# Risker vid användning av USB-minnen och u3

JACOB LÖFVENBERG


FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1350 anställda varav ungefär 950 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömningen av olika typer av hot, system för ledning och hantering av kriser, skydd mot hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

FOI
Totalförsvarets forskningsinstitut
Ledningssystem
Box 1165
581 11 Linköping

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

www.foi.se

FOI-R--2078--SE
ISSN 1650-1942

Underlagsrapport
Oktober 2006

**Ledningssystem**

Jacob Löfvenberg

# Risker vid användning av USB-minnen och u3

FOI-R--2078--SE
ISSN 1650-1942

Underlagsrapport
Oktober 2006

Ledningssystem

| | | |
|---|---|---|
| **Utgivare**<br>FOI - Totalförsvarets forskningsinstitut<br>Ledningssystem<br>Box 1165<br>581 11 Linköping | **Rapportnummer, ISRN**<br>FOI-R--2078--SE | **Klassificering**<br>Underlagsrapport |
| | **Forskningsområde**<br>4. Ledning, informationsteknik och sensorer | |
| | **Månad, år**<br>Oktober 2006 | **Projektnummer**<br>F321 |
| | **Delområde**<br>41 Ledning med samband och telekom och IT-system | |
| | **Delområde 2** | |
| **Författare/redaktör**<br>Jacob Löfvenberg | **Projektledare**<br>Mikael Wedlin | |
| | **Godkänd av**<br>Rolf Andersson | |
| | **Uppdragsgivare/kundbeteckning**<br>Internt | |
| | **Tekniskt och/eller vetenskapligt ansvarig** | |


**Rapportens titel**

Risker vid användning av USB-minnen och u3


**Sammanfattning**

U3 är en ny teknik i samband med USB-minnen som ger möjlighet att ha sina data, tillämpningar och inställningar på USB-minnet. När ett u3-minne (USB-minne med u3) stoppas i värddatorn körs automatiskt ett startprogram på där användaren kan starta och administrera de program som finns på minnet. Det är också möjligt att byta startprogrammet mot nya versioner när sådana blir tillgängliga från tillverkaren. I praktiken är det dessvärre lätt för vem som helst att byta programmet mot vad som helst.

Kombination av automatisk programstart och möjlighet att byta programmet i u3-minnena är tyvärr problematisk ur säkerhetssynvinkel. En riktad attack mot värddatorn kan göras genom att byta programmet mot en hemgjord version som t.ex. installerar ett övervakningsprogram som vidarebefordrar känslig information till lämplig mottagare via Internet. Det är också möjligt att skapa virus som sprider sig via u3-minnen, ungefär som gamla tiders diskettvirus. Säkerhetsproblemen med u3-minnen är alltså påtagliga, särskilt med tanke på den stora spridningen som tekniken har.



**Nyckelord**

USB, u3, säkerhet, sårbarhet, auto run

| | |
|---|---|
| **Övriga bibliografiska uppgifter** | **Språk** Svenska |
| **ISSN** 1650-1942 | **Antal sidor:** 8 s. |
| **Distribution enligt missiv** | **Pris: Enligt prislista** |

| Issuing organization | Report number, ISRN | Report type |
|---|---|---|
| FOI – Swedish Defence Research Agency<br>Command and Control Systems<br>P.O. Box 1165<br>SE-581 11 Linköping | FOI-R--2078--SE | Base data report |
| | **Programme Areas**<br>4. C4ISTAR | |
| | **Month year**<br>October 2006 | **Project no.**<br>F321 |
| | **Subcategories**<br>41 C4I | |
| | **Subcategories 2** | |
| **Author/s (editor/s)**<br>Jacob Löfvenberg | **Project manager**<br>Mikael Wedlin | |
| | **Approved by**<br>Rolf Andersson | |
| | **Sponsoring agency**<br>Internal | |
| | **Scientifically and technically responsible** | |


**Report title (In translation)**

Risks in using USB flash drives and u3


**Abstract**

U3 is a new technology used in combination with USB flash drives. It makes it possible to keep applications, data and configurations on the flash drive. When a u3 stick (USB flash drive with u3) is connected to the host computer, a launch program is automatically run, in which the user can run and administrate the applications on the stick. It is also possible to update the launch program when new versions are made available by the manufacturer. Unfortunately, in practice it is easy for anybody do exchange the launch program for anything.

The combination of automatic program run and the possibility to exchange the launch program is problematic from a security point of view. An attack can be aimed at the host computer by exchanging the launch program for a program that installs a surveillance program, forwarding sensitive information over the Internet to a suitable receiver. It is also possible to create viruses which spread using u3 sticks, similar to floppy disk viruses. Thus, the security problems with u3 sticks are evident, especially considering how widely used the technology is.



**Keywords**

USB, u3, security, vulnerability, auto run

| Further bibliographic information | Language Swedish |
|---|---|
| **ISSN** 1650-1942 | **Pages** 8 p. |
| | **Price acc. to pricelist** |

# Introduktion

I början av 2005 introducerades en ny teknik i samband med USB-minnen. Tekniken kallas u3 och beskrivs som ett sätt att göra mjukvara, inställningar, lösenord mm. mer portabla. Detta sker genom att tillåta (speciellt anpassade) program, tillsammans med alla tillhörande filer, att installeras på USB-minnet. På detta sätt kan användaren köra sina program från USB-minnet på vilken lämplig dator som helst (Windows XP, Windows 2000 sp4 och senare, samt Windows Server 2003), och ta med sig hela sin miljö när han/hon tar med sig USB-minnet. I viss mån behöver programmen ändra på värddatorns systemkonfiguration, men u3-tekniken innebär att alla sådana ändringar återställs när användaren avslutar sitt arbete. När en u3-enhet sätts i USB-porten på en värddator startas automatiskt ett program som heter u3 Launchpad, se figur nedan, som har ungefär samma funktion som Windows startmeny, fast för u3-programmen som finns på USB-minnet. I u3 Launchpad kan användaren starta och administrera sina u3-program.


Figur: u3 Launchpads meny hos ett u3-minne

Under våren och sommaren 2006 började det komma allt fler rapporter på Internet om att vissa tillverkares USB-minnen med u3-funktion (u3-minnen) gick att använda för att på ett dolt sätt köra godtycklig kod på värddatorn. Detta skulle vara ett säkerhetsproblem, eftersom USB-minnen ofta tolkas som en passiv minnesenhet, utan möjlighet att själv starta program. För en attackerare skulle det räcka med att be innehavaren av måldatorn om att få ta del av, eller dela med sig av, någon oskyldig fil. När u3-minnet sätts i måldatorn för att kunna flytta filen, så gör det samtidigt, och omärkligt, sin attack.

# Teknisk beskrivning

Det finns två tekniker som är väsentliga i sammanhanget. Den ena är USB, som är en standard för en mycket generell, extern buss som används på i stort sett alla PC-datorer idag. Den andra är u3-tekniken själv.

## USB

USB (Universal Serial Bus, se www.usb.org) är en mycket allmänt spridd standard för att koppla samman elektroniska enheter. Ursprungligen designades den för att användas i datorsammanhang, men den har blivit så populär att den nu används i allt från mobiltelefoner till TV-apparater. Till datorer kan man via USB koppla bland annat tangentbord, möss, CD-spelare, hårddiskar, nätverkskort, TV-kort och fingeravtrycksläsare.

När en enhet kopplas till en dator via USB så sker en mängd saker. Bland annat identifierar sig den inkopplade enheten för datorn, och berättar vilken typ av apparat det är. Det finns inget som hindrar att det via samma fysiska USB-kontakt kopplas in mer än en sorts enhet. Till exempel finns det kombinerade tangentbord och mus, som delar på en sladd och en kontakt, vilket kan vara praktiskt om antalet USB-portar i datorn är begränsat.

### U3

Ett u3-minne erbjuder användaren två olika funktioner. Dels fungerar det som ett vanligt USB-minne där man kan lagra valfri data, dels innehåller det u3-program som kan startas med u3 Launchpad. Det kan påpekas att u3-programmen visserligen finns i det vanliga USB-minnet, men att de är dolda genom att de är definierade som ”hidden” i Windows.

För att få u3 att fungera rent tekniskt så identifierar sig ett u3-minne dessutom som en CD-ROM-enhet. Detta innebär att när u3-minnet sätts i värddatorn så tillkommer en flyttbar diskenhet (USB-minnesfunktionen) och en CD-ROM-enhet med några enstaka megabyte data på. Orsaken till denna lösning är att det normalt bara är CD-skivor som automatiskt kan starta program på en Windowsdator. Genom att låta USB-minnet utge sig för att vara en CD-ROM-enhet så kan u3 Launchpad startas automatiskt när u3-minnet sätts i värddatorn.

De flesta u3-minnen som vi studerat tillåter uppgradering av systemmjukvaran för u3. Detta sker genom att välja ett särskilt menyalternativ i u3 Launchpad. Detta får användarens webb-läsare att dirigeras till en webb-sida där det framgår om det finns en nyare version av mjukvaran. Vad som händer sedan har vi bara kunnat studera för Sandisks u3-minnen, eftersom de är de enda vi hittat som har en nyare mjukvaruversion tillgänglig. I Sandisks fall så hämtas, dolt för användaren, ett program som heter LPinstaller.exe. När detta program körs hämtar det den senaste versionen av systemmjukvaran via en http-uppkoppling över Internet, från en URL hos Sandisk. LPinstaller uppdaterar sedan u3-minnet och avslutas.

## Säkerhet

### U3

Det kan hävdas att u3-minnen inte tillför några nya säkerhetsproblem. Program som autostartar har alltid varit ett säkerhetsproblem, oavsett vilket medium programmet har förflyttats via. Det enda som är nytt är just mediet, minnespinnen. De flesta användare har vant sig vid att betrakta USB-minnen som en passiv produkt, som visserligen kan innehålla program, men som inte startar dem utan att användaren vill det. Det vi måste göra är att börja betrakta USB-minnen, om inte som potentiella hot, så åtminstone med tillbörlig skepsis. Ett u3-minne kan konfigureras att starta sina u3-program så fort det sätts i värddatorn. Den enda varning användaren får är att u3 Launchpad startas synligt. Vad som händer i övrig går inte att avgöra.

Något som ytterligare försvårar säkerhetsproblemen kring u3-minnen är att det, åtminstone i fallet med vissa tillverkare, går lätt att byta ut u3 Launchpad mot valfritt program. Om det görs på ett väl valt sätt så syns ingen händelse när u3-minnet sätts i värddatorn, utan det är lätt för användaren att tro att det är ett helt vanligt USB-minne som kopplats in. Detta hindrar inte att det i förväg förberedda programmet körs, utan att användaren har någon möjlighet att detektera det.

En annan sak är att om u3 blir vanligt så kommer användarna att vänja sig vid att via externa media flytta program till datorn, och sedan köra dem. Detta kan medföra att användarna inte ser detta som ett problem, och därför blir mindre försiktiga när det gäller att starta okända program. Vi vill knappast ha användare som ser externt tillförda program som något oproblematiskt.

### Virus via U3

I och med att det inte bara är möjligt att automatiskt starta program från u3-minnen, utan också lätt att skriva över det automatstartande programmet, så är det möjligt att använda dem för att sprida virus på ett sätt som påminner om de gamla diskettvirusen. Ett infekterat u3-minne kan innehålla ett virusprogram som infekterar värddatorn, och denna kan i sin tur infektera alla u3-minnen som stoppas i fortsättningsvis. För att detta ska bli möjligt i praktiken krävs en relativt stor population av u3-minnen, något som tycks kunna bli verklighet ganska snart.

### USB

Det grundläggande problemet med u3-minnen handlar egentligen om USB-standarden. Problemet möjliggörs av att en enskild, fysisk apparat kan utge sig för att vara flera enheter inför datorn, och det finns ingen möjlighet för användaren att genomskåda detta innan apparaten kopplas in (och inte nödvändigtvis efteråt heller). Här fungerar u3-minnen som ett tydligt exempel. Ett u3-minne ser ut som ett USB-minne, men utger sig för att vara både ett USB-minne och en CD-ROM-enhet. Det användaren ser är inte detsamma som det datorn ser. I många fall installerar Windows dessutom nödvändiga drivrutiner själv, helt automatiskt, och USB-enheterna får full funktionalitet utan att användaren behöver göra något alls med datorn.

Rent allmänt är det alltså möjligt att locka en användare att via en USB-port koppla in en apparat genom att låta apparaten ha lämpligt utseende och funktion. Gentemot datorn kan apparaten sedan identifiera sig som någon ytterligare enhet, som har möjlighet att göra helt andra saker än vad en apparat av denna typ normalt skulle kunna. Genom att agera tangentbord och/eller mus skulle apparaten helt kunna ta över datorn vid någon lämplig tidpunkt, när användaren rimligen inte tittar på skärmen.

## Experiment

För att undersöka hur u3-minnen uppför sig i praktiken så har vi studerat sex olika sorters u3-minnen från fyra olika tillverkare: Intuix, Kingston, Sandisk och Verbatim. Alla utom ett att minnena erbjöd användaren möjligheten att uppgradera systemmjukvaran för u3, men bara en av tillverkarna hade ny mjukvara tillgänglig att uppgradera med. Utgående från en metod som beskrivits på Internet (http://www.cse.msstate.edu/~rwm8/hackingU3/), studerade vi hur uppgraderingsprogrammet kommunicerade med sina servrar. Vi hittade då programmet LPinstaller.exe som används för att uppdatera systemmjukvaran. Med hjälp av detta var det enkelt att byta ut systemmjukvaran mot en hemgjord version. I demonstrationssyfte skapades ett u3-minne som, när det sätts i värddatorn, inte gör något synligt förutom att byta ut bakgrundsbilden i Windows.

Vi har studerat hur man kan undvika att Windows startar program automatiskt från externa enheter, och speciellt u3-minnen. Hur det går till beror på exakt vilken sorts enhet man vill undvika automatisk start från, och om det ska vara en permanent lösning eller inte. Hur det går till finns beskrivet i ett senare avsnitt.

## Analys

Grundproblemet är, som vi ser det, USB-standarden. Det är möjligt för en fysisk enhet att utge sig för att vara flera olika enheter inför datorn, utan att användaren vet om det. Eftersom USB-standarden är så allmän finns det enhetstyper som kopplas in via USB som har vidsträckta rättigheter att undersöka och hantera sin värddator. Säkerhetsmässigt har detta problem begränsats i praktiken av att det krävs en del kunskap och finess för att tillverka USB-enheter med lämplig funktion och trovärdigt utseende, och samtidigt lyckas övertyga rätt person om att koppla in enheten i sin dator. Vår bedömning är dock att tillverkningen tekniskt skulle kunna utföras av en

duktig elektronikamatör med någon eller några veckors arbete, så för en motiverad attackerare finns inget stort hinder att konstruera denna typ av enheter.

Det som istället har hänt i och med introduktionen av u3-minnen och den stora populäritetet de uppnått, är att ett specialfall av problemet har nått en global spridning och stor penetration på mycket kort tid. Plötsligt är det möjligt för betydligt många fler att konstruera farliga enheter, och dessutom genom ren mjukvarumanipulation. Att dessa enheter ser ut och kan användas som vanliga USB-minnen gör dessutom att det är lätt för en attackerare att motivera varför han/hon vill stoppa enheten i måldatorn. USB-minnen används ju just för att hämta och lämna filer på olika datorer. Möjligheten att använda u3-minnen som bärare av virus är också något som inte är en automatisk följd av de grundläggande problemen med USB. Som vi ser det räcker detta för att säkerhetsmässigt se u3-minnen som ett nytt och eget problem som behöver hanteras på något sätt.

# Rekommendationer

Ur säkerhetssynvinkel är varje typ av automatiskt startande program från externa enheter ett problem. I det avseendet är u3-minnen inget genuint nytt, men aktualiserar och förstärker problemet.

Vi rekommenderar därför följande:

- att automatiskt startande av program (på engelska: auto run) förhindras i så stor utsträckning som aktuellt operativsystem tillåter
- att u3-minnen inte används om USB-minnen kan användas istället
- att det noteras att USB-gränssnittet inte är säkert i sig, utan att man måste lita på den apparat man kopplar in till sin dator.

# Att undvika automatstartande program i Windows

Det enklaste sättet att undvika automatstart i Windows är att trycka, och hålla ner, shift-tangenten när CD-skivan eller u3-minnet sätts i. När skivan eller minnet hittats och monterats av Windows kan tangenten släppas upp igen utan risk. Denna teknik hindrar både CD-skivor och u3-minnen från att automatiskt starta program.

I centralt organiserade nät kan man ändra i Windows ”Group Policies” och därigenom hindra både CD-skivor och u3-minnen från att automatiskt starta program. Ändringar i Windows ”Group Policies” utförs i så fall av den centrala systemadministrationen.

Det går även att ändra den lokala policyn, på den egna maskinen. För att göra det måste man vara administratör, och göra följande:

- Välj Startmenyn-Run
- Skriv gpedit.msc och klicka ”OK”
- På den vänstra panelen, välj ”Computer Configuration”-”Administrative Templates”-”System”
- Dubbelklicka på ”Turn off Autoplay” i den högra panelen (nästan längst ner)
- Välj ”Enabled”.

Det är också möjligt att göra ändringar direkt i Windows register för att förhindra automatstart av program. Den metod som rekommenderas av Microsoft, och många andra, är att sätta [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\CdRom] "Autorun"="0". Detta hindrar dock bara vanliga CD-ROM-enheter att automatiskt starta program; u3-minnen påverkas inte. För att förhindra även u3-minnen från att automatiskt starta program måste man även se till att [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer] "NoDriveTypeAutoRun"="B5". Endast om båda dessa värden är ändrade hindras u3-minnena.

Genom att öppna ”My Computer”, högerklicka på en enhet som stödjer flyttbart minne, välja ”Properties” och sedan fliken ”AutoPlay”, så kan man för ett antal olika medietyper välja vad datorn ska göra när sådant innehåll blir tillgängligt i enheten. Detta är *inte* samma sak som automatstartande program, utan bara ett sätt att få Windows att starta ett visst program när en viss sorts data blir tillgänglig. Ett exempel är att det kan vara praktiskt att ens CD-bränningsprogram startar automatiskt när en tom CD-skiva sätts i CD-brännaren.

# Vidare arbete

Det skulle vara intressant att granska specifikationen för u3. Finns det ett standardiserat sätt som måste användas för att göra uppgraderingarna av systemmjukvaran, eller är det tillverkarspecifikt? Finns det någon möjlighet för u3-minnet att verifiera att uppgraderingen verkligen kommer från tillverkaren? Orsaken till att vi inte studerat specifikationen är att licensavtalet som måste accepteras innan man får ta del av den, inte tillåter sådan granskning.

Att USB medför vissa säkerhetsproblem har vi diskuterat tidigare. Dock har vi inte analyserat på djupet hur omfattande dessa är, vilket skulle kunna vara värdefullt att göra. Finns det problem även hos andra busstandarder som Firewire, PC card och liknande system?

Vad gäller rekommendationer om hur säkerhetsmedvetna användare bör förhålla sig till USB-minnen så finns det några saker som skulle kunna studeras ytterligare. Det kommer allt fler minnen som har någon typ av inbyggt skydd för de data som ligger på minnet. Vanligast är biometrisk autentisering och/eller någon sorts kryptering. Detta är intressant och förtjänar noggrannare studier.

# Webbadresser

Information om hur Sandisks u3-minnen hackades finns på:
http://www.cse.msstate.edu/~rwm8/hackingU3/

Information om u3 kan man hitta på u3:s officiella webbplats:
http://www.u3.com

Exempel på hur en attackerare skulle kunna utnyttja ett u3-minne:
http://blog.xavier.ashe.com/blog/_archives/2006/9/10/2314043.html?seenIEPage=1
http://www.hak5.org/wiki/USB_Switchblade
http://www.thesecure.net/blog/archives/000349.html