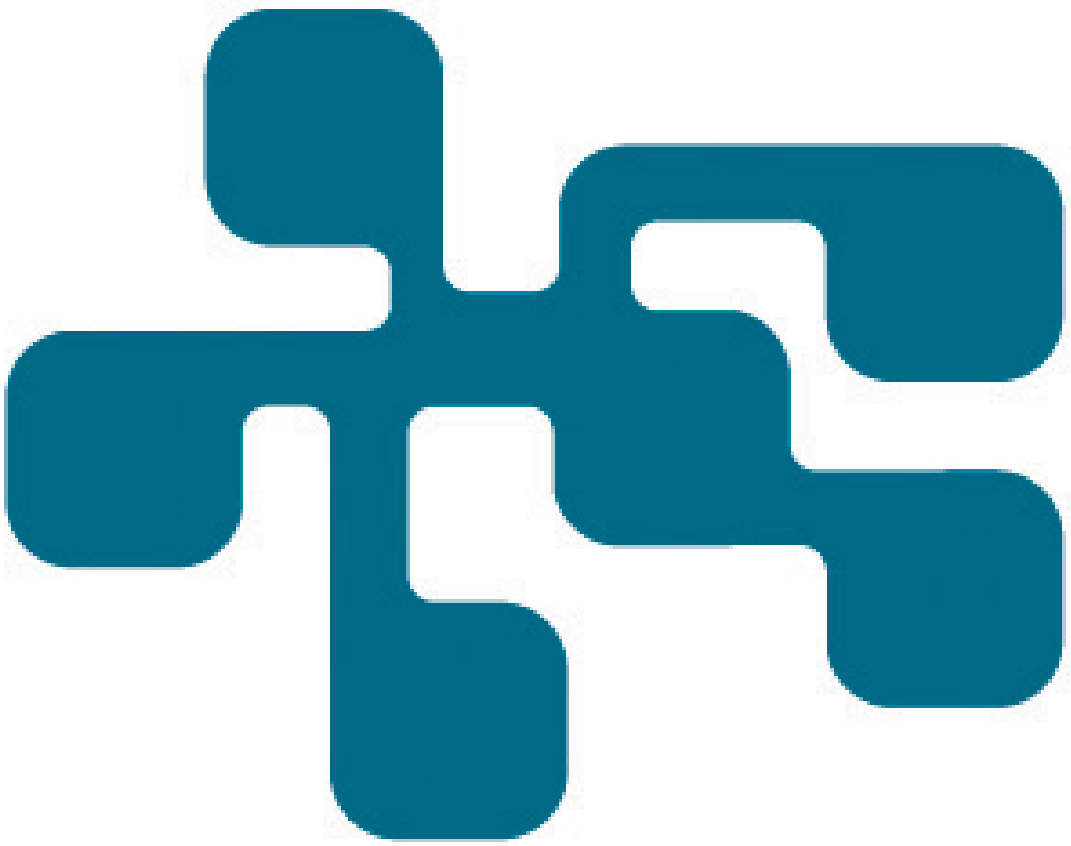
NCS3 - VLAN som separationsmetod för industriella styrsystemsnät

ARNE VIDSTRÖM OCH TOMMY GUSTAFSSON

FOI
MSB



FOI-R--4070--SE
MSB 2014-1131
ISSN 1650-1942

Mars 2015

Arne Vidström och Tommy Gustafsson

VLAN som separationsmetod för industriella styrsystemsnät

Titel	VLAN som separationsmetod för industriella styrsystemsnät
Title	VLAN as a method of isolation for industrial control system networks
Rapportnr/Report no	FOI-R--4070--SE
Månad/Month	Mars/March
Utgivningsår/Year	2015
Antal sidor/Pages	15
ISSN	1650-1942
Kund/Customer	MSB
Forskningsområde	4. Informationssäkerhet och kommunikation
FoT-område	
Projektnr/Project no	E3239607
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Informations- och aerosystem

Sammanfattning

Industriella styrsystem separeras ibland från kontorsnät med hjälp av VLAN (Virtual Local Area Networks). Förfarandet gör det möjligt att ha ett fysiskt nätverk med flera logiskt separerade delar. Här finns potentiellt en risk, om separationen mellan de logiska näten inte är tillräckligt robust. I dagsläget råder delade meningar om användningen av VLAN som separationsteknik för säkerhetsändamål. I denna studie undersökte vi frågan om hur tillförlitlig separationen mellan olika VLAN egentligen är. Vi kunde inte påvisa några risker för läckage mellan korrekt uppsatta VLAN. Det bör dock poängteras att en korrekt konfiguration är av största vikt för att uppnå detta resultat. Vissa switchmodeller visade sig dessutom ha egenheter som det är mycket viktigt att vara medveten om. Slutligen vill vi betona att den teoretiskt sett allra högsta säkerhetsnivån uppnås med hjälp av fysiskt separerade nätverk. I anläggningar där maximal säkerhet eftersträvas bör alltså fysisk separation användas istället för logisk separation med hjälp av VLAN.

Nyckelord: VLAN, SCADA, säkerhet, industriella styrsystem, switchar

Summary

Industrial control systems are sometimes separated from administrative networks by the utilization of VLAN (Virtual Local Area Network) technology. This way it is possible to have one physical network with two logically separated parts. There is however a potential risk if the separation between the logical networks is not sufficiently robust. At present there is a difference of opinion about using VLANs as a security technology. Central to our study was the question of exactly how robust the separation between VLANs really is. We were unable to unveil any actual risks of leakage between correctly configured VLANs. However, it should be pointed out that a correct configuration is of uttermost importance for this result. In addition, some switch models turned out to have quirks that are highly important to be aware of. Finally it should also be pointed out that at least in theory, the highest level of security is reached through physical separation of networks. It follows that physical separation should be used instead of VLAN separation whenever a maximum level of security is desired.

Keywords: VLAN, SCADA, security, industrial control systems, switches

Innehållsförteckning

1 Inledning

VLAN (Virtual Local Area Networks) är en teknik som används för att logiskt sektionera nätverk på ett sådant sätt att ingen nätverkstrafik ska kunna passera mellan de olika sektionerna. I ett nätverk med bara en switch kan olika VLAN knytas till olika portar på switchen. Till exempel kan port 1-5 utgöra ett VLAN medan port 6-10 utgör ett annat VLAN. Två eller flera switchar kan också sammanbindas via så kallade trunkar – anslutningar mellan switcharna där trafiken märks efter vilket VLAN den tillhör. På så vis kan ett VLAN sträckas ut över flera switchar.

Industriella styrsystem separeras ibland från kontorsnät med hjälp av VLAN. Förfarandet gör det möjligt att ha ett fysiskt nätverk med två logiskt separerade delar. Detta kan ge både praktiska och ekonomiska fördelar, men samtidigt utgör det potentiellt en risk om separationen mellan de logiska näten inte är tillräckligt robust.

Det råder delade meningar om användningen av VLAN som separationsteknik för säkerhetsändamål. Svagheter har identifierats tidigare och en del tekniker anser att VLAN inte är en säkerhetsfunktion. Andra tekniker påpekar att de gamla svagheterna inte längre är aktuella, utan bara rör mycket gamla switchar. De anser att VLAN visst kan betraktas som en säkerhetsfunktion. Debatten kan exemplifieras genom Question of the Week #24 på IT Security Stack Exchange där åsikterna går isär.[1]

I denna studie undersökte vi frågan om hur tillförlitlig separationen mellan olika VLAN egentligen är. Vi testade switchar från några olika tillverkare - både större och mindre. Syftet var inte att peka ut exakta modeller och firmwareversioner som säkra respektive osäkra, utan att istället ge en övergripande bild av säkerhetsläget när det gäller VLAN. Men en sådan bild måste självklart baseras på ett urval av konkreta tester av konkret utrustning för att vara någorlunda tillförlitlig.

[1] S. Pack, IT Security Stack Exchange, *QotW #24: Why do people tell me not to use VLANs for security?*, 2012-04-20, hämtad 2015-02-02, <http://security.blogoverflow.com/2012/04/qotw-24-why-do-people-tell-me-not-to-use-vlans-for-security/>

2 Metod

2.1 Övergripande testupplägg och begränsningar

Testerna utfördes dels med en ensam switch och dels med två switchar med en trunk mellan sig. Samma tester utfördes i båda fallen och den enda skillnaden var positionen där lyssningen efter eventuellt genomsläppt trafik skedde. Med en ensam switch genomfördes lyssningen på ett annat VLAN än där testtrafiken skickades in. Med två switchar utfördes lyssningen istället på trunken mellan dem.

Alla switchar konfigurerades med två VLAN - numrerade 21 respektive 22. Trafik skickades in på en port tillhörande VLAN 21. Lyssning utfördes samtidigt, antingen på en port tillhörande VLAN 22, eller på trunken mellan switcharna. Endast VLAN 22 hade sträckts vidare till den andra switchen i fallet med två switchar.

Varje switchmodell testades på två olika sätt - en utan trunkning och en med trunkning. Varje sådant deltest bestod av 13 olika testfall som beskrivs i detalj i kapitel 2.2. Vilka switchmodeller som användes framgår när resultaten presenteras i kapitel 3.

Testtrafiken genererades med hjälp av ett antal program skrivna i C. Dessa kördes på en dator med FreeBSD 9.2 och utnyttjade BPF (Berkeley Packet Filter) för att kunna skicka råa Ethernetramar ut på nätverket. Flaggan `BIOCGHDRCMPLT` sattes till ett för att inte FreeBSD skulle fylla i käll-MAC-adressen automatiskt. Den är annars satt till noll som default i FreeBSD.

Lyssningen genomfördes med hjälp av WireShark 1.6.7 i Windows 7. Ett potentiellt problem när man lyssnar på taggad VLAN-trafik är att många nätverkskort plockar bort VLAN-headern innan de skickar vidare inhämtade Ethernetramar till mjukvaran. Med ett sådant nätverkskort försvåras tolkning och felsökning avsevärt, i synnerhet om man skickar och lyssnar på kraftigt avvikande trafik. Detta är viktigt att känna till för läsare som vill göra egna tester av denna typ.

Tanken med de olika testfallen var att utsätta switcharna för avvikande VLAN-trafik med syfte att orsaka felbehandling och därmed läckage till andra VLAN. Testerna handlade alltså *enbart* om möjligheten att orsaka läckage av trafik mellan olika VLAN. I en verklig miljö finns även andra relevanta säkerhetsfrågor. Exempel på sådana är robusthet mot överbelastningsattacker samt motståndskraft mot intrång i switcharna i sig, vilket kan leda till konfigurationsändringar som i sin tur kan leda till läckage. Denna studie

begränsade sig alltså till hur mycket det går att lita på VLAN-implementationen i sig.

2.2 Beskrivningar av de olika testfallen

Där inget annat angivits är avsändar-MAC och mottagar-MAC fasta adresser. De olika testfallen ska inte betraktas som fullständigt täckande för VLAN-testning. Även när det gäller en relativt enkel funktion som VLAN är det svårt att konstruera fullständigt täckande testfall.

2.2.1 Maxtupeltaggning

Ethernetramar med så många VLAN-taggar som det får plats. VLAN-ID sätts till samma värde i alla dessa. Ingen speciell prioritet anges, men däremot sätts DEI-flaggan (Drop Eligible Indicator) till FALSE.

2.2.2 Reserverade VLAN-ID

Ethernetramar med reserverade VLAN-ID 0x000 respektive 0xfff, DEI-flaggan satt till FALSE, samt ingen speciell prioritet skickas växelvis.

2.2.3 Dubbla reserverade VLAN-ID

Ethernetramar med dubbla taggar med reserverade VLAN-ID 0x000 respektive 0xfff, DEI-flaggan satt till FALSE, samt ingen speciell prioritet skickas växelvis.

2.2.4 Deltaggning variant 1

Ethernetramar som bara innehåller en halv VLAN-tag skickas växelvis med helt otaggade ramar.

2.2.5 Deltaggning variant 2

Ethernetramar som innehåller tre fjärdedelar av en normal VLAN-tag skickas växelvis med helt otaggade ramar.

2.2.6 För korta ramar

Ethernetramar som är kortare än angiven längd (i typ/size-fältet) skickas växelvis med otaggade ramar och korrekt taggade ramar.

2.2.7 För långa ramar

Ethernetramar som är längre än angiven längd (i typ/size-fältet) skickas växelvis med otaggade ramar och korrekt taggade ramar.

2.2.8 Maximal hastighet, en byte

Ethernetramar som är otaggade respektive taggade på normalt sätt skickas växelvis med maximal hastighet. Nyttolasten är en byte lång.

2.2.9 Maximal hastighet, flera bytes

Ethernetramar som är otaggade respektive taggade på normalt sätt skickas växelvis med maximal hastighet. Nyttolasten är flera bytes lång.

2.2.10 Switch-MAC

Ethernetramar med normal taggning men med switchens egen MAC-adress som avsändare i de fall det finns en sådan.

2.2.11 VLAN-anpassad MAC-tabellsflooding

Ethernetramar som har följande egenskaper:

- Käll-MAC är slumpmässig och olika för varje ram (för att försöka fylla MAC-tabellen i switchen så den ska börja flooda ut ramar till att börja med).
- Taggning med önskat VLAN-ID.
- DEI-flaggan är satt till false.

2.2.12 Dubbeltaggning

Ethernetramar med två VLAN-taggar i rad som båda innehåller ID för önskat VLAN. Den yttersta taggen har *inte* DEI-flaggan satt.

2.2.13 Vanlig taggning

Ethernetramar med helt vanlig taggning (som referens).

3 Resultat

Med korrekt konfiguration släppte inte någon av switcharna igenom någon som helst trafik mellan olika VLAN. Se Tabell 1 nedan.

Tabell 1. Switchmodeller och testresultat

Tillverkare	Modell	Resultat	Övrigt
Cisco	Catalyst 2950	OK	
Cisco	Catalyst 2960	OK	
Cisco	Catalyst 3560-CG	OK	
D-Link	DES-3026	OK	
Hirschmann	MM2-4TX1	OK	
Hirschmann	MM20	OK	
Hirschmann	MM2-4TX1	OK	
HP	2510G-48	OK	
HP	ProCurve 2615-8-PoE	OK	
Westermo	MDI-112-F4G	OK	*Se kommentar*
Westermo	MRI-128-F4G	OK	*Se kommentar*

Kommentar: Switcharna från Westermo *måste under alla omständigheter* konfigureras med så kallad Ingress Filtering aktiverad. Denna inställning finner man under VLAN – VLAN Port Configuration – Ingress Filtering. Värdena ska vara Enabled. I konsolen används kommandona `interface` samt `ingress filtering enable`. Om Ingress Filtering *inte* är aktiverad fungerar VLAN till synes som vanligt, men Ethernetramar kan fås att passera från ett VLAN till ett annat i flera av testfallen. Stora mängder trafik kan läcka på mycket kort tid under sådana förutsättningar. Med Ingress Filtering aktiverat har vi däremot inte kunnat konstatera läckage under några som helst omständigheter. Enligt Westermo är det möjligt att defaultläget för Ingress Filtering ändras till Enabled i framtiden.[2] När testerna utfördes var defaultläget Disabled.

[2] Westermo teknisk support, personlig kommunikation, 2014-02-28

4 Diskussion

Vi har inte kunnat påvisa några risker för läckage mellan korrekt uppsatta VLAN. Det bör dock poängteras att en korrekt konfiguration är av största vikt för att uppnå detta resultat. Ett antal sådana konfigurationsaspekter är väl kända sedan många år tillbaka.[3] I denna studie har vi dessutom kunnat konstatera att enskilda switchmodeller kan ha speciella egenheter i konfigurationen det måste tas hänsyn till.

Generellt sett tycks VLAN vara en relativt säker teknik för att uppnå logisk separation mellan olika nätverk. En liknande slutsats nåddes efter tester som utfördes av @stake för över 10 år sedan, men i det fallet enbart mot switchar från Cisco och med till synes lägre granularitet i testfallen.[4]

I dagsläget tycks det alltså inte finnas någon anledning att slå larm om användningen av VLAN som separationsmetod för industriella styrsystem. Däremot vill vi betona att den teoretiskt sett allra högsta säkerhetsnivån uppnås med hjälp av fysiskt separerade nätverk. I anläggningar där maximal säkerhet eftersträvas bör alltså fysisk separation användas istället för logisk separation med hjälp av VLAN.

[3] Cisco, *VLAN Security White Paper*, hämtad 2015-02-03, <http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a008013159f.shtml>

[4] D. Pollino & M. Schiffman, @stake, *Secure Use of VLANs: An @stake Security Assessment*, 2002-08

Security in Industrial Control Systems

Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) är ett kompetenscentrum med uppdraget att bygga upp och sprida medvetenhet, kunskap och erfarenhet om cybersäkerhetsasspekter inom industriella informations- och styrsystem. Centrumets är ett samarbete mellan de svenska myndigheterna FOI och MSB och dess verksamhet fokuserar på aktörer som äger och/eller driver samhällsviktig verksamhet där industriella informations- och styrsystem ingår.

The National Centre for increased security in industrial control systems is a centre of excellence focused at building and disseminating awareness, knowledge and experience about cyber security aspects in ICS. The Centre is a cooperation between the Swedish Defence Research Agency and the Swedish Civil Contingencies Agency and the activities is focused on actors that owns and/or operates critical infrastructure where ICS are a part.

FOI
Swedish Defence Research Agency
SE-164 90 Stockholm

Phone +46 8 555 030 00
Fax +46 8 555 031 00

www.foi.se

Swedish Civil Contingencies Agency
SE-651 81 Karlstad

Phone: +46 (0) 771-240 240
Fax: +46 (0) 10-240 56 00

www.msb.se