



MYNDIGHETEN FÖR SKOLUTVECKLING

Sju punkter om hackerkulturen

Jonas Löwgren

Professor i interaktionsdesign

Området för Konst, kultur och kommunikation

Malmö högskola

Myndigheten för skolutveckling

KARLBERG SVÄGEN 77-81

113 35 STOCKHOLM

TEL: 08-527 78 000 FAX: 08-527 78 001

I Dagens Nyheter den 13 augusti 2003 kunde man läsa att tjugotusen Internet-kunder hos Telia inte kunde komma ut på nätet på grund av viruset Lovesan som slog ut Telias datorer.

Biltillverkaren Daihatsus hemsida i Makedonien (www.daihatsu.com.mk) såg inte ut som vanligt den 7 augusti 2003. I stället för terrängbilar och extraerbjudanden möttes man av uppropet 'BRING THE YUGOSLAVIAN UNION BACK! Tito 4ever!', undertecknat av The Ghost Boys.

Är det här exempel på sådant som hackers gör? Vad är egentligen en hacker?

Vanligen tänker vi kanske på unga pojkar som sitter många timmar i sträck framför sina datorer och behärskar alla deras knep, inställningar och tekniska egenheter. I bästa fall kan vi se skillnad på om de spelar spel, chattar eller programmerar.

Det är inte heller ovanligt att förknippa begreppet hacker med databrott och intrång av olika slag.

Mitt ärende här är att försöka ge ordet hacker ett lite mer precist innehåll, genom att beskriva några grundläggande drag i det som man kan kalla hackerkulturen. Jag vill nämligen påstå att det finns sådana drag, och att de kan användas för att bättre förstå de handlingar som annars ter sig ganska svårbegripliga.

1. 'Information wants to be free.'

En grundläggande värdering i hackerkulturen är att information inte får ägas, utan tvärtom ska delas och spridas så mycket som möjligt. Det gäller naturligtvis digital information, inklusive programkod, eftersom den är så lätt att sprida. Men också andra typer av information – exempelvis är det inte ovanligt bland hackers att engagera sig i upplysningskampanjer kring sekter och kulturer av olika slag.

Begrepp som 'open source' (dvs. fritt tillgänglig källkod till ett dataprogram) och 'copyleft' (i motsats till copyright) bygger på tanken om hackerkulturen som ett *oegennyttigt kollektiv* med gemensamma mål. En programmeringsuppgift som är tillräckligt attraktiv kan motivera kollektivet att lägga ner många tusen oavlönade timmar på att bidra med komponenter och vidareutveckla andras bidrag. För att en sådan kollektiv uppgift ska vara attraktiv krävs dels att den är tekniskt utmanande och dels att den är ideologiskt riktig. Exempelvis är det motbjudande för många hackers att Microsoft tjänar pengar på vad hackers betraktar som tekniskt undermåliga produkter, medan alternativet Linux är gratis och dessutom har större teknisk elegans. Därför har det visat sig attraktivt för många hackers att oegennyttigt bidra till utvecklingen av Linux-projektet.



2. En hacker bedöms efter vad han kan göra med datorer – inte efter sitt utseende, härkomst eller ställning i samhället i övrigt.

(Jag skriver 'han' här och i fortsättningen, eftersom hackerkulturen domineras helt av pojkar och män.) Det här är en hörnsten i hackerkulturen, som man brukar beskriva som en *meritokrati*. Med det menas här att din ställning inom hackerkulturen bestäms helt av din bevisade skicklighet inom det område som hackerkulturen räknar som viktigt, nämligen datorer, nätverk och programmering.

Det här är också förklaringen till att bara tekniskt utmanande uppgifter kan dra till sig några större kollektiva insatser. Enkla uppgifter ger inte tillfälle att visa vilken skicklighet man besitter och därmed vilken position man förtjänar inom hackerkulturen.

3. En hacker är man bara om man kallas så av andra hackers.

Återigen en meritokratiaspekt – bara de som redan tillhör kulturen är skickade att bedöma nya medlemmars position.

Mycket av det som i massmedierna tillskrivs hackers är i själva verket tekniskt mycket enkla uppgifter. Att hitta adressen till en dator där en viss webbplats ligger, att vinna tillträde till den datorn, och att ersätta den befintliga webbsidan med ett eget innehåll är idag uppgifter som kan göras utan något som helst programmeringskunnande. Det finns verktyg att få tag på, om man vet var man ska leta, som gör hela processen automatiskt. Samma sak gäller för virus av olika slag: att skapa ett nytt virus som utnyttjar tidigare kända säkerhetsbrister för att sprida sig kan man göra med ett tryck på en knapp i något lättillgängligt virusskaparverktyg. Att knäcka kopieringsskydd på dataprogram, musik och filmer kan vara mycket svårt, men upplåsta versioner av alla slags kommersiella digitala produkter ligger färdiga att laddas hem.

På åttiotalet, innan de grafiska gränssnitten var allmänt spridda, kunde man få tag på programsnuttar som kallades 'scripts' för att exempelvis ta sig in i ett främmande system där man inte hade användar-ID eller lösenord. De som sysslade med sådant kallades av riktiga hackers lite ringaktande för 'script kiddies' och deras verksamhet betraktades inte som meriterande i termer av tekniskt kunnande. Samma gäller idag för att använda färdiga verktyg i syfte att placera eget innehåll på en webbplats (något som kallas 'web defacement', eller kanske webbkapning på svenska) eller skapa en ny utgåva av ett standardvirus.

Att däremot vara den förste som utnyttjar en hittills okänd säkerhetslucka i programvaran på den dator där webbplatsen i fråga ligger, eller att knäcka kopieringsskyddet på något nytt program (eller varför inte regionkodningen på DVD-filmer, för att nu ta ett aktuellt exempel) på ett särskilt elegant sätt, är meriterande. Det handlar om att besitta stort tekniskt kunnande och visa att man besitter det, vilket är en del av förklaringen till att hackerkulturen har många publiceringsfora för sådana bedrifter.



4. Tillgängliga resurser ska användas.

Om en dator står påslagen men oanvänd nattetid så är det inte moraliskt fel att skaffa sig tillträde till den för att köra program på den. Tvärtom ses det ofta som ett bättre utnyttjande av resurser som datorns ägare inte förstår att nyttja fullt ut.

I hackerkulturens historia finns många exempel på att utnyttja en underutnyttjad resurs på ett sätt som ägaren inte har tänkt sig, särskilt om det krävs stort tekniskt kunnande för att göra det. 'Phone phreaking' gick ut på att kunna ringa telefonsamtal utan debitering, något som krävde stor inblick i telefonväxlarnas tekniska uppbyggnad och funktionssätt. Argumentet att telefonledningarna ändå fanns där, och att det inte medförde något slitage att utnyttja dem, imponerade inte på de amerikanska telefonbolagen som istället såg gratisringandet som ett federalt brott.

5. Tillgängliga resurser ska inte skadas.

Att använda sig av en underutnyttjad resurs är inte det samma som att skada den. Tvärtom är det av vikt för hackerkulturen att inte förstöra de resurser man använder. Exempelvis är det normalt vid en webbkapning att det ursprungliga innehållet bevaras, kanske kopieras till någon tillfällig mapp, innan det nya innehållet läggs dit. Ibland kan det nya innehållet till och med ge direkta instruktioner till systemadministratören om hur det ursprungliga innehållet ska återställas. (Följande instruktioner fanns exempelvis i det nationalistiska upprop som den australiensiska aktivistgruppen Halcon placerade på nrrs.com den 28 april 2000: 'To the admin: I am truly sorry for having to do this to you, the way we came in has been patched, and no content has been destroyed. mv index_old.html index.html to replace this.')

Det man gör inom hackerkulturen syftar till att utvidga sitt kunnande, inte till att förstöra saker. Komplikationen är att en del av det som hackers gör kan leda till tekniska problem, beroende på misstag eller avsett som ett skämt. Sådant kan hackers själva betrakta som harmlöst, eftersom de vet hur 'lätt' man rättar till det, medan de som drabbas kanske inte är lika kunniga.

Man kan ibland spåra en nedlåtande ton bland hackers gentemot dem som står utanför hackerkulturen. Om man väljer att köra Windows NT som server utan de senaste säkerhetsuppdateringarna, för att nu ta ett konstruerat exempel, så ber man faktiskt om dataintrång. Då får man skylla sig själv och läsa på lite bättre.

Ett kanske vanligare sätt att närma sig skillnaderna i tekniskt kunnande mellan hackerkulturen och resten av samhället är att peka på den *tjänst* man gör genom att hitta säkerhetsluckorna och de tekniska bristerna i dagens datasystem. På UnionBanks webbsida i Pakistan (www.unionbank.com.pk) stod följande text att läsa den 10 augusti 2003.



This Website has been officially hacked, but we are not happy to do so. We would surely like this website to be more secured than this. We want Pakistani networks to be more secured and not like this that every other Indian just comes and defaces it. We are just doing it here, so that if the admin wants any help to secure his box, he can email us at switchx@hotmail.com. Lets make Pakistan stronger. If we would be good within ourselves, only then we would be able to fight others. Thankyou. Greetz to JavaBoy, HeavenBoy, PainBhai and the lost love of my life. KillerX signs out.

6. Klaga inte, gör bättre själv.

Om man finner en brist i ett program som man använder, så vänder man sig inte till upphovsmannen och klagar. I stället åtgärdar man bristen och sprider det förbättrade programmet för allas bästa. Det är lätt att se hur det tankesättet passar i sammanhang med öppen källkod ('open source'), där själva grundprincipen är att man ställer resultaten av sitt programmeringsarbete till fritt förfogande för alla andra som har kompetensen att bygga vidare på dem.

Däremot är det bäddat för konflikter med kommersiella affärsmodeller som bygger på att leverantören tjänar pengar på att sälja informationen. Exemplet med kopieringsskyddad programvara, musik, bild eller film är ganska talande här. Motivet för en hacker att försöka knäcka ett kopieringsskydd är kanske dels den ideologiska tanken att (digital) information ska vara fri, dels den tekniska utmaningen som ligger i uppgiften. Naturligtvis finns också den personliga vinsten i att slippa betala för informationen, men hackerkulturen skiljer sig från andra synsätt i den här frågan. Det vore inte hackermässigt att börja sälja ett program som man knäckt kopieringsskyddet på (även om det säkert vore lönsamt), men däremot att sprida beskrivningen av hur man gick till väga.

En vanlig reaktion bland leverantörerna av kopieringsskyddad digital information har varit att försöka uppfinna nya kopieringsskydd med ännu större säkerhet. Problemet med en sådan strategi är att det samtidigt blir en större teknisk utmaning att knäcka skyddet, och därmed än mer meriterande inom hackerkulturen. Konsekvensen blir ett slags kapprustning som knappast ens gynnar kunderna i slutändan.



7. Ifrågasätt auktoriteter, stöd decentralisering.

Ett återkommande tema inom hackerkulturen är att argument ska vara rationella och baseras på förstahandskällor: fakta och information som ska vara tillgängliga för alla inblandade, i linje med tanken om att information inte kan ägas. 'Auktoritet' i det här sammanhanget förknippas med att utöva makt i stället för sund argumentation.

Myndigheter och andra som besitter auktoritet i samhället ses ofta med skepsis inom hackerkulturen, särskilt inom den tankeriktning som kallas *cyberpunk*. Linus Walleij, en framstående svensk hacker och anarkist definierar cyberpunk som 'en person i ett högteknologiskt samhälle som har information och/eller kunskap som de styrande makterna hellre hade velat behålla för sig själva.'

Cyberpunk är en i allt väsentligt pessimistisk hållning, där samhället ses som strukturer av globala informationssystem som styr folket. Framtiden är närmast en dystopi i stort, men för hackern är det annorlunda. Han har det kunnande som krävs för att klara sig bra i en sådan värld, om han bara förstår läget korrekt och kämpar mot systemet med de medel som står honom till buds.

Även utanför den mer aggressiva cyberpunken är *integritet* en stor sak inom hackerkulturen, där det stora tekniska kunnandet gör att man gott förstår hur de allt mer omfattande informationssystemen skulle kunna missbrukas. Det är ingen slump att många kollektiva utvecklingsprojekt behandlar olika krypteringstekniker, eller att kunnande om datasäkerhet värderas högt inom hackerkulturen. Ibland används till och med hackerkulturens stora tekniska kunnande som ett slags förtäckt hot, som i avslutningen av Simple Nomads föredrag vid hackerkonferensen DefCon11:

I'd like to close with jrandom's infamous paraphrasing from Fight Club: "The people you are after are the people you depend on. We develop your apps, we backup your data. We route your packets, we defend you while you sleep. Do not fuck with us."
<www.nmrc.org/pub/report/sn-dc-2003.html>

Efter de här sju punkterna ska vi nu återvända till exemplen i inledningen: viruset Lovesan (som senare mest kom att kallas Blaster) och budskapet på Daihatsus webbsida i Makedonien. Hur skulle de betraktas inom hackerkulturen? Som värdiga uppvisningar av ett överlägset tekniskt kunnande – ett hack, som man säger – eller som ointressanta pojkstreck?

Det kan vi inte avgöra genom den offentliga rapporteringen. En liten ledtråd finns i binärkoden till Lovesan, alltså den fil som utgör själva det körbara programmet. Sådana filer är normalt inte läsbara i vanlig mening, de innehåller ingen text som vi begriper utan ser bara ut som rappakalja när man skriver ut dem. Men i Lovesans binärkod finns följande text insprängd.

msblast.exe I just want to say LOVE YOU SAN!! billy gates why do you make this possible? Stop making money and fix your software!!



Utan att vara särskilt insatt i Lovesans konstruktion går det inte att säga om den representerar en betydande teknisk bedrift i hackerögon. En ledtråd finns i ett uttalande av Patrik Runald på datasäkerhetsföretaget F-Secure, som säger till TT den 18 augusti att viruset är 'relativt dåligt gjort.' Med det syftar han på att viruset inte lyckas skilja datorer med Windows 2000 från sådana med Windows XP, vilket ibland medför att den attackerade datorn kraschar. Runald själv tillämnar utan tvekan ett kvalificerat hackeromdöme (jämför punkt 5, ovan) då han bland annat menar att det inte är något allvarligt i sig att datorn kraschar. Det skulle antyda att Lovesan inte är något framstående verk av tekniskt kunnande. Samtidigt är tonen i det lilla meddelandet till Microsofts ägare Bill Gates är ganska tydlig. Avsändaren synes vilja påvisa de tekniska bristerna i Microsofts programvara och på något sätt därmed göra oss andra en tjänst.

Den makedonska webbsidan är uppenbarligen ett exempel på politisk aktivism. Om det också är ett hack beror på hur upphovsmännen har gått till väga. Verktygen för mer eller mindre automatisk webbkapning är fritt tillgängliga, och det är ingen nyhet att de används också för opinionsbildande ändamål. Om däremot en elegant och hittills okänd teknik har använts för att vinna tillträde till Daihatsus webbdator så kan det handla om ett hack.

Och: hur ska vi förhålla oss till dessa och andra exempel? Att i viss mån förstå motiven bakom en hackers handlingar, värdegrunden för den kultur han tillhör, är naturligtvis inte det samma som att godta eller stödja handlingarna. Det moraliska och juridiska dömandet sker på andra arenor med andra normer.

Virus, webbkapningar, dataintrång och annat som förknippas med hackers kan vara gjorda av många olika skäl. Det kan till exempel handla om att tjäna pengar genom brott, om politisk eller annan samhällelig aktivism, om nöjet i att ställa till besvär för andra, eller om att göra handlingar som får synliga resultat i massmedierna. Sådana motiv skiljer sig från det renodlade hackermotivet: att visa upp ett överlägset kunnande.

Men därmed vill jag inte säga att hackers aldrig gör sig skyldiga till brott. Naturligtvis kan samma person ha flera motiv för sitt handlande. Det är också så att det specialiserade kunnande som hackerkulturen besitter har ganska stor potentiell kraft. Det är kort sagt ganska användbart för andra syften, exempelvis ekonomiska brott eller aktivism. Om en aktivist har en hackerkompis så är det kanske inte så konstigt att de tillsammans prövar webbkapning som politisk metod.

Oavsett om hackerkulturen i sig innehåller brottsliga motiv eller inte, kan vi konstatera att den i viss mån är en motkultur. Den har ganska starka elitistiska inslag genom sin strikta meritokrati. Ett annat konkret exempel på elitism är det skriftspråk som används främst bland engelskspråkiga hackers och som utan att vara en kod faktiskt är ganska svårläst för oss andra. Både terminologin och skrivsättet är ganska egna – exempelvis använder man gärna ordet 'l33t' för att tala om sig själva (av det engelska ordet elite, stavas 'leet, skrivs med siffran 3 i stället för bokstaven E).



En av hackerkulturens kanoniska texter är det som kallas The Hacker's Manifesto. Det skrevs i mitten på åttiotalet, citeras fortfarande ofta, och måste sägas beskriva hackerkulturens kärna på ett utmärkt sätt. Här är ett utdrag som visar ganska väl i vilket avseende hackerkulturen kan sägas vara en motkultur.

This is our world now... the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.

Ett sådant synsätt kan ganska lätt förenas med bristande respekt för samhällets lagar och normer, och för demokratiskt fattade beslut.

Till sist: Varför har jag valt just sju punkter? Svaret är att nästa möjliga antal vore elva, och då skulle den här texten bli alldeles för lång. Om du förstår varför just talen sju och elva var aktuella, så har du också där ett exempel på ett vanligt element i hackerkulturen. Det är tänkt som ett slags skämt för de invigda, i det här fallet de matematiskt invigda (vilket är ett kunskapsområde som skattas ganska högt inom hackerkulturen). Om du inte förstår så ger det kanske också en känsla för vad kunskapsbaserad elitism kan innebära.

Mer detaljer, längre citat och en del lästips hittar du på webzone.k3.mah.se/k3jolo/HackerCultures om det skulle intressera. The Hacker's Manifesto citerar jag i sin helhet i bilagan som följer, då jag tror att den sammanfattar mycket av nyckeln till hackerkulturen.

OM FÖRFATTAREN

Jonas Löwgren arbetar som professor i interaktionsdesign vid området för Konst, kultur och kommunikation, Malmö högskola. Där sysslar han mest med design för konvergerande medier, interaktiv visualisering och informationsteknikens designteori. Han är inte någon hacker, eftersom riktiga hackers aldrig har kallat honom det (se punkt 3 ovan). Dock har han befunnit sig i närheten av hackerkulturen i drygt tjugo år, först som ett slags wannabe och senare som universitetslärare och forskarkollega. Mer info finns på webzone.k3.mah.se/k3jolo.



BILAGA: The Hacker's Manifesto

Texten nedan har cirkulerat i hackerkretsar i många år och kallas allmänt för The Hacker's Manifesto. Den publicerades först i det tongivande hacker-magasinet Phrack, #7 <www.2600.com/phrack07.html>.

The following was written shortly after my arrest...

\The Conscience of a Hacker/\

by +++The Mentor+++

Written on January 8, 1986

Another one got caught today, it's all over the papers. "Teenager Arrested in Computer Crime Scandal", "Hacker Arrested after Bank Tampering"... Damn kids. They're all alike.

But did you, in your three-piece psychology suit and 1950's technobrain, ever take a look behind the eyes of the hacker? Did you ever wonder what made him tick, what forces shaped him, what may have molded him?

I am a hacker, enter my world...

Mine is a world that begins with school... I'm smarter than most of the other kids, this crap they teach us bores me... Damn underachiever. They're all alike.

I'm in junior high or high school. I've listened to teachers explain for the fifteenth time how to reduce a fraction. I understand it. "No, Ms. Smith, I didn't show my work. I did it in my head..." Damn kid. Probably copied it. They're all alike.

I made a discovery today. I found a computer. Wait a second, this is cool. It does what I want it to. If it makes a mistake, it's because I screwed it up.

Not because it doesn't like me...

Or feels threatened by me...

Or thinks I'm a smart ass...

Or doesn't like teaching and shouldn't be here... Damn kid. All he does is play games. They're all alike.

And then it happened... a door opened to a world... rushing through the phone line like heroin through an addict's veins, an electronic pulse is sent out, a refuge from the day-to-day incompetencies is sought... a board is found.

"This is it... this is where I belong..."



I know everyone here... even if I've never met them, never talked to them, may never hear from them again... I know you all... Damn kid. Tying up the phone line again. They're all alike...

You bet your ass we're all alike... we've been spoon-fed baby food at school when we hungered for steak... the bits of meat that you did let slip through were pre-chewed and tasteless. We've been dominated by sadists, or ignored by the apathetic. The few that had something to teach found us willing pupils, but those few are like drops of water in the desert.

This is our world now... the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.

Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.

I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike.

