – S. van Staden

|  |  |  |
| --- | --- | --- |
| Naam: S. van Staden | | |
| Omschrijving | tijd | Datum |
| Vaste contacturen – Notification gemaakt in app | 9 uur | 5-10-2015 |
| Notify verder uitgewerkt code opgeruimd en popup processing  <https://msdn.microsoft.com/en-us/library/system.windows.forms.notifyicon(v=vs.110).aspx>  <https://msdn.microsoft.com/en-us/library/system.windows.forms.notifyicon.showballoontip(v=vs.110).aspx>  SMP protocol geimplemteerd  <https://en.wikipedia.org/wiki/Socialist_millionaire> | 4 uur | 6-10-2015 |
| Skype call | 2 uur | 7-10-2015 |
| Closed session, messagebox, reset button en layout | 3 uur | 8-10-2015 |
| Layout applicatie | 3 uur | 9-10-2015 |
| Skype gesprek oberleg multicahtroom | 2 uur | 10-10-2015 |
| Testen websocket server multichat skype call | 5 uur | 11-10-2015 |

## Week 5 – Sidney Prins

|  |  |  |
| --- | --- | --- |
| Naam: Sidney Prins | | |
| Omschrijving | tijd | Datum |
| Vaste contacturen | 9 uur | 5-10-2015 |
| Skype call en doorwerken erna | 4 uur | 7-10-2015 |
| Chatapplicatie, fouten ovangen | 4 uur | 8-10-2015 |
| Skype call en verder aan mpOTR gewerkt | 5 uur | 10-10-2015 |
| Connectie tussen 2 applicaties mpOTR opzetten skype call | 5 uur | 11-10-2015 |

## Week 6 – S. van Staden

|  |  |  |
| --- | --- | --- |
| Naam: S. van Staden | | |
| Omschrijving | tijd | Datum |
| Vaste contacturen – Mpotr | 9 uur | 12-10-2015 |
| mpotr | 4 uur | 13-10-2015 |
| Skype call | 2 uur | 14-10-2015 |
| Skype call en programming testing | 5 uur | 18-10-2015 |
|  |  |  |
|  |  |  |
|  |  |  |

## Week 6 – Sidney Prins

|  |  |  |
| --- | --- | --- |
| Naam: Sidney Prins | | |
| Omschrijving | tijd | Datum |
| Vaste contacturen – Mpotr | 9 uur | 12-10-2015 |
| Skype call | 2 uur | 14-10-2015 |
| MPOTR verder werken | 4 | 17-10-2015 |
| Skype call en programming testing | 5 uur | 18-10-2015 |

## Week 7 – S. van Staden

|  |  |  |
| --- | --- | --- |
| Naam: S. van Staden | | |
| Omschrijving | tijd | Datum |
| Programming | 6 uur | 19-10-2015 |
| SMP meerdere gebruikers | 4 uur | 20-10-2015 |
| Skype Call | 4 uur | 21-10-2015 |
| save button en chatroom | 1 uur | 22-10-2015 |
| Encrypt decrypt  Installeren power tools f# for refactoring  <https://visualstudiogallery.msdn.microsoft.com/136b942e-9f2c-4c0b-8bac-86d774189cff> | 2 uur | 23-10-2015 |
| Skype call | 2 uur | 24-10-2015 |
| Login account en history encrypt decrypt | 2 uur | 25-10-2015 |

## Week 7 – Sidney Prins

|  |  |  |
| --- | --- | --- |
| Naam: Sidney Prins | | |
| Omschrijving | tijd | Datum |
| Verder werken aan MPOTR en lay-out van formulier anapassen | 7 uur | 19-10-2015 |
| Skype call | 4 uur | 21-10-2015 |
| AES Encrypt/decrypt | 2 uur | 22-10-2015 |

## Week 8 – S. van Staden

|  |  |  |
| --- | --- | --- |
| Naam: S. van Staden | | |
| Omschrijving | tijd | Datum |
| Programming DSA fingerprint in history | 12 uur | 26-10-2015 |
| Programming DSA, 3 verschillende chattypes en skype call | 4 uur | 27-10-2015 |
| Programming chattypes Sha, password | 2 uur | 28-10-2015 |
| Skype call, documentatie | 4 uur | 29-10-2015 |
| IV, Salt, RNGCryptoServiceProvider, refactor en skype call | 8 uur | 01-11-2015 |