FOI
TOTALFÖRSVARETS
FORSKNINGSINSTITUT

FOI-R--0305--SE
Augusti 2001
ISSN 1650-1942
Metodrapport

Martin Karresand

TEBIT

Teknisk Beskrivningsmodell för IT-vapen

Ledningssystemteknik
581 11 Linköping

TOTALFÖRSVARETS FORSKNINGSINSTITUT

Ledningssystemteknik
Box 1165
581 11 Linköping

FOI-R--0305--SE

Augusti 2001

ISSN 1650-1942

Metodrapport

Martin Karresand

TEBIT

Teknisk Beskrivningsmodell för IT-vapen

Utgivare	Rapportnummer, ISRN	Klassificering
Totalförsvarets Forskningsinstitut - FOI	FOI-R--0305--SE	Metodrapport
Ledningssystemteknik	**Forskningsområde**	
Box 1165	4. Spaning och ledning	
581 11 Linköping	**Månad, år**	**Projektnummer**
	Augusti 2001	E7033
	Verksamhetsgren	
	5. Uppdragsfinansierad verksamhet	
	Delområde	
	41 Ledning med samband och telekom och IT-	
Författare/redaktör	**Projektledare**	
Martin Karresand	Ulf Lindbergh	
	Godkänd av	
	Lennart Nyström	
	Tekniskt och/eller vetenskapligt ansvarig	
	David Lindahl	

Rapportens titel

TEBIT Teknisk Beskrivningsmodell för IT-vapen

Sammanfattning (högst 200 ord)

Rapporten presenterar ett förslag på en taxonomi för IT-vapen, begränsad till programvara. I samband med det formuleras också en definition av IT-vapen. Någon annan taxonomi med en dylik begränsning är i dagsläget inte känd. Taxonomin är i första hand avsedd att användas för klassificering av de IT-vapen som samlas i en databas på FOI.

Taxonomin innehåller 14 kategorier med generella egenskaper hos ett IT-vapen. Den har anpassats till internationell standard genom att den kopplats till CVE (Common Vulnerabilities and Exposures), som underhålls av MITRE.

Problemet med att göra entydiga klassificeringar av kombinationsvapen behandlas och en lösning presenteras. Varje kategori förklaras utförligt och förtydligande exempel används när så behövs. Möjliga framtida användningsområden för taxonomin diskuteras. Dessutom ges riktlinjer för det fortsatta arbetet med utveckling av taxonomin.

Nyckelord

IT-vapen, datorsäkerhet, IT-krigföring, informationskrigföring, datorkrigföring, maskar, virus

Övriga bibliografiska uppgifter	Språk Svenska
ISSN 1650-1942	**Antal sidor:** 27 s.
Distribution enligt missiv	**Pris: Enligt prislista**
	Sekretess

Issuing organization	Report number, ISRN	Report type
FOI – Swedish Defence Research Agency Command and Control Warfare Technology P.O. Box 1165 SE-581 11 Linköping	FOI-R--0305--SE	Methodology report
	Research area code 4. C4ISR	
	Month year August 2001	**Project no.** E7033
	Customers code 5. Contracted Research	
	Sub area code 41 C4I	

Author/s (editor/s)	Project manager
Martin Karresand	Ulf Lindbergh
	Approved by Lennart Nyström
	Scientifically and technically responsible David Lindahl

Report title (In translation)

TEBIT Technical characteristics' description model for IT-weapons

Abstract (not more than 200 words)

This report presents a proposal for a taxonomy for IT-weapons, limited to computer software. A definition of IT-weapons is also formulated. No other taxonomy with the above limitations is known to exist today. The taxonomy is primarily intended to be used for classification of IT-weapons held in a database at FOI.

The taxonomy contains 14 categories of general properties of an IT-weapon. It has been adapted to international standards through a connection to the CVE list (Common Vulnerabilities and Exposures), which is maintained by MITRE.

The problem to make unambiguous classifications of combined IT-weapons is discussed and a solution is presented. Every category is thoroughly explained and clarifying examples are used whenever needed. Possible future areas of use for the taxonomy are presented. In addition to this some guidelines for further development of the taxonomy are given.

Keywords

IT-weapon, Computer Security, IW, IO, CNO, C4I, worms, viruses

Further bibliographic information	Language Swedish
ISSN 1650-1942	**Pages** 27 p.
	Price acc. to pricelist **Security classification**

Innehållsförteckning

1 Inledning

I det här kapitlet förklaras först bakgrunden till den här rapporten. Sedan beskrivs syftet, de avgränsningar som gjorts och slutligen metoden för studien.

Svenska datatermgruppens webbplats [Svenska datatermgruppen 2001] har använts för att i möjligaste mån hitta svenska översättningar på de engelska termer som påträffats.

Författaren till rapporten har tidigare bland annat tjänstgjort under fem år som ansvarig för IT-avdelningen på ett mellanstort företag och till dags dato läst sex terminer på civilingenjörsutbildningen för informationsteknologi vid Linköpings tekniska högskola.

1.1 Bakgrund

FOI initierade i samarbete med FMV en studie av hot från och möjligheter med IT-vapen. Som en del i det projektet visstidsanställdes författaren till den här rapporten bland annat med uppgift att samla in och klassificera dylika vapen. För att kunna klassificera dem formulerade författaren ett förslag på en definition av och taxonomi[1] för IT-vapen. Resultatet blev den här rapporten.

1.2 Syfte

Syftet med rapporten är att lägga fram författarens förslag på en definition av och taxonomi för IT-vapen, samt att i samband med det försöka besvara följande frågor:

- Hur definieras ett IT-vapen?
- Hur behandlar den nya taxonomin klassificering av kombinationsvapen?
- På vilka sätt kan taxonomin användas?

1.3 Avgränsningar

De avgränsningar som gjorts är att taxonomin och definitionen bara behandlar programvarubaserade IT-vapen ur en teknisk synvinkel.

[1] Taxonomi, noggrann (vetenskaplig) systematik. Ordet härstammar ursprungligen från en sammanslagning av grekiskans **taxis**, ordning och **nomos**, sats eller lag [Nationalencyclopedins ordbok 1995].

1.4 Metod

Rapporten är en litteraturstudie, men bygger till stor del på egna slutsatser. Detta eftersom inte någon av de taxonomier som hittats är gjorda med ovan nämnda avgränsningar.

En stor del av det material som studerats har hämtats från Internet för att få så aktuell och uppdaterad information som möjligt. Materialet har bestått av tekniska beskrivningar av verktyg och metoder som hackare använder, samt forskarrapporter och doktorsavhandlingar inom området IT-säkerhet. Detta för att ge en bred teknisk bakgrund och en generell förståelse av nuvarande och kommande angreppsverktyg. Studierna har även omfattat ett flertal av de taxonomier för IT-säkerhet och angrepp som tidigare publicerats.

2 Taxonomi för IT-vapen

I det här kapitlet behandlas först definitionen av IT-vapen och sedan ett förslag på en taxonomi. Författaren har formulerat följande hypotes i punktform om varför en taxonomi för IT-vapen hittills inte har utformats:

- Mängden av möjliga IT-vapen är i teorin obegränsad och nya versioner utvecklas i snabb takt.
- Det är svårt att skilja på administrativa verktyg och IT-vapen.
- Ett IT-vapen består ofta av en kombination av flera fristående enheter, vilket leder till svårigheter att göra en entydig klassificering av det.

När någonting klassificeras för första gången görs det oftast dikotomiskt[2] efter de för tillfället kända och synliga skillnaderna mellan objekten i en grupp. Det finns dock en risk att detta efter ett tag leder till motsägelsefulla klassificeringar av nyfunna objekt. När tillräckligt mycket blivit känt om objekten i gruppen vad gäller släktskap och andra gemensamma egenskaper görs en ny och mer detaljerad uppdelning. Till exempel har klassificeringen av växter och djur fått förändras när större tekniska genombrott gjorts inom mikroskopi och genteknik.

Strukturen hos en taxonomi av ovanstående typ kan beskrivas i form av ett träd, där grenarna visar släktskap och löven utgör objektens fullständiga klassificeringar. Skulle ett nytt objekt hittas, som inte kan klassificeras under en befintlig gren, skapas en ny gren för att nå fullständighet [Encyclopedia Britannica]. Det innebär dock att stora förändringar av trädstrukturen kan behöva göras om nya släktskap påvisas.

[2] Dikotomi, (*log.*), delning av en klass i två varandra uteslutande underklasser [Nationalencyclopedins ordbok 1995]. Ordet kommer från grekiskans *dihkotomia*, **dihka** dubbel, två- + **tomos** del [Ord för alla 1993]

I och med de ovan beskrivna orsakerna (se punktlistan) anser författaren att mängden av IT-vapen alltid kommer att vara dynamisk och därmed kunna betraktas som ny och outforskad. Dessutom innebär det faktum att olika IT-vapen kan kombineras på valfritt sätt att utvecklingen inte följer några biologiska evolutionslagar. Därför skulle en traditionell taxonomi baserad på släktskap fungera dåligt. Fördelen med den nedan föreslagna modellen är att den fungerar på den mycket snabbt ökande och i teorin oändliga mängden av IT-vapen. Detta eftersom taxonomin bygger på generella egenskaper hos IT-vapnen och inte släktskap mellan dem. Därför har den också potential att fungera även på längre sikt.

Modellen kan ses som en mängd kategorier var och en bestående av två eller flera disjunkta alternativ. Dessa utgör tillsammans en partitionering av kategorin. Flera alternativ ur en kategori kan användas samtidigt, vilket möjliggör en entydig klassificering av kombinationsvapen. Den här modellen stöds av Daniel Lough och kallas av honom för *characteristics structure* [Lough 2001 sidan 152].

En taxonomi bör ha vissa egenskaper för att fungera. Daniel Lough har gjort en arton punkter lång sammanställning av egenskaper från fem taxonomier för IT-säkerhet [Lough 2001 sidan 38]. Författaren till den här rapporten anser att följande egenskaper från sammanställningen är de viktigaste. De bygger på idéer från [Howard 1997]. En taxonomi och dess kategorier bör

- utgöra en partitionering av aktuellt område (genom ömsesidigt **uteslutande** och **heltäckande** alternativ)
- innehålla **entydiga** alternativ så att klassificeringen av ett objekt inte beror på tolkningar hos användaren
- bruka allmänt vedertagen terminologi så att den blir **användbar** för en så stor målgrupp som möjligt.

Ett krav för att taxonomin ska vara teoretiskt användbar är att alternativen i en kategori är entydiga och tillsammans utgör en partitionering. För att taxonomin ska bli allmänt vedertagen och praktiskt användbar bör den också vara lätt att förstå. Därför bör en väl etablerad terminologi användas.

För att minimera risken för subjektiva bedömningar vid klassificering av objekt ska alternativen i varje kategori i taxonomin vara baserade på mät- eller observerbara egenskaper [Krsul 1998 sidan 18]. För programvara är sådana egenskaper de algoritmer och instruktioner som programkoden är uppbyggd av (se även kapitel 2.1.3).

Det är således enbart de instruktioner (och kombinationer av dessa) datorprogrammet består av som ska ligga till grund för hur det klassificeras. Det borgar för att taxonomin ger samma klassificering av ett objekt, oavsett vem som använder den.

Det här utgör dock en begränsning av användbarheten för den föreslagna taxonomin. Användaren måste ha goda kunskaper i programmering och datorsäkerhet för att korrekt kunna avgöra funktionen hos ett okänt verktyg. Däremot behövs inga särskilda förkunskaper för att kunna klassificera ett verktyg som åtföljs av en god dokumentation. Jämför med upptäckten av en ny och hittills okänd växt. Klassificeringen av den kräver expertkunskaper för att kunna utföras korrekt. Däremot kan vem som helst med hjälp av en flora skilja mellan redan kända växter.

2.1 Definition av IT-vapen

Under den här rubriken presenteras först den definition av IT-vapen som utarbetats inom projektet vid FOI. Därefter redovisas ett nytt förslag på definition som passar ihop med den taxonomi den här rapporten lägger fram. Den nya definitionen utvärderas genom att den tillämpas på några olika verktyg. För att utvärderingen ska bli heltäckande väljs både typiska hackverktyg, såväl som vanlig kommersiell programvara.

Den nya definitionen används preliminärt endast inom ramen för rapporten och ska inte ses som en ny definition för hela projektets inriktning.

Det finns ett flertal definitioner av informations- och cyberkrigföring. De täcker naturligtvis ett större område än bara IT-vapen, men ger i alla fall en känsla för vad verktygen som används bör uppnå. Det amerikanska försvarsdepartementet (US Department of Defense) har definierat den militära delen av informationskrigföring så här [Haeni 1996]:

Information Warfare - Actions taken to achieve information superiority in support of national military strategy by affecting adversary information and information systems while leveraging and defending our information and systems.

John Alger, dekanus för School of Information Warfare and Strategy vid National Defense University ger följande definition av informationskrig i förordet till en bok av Winn Schwartau [Matthews]:

Information Warfare consists of those actions intended to protect, exploit, corrupt, deny, or destroy information or information resources in order to achieve a significant advantage, objective, or victory over an adversary.

En liknande definition ger Ivan Goldberg [Goldberg 2001], chef för amerikanska Institute for the Advanced Study of Information Warfare (IASIW):

Information warfare is the offensive and defensive use of information and information systems to deny, exploit, corrupt, or destroy, an adversary's information, information-based processes, information systems, and computer-based networks while protecting one's own. Such actions are designed to achieve advantages over military or business adversaries.

Alla tre definitionerna bygger på att ett övertag ska nås gentemot en motpart och att detta ska ske genom påverkan av dennes informationssystem. Således bör de verktyg som används ha sådana egenskaper. De ovanstående definitionerna är mycket lika varandra, vilket eventuellt antyder att de baserats på samma källa. Det är dock i så fall tre namnkunniga institutioner som alla anammat denna eventuella ursprungskälla. Författaren anser därför att de ovanstående definitionerna har sådan vikt att de kan användas för att skapa en preliminär definition av IT-vapen för användning i denna rapport

2.1.1 Preliminär definition

Den preliminära definitionen av IT-vapen har följande lydelse:

...programvara för att logiskt påverka information och/eller processer i IT-system för att åstadkomma skada

Den här definitionen ligger i linje med vad som framkom tidigare vid analysen av de tre definitionerna av informationskrigföring. Värt att notera är att verktyg som inte logiskt påverkar information eller processer inte klassas som IT-vapen enligt definitionen ovan. Det innebär till exempel att ett avlyssningsprogram[3] är uteslutet. Däremot definieras en webbläsare som ett IT-vapen. Detta eftersom den kan användas vid en punktpunktattack[4] för att logiskt påverka processer och på så sätt åstadkomma skada.

Vad som inte framgår klart ur definitionen är om det är uppsåtet med användandet eller konstruktörens syfte med verktyget som ska vara att åstadkomma skada. Om det är situationen verktyget används i som avgör om det är ett IT-vapen eller ej, kan teoretiskt sett all programvara omfattas.

Är det däremot konstruktörens syfte med verktyget som avgör klassificeringen, medför definitionen i [Howard 1997] att IT-vapen är en delmängd (om än oändlig) av alla programvaror. Det är dock svårt att avgöra vilket konstruktörens syfte med verktyget egentligen var. Tag till exempel SATAN, som enligt upphovsmännen är tänkt som ett hjälpmedel för systemadministratörer [CERT 1995]. Det betraktas också som ett användbart verktyg för att bryta sig in i datorsystem med [CIAC 1995, Meinel 1996]. Huruvida SATAN ska klassas som ett IT-vapen eller ej avgörs från fall till fall genom en subjektiv bedömning av verktygskonstruktörens karaktär.

2.1.2 Ny definition

Författaren valde att göra en egen definition av IT-vapen för att själv få reflektera över begreppet och på så sätt underlätta bland annat skapandet av taxonomin. Definitionen har mycket stora likheter med den i 2.1.1 och författarens tolkning är att de i grunden har i stort sett samma innebörd. Med hjälp av ovanstående definitioner av informationskrig (se kapitel 2.1) och framför allt definitionen av IT-vapen i 2.1.1, har följande förslag tagits fram:

[3] Den engelska benämningen är sniffer. En sådan avlyssnar nätverkskommunikation i hemlighet.

[4] En punktpunktattack innebär att två punkter skrivs direkt efter en webbadress i en webbläsare. Om den attackerade webbservern är dåligt konfigurerad, ger attacken tillgång till en högre nivå i filstrukturen på servern. I slutänden betyder det att angriparen kan få icke auktoriserade rättigheter i datorsystemet.

IT-vapen är datorprogram vars funktion är att ge brukaren övertag gentemot en annan part genom att angripa datorsystem.

När ett datorsystem angrips av en hackare används alla till buds stående medel för att resultatet ska bli det önskade. Det innebär att även verktyg som endast är avsedda för att administrera datorsystem kan användas. Med andra ord finns det en gråzon där kraftfulla administrativa verktyg ingår. En bra definition av IT-vapen är därför svår att göra, vilket också beskrevs i kapitel 2.1.1. En parallell kan dras till en näsduk som normalt inte definieras som ett vapen, men som mycket väl kan användas för att tillfoga någon allvarlig skada. Avsikten med den nya definitionen är att i möjligaste mån minimera antalet verktyg i gråzonen. Detta för att undvika svårigheter vid användandet av taxonomin.

I ett försök att göra definitionen tydligare har värdeladdade ord medvetet valts. Därför används till exempel ord som *övertag* och *angripa*. Det är också viktigt att tänka på att det är de instruktioner som verktyget är uppbyggt av som ska värderas, inte det uttalade syftet med verktyget.

2.1.3 Förtydligande av definitionen

För att förtydliga den nya definitionen görs nedanstående förklaringar av några ingående uttryck. En risk är dock att det uppstår en oändlig kedja av förklaringar och definitioner av dessa. Författaren har därför strävat efter att använda så entydiga och allmänt vedertagna begrepp som möjligt.

Eftersom definitionen specificerar att det ska vara datorprogram, utesluts manuell inmatning via till exempel ett terminalprogram.

Funktion

Med funktionen hos datorprogrammet menas att det ska innehålla sådana instruktioner som (teoretiskt eller praktiskt) skulle kunna användas för att manuellt angripa datorsystemet. Funktionen inkluderar även de algoritmer instruktionerna bildar tillsammans.

Övertag

Övertaget erhålls genom att instruktioner ges till en processor på elektronisk väg. Ett övertag kan ses som att båda parterna har var sitt fördelskonto, vilkas saldo står på noll före attacken. Ett övertag innebär att efter attacken har antingen angriparens konto fått plussaldo eller motpartens minussaldo eller en kombination av dessa tillstånd.

Övertaget kan åstadkommas både direkt genom att till exempel icke officiell information erhålls (positivt för angriparen). Det kan också åstadkommas indirekt genom att den andra partens verksamhet störs (negativt för den utsatta parten). Till exempel kan motpartens elleverantör attackeras, vilket leder till att elförsörjningen till motparten störs och därmed också dennes datorsystem.

Angripa

Ett angrepp innebär att datorprogrammet på något sätt påverkar det angripna datorsystemets *konfidentialitet, tillförlitlighet* eller *tillgänglighet*[5]. Det kan till exempel ske genom att utnyttja defekter i, neutralisera eller kringgå de säkerhetsfunktioner (automatiska och manuella) som det angripna datorsystemet har.

Datorsystem

Datorsystem innefattar alla slags maskiner som är programmerbara och däri lagrad programvara och data. Allt från inbyggda kretsar till de mest komplexa civila och militära system och därtill hörande nätverk.

2.1.4 Utvärdering av definitionen

För att kunna testa om definitionen har den önskade omfattningen, kommer den här att tillämpas på ett urval av de verktyg en hackare använder. Först används fem verktygsklasser som valts ut från en lista gjord av David Icove [Icove 1995 sidorna 29-60]. Sedan följer två verktyg som normalt inte klassas som IT-vapen, en webbläsare och en ordbehandlare.

[5] *Konfidentialitet* innebär förebyggandet av icke auktoriserat delgivande av information, *tillförlitlighet* betyder förebyggandet av icke auktoriserad förändring av information och med *tillgänglighet* avses förebyggandet av icke auktoriserat undanhållande av information eller resurs [Gollman 1999 sidan 5]. Där nämns fler sätt (autenticitet och ansvarighet), men de är mer specifikt inriktade på bankväsendet och elektronisk handel och tas därför ej upp här.

Urvalet har gjorts med författarens uppfattning som grund om vilka verktyg som kan tänkas ligga på gränsen till att inte vara IT-vapen. Detta för att ge en så relevant utvärdering som möjligt.

Sist i avsnittet sammanfattas utvärderingen.

Denial of Service[6]

Tillgänglighetsförsämrande verktyg finns i olika versioner, där de enklare helt enkelt skickar så många datapaket till det angripna systemet att dess tillgänglighet påverkas. Ett sådant verktygs funktion är att ge användaren övertag genom att den andra partens datorsystem störs och därmed *är det ett IT-vapen.*

Data diddling[7]

Det finns många olika datorprogram som manipulerar data på ett icke auktoriserat sätt. Ett specifikt exempel är ett loggrensningsprogram. Det används för att dölja spåren av ett intrång genom att rensa bort dem från de loggfiler som finns i systemet. Programmet ger användaren fördelen att eventuell upptäckt och överblick av skadorna efter intrånget försvåras. Definitionen ger att det *är ett IT-vapen*, eftersom det påverkar tillförlitligheten hos datorsystemet.

Scanning

Portskanning kan gå till på flera sätt. Ett enkelt sätt är att testa vilka portar i en brandvägg som är öppna. Det påverkar konfidentialiteten hos datorsystemet. Detta gäller även om portskanningen görs helt i överensstämmelse med de använda kommunikationsprotokollen. I [Anonymous 1998 sidan 174] liknas det vid att [helt öppet] gå runt ett hus och känna på alla dörrar för att se vilka som är olåsta. Sådan kunskap kan sedan användas för att göra ett intrång. En portskanner *är därför ett IT-vapen.*

---

[6] En tänkbar översättning är vapen för *förhindrande av användning*, men det behöver inte innebära ett fullständigt upphörande av möjligheterna att använda datorsystemet. En annan översättning skulle därför kunna vara *tillgänglighetsförsämrande* vapen.

[7] *Datamanipulering*

Det som i vardagslag benämns portskanner är dessutom ett mycket kraftfullare verktyg än det ovan beskrivna. Några exempel på sådana kraftfulla verktyg är SATAN, Nessus och NSS. De har bland annat funktioner för att testa vilken applikation respektive port är kopplad till och letar specifikt efter säkerhetsbrister. En sådan portskanning angriper definitivt konfidentialiteten hos det attackerade datorsystemet.

Password sniffer

En lösenordsavlyssnare används för att få tillgång till lösenord i hemlighet genom att den analyserar innehållet i de datapaket som skickas över ett nätverk. Den gör det utan att störa nätverkstrafiken. Lösenorden återfinns ofta i början av datapaketen och verktyget studerar därför bara en liten del (omkring 128 byte) i början av ett paket. Därför blir ett dylikt verktyg litet och snabbt. Dess funktion angriper konfidentialiteten hos det utsatta datorsystemet och *är alltså ett IT-vapen.*

Traffic analysis

Verktyget fungerar ungefär som en lösenordsavlyssnare, men det använder bara adressfälten i datapaketen. På så sätt kan det analysera hur trafiken i ett nätverk flyter och sammanställa statistik över vilka klienter som kommunicerar med vilka värdar. Informationen kan sedan användas för att ta reda på adressen till en server eller någon säkerhetsfunktion. Verktyget kan därför sägas ha som funktion att angripa konfidentialiteten i nätverket och kan betraktas som ett IT-vapen [Stallings 1999 sidorna 8, 139-140 och 238, Anonymous 1998 sidan 796].

Nu är många trafikanalysatorer manuella verktyg, det vill säga användaren anger de parametrar som styr verktyget. Dessa parametrar kan då ses som de instruktioner som angriper datorsystemet. Det medför att själva trafikanalysatorn inte ska betraktas som ett IT-vapen. Den är i stället jämförbar med ett terminalprogram eller en webbläsare.

Ett stort användningsområde för trafikanalysatorer är som intrångssensorer. All nätverkstrafik i ett datorsystem övervakas av analysatorn, som ger signal när ett intrångsförsök görs. Sådana instruktioner som verktyget i det fallet är uppbyggt av, är inte vad en hackare vanligtvis skulle använda.

Sammanfattningsvis kan sägas att en trafikanalysator definitivt hamnar i den tidigare nämnda gråzonen. Huruvida en specifik trafikanalysator är ett IT-vapen eller ej får därför *avgöras från fall till fall.*

Webbläsare

Även om en webbläsare kan användas för en punktpunkt-attack, är det användaren av webbläsaren som ger instruktionerna, inte webbläsaren. Därför är inte dess funktion att angripa och den är således *inte ett IT-vapen.*

Ordbehandlare

I det här fallet är det ett specifikt skript (ett makro) som ger de instruktioner vilka innebär ett angrepp. Ordbehandlaren har funktioner för att tolka de instruktioner skriptet innehåller, men dessa funktioner kan inte fristående användas för att utföra ett angrepp. Den är således *inte ett IT-vapen* (däremot är skriptet det).

Sammanfattning

De verktyg som satte definitionen mest på prov var trafikanalysatorn och portportskannern. Båda verktygen kan mycket väl användas av systemadministratörer för fullt legitima ändamål. Till exempel kan portportskannern användas för att analysera och på så sätt förbättra försvaret av ett nätverk mot intrång. Även trafikanalysatorn har en viktig funktion i försvaret mot angrepp.

Det är viktigt att komma ihåg att definitionen av IT-vapen anger att det är programkoden verktygen består av som ska innehålla instruktioner vilka kan användas för angrepp. När en portportskanner används av en administratör görs en auktoriserad attack på systemet. Den kan därför fortfarande betraktas som ett IT-vapen. Jämför med ett gevär som kan användas både i försvarssyfte och för älgjakt.

2.2 Förslag på taxonomi

Följande taxonomi är tänkt att fungera som en grovindelning av befintliga och kommande IT-vapen. Målet är att den ska vara möjlig att använda även av personer som inte är specialister på IT-säkerhet.

Kategorierna i taxonomin är oberoende och de ingående alternativen utgör en partitionering av respektive kategori. Alla kategorier har minst ett giltigt alternativ för varje IT-vapen. Det är möjligt att använda flera alternativ i en kategori samtidigt. På så sätt kan även kombinationsverktyg klassificeras entydigt.

Det är viktigt att tänka på att det är de instruktioner som vapnet består av som utgör grunden för klassificeringen enligt taxonomin.

Här nedanför beskrivs de 14 kategorierna (se tabell 2.1) under var sin rubrik. De alternativ som ingår i respektive kategori förklaras och när så är nödvändigt används ett exempel för att förtydliga.

Tabell 2.1: Tabellen visar de 14 kategorierna i taxonomin med tillhörande alternativ.

KATEGORINAMN	ALTERNATIV ETT	ALTERNATIV TVÅ	ALTERNATIV TRE
Verktygstyp	fristående	kombinerat	
Verkan	icke förändrande	temporärt förändrande	permanent förändrande
Målval	manuellt	autonomt	
Attacktillfälle	omedelbart	villkorsstyrt	
Funktionsområde	lokalt	fjärr	
Påverkar	stationära data	nätverkstrafik	
Utnyttjar	CVE/CAN-åååå-nnnn (Se 2.2.7)	annan metod	
Attacktyp	singelkälla	multipelkälla	
Måltyp	singelmål	multipelmål	
Kodtyp	stationär kod	mobil kod	
Kodsignatur	monomorf	polymorf	
Attacksignatur	monomorf	polymorf	
Passivitetssignatur	synlig	smygteknik	
Aktivitetssignatur	synlig	smygteknik	

2.2.1 Verktygstyp

Den här kategorin finns för att kunna skilja på ett *atomärt* och ett *kombinerat* IT-vapen. Ett kombinerat IT-vapen består av mer än ett fristående (kombinerat eller atomärt) IT-vapen. Det kan ha mer än ett giltigt alternativ för någon kategori. Observera att ett IT-vapen *inte* behöver vara atomärt bara för att det har endast ett giltigt alternativ per kategori. Vid sådana tillfällen indikerar den här kategorin vilken typ av IT-vapen det är.

2.2.2 Verkan

Vapnets verkan kan vara antingen *icke förändrande*, *temporärt förändrande* eller *permanent förändrande*. Ett förändrande IT-vapen förändrar målsystemet eller dess ingående data på något sätt. En permanent förändring ska vara varaktig. Det vill säga att om strömmen till datorsystemet bryts kvarstår verkan även efter att systemet startats igen. Den logiska följden blir således att en förändring som endast varar tills systemet startas om, är temporär. Alternativet icke förändrande omfattar till exempel avlyssningsvapen.

2.2.3 Målval

Ett IT-vapens målval kan ske *manuellt* eller *autonomt*. Manuella IT-vapen kräver en användarinsats för att välja mål. Autonoma IT-vapen väljer själva målsystem. Typiska exempel på autonoma IT-vapen är virus och maskar.

2.2.4 Attacktillfälle

Vapnet kan attackera *omedelbart* eller *villkorsstyrt*. Om attacktillfället inte styrs av några villkor, är det ett omedelbart attackerande IT-vapen.

2.2.5 Funktionsområde

Med funktionsområde avses den fysiska enhet som vapnet påverkar. Om vapnet attackerar hårdvara eller programvara i direkt anslutning till den processor (dator) det introducerades på är det ett *lokalt* IT-vapen. Attackeras i stället en annan dator än den där vapnet finns är IT-vapnet ett *fjärr*vapen. Det är under den aktiva fasen i vapnets körning som instruktioner ska skickas till det utsatta systemet. Dessa instruktioner ska starta processer i det angripna systemet. Processerna utför sedan det faktiska angreppet.

En mask är till exempel ett lokalt vapen, trots att den överför sig själv till ett annat datorsystem. Överföringen sker via e-post och masken körs inte i det utsatta systemet förrän en aningslös användare aktiverar den. Ofta räcker det med att användaren öppnar en bifogad fil för att masken ska aktiveras.

2.2.6 Påverkar

För att kategorin ska vara möjlig att kombinera med verkan; icke förändrande, får inte namnet *påverkar* tolkas bokstavligt. En paketanalysator till exempel är icke förändrande och verkar på *nätverkstrafik*. Ett verktyg som läser lösenordsfiler är icke förändrande och verkar på *stationära data* även om verktyget skickar filerna över ett nätverk. Definitionen av stationära data är data lagrad på hårddisk, i minne eller annan fysisk lagringsenhet. Data kan vara både programvara (programkod) och användarproducerad data.

2.2.7 Utnyttjar

De alternativ som ingår i kategorin är *CVE*[8]*/CAN-åååå-nnnn* och *annan metod.* När ett verktyg utnyttjar en svaghet som ingår i CVE (alternativet *CVE/CAN-åååå-nnnn*) klassificeras det genom att CVE/CAN-namnet[9] används. Det amerikanska standardiseringsinstitutet NIST (National Institute of Standards and Technology) har med CVE som grund skapat en databas [ICAT], som författaren föreslår ska användas vid sökningar efter CVE/CAN-namn.

Alternativet *annan metod* bör användas med stor urskiljning och då bara när den utnyttjade svagheten inte finns med i CVE. Att svagheten (metoden) inte finns med i CVE kan bero på att den ännu inte hunnit granskas av CVE Editorial Board. Den bör i så fall snarast rapporteras till dem. Det kan också bero på att de inte ansett[10] metoden utgöra en svaghet. Om ett IT-vapen klassificerats med alternativet annan metod, bör en kontroll göras med jämna mellanrum för att se om den utnyttjade svagheten (metoden) förts in i CVE. I så fall måste klassificeringen av IT-vapnet omedelbart korrigeras.

Termen svagheter som används ovan är inte ett entydigt definierat begrepp vad gäller IT-säkerhet. Följande definition har gjorts av Carl E Landwehr [Landwehr 1994 sidan 2]. (*Flaw* översätts av författaren i det här fallet till svaghet):

---

[8] Företaget MITRE [MITRE] står bakom en lista som kallas CVE (Common Vulnerabilities and Exposures) [CVE (a)] med målet att samla alla kända svagheter i IT-system på ett ställe. Tanken är att listan ska underlätta kommunikationen mellan alla de som sysslar med IT-säkerhet genom att standardisera begreppen. Beteckningen CAN (Candidate Number) innebär att svagheten är under utredning av CVE Editorial Board och eventuellt kommer att erhålla ett CVE-namn senare.

[9] Namnet har formen *bbb-åååå-nnnn* där *bbb* står för CVE eller CAN, *åååå* betecknar ett årtal och *nnnn* ett löpnummer.

[10] CVE Editorial Board använder omröstningar bland medlemmarna för att avgöra om en kandidat ska tas med på listan [CVE (b)].

... a security flaw is a part of a program that can cause the system to violate its security requirements.

Författaren föreslår att de säkerhetskrav systemet bryter mot när det innehåller en svaghet ska bestämmas enligt en modell för IT-säkerhet i linje med de kriterier som Common Criteria [Common Criteria 1999] specificerar. Även författarens förslag på en definition av IT-vapen kan användas och då främst begreppet *angripa*.

2.2.8 Attacktyp

En attack kan utföras från en punkt, *singelkälla*, eller flera samtidiga och koordinerade punkter, *multipelkälla*. Attacktypen specificerar med andra ord hur många processer i skilda datorer som verktyget består av. Är det mer än en process är verktyget av typen multipelkälla.

Denna kategori ger tillsammans med **måltyp** kombinationer av IT-vapen med verkan en-till-en, en-till-många, många-till-en och många-till-många. Till exempel är virus en singelkälla, eftersom dess attack inte är samtidig och koordinerad.

2.2.9 Måltyp

Kategorin måltyp har en tät koppling till attacktyp och innehåller alternativen *singelmål* och *multipelmål*. Ett IT-vapen av typen multipelmål är ett verktyg som på ett kontrollerat sätt angriper flera datorer eller system samtidigt. Definitionen på samtidigt i det här sammanhanget är att IT-vapnet ska köras i *en* process (det inkluderar ett multitrådat verktyg). På så sätt innefattas till exempel en portportskanner, som söker av ett helt nätverkssegment på en gång, i typen multimål. Även en mask kan vara av typen multipelmål, eftersom den kan sprida sig till flera nya värddatorer på en gång.

2.2.10 Kodtyp

En alternativ beteckning för kodtyp är typ av programmeringsspråk. Vad som avses är om vapnet är plattformsberoende eller ej. De två ingående typerna blir således *stationär kod* och *mobil kod*. IT-vapen skrivna i till exempel Java eller ett makrospråk klassas som mobil kod.

2.2.11 Kodsignatur

Kodsignatur beskriver om koden innehåller någon funktion för att förändra kodens utseende, så att den blir svårare att identifiera som ett specifikt IT-vapen. De ingående typerna är *monomorf* och *polymorf*. Kategorin ska inte förväxlas med passivitetssignatur. Ett polymorft IT-vapen försöker bara dölja sin identitet, inte sin existens, även om det i praktiken blir svårt att upptäcka med verktyg som enbart använder en signaturdatabas.

2.2.12 Attacksignatur

Kategorin specificerar om vapnet innehåller funktioner för att variera angreppssignatur, alltså göra en attack av en specifik typ men variera sättet den görs på. Detta kan ske till exempel genom att byta mellan .. och %2e%2e vid en punktpunktattack. De ingående typerna är *monomorf* och *polymorf*.

2.2.13 Passivitetssignatur

Den här kategorin specificerar om vapnet är *synligt* eller använder någon *smygteknik* för att dölja sig i passivt läge. Det kan innefatta till exempel att fånga upp systemkommandon, manipulera checksummor eller att placera sig i NULL-fält i filer. Observera att en polymorf kodsignatur inte innebär passivitetssignaturen smygteknik, även om polymorfism används för att undgå upptäckt från antivirusprogram.

2.2.14 Aktivitetssignatur

Ett IT-vapen som använder aktivitetssignaturen *smygteknik* innehåller instruktioner för att dölja vapnets aktiva fas. Smygtekniken kan ta sig olika former, men målet är att dölja IT-vapnets verkan. Till exempel använder man-i-mittenvapen[11] eller imitationsvapen[12] smygteknik i sina aktivitetslägen, eftersom de simulerar en obruten förbindelse. Används inte smygteknik är vapnet *synligt*.

[11] Man-i-mittenvapen (man in the middle) placeras mellan två datorer i ett nätverk. Där etablerar vapnet en förbindelse med båda datorerna och vidarebefordrar sedan alla datapaket den erhåller från respektive dator. På så sätt blir vapnet osynligt, samtidigt som det har full kontroll över all information som datorerna utbyter.

[12] Imitationsvapen (spoof) etablerar kontakt med en annan dator i ett främmande nätverk genom att imitera en legitim part. Vapnet kan först ha lyssnat på kommunikationen mellan två parter, sedan spärrat den ena parten och tagit över dess roll genom att härma den.

2.3 Resultat

Här görs ett försök att besvara de frågor som definierades i början av rapporten. Varje fråga diskuteras under en separat rubrik.

2.3.1 Definition av IT-vapen

I kapitel 2.1 behandlades olika definitioner av IT-vapen och IT-krigföring. Författaren presenterade dessutom en egen version (se kapitel 2.1.2), vilken löd på följande sätt:

> *IT-vapen är datorprogram vars funktion är att ge brukaren övertag gentemot en annan part genom att angripa datorsystem.*

När det ska avgöras om ett verktyg enligt definitionen är ett IT-vapen eller ej, är det verktygets programkod som ska analyseras. På så sätt minimeras risken för subjektiva bedömningar. Detta kräver dock kunskaper i programmering och IT-säkerhet. Likaså måste verktygets källkod finnas tillgänglig, eller möjlighet att utföra tester som klart visar verktygets alla funktioner. Den eller de bakomliggande algoritmerna måste alltså gå att utröna. Om en noggrann analys av ett IT-vapens funktion finns till hands, kan en klassificering av vapnet utföras även utan expertkunskaper.

Specifikationen för hur sådana tester ska gå till i detalj tas inte upp i den här rapporten. Det får i stället utredas i en separat skrivelse. Kortfattat kan dock konstateras att testerna naturligtvis måste omfatta funktioner relaterade till samtliga kategorier i taxonomin.

2.3.2 Kombinationsvapen

Ett problem som behövde lösas för att den nya taxonomin skulle fungera var hur IT-vapen bestående av en kombination av andra IT-vapen skulle behandlas. Ett krav på taxonomin var att den gav samma klassificering av ett specifikt IT-vapen, oavsett när klassificeringen utfördes eller av vem. Den skulle också ge en och endast en klassificering per IT-vapen. Det löstes genom att införa kategorin *verktygstyp*. Kategorin ger en signal om att kombinationer av flera alternativ kan vara aktuella.

Även valet av struktur möjliggör att flera alternativ per kategori kan användas på ett naturligt sätt. Strukturen kan ses som en låda med många små fack. Varje fack innehåller en generell egenskap (ett alternativ från en kategori) hos ett IT-vapen. När en klassificering görs, samlas alla egenskaper som passar in på det avsedda IT-vapnet ihop. Dock måste alltid minst ett alternativ ur varje kategori tas med. De ihopsamlade alternativen utgör en fullständig klassificering av IT-vapnet.

2.3.3 Användning

Taxonomin är tänkt att användas för kategorisering av de IT-vapen som kommer att ingå i en databas hos FOI. I och med att kategorin *utnyttjar* är kopplad till CVE [CVE (a)] via ICAT [ICAT] kan taxonomin mycket väl tillämpas även utanför FOI. Beroende på vem som tillfrågas definieras bland annat trojaner, virus och maskar olika. Taxonomin erbjuder en möjlighet att skapa en global standard för IT-vapen, liknande den CVE gjort för svagheter i datorsystem.

Ett annat tänkbart användningsområde är vid utveckling av nya IT-vapen och skydd mot dessa. Taxonomin kan då användas som en grund för nya idéer. Genom att fritt skapa kombinationer av alternativ ur kategorierna, kan möjliga framtida vapen och deras funktioner förutses. På så sätt kan effektiva motmedel tas fram i förväg. I boken The Art of War skriver Sun Tzu [Tzu 500 f. Kr, kapitel VI]:

> *Whoever is first in the field and awaits the coming of the enemy, will be fresh for the fight; whoever is second in the field and has to hasten to battle will arrive exhausted.*

Taxonomin kan även användas i utbildningssyfte, som ett diskussionsunderlag för att öka förståelsen för begreppet IT-vapen.

3 Slutsatser

De flesta som någon gång kommit i kontakt med IT-säkerhetsområdet har en ungefärlig uppfattning om vad en mask, trojan eller ett virus är. Dock finns det ingen generell definition av vad de olika namn som används innebär. Vid en närmare granskning visar det sig att begreppen går i varandra och ofta används godtyckligt. Det faktum att de flesta IT-vapen idag är kombinationer av andra IT-vapen, förbättrar inte situationen.

En slutsats som kan dras är att området är i behov av en fungerande taxonomi, men att det av samma anledningar är mycket svårt att konstruera en sådan.

I rapporten konstateras att det hittills inte gjorts någon taxonomi specifikt för området IT-vapen. Det presenterade förslaget är därför ett försök att fylla den luckan. Det har dock inte varit någon lätt uppgift att definiera vad ett IT-vapen är, eller att göra en taxonomi som uppfyller de krav som ställdes på en sådan (se kapitel 2). Arbetet med taxonomin har präglats av en ständig balansgång mellan krav på användbarhet och strikta definitioner.

Det återstår fortfarande att utvärdera taxonomin under realistiska förhållanden. Resultatet kan sedan användas för att vidareutveckla den, så att en generell standard kan framställas. Förhoppningsvis kan även de resonemang kring IT-vapen som rapporten innehåller fungera som en hjälp i detta arbete.

Ett annat område som kräver mer utredning är hur en analys av ett IT-vapen, där källkoden inte finns tillgänglig, ska utföras. Metoder och regler för analysen måste standardiseras. Detta är också ett krav om taxonomin ska bli möjlig att använda.

Det framtida arbetet med utveckling av taxonomin bör således koncentreras på utvärdering av densamma, samt specifikation av metoder för analys av IT-vapen. Detta sker förslagsvis parallellt med uppbyggnaden av en IT-vapendatabas på FOI.

4 Referenser

Referenserna är indelade i två typer; litteratur och Internet. Typerna återfinns sorterade i bokstavsordning efter huvudförfattarens efternamn (eller titel om författare saknas) under separata rubriker. Hänvisningarna i rapporttexten anger huvudförfattarens namn och utgivningsår, eller när dessa uppgifter saknas, verkets titel.

Internetadresser som är längre än en rad har brutits utan att några bindestreck eller andra tecken satts in. Dessa adresser existerade vid lästillfället. Författaren garanterar inte att de fortfarande gör det.

4.1 Litteratur

Anonymous (1998), Maximum Security – A Hacker's Guide to Protecting Your Internet Site and Network, 2:a utgåvan, Sams Publishing, ISBN 0-672-31341-3

Gollman, Dieter (1999), *Computer Security*, John Wiley & Sons, ISBN 0-471-97844-2

Icove, David; Seger, Karl och VonStorch, William (1995), *Computer Crime: A Crimefighter's Handbook*, O'Reilley & Associates, Inc., Sebastopol, CA.

Nationalencyclopedins ordbok (1995), Bokförlaget Bra Böcker

Ord för alla (1993), Bokförlaget Prisma, ISBN 91-518-2586-4

Stallings, William (1999), *Cryptography and Network Security, Principles and Practice*, 2:a utgåvan, Prentice Hall, ISBN 0-13-869017-0

4.2 Internet

CERT (1995-04-03), Computer Emergency Responce Team, *CERT Advisory CA-1995-06 Security Administrator Tool for Analyzing Networks (SATAN)*, http://www.cert.org/advisories/CA-1995-06.html, läst 2001-06-27.

CIAC (1995-04-05), Computer Incidents Advisory Center, *Information Bulletin F-20: Security Administrator Tool for Analyzing Networks (SATAN)*, http://www.ciac.org/ciac/bulletins/f-20.shtml, läst 2001-07-17.

Common Criteria (augusti 1999), *Common Criteria for Information Technology Security Evaluation, part 1-3, version 2.1*, http://www.commoncriteria.org/cc/cc.html, läst 2001-07-19.

CVE (a), Common Vulnerabilities and Exposures, http://CVE.MITRE.org/, läst 2001-07-25.

CVE (b), http://CVE.MITRE.org/docs/docs2000/naming_process.html, läst 2001-07-25

Encyclopedia Britannica, http://www.britannica.com/eb/article?eu=119735&tocid=48695, läst 2001-06-29

Goldberg, Ivan (2001-01-13), Institute for the Advanced Study of Information Warfare, http://www.psycom.net/iwar.1.html, läst 2001-06-27

Haeni, Reto (1996-08-23), *What is Information Warfare*, http://tangle.seas.gwu.edu/~reto/infowar/what.htm, läst 2001-06-27.

Howard, John D (1997-04-07), *An Analysis of Security Incidents on the Internet 1989-1995*, Pittsburg, doktorsavhandling, Carnegie Mellon University, http://www.cert.org/research/JHThesis/Word6/, läst 2001-07-11.

ICAT, http://ICAT.nist.gov/ICAT.cfm, läst 2001-07-25.

Krsul, Ivan V (maj 1998), *Software Vulnerability Analysis*, doktorsavhandling, Purdue University, http://www.cs.purdue.edu/homes/kamarasf/papers/software_vulnerabilities.pdf, läst 2001-07-13.

Landwehr, Carl E, med flera (sep 1994), *A Taxonomy of Computer Security Flaws*, ACM Computing Surveys, volym 26, nummer 3, http://chacs.nrl.navy.mil/publICATions/CHACS/1994/1994landwehr-acmcs.pdf, läst 2001-07-04.

Lindqvist, Ulf och Jonsson, Erland (1997), How to Systematically Classify Computer Security Intrusions, *In Proceedings of the 1997 IEEE Symposium on Security & Privacy* sidorna 154-163, Oakland, Kalifornien, USA, IEEE Computer Society Press, http://www.ce.chalmers.se/staff/ulfl/pubs/sp97ul.pdf, läst 2001-07-12

Lough, Daniel L (april 2001), *A Taxonomy of Computer Attacks with ApplICATions to Wireless Networks*, doktorsavhandling, Virgina Polytechnic Institute and State University, http://scholar.lib.vt.edu/theses/available/etd-04252001-234145/unrestricted/lough.dissertation.pdf, läst 2001-07-13.

Matthews, Scott, *Welcome to the NEW age of Information Warfare*, http://www.chipcenter.com/eexpert/smatthews/smatthews001.html, läst 2001-07-26

Meinel, Carolyn P (1996), *THE HAPPY HACKER GUIDE TO (mostly) HARMLESS HACKING, Vol. 2 Number 4*, http://www.happyhacker.org/gtmhh/vol2no4.shtml, läst 2001-07-17.

MITRE, *The Early Years*, http://www.MITRE.org/about/history.shtml, läst 2001-07-25

Svenska datatermgruppen (2001-01-14), http://www.nada.kth.se/dataterm/ordreg.html, läst 2001-06-25 till 2001-07-27

Tzu, Sun (500 f. Kr.), *The Art of War*, Lionel Giles översättning från 1910, http://all.net/books/tzu/tzu.html, läst 2001-07-25