Svar till SSNf angående projekt SKA 3.1, Säker Kund Anslutning

12 Mars 2008
Version 3.0

Innehållsförteckning

1 Bakgrund

Cisco har alltid varit myckget fokuserat på säkerhet och säkerhetsfrågor. Vi jobbar nära våra kunder och lägger alltid högsta prioritet på att förebygga och åtgärda eventuella säkerhetsproblem i våra kunders nät.
Cisco satsar även mycket på att förstå och analysera nätverksteknologier och lösningar med avseende på säkerhet och säkerhetsrisker, allt för att minimera att våra kunder skall drabbas av allvarliga problem.
Den säkerhetsrisk som nu uppmärksammats av SSNf, i form av ”ARP-spoofing”, har vi känt till sedan vi började bygga ETTH nätverk i början av år 2000. Vi har ett flertal sätt att lösa problematiken på, så att de kunder som väljer att bygga sina ETTH nätverk med produkter från Cisco, inte skall behöva vara oroliga för att slutanvändarna skall bli hackade på grund av bristande funktionalitet i nätverket. Nytt för denna version (3.0) är att även protokollen UPnP och IPv6 skall skyddas/filtreras.

2 Lösningar

2.1 DAI

Det allra bästa sättet att skydda sig mot denna säkerhetsrisk är att se till att det protokoll som primärt används för attacken skyddas/kontrolleras mot falsk information. Protokollet i det här fallet är ARP (Adress Resolution Protocol) . ARP är standardiserat men saknar egen inbyggd skyddsmekanism som gör att falska paket ej kan skickas. I detta fall måste nätet ebjuda användare skydd mot falska ARP paket.
Cisco har därför i sina intelligenta access switchar en inbyggd funktion som skyddar mot bland annat sådana falska ARP paket, funktionen heter DAI (Dynamic ARP Inspection), läs mer om den på länken nedan:
(med CCO login):
http://www.cisco.com/en/US/partner/products/ps6580/products_configuration_guide_chapter09186a0080513330.html#wp1041210
(utan CCO login):
http://www.cisco.com/en/US/products/ps6580/products_configuration_guide_chapter09186a0080513330.html
Om man använder DAI i access switcharna i sitt bredbandsnät är man helt skyddad mot ARP-spoofing attacker eftersom alla ARP-paket kontrolleras av switchen innan de skickas vidare in i nätet och alla ARP-paket som är falska kastas direkt av switchen.

De swichar som supportar funktionen DAI är:
Cisco ME 3400 (Metro Access SW Licence)
Cisco Catalyst 3750
Cisco Catalyst 3560
Cisco Catalyst 3550
Cisco Catalyst 4500

Cisco Catalyst 6500
Cisco 7600

2.2 PVLAN

Ett annat sätt att skydda sig mot ARP-spoofing är att använda funktionen PVLAN, (Private Virtual LAN). Med PVLAN funktionen så Layer-2 isolerar man samtliga användare som tillhör samma L2 broadcast domän från varandra så att inga paket kan skickas direkt mellan två användare utan att passera en router. Detta gör att protokoll som ARP inte kan nyttjas för att lura användare att skicka sin trafik fel väg genom nätet. PVLAN fungerar mellan switchar och kan användas i både ring- och stjärn-designer. Tillsammans med funktionen Sticky ARP (beskriven nedan) i routrarna så skyddas användarnas trafik i båda riktningar.

För mer information om PVLAN se vidare på:
(med CCO login):
http://www.cisco.com/en/US/partner/products/ps6580/products_configuration_guide_chapter09186a008051337d.html#wp1038379
(utan CCO login):
http://www.cisco.com/en/US/products/ps6580/products_configuration_guide_chapter09186a008051337d.html

Switchar som supportar funktionen PVLAN är:
Cisco ME 3400 (Metro Base SW License)
Cisco Catalyst 3750
Cisco Catalyst 3560
Cisco Catalyst 4500
Cisco Catalyst 6500
Cisco 7600

2.3 PVLAN Edge, Protected Port

I nät med äldre eller lite enklare access switchar från Cisco finns funktionen Protected Port / PVLAN Edge att tillgå för att säkra användarna mot ARP-spoofing. Protected Port funktionen fungerar likt funktionen PVLAN beskriven ovan men med den begränsningen att Layer-2 isoleringen endast fungerar inom en switch eller i en ej redundant länk av switchar. Vill man nyttja funktionen Protected Port i en ring-design månste varje switch i ringen ha ett eget VLAN för att inte Layer-2 paket (inkl ARP) skall kunna skickas mellan användare. Att VLAN-separera på switch nivå brukar dock inte vara några problem för

Operatörer/Stadsnät och Cisco har flera mycket stora kunder som nyttjar detta för att säkra upp sina nät mot bland annat ARP-spoofing.
Tillsammans med funktionen Sticky ARP (beskriven nedan) i routrarna så skyddas användarnas trafik i båda riktningar.

Det är ej att rekomendera att använda funktionen Protected Port om man har access-switchar i sitt bredbandsnät som klarar av någon av de funktioner som beskrivits ovan då de ger ett bättre och mer flexibelt skydd mot ARP-spoofing.

För mer information om Protected Port se vidare på:
(med CCO login):
http://www.cisco.com/en/US/partner/products/hw/switches/ps646/products_configuration_guide_chapter09186a00804760e7.html#wp1158863
(utan CCO login):
http://www.cisco.com/en/US/products/ps6580/products_configuration_guide_chapter09186a00805133b0.html#wp1029319

Switchar som endast supportar funktionen Protected Port / PVLAN Edge är:
Catalyst 2950
Catalyst 3500xl

2.4 Per Interface Sticky ARP

Funktionen Sticky ARP förhindrar att en användare kan förvanska/förfalska den tabell en router använder för att få information om hur den hittar en klient på ett Ethernet LAN, dvs ARP-tabellen. Om informationen i denna tabell är förfalskad genom att en hacker utnyttjat ARP-protokollets svagheter och gjort en så kallad ARP-spoofing attack mot routern kommer routern att skicka samtliga datapaket tänkt till en viss användare som är attackerad till hackerns dator och kan där analyseras efter tex lösenord mm.
Med hjälp av funktionen Sticky ARP ser routern till att en användares information i en ARP-tabell inte kan bli förfalskad och därigenom kommer routern aldrig att skicka information tänkt till en viss användare till en hackers dator.

För mer information om Sticky ARP se vidare på:
(med CCO login):
http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1838/prod_bulletin0900aecd80327e21.html
(utan CCO login):
http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a0080435872.html#wp1139323

2.5 PACL

Funktionen PACL (Port Access Control List) kan filtrera datapaket som skickas in eller ut från en användarport. Att använda access filter är inte en lösning för problemet med ARP-spoofing eftersom man ej kan filtrera bort ARP-paket helt och hållet eftersom de behövs för att kommunikation över ett Ethernet baserat nät skall fungera. Eventuellt kan man nyttja PACL:er som en kortsiktig workaround för problmet eftersom det stoppar möjligheten att utföra långvaraiga man-in-the-middle attacker så som de hacker verktyg som finns tillgängliga idag nyttjar problemet, dock har man inte ett skydd mot ARP-spoofing med PACL:er eftersom felaktiga ARP-paket kan skickas till andra användare i nätet och även om inte attacken fungerar som den är tänkt så stoppar man kommunikationen (DOS, Denial of Service) för de användare man försöker ARP-spoofa.

För mer information om PACL:er se vidare på:
(med CCO login):
http://www.cisco.com/en/US/partner/products/ps6580/products_configuration_guide_chapter09186a00805133bf.html#wp1140852
(utan CCO login):
http://www.cisco.com/en/US/products/ps6580/products_configuration_guide_chapter09186a00805133bf.html

3 Andra säkerhetsrisker och hur man skyddar sig mot dem.

Vi vill gärna ta tillfället i akt att poängtera att ”ARP-spoofing” bara är ett av de allvarliga säkerhetsproblem som måste hanteras när man bygger IP-nät. Nedan beskrivs några andra viktiga säkerhetsproblem som också måste beaktas:

3.1 IP-hijacking:

Eftersom en användares identitet på Internet består av en IP-adress är det viktigt för en operatör eller stadsnätsägare att alltid veta vem som är ansvarig för den IP-adressen vid en given tidpunkt för att kunna lösa spårbarhet om det skulle vara så att myndigheterna behöver veta vem det är som tex har hackat eller gjort andra brott på Internet. Eftersom ett IP-nummer ofta är det enda som identifierar en användare är det viktigt att nätet inte tillåter att tex en hacker kapar eller tar över en IP-adress från en annan användare och därför utger sig för att vara någon annan när han tex begår ett brott via internet. En funktion som löser detta väldigt effektivt och samtidigt är väldigt enkel och dynamisk är IPSG, IP Source Gurad. IPSG skapar automatiskt filter listor i access-switcharna som endast tillåter de IP-adresser som en användare fått tilldelats sig. Eftersom allting i funktionen IPSG sker dynamiskt behöver inte mer tid läggas för att operationellt styra nätet än tidigare samtidigt som man har fått ett betydligt bättre skydd mot så kallad IP-hijacking. IPSG tillsammans med DAI ger en väldigt bra säkerhet för användare i bredbandsnät eftersom de hindrar hackare och andra brottslingar från att både stjäla en användares identitet (IP-hijacking) och agera som en MiM (Man-in-the-Middle) nod. När en klients DHCP Lease tid har gått ut rensar switchen gamla IP-addresser via en process som körs automatiskt i bakgrunden, switchens kontroll av MAC-adressen samt DHCP servrarnas sk. ”grace period” är en del av skyddet.

3.2 Användarport-konfiguration:

Man bör noga överväga vilken typ av information som skall vara tillgängling på användarportsnivå. Cisco rekommenderar att blockera information som kan användas i skadligt syfte och som inte fyller någon funktion för normala slutanvändare.

3.2.1 CDP:

Det har sedan länge varit en rekomendation från Cisco att stänga av CDP, Cisco Discovery Protocol på användar-portar då informationen i CDP

paket kan avslöja en hel del för en hackare om vilken utrustning han är inkopplad på mm.

3.2.2 STP:

Det har sedan länge varit en rekomendation från Cisco att stoppa all utgående och filtrera bort all inkommande STP, Spanning Tree Protocol, trafik. Det finns inga skäl att skicka ut STP information till en användare och inte heller vill man att en användare skall kunna generera STP trafik som switchen skall agera på.

3.2.3 Switchport block multicast:

En användar-port bör ej skicka ut data paket som inte är skickat till en specificerad användare. Det gäller både multicast och unicast trafik (se nedan). All trafik som skickas ut på en användar port kan analyseras av en eventuell hacker för att ge information om vilka tjänster, användare, funktioner, applikationer mm som nyttjas i nätet. Med denna information kan sedan en hacker försöka lansera attacker mot osäkra användare och system. Med funktionerna Switchport block multicast och Switchport block unicast ser switchen till att endast trafik riktad till en specificerad användare skickas ut på den användarens access-port. All annan trafik, samt trafik till okända användare (så kallad flooding) stoppas av switchen.

3.2.4 Switchport block unicast:

Se Switchport block multicast ovan.

4 Filtrering och UPnP

4.1 Filtrering i Access Switchar

Normalt sätt används automatiska filterings funktioner i Access switchar för Stadsnät och Bredbandsnät. Dessa funktioner är PVLAN (Private VLAN) eller Protected Port. Den funktionen som de ger är full filtrering/blockering av all Layer-2 trafik mellan användare inom samma VLAN (för Protected Port, inom samma VLAN inom samma switch). Med all trafik menas både Layer-2 unicast och multicast trafik.
Denna filtrering/blockering av Layer-2 trafik mellan två användare skyddar mot all typ av attack mellan användare i stadsnätet samt skyddar det mot öppna protokoll som är tänkta att hjälpa användare inom sitt hemma nät, UPnP är ett sådant exempel.
Skulle man ej vilja använda de automatiska filterings funktioner enligt ovan så supportar Cisco i sina rekomenderade Access Switchar för stadsnät och bredbandsnät filtrerings funktioner per port (Port access lista) och per VLAN (VLAN access lista). Med hjälp av dessa filterfunktioner kan en administratör själv bestämma vilken trafik som skall tillåtas från en användarport. Dessa filter kan filtrera på både Layer-2 och Layer-3 information och självklart hanteras både Unicast och Mulitcast trafik. Det går självklart att kombinera dessa filter med andra skydd mot t.ex. ARP-spoofing mm. Exempel på hur ett sådant filter skulle se ut för en port ansluten mot en bredbandsanvändare finns under punkt 4.1.1 nedan.

4.1.1 Filtreringsexempel

```
ip access-list extended BLOCK-UNWANTED-IP-TRAFFIC
   permit igmp any any
   deny   ip any 224.0.0.0 15.255.255.255
   permit ip any any
```

4.2 UPnP skydd i Stadsnätet

UPnP är ett protokoll för att förenkla visionen om det digitala hemmet. För att personer med ringa eller som helt saknar kunskaper om data nätvärk och hur man säkert och effektivt ansluter enheter med varandra enkelt skall kunna köpa och installera utrustning behövs hjälpmedel som t.ex. UPnP protokollet.
Dessa protokoll är utvecklade för att endast kommunicera med enheter ägda av samma person och/eller företag. På grund av detta är det mycket viktigt att inte dessa protokoll skickas via Stadsnätet och Bredbandsnätet mellan användare som på grund av det kan komma att koppla samman sina privata enheter, som t.ex. nätverks skrivare och nätverks hårddiskar med okända användare på samma stadsnät och råka ut för obehagligheter pga detta.

4.2.1 UPnP filtrering

Att filtrera UPnP är mycket enkelt i Access Switchar från Cisco. Rekomenderade funktioner som PVLAN stoppar UPnP automatiskt från att sprida sig mellan användare inom stadsnätet. Vill man själv skapa filters för att stoppa dessa protokoll så kan port access listor enligt ovan användas. Dessa filter fungerar tillsammans med andra skyddsmekanismer mot ARP-spoofing etc för att få ett komplett skydd i Stadsnätet.

4.3 IPv6

Ipv6 är idag inte speciellt vanligt förekommande på det publika internet och är helt avstängt i de flesta svenska bredbandsnät. IPv6 trafik är därför EJ något som man vill att kunder skickar in i bredbandsnäten pga ökade risker för ”hacking” mellan användare. Nyare persondatorer har ofta en IPv6 protokollstack förinstallerad och därför kan ett extra skyddslager i bredbandsaccessen vara nödvändigt för att skydda kunderna mot attacker mot den ”stacken”.

4.3.1 IPv6, Skydd mot avlyssning etc

Genom att använda de funktioner som beskrivits ovan stoppas all möjlighet för en kund att genom IPv6 komma åt information från andra kunder i bredbandsnätet oavsett om en kund avsiktligt eller oavsiktligt startat IPv6 på sin dator.