Network WarWare

(HS-IDA-EA-99-201)

Ola Andersson (a96olaan@ida.his.se**)**

Patrik Johansson (c96patjo@ida.his.se**)**

Institutionen för datavetenskap
Högskolan i Skövde, Box 408
S-54128 Skövde, SWEDEN

Examensarbete för programmet för ”Software Engineering” under vårterminen 1999.

Handledare: Torbjörn Andreasson Ericsson Microwave Systems

Network WarWare

Examensrapport inlämnad av Ola Andersson och Patrik Johansson till Högskolan i Skövde, för Teknisk Kandidatsexamen (B.Sc.) vid Institutionen för Datavetenskap.

991014

Härmed intygas att allt material i denna rapport, vilket inte är mitt eget, har blivit tydligt identifierat och att inget material är inkluderat som tidigare använts för erhållande av annan examen.

Signerat: _____

Signerat: _____

Network WarWare

Ola Andersson (a96olaan@ida.his.se**)**

Patrik Johansson (c96patjo@ida.his.se**)**

Sammanfattning

Examensarbetet syftar till att kartlägga olika metoder för att attackera ett datorsystem uppbyggt kring kommersiella produkter över ett nätverk. Arbetets inriktning har varit att göra en så komplett kartläggning som möjligt med den tid och de resurser som funnits tillgängliga. Arbetet är gjort på Ericsson Microwave Systems AB.

Nyckelord: Datasäkerhet, Datakommunikation, Kartläggning, Metoder, Intrång, Sabotage.

Innehållsförteckning

1 Inledning

Detta examensarbete är utfört av Ola Andersson och Patrik Johansson under våren 1999 som en avslutning på utbildningen ”Programmet för Software Engineering” vid Högskolan i Skövde. Efter genomförd utbildning blir studenten utbildad programvaruingenjör med möjligheter att jobba med utveckling och underhåll av programvara. Utbildningen omfattar 120 poäng och resulterar i en kandidatexamen. Syftet med examensarbetet är att låta studenten komma i kontakt med näringslivet och där praktiskt tillämpa de kunskaper som inhämtats under utbildningstiden.

Detta arbete är gjort åt Ericsson Microwave Systems (EMW) som är ett företag inom Ericsson koncernen. EMW sysslar främst med olika typer av mikrovågs-kommunikation för olika tillämpningar både inom den civila och den militära sektorn.

Arbetet handlar om datasäkerhet och EMW anser att detta är en viktig aspekt inför utveckling av framtidens informationssystem. Examensarbetets inriktning är delvis en komplettering av de kunskaper som vi fått i och med utbildningen men likväl ett nytt område för oss då vi tidigare inte hade några särskilda kunskaper inom datasäkerhet.

2 Problembeskrivning

Vilka problem finns?

De operativsystem, programvaror, protokoll, topologier osv. som idag säljs kommersiellt (COTS[1] produkter) är inte designade med vikten på säkerhet utan snarare på funktionalitet och effektivitet. Säkerheten har inte glömts av, men har sällan kommit i första hand.

För Ericsson är detta intressant därför att framtida ledningssystem i hög grad kommer att vara baserade på COTS produkter. Intrångssäkerhet, sabotage, etc. är mycket viktiga områden som måste behärskas vid utveckling av dessa system och detta examensarbete kan betraktas som ett led i dessa studier. Om EMW i framtiden skall kunna bygga system som är säkra mot attacker måste de känna till vilka möjliga attackformer som kan existerar.

Vid framtida programvaruutveckling på EMW kan vårt arbete användas för att utveckla system som tar hänsyn till och är skyddade mot de kartlagda attackformer som vi funnit.

Målet med arbetet

Examensarbetet syftar till att kartlägga och ge en förståelse för de tillvägagångssätt som idag existerar för att attackera ett datorsystem remote[2] byggt kring COTS produkter. Examensarbetet ska kunna ligga till grund för fortsatt arbete inom området datasäkerhet och fungera som underlag vid framtida utveckling av nya system på företaget.

Förklaring

Examensarbetet är en kartläggning och avser inte att lösa ett konkret problem. Därför har vi inte haft några fasta mål såsom ett visst antal sidor stor rapport eller t.ex. ett färdigt program med viss funktionalitet. Målet har varit att göra en så komplett kartläggning som möjligt med avseende på tid och resurser som finns till förfogande.

---

[1] ”Commercial-Of-The-Shelf” är produkter som vem som helst kan gå in i en affär och handla, t.ex. Windows NT, en IBM dator etc.

[2] Ett engelskt ord som inte har någon svensk motsvarighet men som ungefär betyder "fjärr". Exempelvis så går det att istället för att säga att en dator fjärradministreras så går det att säga att datorn administreras remote.

3. Problemställning för examensarbetet

Den huvudsakliga frågan som skulle besvaras var: Vilka generella tillvägagångsätt finns det för att göra en attack och hur kan de klassificeras? En attack definierar vi som: att göra ett intrång eller försök till intrång, eller att göra ett angrepp mot ett datorsystems tillgänglighet.

Examensarbetet skall resultera i en rapport över funna tillvägagångssätt och metoder för att göra en attack mot ett datorsystem. Vårt mål med denna rapport var att belysa alla de generella metoder som faktiskt existerar och ge en förståelse för dem. Det var även tänkt att vi skulle utveckla ett program för att testa ett datorsystems säkerhet med avseende på de metoder som vi funnit.

Eftersom vi inte kunde titta på alla COTS produkter valde vi att titta närmare på två system: Sun Solaris samt Windows NT. Då nya datorer och tjänster utvecklas för varje dag, valde vi att studera mer generella tekniker/metoder än specifika fall. Förhoppningsvis kan vi på detta sätt hålla innehållet i rapporten aktuellt längre.

Vi har valt att låta arbetet reflektera teknikerna/metoderna ur en attackerares synvinkel. På detta sättet skiljer sig detta arbete från annan litteraturer inom området. Vi valde denna inriktning på arbetet på grund av att vi troligtvis kunde täcka in fler säkerhetsaspekter. Vi ansåg också att för att kunna försvara ett datorsystem så är det nödvändigt att veta de möjligheter som finns för en anfallare.

Eftersom vi var två som skulle göra examensarbetet tillsammans var vi tvungna att dela upp arbetet i formella ansvarsområden. Från början gjorde vi en väldigt grov indelning enligt följande. Ola skulle ta formellt ansvar för metoder som rörde sabotage och Patrik för metoder rörande spionage.

4. Lösningsmetod

Tillsammans med handledare kom vi fram till en tidsplanering och att vi skulle dela in arbetet i följande faser.

1) Planering
2) Instuderingsfas
3) Rapportskrivande fas
4) Exprimentering och utveckling av program.

Planering

Under denna fas tänkte vi att vi skulle planera den tid vi förfogade över samt fundera ut vilka resurser som arbetet kunde komma att kräva. Resultatet skulle bli en så kallad uppdragsspecifikation som EMW krävde.

Instuderingsfas

Under instuderingsfasen tänkte vi inhämta så mycket information som möjligt från Internet för att erhålla ”färsk” information. Utvecklingen är snabb inom området och därför blir ofta tryckta böcker snabbt inaktuella vilket innebär att de senaste attackformerna inte finns med.

En annan tanke var att vi kunde få en bredare och mer komplett bild av området om vi hämtade information från Internet då vi där kunde ta del av en mängd källor istället för ett fåtal. Vi kunde både få hackerns synsätt och säkerhetsexperters synsätt. Om vi hade valt att använda oss av tryckt litteratur är risken stor att vi inte fått ta del av hackerns synsätt. Eftersom hackers och säkerhetsexperter använder sig av Internet dagligen för dela sin kunskap och information antog vi att det var där vi skulle finna mest intressant material.

Rapportskrivningsfas

Denna fas planerade vi att låta överlappa med instuderingsfasen då vi ansåg att det skulle underlätta rapportskrivandet. Vi skulle då inte bli tvungna att gå tillbaka och repetera upp våra kunskaper då det var dags att skriva rapporten.

Experimentering

För att försäkra oss om att de funna teknikerna fungerade såsom det var avsett skulle vi få testdatorer där vi kunde testa teknikerna. Vi skulle även kunna utveckla det program som vi avsåg att göra på dessa datorer. En svårighet med detta var att vi inte kunde testa metoder i ett större nätverk (med t.ex. brandväggar och routrar) då Ericsson av förståeliga skäl inte ville tillåta att vi anslöt testdatorerna till deras nätverk.

Programvaruutveckling

För att mer praktiskt tillämpa de kunskaper som vi fått under vår studietid planerade vi att göra ett program. Detta program skulle kunna ses som en grund till ett mer fullständigt program som senare skulle kunna användas för att testa de olika attackformer som vi beskrivit i vår rapport. Programmet skulle kunna byggas ut då vi

ansåg att vi bara kunde implementera ett fåtal tekniker och tillvägagångsätt med avseende på den tid som fanns till förfogande.

Verifiering

Då arbetets syfte var att göra en kartläggning och inte resultera i ett program med viss funktionalitet för att lösa ett visst problem kunde vi inte komma på någon verifieringsteknik för arbetet. Vi skulle inte ha något konkret att verifiera mot. Det vi skulle kunna göra var att diskutera med handledaren om huruvida innehållet i rapporten var det önskade.

5. Genomförande

Ansvarsområden

Det visade sig ganska snart att det inte gick att dra tydliga gränser mellan vad som var metoder för spioneri och för sabotage. Därför delade vi efterhand upp arbetet enligt nedan. Det bör nämnas att vi jobbade nära varandra och hela tiden bollade de problem och idéer som uppstod.

Uppdelningen blev som följer. Ola har ansvarat för: scanners, sniffers, IP spoofing, IP hijacking och lösenordsknäckning. Patrik har ansvaret för: virus, trojaner, dålig konfiguration, ”denial of service” och ”buggar och exploits”.

Planering

Denna fas fortskred som vi hade tänkt. Det var dock problem med att uppskatta hur lång tid olika moment skulle ta, så vi gjorde en relativt grov tidsskiss. Denna tidsskiss visades sig stämma relativt bra då den höll hela arbetet ut.

Instuderingsfas

Instuderingsfasen gick som vi tänkt och vi fann det material som vi sökte. Rent allmänt fungerade Internet som en bra informationskälla. Vi blev till och med överaskade över att det fanns så många sidor som tillhandahöll information om säkerhetsrelaterade ämnen.

Rapportskrivande fas

Rapporten som vi skrev missbedömde vi från början. Vi trodde att arbete skulle resultera i en 30-40 sidor tjock rapport. Storleken ändrades kontinuerligt tills att det stod klart att det skulle bli en rapport på ungefär 90 sidor istället. Detta innebar i praktiken att dokumentet tog längre tid att skriva än vad vi uppskattat från början. Vi har under arbetes gång inte känt att vi gått in i någon vägg utan arbetet har flutit på bra. Eftersom vi skulle skapa en rapport till Ericsson, skrev vi olika kapitel utifrån vår uppdelning av arbetet. Dessa kapitel satte vi senare samman till en rapport. Därefter gick vi igenom rapporten för att se till att våra kapitel passade bra ihop varvid vi tog bort redundant information. Precis som vi förutsåg började vi skriva rapporten på ett tidigt stadium, vilket vi tror var lyckat. De kapitel som vi skrev till en början fick senare oftast omarbetas då de inte höll samma klass som de senare.

Experimentering

På ett tidigt stadium av instuderingsfasen insåg vi att tiden inte skulle räcka till för att både göra ett program och en utförlig rapport. Förutom tidsbristen fanns det även andra anledningar för att vi inte valde skapa ett program. Det skulle t.ex. bli svårt att göra ett testverktyg som fungerade bra under både UNIX och Windows NT.

För experimentering fick vi ett litet laborationsnät där vi kunde testa olika program. Testningen skedde som vi tänkt oss om än inte lika djupgående som vi till en början planerat. Tidsplanen ändrades inte på grund av förändringen.

6. Resultat

Vi har gjort en omfattande kartläggning av olika tekniker. Rapporten går inte alltid så djupt in men den täcker alla tillvägagångssätt som vi funnit beskrivna på Internet. Rapporten bör ge läsaren en bra överblick av de olika nätverksattackformerna som existerar och hur de kan utföras. Vi tyckte att det var synd att vi inte hittade mer verkliga exempel som vi kunde skriva om i rapporten. Detta kunde göra rapporten mer intressant. Läsaren skulle troligtvis på ett lättare sätt förstå hur en attack kan gå till och vilka skador som attacker kan göra.

Verifieringen skedde genom att vi efter halva tiden höll en halvtidspresentation och att vi höll en slutpresentation på Ericsson då vi ansåg att arbetet var klart. Genom dessa presentationer kunde vi få feedback på vårt arbete och använda denna feedback för att styra arbetet i den riktning som Ericsson ville. Under dessa tillfällen har vi fått positiv feedback. Några direkta omarbetningar av arbetet har inte skett, utan arbetet har utvecklats så som det var tänkt. Vi upplevde att vi fick styra arbetets inriktning till en stor del själva. Troligtvis därför att ingen från början visste vad vår kartläggning skulle resultera i.

7. Kritisk granskning

Vi har upplevt det jobbigt att det fanns krav från skolan att vi inte kunde göra ett gemensamt arbete utan uppdelningar. Vi tror att om vi fått jobba mera som ett team så hade vi kunnat åstadkomma ett bättre resultat. Vi var tvungna att nästan omedelbart bestämma vem som skulle ansvara för vad inom arbetet. I början av arbetet var det svårt att bedöma hur stora dessa områden skulle bli. Vi tror att det hade varit bättre om dessa ansvarsområden växt fram i takt med arbetet istället.

Det kändes positivt att Ericsson gav oss såpass fria tyglar som vi fick för att bestämma upplägg och innehåll av examensarbetet. Om vi inte fått så fria tyglar hade detta troligtvis resulterat i att arbetet blivit striktare. Resultatet av detta hade troligtvis varit att rapporten inte blivit lika omfattande.

Även om tidsplaneringen höll så kände vi oss ändå stressade mot slutet. Det borde vi ha kunnat förhindra genom att ha varit lite mer framåtseende. Dock tror vi att det är vanligt förekommande med stress innan deadlines. Det kändes som att vi kunde putsat på rapporten i evigheter utan att bli helt nöjda.

Allt eftersom arbetet fortskridit har vi blivit bättre på att formulera oss och på att skriva korrekta texter. Vi har blivit bättre på att få fram det som skall sägas på ett mer fullständigt och korrekt sätt. Vi har lärt oss massor i området datasäkerhet och inom datakommunikation. Eftersom arbetet bedrevs på Ericsson, där vi jobbade som vilka Ericsson-anställda som helst, med eget kontor osv., lärde vi oss hur det kan vara att arbeta på ett multinationellt företag med avseende på rutiner och hur personer med vår utbildning jobbar. Vi tycker att det har varit bra att vi jobbat i Ericssons lokaler då vi lätt kunnat fråga handledare om oklarheter samtidigt som vi tror att vi fått mer gjort än om vi suttit hemma eller på skolan och jobbat.

8. Fortsatt arbete

Eftersom området datasäkerhet är mycket omfattande finns det naturligtvis avsevärt mycket mer arbete att utföra än det vi har gjort. Vi skulle gärna vilja se att framtida arbeten gräver djupare inom de områden som vi hittat. Det händer såpass mycket inom området datasäkerhet att det vore bra om detta arbete hela tiden kompletteras med nya tekniker och metoder som dyker upp. På så sätt kan arbetet hållas aktuellt längre.

En annan fundering som kommit upp under arbetet är varför inte Högskolan i Skövde har någon kurs inom datasäkerhet. Detta tycker vi hade varit bra då det på skolan utbildas människor som kommer att utveckla framtida datorsystem och de vore bra om dessa människor hade kunskap inom datasäkerhet.

Vi har fått förfrågan av handledaren om vi vill skriva en artikel för en populärvetenskaplig tidskrift. Artikeln skulle sammanfatta de tillvägagångsätt som vi kartlagt då vi tror att många tycker att vårt arbete kan vara intressant.