**Vragen**

1. MPOTR
2. welke cryptografische encryptie willen we implementeren
3. welke protocollen (OTR)
4. Schema maken van applicatie UML Model

Antwoorden

**MPOTR**

<https://github.com/DrWhax/mpOTR>

Idee om een chatroom op te zetten met meer dan 2 personen. OTR is een protocol gemaakt tussen 2 personen, om een betrouwbare verbinding op te zetten voor meer dan 2 personen.

**Confidentiality**

Een gesprek tussen personen moet prive blijven en niet inzichtbaar voor andere gebruikers.

**Entity authenication**

Authenicatie om ervoor te zorgen dat de gebruikers ook echt de gebruiker zijn. In mpOTR worden eerst alle mensen 1 op 1 geautheniceerd, daarna stuurt iedereen wie ze verwachten die meedoen aan het gesprek. Als iemand dan mee wilt doen, moeten alle gebruikers deze gebruiker accepteren.

**Origin authenication**

Het moet mogelijk zijn voor Alice om te weten of Bob of Charlie het heeft gestuurd en van welke chatroom het komt. Verder moet Alice, Bob kunnen overtuigen dat Charlie een bericht heeft verstuurd, maar Dave, die niet meedoet, moet dat niet kunnen weten, ook al zegt Alice dat.

**Forward secrecy**

Keys worden verwijderd wanneer ze zijn gebruikt om te encrypten/decrypten, verder is het idee om elk bericht met een ander key te encrypten, om te voorkomen als de key word gestolen, maar 1 bericht kan worden ontsleuteld.

**Deniability**

Het moet mogelijk zijn voor Alice om te zeggen dat ze nooit berichten heeft verstuurd, maar tegelijkertijd moeten Bob en Charlie wel weten dat ze echt van Alice komen.

**Repudiation**

Geen fysiek bewijs dat Alice iets heeft gezegd, maar moet wel zo worden gemaakt dat Alice weet dat Charlie iets in chatroom 1 heeft gezegd, maar niemand anders zou dit dan mogen weten.

**Forgeability**

Moet mogelijk zijn makkelijk om een gesprek te ‘maken’ in nepheid, zodat het makkelijk is om te zeggen dat het gesprek nep is.

**Malleability**

Makkelijk om message 1 van transcript 1 om te switchen naar message 2 van transscript 2, ter bewijs dat het bewijs is die zomaar is gemaakt.

**Anonymity and pseudonymity**

Anonimiteit behouden

**Welke cryptografische encryptie willen we implementeren**

<https://en.wikipedia.org/wiki/PBKDF2>

De gebruikte cryptografische encrypties die zich in OTR bevinden:

* AES symmetrische key 128 bits
* Diffie hellman key exchange 1635 bits group size
* SHA-1 hash

**Welke protocollen (OTR, openSSL, textsecure)**

OTR over socket server

**Schema maken van applicatie UML Model**

We gaan Windows applicatie maken die communiceert via een websocket. De websocket draait op F#.

De bedoeling is om de OTRLib te gebruiken van C#. Deze om te zetten naar F# Wanneer dit te veel problemen op levert. Dan gaan we proberen de windows applicatie te maken in C# en de socket in F#

<http://www.codeproject.com/Articles/644318/Off-The-Record-OTR-Security-Protocol>

Could have : MPOTR

