## Attackmetoder

MITMEtt farligt scenario är om data som skickas från klient till server kan stoppas på vägen av en illvillig part (kallad man in the middle, MITM) och använder denna information för att ”ta över” uppkopplingen mot servern. Förutsatt att detta lyckas styr MITM all kommunikation mellan server och klient. Han får således tillgång till all sekretessbelagd information som skickas och har även möjlighet att utföra egna handlingar i klientens namn.   
Vårt system avhjälper detta genom att klient/server att först autentiserar sig mot varandra med hjälp av certifikat signerade av en TTP. Med hjälp av certifikaten i respektive truststore blir aldrig MITM ett problem då denne inte kan mer än vidarebefordra dessa meddelanden.

När klienten påbörjar uppkopplingen mot servern (skickar ”client hello” som beskrivet i första delen) kan en MITM genskjuta klientens paket, modifiera det och därmed se till att serverns paket når honom först. Emellertid har han inte tillgång till klientens privata nyckel och kan därför inte skapa en egen session mot servern. Detta innebär också att han inte heller har möjlighet att få tag i den symmetriska nyckeln som krypterar överföringen av patientjournalerna.

Med andra ord, MITM kan inte heller utge sig för att vara någon av parterna eftersom han saknar de privata nycklarna som krävs för autentiseringen. Detta innebär också att när överförandet av den känsliga informationen börjar har MITM ingen möjlighet att ta del av den, även om han får tag i alla paket.

Utöver detta säkerställer MAC att de mottagna paketen är detsamma som de avsända. Alla försök att sabotera dem längs vägen kommer därmed noteras.

Systemet kan därför anses vara väldigt motståndskraftigt mot MITM-attacker så länge de privata nycklarna förblir okända för alla andra utom just den tilltänka användaren. Tilläggas kan dock att en MITM kan utföra en DOS-attack på grund av möjligheten att man strypa paketflödet i en av riktningarna.

Spoofing  
Systemet är känsligt för spoofing-attacker, i och med att alla keystores integritet är vital för att stänga ute obehöriga. En ”falsk” klient som samlar in information om en användares keystore skulle få tillgång till såväl nyckelpar som certifikat. Detta medför att den specifika användarens inloggning skulle vara röjd och samtliga journaler denne användare har tillgång till utsatta för risk. Detta kan motverkas genom att utbilda användarna i vad de bör kontrollera för att verifiera klientens äkthet, innan de börjar använda klienten.

I och med att det är troligt att någon form av malware måste användas till att utföra spoofing-attacken kan man även vidta åtgärder på de fysiska maskinerna där klienten finns installerad. Att t.ex. begränsa nedladdnings-/installationsmöjligheterna på samtliga datorer där klienten finns installerad skulle kunna förhindra obehöriga från att få tillgång till journaldatabasen. Detta kan dessvärre vara svårt att implementera eftersom det kan finnas verksamhet som gör att man inte kan genomföra den typen av restriktioner.

Avlyssnad kommunikation  
Det finns alltid en risk för att paket innanhållande journalinformation snappas upp av någon som avlyssnar kommunikationslinjen mellan klient och server. Eftersom dessa paket är krypterade med en svårforcerad symetrisk kryptering (AES med 128 bitars nyckel) är det rimligt att anta att man med dagens datorkraft inte kan forcera krypteringsskyddet inom rimlig tid. Detta innebär således att när uppkopplingen mot servern övergått till det krypterade läget kan användaren känna sig säker på att ingen kan snappa upp informationen längs vägen.

Det går däremot inte att skydda paket mot offline-attacker i all evighet, vilket innebär att någon med datorkraft och tid nog förr eller senare kommer åt journalinformationen oavsett hur svårforcerad krypteringsalgoritmen är. Även de starkaste symmetriska krypteringsalgoritmerna som inkluderas i mjukvaran, så som AES, kommer med stor säkerhet gå att forcera i framtiden. Detta eftersom beräkningskapaciteten för den här typen av operationer ökar i samband med att ny datorteknik görs tillgänglig.

Falska certifikat  
En icke-auktoriserad användare skulle kunna försöka skapa ett förfalskat certifikat och med hjälp av detta försöka få tillgång till materialet på servern. Emellertid skulle detta inte vara signerat av CA-certifikatet och skulle således uppdagas som falskt. Systemet utestänger alltså alla som inte fått ett certifikat utfärdat, vilket gör att man inte kan penetrera systemet utan ett giltigt certifikat.

Enda möjligheten att lyckas med ovan nämnda attack är om utfärdaren av klientcertifikaten skulle hackas och utfärda certifikat till obehöriga.

En annan variant hade varit att i klientens trust store placera ett falskt certifikat och med hjälp av detta försöka få klienten att koppla upp sig mot en falsk server. Detta kräver dock lösenordet till klientens truststore, vilket bör vara därmed mindre intressant att hacka (än lösenordet till klientens keystore) i och med att detta inte ger direkt tillgång till servern. Ett osannolikt men dock möjligt scenario hade varit att man genom att plantera falska ”Trusted CertEntries” skulle kunna få klienter att koppla upp sig mot en falsk server och få ut felaktig journalinformation.

Falska certifikat kan dock användas som en del i en DOS-attack, vilket behandlas nedan.

Lösenordspolicy  
En strikt lösenordspolicy är nödvändig för att kunna undgå vanliga typer av attacker för att forcera lösenord. Lösenordet bör vara minst 12 tecken långt, innehålla varierande teckentyper och inte bestå av ord. En sådan policy gör det förvisso svårare för användarna att minnas sina lösenord men har å andra sidan säkrat systemet mot Brute force och Dictionary-attacker.

Vårt system loggar antalet felaktiga för att skydda enskilda keystores och kan göra systemadministratörer varse om att försök görs att hacka en specifik användare. Skyddet för keystores bygger utöver detta på användaren väljer ett starkt lösenord och på att datorer som har klienten installerad förblir fria från malware. Med restriktioner i vad som får finnas laddas ned/installeras på berörda datorer kan man minska sannolikheten att en angripare lyckas installera program designade för att utföra ovan nämnda attacker.

Eftersom lösenordet inte sparas i vare sig klartext eller hashad version, utan enbart är nyckeln i algoritmen som låser upp en specifik keystore, finns det ingen risk för attacker som innefattar dumpning av en lösenordsfil. Regnbågstabeller och memory-tradeoff-attacker kan därför inte användas för att knäcka lösenordet.   
  
Mänskliga faktorer  
Innan systemet tas i bruk måste samtliga användare informeras om vikten av att inte lämna oavslutade sessioner igång då detta kan leda till att obehöriga får tag i/ändrar journalinformation.

Användarna bör instrueras att välja ett starkt lösenord (se lösenordspolicy) och byta det vid misstanke om att någon annan fått kännedom om det eller på uppmaning från en administratör. Lösenordsbyte å regelbunden basis är däremot inte en policy som kommer att genomdrivas. Att byta ett redan starkt lösenord försvårar maximalt en bruteforce-attack med en faktor 2 och uppmuntrar användarna till att välja lösenord som är lätta att minnas men svaga.

Användarna ska också uppmanas att aldrig ge ut lösenordet till någon och att också rapportera alla typer av försök att fiska lösenord till systemadministratörer.  
  
Utöver detta måste det finnas restriktioner mot att på spara och hantera journalinformation utanför klienten, eftersom okrypterade lokala kopior av informationen utgör en säkerhetsrisk.

DOS-attackDet är svårt att skydda sitt system mot attacker som är designade för att överbelasta ett och på så vis utestänga legitima användare. Icke desto mindre kan man försvåra processen genom att kräva att användare uppfyller vissa krav för att tillåtas koppla upp sig.

I detta fall görs detta genom att klienten kräver att användaren har en keystore som denne kan låsa upp med hjälp av användarnamn och lösenord. Så även under förutsättning att en eller flera datorer med klienten installerade skulle bli en del av ett botnet skulle systemet fortfarande bara kunna angripas av användare med en keystore.

Man behöver däremot inte ha ett äkta certifikat för att iscensätta en DOS-attack. Detta möjliggör ett angreppsscenario liknande en slowloris-attack, där en eller flera datorer med klienten installerad skapar keystores med falska certifikat. Sedan startar dessa mängder av uppkopplingar och låter servern vänta på att användaren ska skicka sitt certifikat. Detta gör att servern fyller upp sin kvot för maximalt antal användare som kan vara uppkopplade samtidigt och hindrar därmed användare från att ansluta till servern.

Genom att enbart tillåta att administratörer hanterar skapandet av nya användare och keystores kan dock en sådan attack försvåras avsevärt.

### Avläsning av knapptryckningar / Keystroke logging

Som tidigare nämnt är systemet beroende av att lösenordet till varje klients keystore. Att plantera en keystroke logger på en dator där klienten finns kan få tag i såväl lösenord som användarnamn och ID.

Eftersom en keystroke logger kan underminera säkerheten i hela systemet är det av yttersta vikt att den typen av mjukvara/hårdvara inte finns installerad på datorerna.

Elektromagnetisk avläsning av knapptryckningar är i fallet ett orimligt scenario eftersom datorerna befinner sig inne på ett sjukhus där mängder av datorer används simultant. Att urskilja en specifik dators knapptryckningar för att kunna få ut ett lösenord är under sådana omständigheter inte möjligt med dagens teknik.

### Sammanfattning

Det finns i synnerhet två skeden där systemet är utsatt för risk, nämligen när användaren skriver in sitt alias/lösenord och när den faktiska journalinformationen överförs. I den förstnämnda ligger stort ansvar på användaren och på maskinen där klienten är installerad medan systemet själv försvarar mot det sistnämnda.

Journalsystemet skyddar mycket väl mot alla typer av MIT M och Eavesdropping-attacker. All känslig information skickas krypterad med 128 bitars AES-kryptering och den hemliga nyckeln aldrig skickas mellan servern och klienten. Det senare görs genom att förhandla fram nyckeln till denna symmetriska kryptering med hjälp av Diffle-Huffmanns metod.

Systemet är dock känsligt för alla typer av lösenordsstöld som kan inträffa på lokal nivå. Här krävs en kombination av ett svårforcerat lösenord, säkra datorer och medvetenhet hos användarna för att upprätthålla hög säkerhet.