Dolda Kanaler

En översikt

KRISTOFFER LUNDHOLM, HENRIK KARLZÉN, JACOB LÖFVENBERG

FOI
Totalförsvarets forskningsinstitut
Informationssystem
Box 1165
581 11 Linköping

Tel: 013-37 80 00
Fax: 013-37 81 00

www.foi.se

FOI-R–3037–SE
ISSN 1650-1942

Användarrapport
September 2010

Informationssystem

Kristoffer Lundholm, Henrik Karlzén, Jacob Löfvenberg

Dolda Kanaler

En översikt

Titel	Dolda Kanaler En översikt
Title	Covert Channels An overview
Rapportnr / Report No.	FOI-R–3037–SE
Rapporttyp	Användarrapport
Report Type	User report
Månad / Month	September / September
Utgivningsår / Year	2010
Antal sidor / Pages	19
ISSN	
Kund / Customer	FM
Projektnr / Project No.	E53195
Godkänd av / Approved by	

FOI, Totalförsvarets Forskningsinstitut
Avdelningen för Informationssystem
Box 1165
581 11 LINKÖPING

FOI, Swedish Defence Research Agency
P.O. Box 1165
SE-581 11 LINKÖPING

Sammanfattning

Dolda kanaler är ett sätt att obemärkt kommunicera information på ett sätt som bryter mot ett systems säkerhetspolicy. Det finns många sätt att implementera dolda kanaler presenterade i litteraturen, varav några finns beskrivna i denna rapport.

Forskningen kring dolda kanaler i informationssystem drog igång i början på 70-talet. Vid den tiden handlade forskningen om hur information kunde läcka mellan säkerhetsnivåer då användare med olika klassning använde samma stordator. Utvecklingen sedan dess har dragit sig bort från kanaler i stordatorer till att numera huvudsakligen handla om dold informationsöverföring i datornät.

Forskningsfältet för dolda kanaler är i dagsläget relativt spretigt och en stor del av de artiklar som publiceras handlar om en ny kanal som har skapats eller hur en tidigare presenterad kanal kan detekteras eller eliminieras. Det finns dock ett mindre antal artiklar som handlar om mer generella metoder för att upptäcka, eller förhindra användningen av, dolda kanaler.

På grund av att dolda kanaler kan användas för att läcka information ur system med olika grad av känslig information är kunskap inom området viktig för Försvarsmakten. Detta gäller speciellt nu när fler och fler system kopplas samman, eftersom sådan sammankoppling kräver att endast information som ska kommuniceras faktiskt överförs. Viktiga forskningsproblem ur Försvarsmaktens synvinkel är framför allt tekniker och metoder för att förhindra och detektera dolda kanaler.

Nyckelord: dold kanal, informationssäkerhet

Abstract

Covert channels can be used to send information in a way that is hard to detect, and that violates a system's security policy. Some, of the many ways described in the literature of how to implement a covert channel are presented in this report.

The research on covert channels started in the early seventies. At this time, the main issue for researchers was leakage of information between security levels when users with different security clearance accessed the same mainframe simultaneously. The subject has since then evolved from studying covert channels in mainframes towards studying covert channels in computer networks.

The covert channel research field is rather diverse Most of the recently published papers concern the discovery of a new channel or the possible detection or removal of a previously published channel. However, there are a small number of papers covering more general methods for covert channel identification or mitigation.

Due to the property of enabling leakage of information from systems with sensitive information, knowledge regarding covert channels is necessary for the Swedish Armed Forces. This is especially true when systems are increasingly interconnected—as they often are these days—since such interconnections often require that only information meant to be communicated is actually transmitted.Thus, for the Swedish Armed Forces, important research problems are mainly techniques and methods for preventing and detecting covert channels.

Keywords: covert channel, information security

Innehållsförteckning

1 Inledning

Denna rapport är ett resultat av FoT-projektet Spaning och motmedel på informationsarenan. Rapporten beskriver området dolda kanaler och diskuterar dess relevans för Försvarsmakten (FM). Vidare diskuteras huruvida en förlängning av projektets inriktning mot studier av forskningsområdet dolda kanaler är möjlig eller önskvärd med bäring på nyttan för FM.

1.1 Bakgrund

Projektet Spaning och motmedel på informationsarenan omfattar en rad olika områden relaterade till attacker mot, och möjligt försvar av, informationssystem. Ett av dessa områden som i högsta grad är relevant för alla typer av organisationer som hanterar känslig data, och således även FM, är dolda kanaler, det vill säga metoder för att obemärkt kommunicera mellan datorsystem som inte tillåter detta.

1.2 Syfte

Syftet med rapporten är att ge läsare en överblick över vad som innefattas i begreppet dolda kanaler samt hur kunskap om dessa kan vara relevanta för FM:s verksamhet. Syftet delas upp i följande delområden:

- grundläggande förklaring
- beskrivning av forskningsfältet
- presentation av relevans för FM

2 Introduktion till dolda kanaler

Begreppet dolda kanaler motsvaras på engelska av begreppen ”covert channel” och ”hidden channel”. De två engelska begreppen kan ses som synonyma men det är oftast ”covert channel” som används i litteraturen. Detta kapitel innehåller en beskrivning av vad som historiskt ansågs vara problemet med dolda kanaler samt hur det ser ut i dagsläget.

2.1 Historisk bakgrund

Lampson introducerade begreppet ”covert channel” för hur information kan läcka mellan säkerhetsnivåer i en stordator via en kanal som inte är avsedd för informationsöverföring. Den definition som Lampson gav var: ”*Covert* channels, i.e. those not intended for information transfer at all, such as the service program’s effect on the system load.”

Definitionen ovan illustrerar väl den problematik som diskuterades i början av sjuttiotalet. De dolda kanaler som studerades var otillåten kommunikation mellan processer i stordatorer, där processerna kördes på olika säkerhetsnivåer. En modernare och mer omfattande definition av ”covert channel” kommer från ”light pink book” publicerad av National Computer Security Center. Definitionen är ganska teoretisk men kan beskrivas som att *all möjlig kommunikation mellan två entiteter i ett system ska anses ske via en dold kanal om kommunikationen är otillåten enligt systemets policy, samt att systemet är konstruerat för att förhindra otillåten komunikation*. Det är alltså, enligt dessa definitioner, bara meningsfullt att prata om dolda kanaler i system där systemet försöker se till att säkerhetspolicyn följs. Vi kallar detta för den strikta definitionen av en dold kanal, till skillnad från den utvidgade definitionen som beskrivs i nästa avsnitt.

2.2 Dolda kanaler idag

I dagens datorbaserade informationssystem, vilka ofta består av flera system sammankopplade i nät, har betydelsen av dolda kanaler vidgats till att innefatta:

> otillåten överföring av information på ett sätt som inte förhindras eller detekteras av befintliga övervakningssystem.

Vi kallar detta för den utvidgade definitionen av dolda kanaler. Skillnaden mot den strikta definitionen är att systemet inte *aktivt måste försöka* se till att policyn följs. Det är denna definition vi valt att huvudsakligen utgå från i denna rapport.

Det finns många exempel på dolda kanaler i nät och en mer ingående beskrivning av forskningen som den ser ut idag finns i kapitel 3. I detta avsnitt presenteras några nätbaserade exempel på dolda kanaler som senare kommer att användas i avsnitt 2.6 som beskriver motmedel.

Ett exempel på en dold kanal som kan användas i vanliga IP-nät är att skicka data i oanvända fält i IP- eller TCP-huvuden. Denna typ av kanal kan nå ganska hög kapacitet men är relativt enkel att detektera.

En mer svårdetekterad kanal kan skapas genom att skicka data i initieringsvärdet för en TCP-anslutning. Detta värde slumpas normalt fram men kan alltså bytas ut, helt eller delvis, mot delar av det meddelande som ska skickas dolt. För att skicka mer data än vad som ryms i ett fält, upprättas och avslutas så många anslutningar som behövs.

En dold kanal över ett nät kan även skapas genom att en sändare använder en tillåten dataström och i varje givet ögonblick väljer att antingen skicka data eller inte skicka data, och låter detta indikera etta eller nolla. Kapaciteten för den här typen av kanal är starkt beroende på fördröjningar i nätet, något som beskrivs närmare i nästa avsnitt. Det är värt att notera att den här typen av dold kanal kan användas för att skicka meddelanden till en tredje part som har möjlighet att se trafiken men inte nödvändigtvis läsa den. Ett exempel på detta är en entitet som kan se en krypterad anslutning men som inte kan läsa innehållet.

2.3 Typer av dolda kanaler

Alla dolda kanaler måste ha någon form av synkronisering mellan sändare och mottagare. Anledningen till detta är att mottagaren måste veta när det finns något att hämta och sändaren måste veta när mottagaren har läst av det nuvarande meddelandet så att det kan bytas ut mot nästa. Synkroniseringen kan ske antingen via lagrade variabler (likvärdiga med de variabler som överför data i lagringskanaler, se nedan) eller via en gemensam tidsreferens (systemklocka).

Trots att innebörden av begreppet dold kanal har ändrat sig över tiden är de begrepp som beskriver en dold kanals egenskaper giltiga oavsett vald definition. Traditionellt delas begreppet dolda kanaler in i dolda lagringskanaler och dolda tidskanaler, dock är det inte alltid lätt att avgöra vilken klass en viss kanal tillhör.

I en dold **lagringskanal** (eng. storage channel) sker kommunikation genom att den sändande entiteten skriver information (direkt eller indirekt) till ett lagringsställe och den läsande entiteten läser (direkt eller indirekt) från detta lagringsställe.

Ett exempel på en lagringskanal i operativsystemet UNIX utnyttjar det faktum att ett felmeddelande erhålls då en process försöker ta bort en mapp som inte är tom. Detta felmeddelande fås även om processen inte har rättigheter att se någon av filerna som ligger i mappen. För att utnyttja detta kan en process med högre rättigheter skapa och ta bort en nonsensfil i en förutbestämd, i övrigt tom mapp, skapad av processen med lägre rättigheter. Processen med lägre rättigheter kan sedan försöka ta bort mappen. Erhållandet eller frånvaron av felmeddelande används för att indikera etta eller nolla.

I en dold **tidskanal** (eng. timing channel) sker kommunikationen genom att en entitet med högre behörighet påverkar en gemensam resurs (exempelvis användning av CPU eller sändningstakt för IP-paket) på ett sådant sätt att en entitet med lägre behörighet kan observera detta och därmed avkoda den skickade datan.

Ett exempel på en tidskanal i IP-nät är att koda den data som ska skickas som variationer i tidsavstånd mellan angränsande paket i en legitim dataström. Denna kanal kräver att en legitim kanal kan upprättas till mottagaren. När denna sedan är upprättad skickas den dolda datan genom att göra en kort eller en längre paus mellan skickandet av två paket, vilket representerar en etta respektive en nolla.

2.4 Angränsande områden

Det finns ett antal områden som är besläktade med dolda kanaler, eller är specialfall som är tillräckligt säregna för att nämnas separat. Gemensamt för dessa är att det handlar om information som överförs på ett, för systemet, oavsiktligt sätt.

2.4.1 Steganografi

Steganografi handlar om olika sätt att gömma information i annan information så att det inte framgår att den finns där. Ett modernt exempel är att gömma information i digitala bilder genom att göra mycket små, för ögat osynliga, förändringar i bildinformationen

där olika typer av förändringar representerar olika datavärden. Motsvarande tekniker finns även för ljud- och videodata. Att den grundläggande idén är gammal visas av det historiska exemplet från 499 f.Kr. i antikens Grekland då Histiaeus lät raka håret av en slav, tatuera in ett meddelande, lät håret växa ut igen och skickade slaven till mottagaren av det gömda meddelandet.

Det är svårt att göra en tydlig gräns mellan dolda kanaler och steganografi. Begreppen är likartade och den största skillnaden är att de används i olika sammanhang. Steganografi handlar alltid om att meddelandeinformationen göms i annan, yttre information. Oftast är den yttre informationen multimediadata och gömmandet sker vid ett enskilt, avslutat tillfälle. Dolda kanaler kan, men behöver inte, handla om att meddelandeinformationen göms i annan, yttre information. Den yttre informationen som används för dolda kanaler är numera oftast nätverksprotokolldata och gömmandet sker fortlöpande under en kommunikationssession.

2.4.2 Sidokanaler

En sidokanal (eng: side channel) är en kanal som inte är planerad av systemdesignern och som oavsiktligt läcker känslig information. Begreppet används främst inom kryptovärlden som en beteckning på nyckelläckande svagheter i den fysiska implementationen av ett kryptosystem. Ett exempel på en sidokanalsattack är att det kan vara möjligt att knyta information om kryptonyckeln till variationer i strömförbrukning eller tidsåtgång hos en kryptoprocessor. I vissa scenarier är tillgång till denna information helt rimlig att anta, till exempel i fallet med kreditkort, kort till TV-mottagare och många andra tillämpningar.

2.4.3 Subliminala kanaler

Subliminala kanaler är ett specialfall av steganografi och dolda kanaler. Subliminala kanaler kommunicerar information inuti vissa kryptografiska protokoll [1], men inte som en del i den normala informationsströmmen. Istället utnyttjas att flera av dessa protokoll använder slumpinformation som en säkerhetsnödvändig del i protokollet. Eftersom det är slumpinformation utan några andra krav på sig går det att byta ut den på ett sätt så att annan information kan döljas utan att det stör funktionen hos det underliggande kryptografiska protokollet.

2.5 Dokumenterade exempel

Detta kapitel innehåller ett par exempel där dolda kanaler har använts samt ett exempel på ett system där mycket möda lades ner för att säkerställa att systemet inte innehöll några dolda kanaler.

[1] exemplen vi sett berör digitala signaturer

En verklig användning av en dold kanal beskriven av Schwartz, om än inte i något datorsystem, rör anbudssignalering. När amerikanska radio frekvenser skulle auktioneras ut använde budgivare slutsiffrorna i sina respektive bud för att kommunicera sin identitet till andra i den annars anonyma budgivningen. Detta för att kunna kringgå de stränga regler som implementerats och därmed få till uppgörelser bolag emellan.

Ett annat exempel på hur dolda kanaler använts rapporterades på hackerkonferensen BlackHat 2004. En grupp visade här att man hade dolt sin kommunikation i fältet för meddelande-ID i e-post. En variant av detta, rapporterat av Madsen, har användts av terrorister där de dolt meddelanden om planerade attentat i Västafrika i så kallade Nigeriabrev.

Ett välkänt exempel på ett verktyg för dolda kanaler är Loki, ett program för att tunnla data via ICMP, som presenterades 1996. Samma metod användes senare skarpt av bland andra Back Orifice 2000, en mycket populär trojan skapad av en ledande hackergrupp.

Ett system där mycket arbete lades ner för att se till att det inte innehöll några dolda kanaler var de sändare som på slutet av 1970-talet utvecklades för att USA skulle kunna visa för Sovjet att USA inte hade fler kärnvapenbestyckade robotar än vad som avtalats.

Bakgrunden till behovet av dessa sändare var att USA enligt avtalet fick ha maximalt 100 så kallade Minuteman-robotar. Då det bedömdes som möjligt för Sovjet att slå ut 100 silos i ett initalt angrepp bestämdes att de 100 robotarna skulle flyttas slumpmässigt mellan 1000 silos. Anledningen till detta var att det bedömdes som osannolikt att alla 1000 kunde förstöras och om det inte gick att veta var de 100 robotarna fanns, skulle några troligen kunna användas för en motattack. För att påvisa för Sovjet att det endast fanns 100 robotar, skulle sändare installeras i alla silos. Dessa skulle på begäran kunna skicka en bit information till Moskva med information om huruvida det fanns en robot i silon eller inte.

Problemet var att designa sändarna så att de kunde vidarebefodra om det fanns en robot i en silo eller inte samt ett unikt ID för varje sändare (detta ID matades in i sändaren då den var på plats och skulle vara hemligt), utan att någon ytterligare information kunde skickas, till exempel vilken silo det rörde sig om.

För att unikt identifiera en av 1000 silos krävs bara 10 bitar information. För att garantera både att informationen från sändarna var korrekt samt att ingen övrig information skickades, skulle den data som skickades krypteras med både amerikanska och sovjetiska krypton. Mycket arbete lades ner på att försäkra sig om att ingen dold information kunde skickas utan att det upptäcktes.

Det var i anslutning till detta som subliminala kanaler upptäcktes, vilka kunde ha varit ett stort hot mot hela programmet. Den slumpmässiga förflyttningen av robotar lades dock ner innan dessa sändare togs i drift, mycket på grund av att spänningarna mellan supermakterna minskat samt den oskäligt stora kostnaden för att flytta runt alla robotar.

2.6 Motmedel

Det finns (minst) fem sätt att hantera en känd dold kanal i ett system:

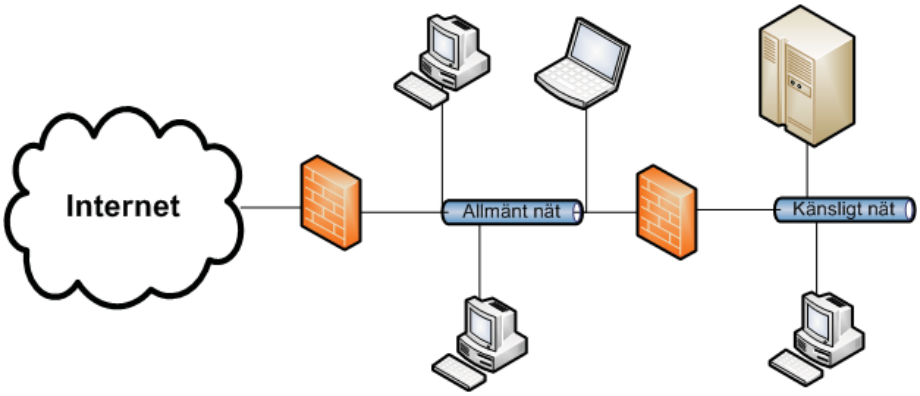

Bild 1: Organisationens nät

- Designa eller modifiera systemet på ett sådant sätt att den dolda kanalen inte är möjlig att använda.
- Minska den möjliga kapaciteten hos den dolda kanalens så mycket att ingen viktig information kan läckas inom en rimlig tidsrymd.
- Övervaka den dolda kanalen så att åtgärder kan vidtas om den används.
- Dokumentera att den dolda kanalen är möjlig.
- Ignorera den dolda kanalen.

Redan tidigt insågs att det inte är praktiskt möjligt att bygga ett system med multipla säkerhetsnivåer och flera användare på ett sådant sätt att *alla* dolda kanaler förhindras. Trots detta är det den önskvärda lösningen på problemet. För de kanaler som inte är praktiska att ta bort måste några av de andra metoderna användas, gärna i kombination. För att en kanal ska kunna ignoreras bör den ha en försumbar kapacitet (TCSEC, en amerikansk försvarsstandard för IT-säkerhet, föreskriver en kapacitet mindre än 0,1 bitar per sekund).

2.6.1 Exempel på motmedelsanvändning

Detta avsnitt presenterar ett par tänkta exempel på dolda kanaler samt hur dessa kan hanteras. För alla exempel i detta avsnitt tänker vi oss följande scenario: En organisation har två nät, ett allmänt nät kopplat till internet via en proxy med brandvägg samt ett nät på vilket mer känslig information hanteras. Det känsliga nätet är kopplat till det allmänna via en restriktiv gateway som även inkluderar intrångsdetektering (IDS) och en brandvägg, se bild 1.

Som nämndes ovan är det bästa sättet att hantera en dold kanal att modifiera systemet så att kanalen elimineras. Denna strategi väljs av organisationen för att neutralisera alla eventuella dolda kanaler som skickar information i oanvända fält i IP- eller TCP-huvuden. För att bli av med dessa kanaler konfigurerar organisationen om brandväggen mot internet till att nollställa alla oanvända fält i IP- och TCP-huvuden för både inkommande och utgående trafik.

För att förhindra att information läcker via en kanal som använder initieringsvärdet i TCP utökar organisationen sin gateway med en modul som byter ut initieringsvärdet för TCP-anslutningar till ett nytt, innan anlutningar upprättas. För att anslutningarna ska fungera trots att paket blivit modifierade måste gatewayen hålla reda på alla anslutningar och översätta TCP-sekvensnumret mellan det som används i det känsligare, inre nätet och det nya som gäller mot det allmänna. Organisationen väljer även att övervaka alla anslutningar mot internet för att leta efter användare som skapar och avslutar ett stort antal anslutningar utan att skicka någon data. Dessa granskas sedan mer ingående för att utröna om de försöker skicka data dolt.

Informationsöverföringen i en tidskanal sker, som tidigare beskrivits, via modulering av en gemensam resurs. Så länge det finns gemensamma resurser är det svårt att garantera att det inte finns någon tidskanal mellan det känsligare och det allmänna nätet. Att inte koppla ihop dem har övervägts av organisationen, dock ansågs nyttan med att kunna kommunicera mellan näten vara större än risken för läckor.

För att minska risken att en tidskanal används för att hämta information från det känsligare nätet, modifierar organisationen sin gateway så att alla paket fördröjs mellan noll och en halv sekund. Den försämring i kapacitet som detta medför anses vara försumbar för vanlig datatrafik samtidigt som eventuella dolda kanaler antas få sin kapacitet sänkt till maximalt någon bit per sekund.

3 Forskningsfältet

Detta kapitel presenterar några exempel på forskningsinriktningar inom forskningsfältet dolda kanaler för att sedan ge en mer ingående beskrivning av forskningen kring motmedel mot dolda kanaler.

3.1 Kapacitet

Många rapporter ger siffror på specifika kanalers kapacitet även om en del är mer generella. Exempelvis nämner Fisk et al. att steganografisk kapacitet kan vara mer än 50% av den öppna kanalens. Moskowitz et al. observerar vidare att man även bör använda andra aspekter än enbart kapacitet för att beskriva en dold kanal, nämligen tre faktorer vilka gemensamt går under benämningen ”Small message criterion”: Den första faktorn gäller hur kort ett meddelande kan vara för att ändå vara betydelsefullt, den andra hur störningskänslig informationen som skickas i den dolda kanalen är och den tredje hur tidskritisk överföringen av informationen är. Läckor med små meddelanden kan vara mycket allvarliga trots sin begränsade storlek eftersom de exempelvis kan

innehålla kryptonycklar; ökade störningar förstör fler dolda meddelanden och kräver större överförda mängder för att felrättande koder ska kunna användas; i exempelvis skarpa situationer är det ofta viktigt att få tag i information omedelbart varför skyndsamhet är av vikt. Vidare noterar Wang et al. att TCSEC:s historiska indelning av kanaler efter kapacitet är riskabel då olika kanaler kan användas tillsammans i aggregat.

3.2 Anonymitet och dolda kanaler

Det existerar vissa kopplingar mellan dolda kanaler och anonymitet. Medan dolda kanaler kan hindras med separering av processer baserar sig anonymitet på att det inte finns fullständig separering mellan desamma eftersom fullständig separation skulle betyda att det trivialt går att ta reda på vem som gör vad (det finns inga andra att gömma sig bland i ett givet system), vilket noterades av Murdoch et al. Bailey et al. visade att RFID-system som bejakar anonymitet och samtidigt är publikt verifierbart fria från dolda kanaler är omöjliga att konstruera på grund av att anonymiteten innebär att en RFID-enhet kan utge sig för att vara en annan och genom val av vilken kan information kommuniceras på ett sätt som är dolt.

3.3 Dolda kanaler i nätprotokoll

Många rapporter presenterar dolda kanaler som utnyttjar oanvända fält i meddelanden för olika nätprotokoll. Det faktum att fält som ofta inte används existerar beror främst på att de olika protokollen används på ett annat sätt nu än vad som var tänkt från början. Ett exempel på hur en dold kanal kan skapas på detta sätt är att manipulera options-fältet i IP-paket, ett annat att ändra på time-to-live vilket kan resultera i överföringskapacitet på 200–1200 bitar per sekund. Förutom dolda kanaler i IP finns sådana beskrivna för samtliga lager i nätstacken I länklagret (Ethernet) finns en möjlig dold kanal i kollisionsdetekteringen och i övrigt finns dolda kanaler beskrivna för bland andra HTTP, ICMP, VoIP samt instant messaging. Levy et al. noterade dock att många till synes oviktiga eller oanvända fält i nätprotokoll trots allt inte är slumpmässiga ens i legitim kommunikation – eftersom de ofta har förvalda värden.

Ahsan beskriver en dold kanal som utgörs av den ordning ett antal TCP/IP-paket skickas i med en kapacitet på 1/3000 av den öppna kanalen. Eftersom TCP sätter in paketen i rätt ordning igen när IP-överföringen är klar påverkar det hela inte legitim användning. Av samma skäl måste man dock läsa av den dolda kommunikationen innan mottagarens TCP-lager tar emot meddelandet från IP-lagret.

En dold kanal som använder DNS som mellanhand har beskrivits i flera källor, men ursprungligen av Kaminsky. Denna typ av kanal utnyttjar att DNS-servrar cachelagrar återkommande förfrågningar varpå två datorer kan kommunicera genom att den ena frågar (eller inte frågar) om en viss domän varefter den andra frågar och då kan mäta svarstiden för att se om informationen ligger i cachen eller inte. För att inte andra datorers förfrågningar ska påverka är det viktigt att inte fråga efter en alltför vanlig adress

även om det måste vägas mot hur suspekt det verkar när det plötsligt blir mycket trafik som efterfrågar adressen till en mycket ovanlig, eller rent av icke-existerande, domän. Eftersom varje förfrågning och svar ligger på 150 byte blir kanalkapaciteten cirka 1 bit per 300 byte och det faktum att cachen inte töms förrän efter cirka en timme begränsar ytterligare. Att en mellanhand används för kommunikationen kan dock vara av särskilt intresse och en artikel förutspår att metoden kan komma att användas exempelvis för styrning av botnät.

3.4 Dolda kanaler i hårdvara

Dolda kanaler i hårdvara kan på olika sätt vara värre än i mjukvara. Kanaler i processorarkitekturen är särskilt allvarliga då processorer har systemets högsta klockfrekvens vilket ger större kapacitet och enkel synkronisering. Dessutom är hårdvara mer tillförlitlig än mjukvara. En rapport fokuserade på hur multitrådning kunde utnyttjas för dolda kanaler och föreslaget motmedel kostade 10–25 % i systemeffektivitet. Andra hårdvarurelaterade dolda kanaler som beskrivits inkluderar temperaturpåverkan samt manipulering av avbrottsstyrd hårdvara eller hårddiskarmens rörelser.

3.5 Forskning om motmedel

Det finns många föreslagna medel för att motverka dolda kanaler och några har redan diskuterats i rapporten. Mycket av forskningen fokuserar på enskilda specifika kanaler men ett antal mer generella motmedel finns. Dessa verkar genom detektering vid design eller körning, kapacitetsreducering eller fullständig eliminering när sådan är möjlig. I detta avsnitt presenteras motmedlen inklusive hur de använts i praktiken, samt vilka teoretiska och praktiska begränsningar som finns. Dessutom ges ett antal exempel på hur de använts för att hantera eller utvärdera problemet med dolda kanaler i verkliga system, samt automatiserade verktyg för detsamma. Värt att notera är att det även existerar verktyg för implementering av dolda kanaler, exempelvis NUSHU för Linux av Rutkowska.

3.5.1 Grundläggande modeller

Denning introducerade ett matematiskt ramverk och en modell för så kallade syntaktiska informationsflöden. Denna modell används för åtkomstkontroll och består av, och reglerar, objekt, processer, säkerhetsklasser samt operationer på dessa. I Denning introducerades ett automatiskt verktyg för denna modell för användning under ett systems kompileringsstadium. Det observerades dock att vissa dolda kanaler missades av verktyget när man kontrollerade systemet mot modellen och att ytterligare kontroll därmed behövdes vid körning samt att dolda kanaler relaterade till hårdvara inte täcktes in.

Många metoder för att hitta dolda kanaler bygger på så kallad icke-interferens, en modell för säkerhetspolicyer som togs fram av Goguen och Meseguer. Icke-interferens

innebär att användare på lägre nivå inte påverkas av indata och kommandon från användare på högre nivå. Jämfört med exempelvis Bell-LaPadula-modellen är icke-interferens på sätt och vis striktare då dolda kanaler inte elimineras i det förra.

Kemmerer har presenterat Shared-Resource Matrix (SRM) vilken består av en grafisk matris som modellerar vilka subjekt som kan påverka vilka delar av gemensamma objekt och hur subjekt påverkas av de senare. Användning av SRM ger färre falsklarm vad gäller identifierade dolda kanaler än många tidigare metoder och det faktum att den ger en grafisk överblick gör att inte bara experter kan dra nytta av dess utdata. På så vis kan modellen användas av hela utvecklingsteamet och, genom att den underliggande matrisen hålls uppdaterad, genom hela livscykeln. Honeywells Multics, ett av de första operativsystemen för användning av flera användare samtidigt och som certifierades för en mycket hög assuransnivå, utvärderades bland annat genom användning av SRM samt en metod som bygger på icke-interferens, vilket beskrivs närmare av Loepere och Haigh et al.

Tsai et al. gav en semantisk informationsflödesmodell för analys av programmeringskod. Modellen undersöker vad som kan utgöra dolda kanaler bland annat genom att titta på vad som kan läsas, ändras och vilka relationer mellan funktioner som finns. Chen et al. byggde vidare på denna modell inom området för språkbaserad mjukvarusäkerhet där alla variabler definieras som tillhörande hög eller låg nivå.

3.5.2 Ytterligare metoder

Ahmed et al. beskriver en metod kallad ”dynamisk dold faktor” som grundar sig på att dolda kanaler som förflyttar information ett steg ner i säkerhetsnivåerna är mindre allvarliga än de som förflyttar informationen flera steg. Genom att hålla reda på vad som potentiellt läckt tidigare kan man då begränsa de dolda kanalernas påverkan och ta beslut om vilken process som ska få exekvera samt huruvida man ska låta realtidsegenskaperna stå tillbaka för dold kanal-säkerhet eller tvärtom.

En typ av metoder för att reducera dolda kanalers bandbredd utan att upptäcka dem baserar sig på att störa på olika sätt. Hu beskrev metoden ”fuzzy time” som innebär att man stör allt som kan utgöra ”klockor” i systemet för att reducera bandbredd i tidskanaler. Fullkomlig eliminering är dock knappast möjlig då någon form av synkronisering behövs processer emellan men metoden är å andra sidan normalt inte särskilt kostsam vad gäller förlust i effektivitet för legitima processer.

I vissa protokoll för samarbete är det viktigt att undvika hemliga samförstånd och en mellanhand är därför lämplig. Alwen et al. beskrev ett exempel på en sådan. Denna mellanhand lägger på slumpdata i efterhand för att eliminera eventuella dolda kanaler och även om mellanhanden inte går att lita på kan denne inte förstöra systemets övriga säkerhetsegenskaper, förutom temporärt tillgängligheten. Då metoden är tänkt att användas i budgivningar med ronder är det också viktigt att budgivarna inte kan kommunicera ens genom att avbryta sin medverkan. Därför hålls sådan information hemlig och defaultmeddelanden brukas istället för den avhoppade budgivarens normala meddelanden.

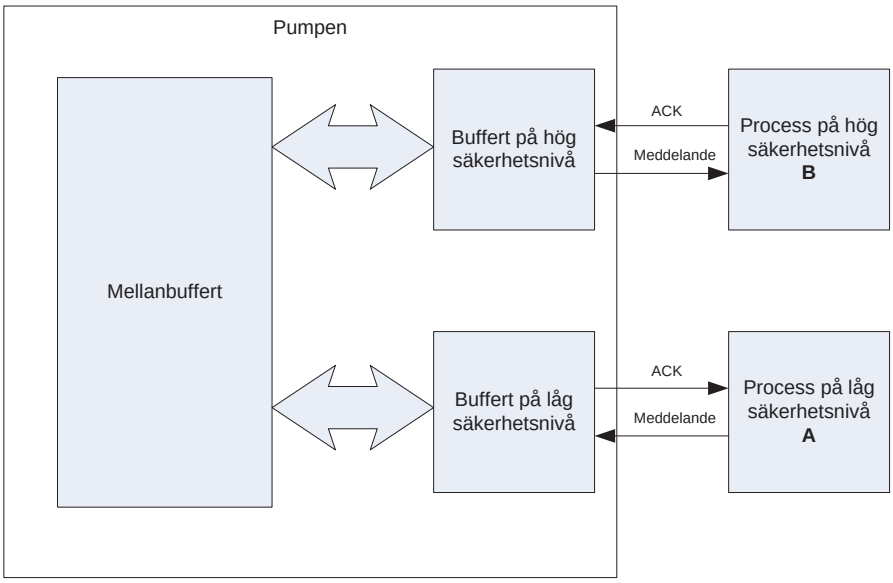

Bild 2: Översikt över datapumpens beståndsdelar

3.5.3 Filtrerande datapump

Det finns en konstruktion för att minska kapaciteten för dolda tidskanaler som inte påverkar normal kommunikation lika mycket som införande av en enkel, slumpmässig fördröjning gör. Denna konstruktion kallas för en pump. Syftet med pumpen är att möjliggöra att meddelanden kan skickas från en lägre säkerhetsnivå till en högre samtidigt som det blir svårare att skicka dolda meddelanden via tidsmodulering av de mottagningsbevis (ACK) som måste skickas för att bekräfta mottagandet av meddelandets delar.

Pumpen består av tre buffertar som kopplas in mellan de kommunicerande parterna A och B. Buffertarna är kopplade till varandra för att i tre steg skicka meddelanden från en lägre säkerhetsnivå A till en högre B. I bild 2 visas hur de olika buffertarna i pumpen är sammankopplade. Enkelt beskrivet förhindras en dold tidskanal genom att bufferten på låg säkerhetsnivå tar emot meddelandet som ska till B och svarar med ett mottagningsbevis så fort meddelandet vidarebefodrats till den mellersta bufferten. Således är det den mittersta bufferten som styr när ett mottagningsbevis ska skickas.

En dold kanal kan potentiellt skapas genom att B kan låta mellanbufferten bli full och därigenom hindra den att ta emot fler meddelanden från den lägre bufferten. Detta leder i sin tur till att det är processen på hög säkerhetsnivå som styr när ett mottagningsbevis ska skickas eftersom inga nya meddelanden kan läggas in i mellanbufferten förrän ett meddelande tagits ut.

För att komma till rätta med detta fördröjs alla mottagningsbevis med en slump-

mässig tid som beror på ett medelvärde av lagringstiden i mellanbufferten för ett antal av de senast mottagna meddelandena, det vill säga konsumtionstakten. Om ingen dold information försöker skickas kommer sändare och mottagare att lägga in och ta ut meddelanden ur buffertarna i ungefär samma takt vilket leder till att medelvärdet kommer att vara lågt och den slumpmässiga fördröjningen liten.

För att skicka dold information från B till A måste B vänta tills mellanbufferten är full vilket ökar medelvärdet för svarstiden markant. Denna ökning av medelvärdet kommer att öka det slumpmässiga tidstillägget för när mottagningsbevis skickas till A. Detta leder i sin tur till att längre fördröjningar måste införas innan mottagningsbevis skickas. Längre fördröjning leder dock återigen till att den slumpmässiga fördröjningen ökar.

3.6 Motmedlens begränsningar

De ovan beskrivna metoderna för hantering av dolda kanaler har vissa praktiska och teoretiska begränsningar. Förutom de som beskrivits tidigare i kapitlet ges ytterligare några begränsningar här.

Ett problem med modeller som ligger på högre abstraktionsnivå eller enbart verifierar specifikationer är att mer konkreta nivåer, såsom implementering, ofta skiljer sig från de abstrakta, med avseende på vad som verkligen händer i systemet. Eckmann har visat att verktyg för icke-interferens- och syntaktiska informationsflödesmodellerna samt SRM lider av dessa begränsningar och de rapporterar därmed flöden som suspekta fastän de inte kan ske i implementeringen, så kallade formella flöden. Att applicera modeller på en lägre nivå är dock inte uppenbart att föredra då det exempelvis kan leda till mer omfattande arbete samt begränsningar vad gäller programmeringsspråk. Kemmerer har å andra sidan noterat att det ofta är lättare att åtgärda problem på en lägre nivå, varför det underlättar om den ursprungliga analysen görs där.

Harrison et al. visade att det inte kan existera någon generell algoritm som kan avgöra säkerheten hos alla flernivåsäkerhetssystem med icke-interferens.

4 Relevans för Försvarsmakten

Detta kapitel resonerar kring dolda kanaler i dataslussar och i interna nät med extern anslutning. Dolda kanaler kan förekomma i alla system som innehåller känslig information, och därför ska beskrivningen nedan bara ses som exempel på hur problemen kan vara relevanta för FM:s system.

4.1 Interna nät med extern anslutning

När termen dold kanal används är det oftast okända informationsläckor ut ur ett system som avses. Dock kan dolda kanaler lika gärna användas för att *föra in* information i ett system på ett sätt som inte är förenligt med systemets säkerhetspolicy. Nedan

listas några generella exempel på hur dolda kanaler kan tänkas användas på ett för systemägaren oönskat sätt, och vilka motiv som kan tänkas ligga bakom.

- **Insider som vill föra ut information**
  För en insider är det troligen lättare att kopiera information till exempelvis ett USB-minne än att sätta upp en dold kanal till utsidan. Det finns dock vissa speciella fall där en dold kanal är ett bättre alternativ. Exempel på detta är om informationen som ska föras ut produceras gradvis och är till nytta för mottagaren bara om den är färsk.

- **Insider som vill föra in information**
  Ett exempel på detta är en anställd som vill kunna surfa eller lyssna på internetradio trots att detta är otillåtet och blockerat. Problemet i detta fall är antagligen inte införandet av den avsedda informationen, utan vad som kan följa med in eller ut av misstag.

- **Extern part som vill föra ut information**
  För att kunna föra ut information behöver den externa parten få in en trojan i systemet som sedan upprättar en dold kanal för att skicka ut informationen.

- **Extern part som vill kunna skicka in information**
  En extern part som har lyckats installera en trojan i ett system kan utnyttja denna i mycket större grad om trojanen kan instrueras och uppdateras även efter själva installationstillfället.

Som synes är varje kombination av aktör och riktning möjlig. Kombinerat med det stora antal typer av dolda kanaler som finns, menar vi att hotet från dolda kanaler är högst relevant för varje form av känsligt IT-system, till exempel de som används inom FM.

4.2 Dataslussar

IT-system kopplas ihop allt mer, vilket ger stora fördelar avseende kommunikation och förmåga att ta till sig information från omvärlden. Vi tror att IT-säkerhetsområdet under lång tid kommer att drivas av den tilltagande sammankopplingen av nät med olika sekretessgrad eller olika systemägare.

I dagsläget pågår utveckling, och viss användning, av dataslussar inom FMV och FM. Dessa ska kunna möta just behovet av att koppla samman system med olika informationsklassning eller systemägare på ett sådant sätt att endast tillåtna informationsflöden är möjliga. En datasluss måste alltså aktivt hindra att otillåten information passerar genom slussen, vilket är detsamma som att förhindra dolda kanaler enligt den strikta definitionen. Vid design och användning av dataslussar måste hotet från dolda kanaler beaktas och på något sätt hanteras. Med tanke på den stora variation som finns med avseende på utformning av dolda kanaler är det en stor utmaning att bygga en datasluss med tillräckligt hög assurans för att kunna koppla samman system som tidigare har ansetts kräva fysisk separering.

5 Diskussion

Forskningsfältet kring dolda kanaler är relativt spretigt vilket visar sig i att ett stort antal kanaler av väldigt varierande typ, samt potentiella motmedel mot dessa, presenterats. Anledningen till att så många typer av kanaler kan skapas, är troligen att en dold kanal kan bestå av i stort sett vad som helst. Det enda som krävs är att en sändare kan påverka något som en mottagare kan observera.

Nuförtiden är det huvudsakligen den utvidgade definitionen av dolda kanaler som används i publikationer. En anledningen till detta tror vi är att det är mycket lättare att skapa dolda kanaler enligt denna definition. En annan anledning är troligen att det inte finns så många system som uppfyller de krav som ställs för att den striktare definitionen ska vara uppfylld.

Enligt vår mening har inte FM behov av forskning kring *nya* dolda kanaler. Detta då det i dagsläget redan finns ett så stort antal publicerade typer av dolda kanaler att de närmast är att betrakta som heltäckande. Det finns redan en kanal för varje behov. Däremot menar vi att det behövs forskning om hur problemet med dolda kanaler ska kunna hanteras när system som tidigare varit isolerade från varandra kopplas samman. Ett i våra ögon viktigt spår inom detta område är hur hotet från dolda kanaler påverkar kraven på dataslussar och andra tekniker för att möjliggöra säker sammankoppling av nät med olika säkerhetsnivå eller olika systemägare.

Koppling av nät med skyddsvärt innehåll till andra nät leder till ett behov av assurans i de skyddsvärda näten på en nivå som inte fanns när de var isolerade. Detta eftersom dolda kanaler är mycket svåra, möjligen till och med omöjliga, att hantera enbart genom att införa en ”dörrvakt” som granskar informationsflödet mellan näten. Vid sammankoppling av sådana nät blir därför sekretessen hos informationen i det skyddsvärda nätet beroende också av riktigheten hos den programvara som används samt användarnas rättigheter och beteende, eftersom det annars finns risk att kunna drabbas av dolda kanaler. För att nå tillräcklig assuransnivå för informationsflödet måste därför noggranna kontroller av, samt säkra rutiner för, det skyddsvärda nätet införas. I ett isolerat nät kan däremot användare ha stora rättigheter och programvaran kan vara ogranskade standardprogram utan att sekretessen är hotad (riktigheten och tillgängligheten kan dock inte garanteras).