DEC 2017 - NO. 3

BAVARIAN JOURNAL OF APPLIED SCIENCES®

Industrial-Ethernet-Protokolle: Sicherheitsrisiko Layer-2-Switch

Peter Semmelbauer

ABSTRACT

Der Einsatz bewährter, ethernetbasierter Technologien in der Automatisierungstechnik bringt viele Vorteile, aber birgt auch große Gefahren. Angriffsszenarien, die bisher nur im Office-Netzwerk eines Unternehmens anwendbar waren, lassen sich nun auch für Attacken auf Automationsebene nutzen. Ein bekanntes Szenario ist Port-Stealing. Dabei wird eine Schwachstelle in der Architektur von Layer-2-Switches genutzt. Wie ein solcher Angriff bei industriellen Ethernet-Protokollen funktioniert, wird nachfolgend am Beispiel von Profinet IO gezeigt.

Using well-established, Ethernet-based systems in automation technology has many advantages, however, also harbors great dangers. Attack scenarios which had so far been limited to corporate office networks have now been extended to the automation level. Port stealing is a well-known method. The port stealing attack exploits weak spots in the layer 2 switch architecture. Using the example of Profinet IO, the following article illustrates how such an attack on industrial Ethernet communication protocols works in practice.

KEYWORDS

Profinet IO, Hacking, Industrial Security, Profinet Hacking, Layer 2 Angriff/ attack, Port Stealing

Profinet IO, hacking, industrial security, Profinet hacking, layer 2 attack, port stealing

Switches sind Kopplungselemente, welche die Teilnehmer eines Netzwerks miteinander verbinden und Pakete anhand von Informationen der Sicherungsschicht (Schicht 2 des ISO/OSI-Modells) weiterleiten. Jeder Teilnehmer eines Netzwerks besitzt eine Hardware-Adresse (MAC-Adresse). Um einem Gerät einen (physikalischen) Port zuzuordnen, analysiert der Switch die auf einem Port empfangenen Pakete und liest die Quell-MAC-Adresse aus. Er speichert diese in einer Tabelle, der Source-Address-Table (SAT) ab. Empfängt der Switch ein Paket von Endgerät 2 mit der Quelladresse ...:02, welches die Zieladresse ...:01 enthält, kann er anhand der Einträge in der SAT feststellen, hinter welchem Port der Empfänger (Endgerät 1) zu finden ist (Port 1) und leitet es dorthin weiter (vgl. Beispiel Abbildung 1).

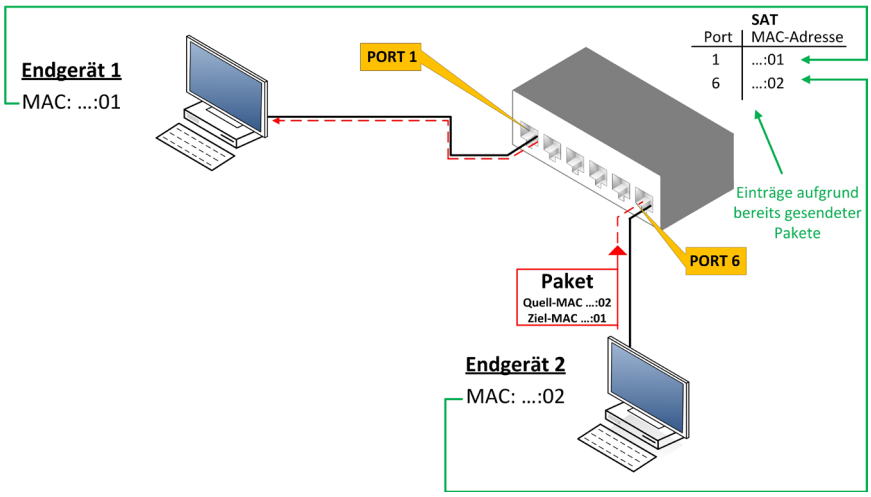


Abbildung 1: Switch erkennt anhand der Einträge in der SAT den jeweiligen Port.

Wechselt ein Gerät den Port, muss der Switch diesen Vorgang erkennen, um eine Weiterleitung von Paketen an diesen Teilnehmer sicherzustellen. Der Switch handelt dynamisch und schreibt die SAT entsprechend um. Allerdings kann ein Angreifer diesen Mechanismus nutzen und Pakete ”stehlen” (daher Port-Stealing). Hierzu muss dieser einen physikalischen Zugang zum Switch besitzen (Port 3). Sendet er ein (manipuliertes) Paket mit der MAC-Adresse von Endgerät 1 als Quelle und einer beliebigen als Ziel (im Beispiel seine eigene), wird die SAT aktualisiert und der Angreifer erhält das an Endgerät 1 adressierte Paket (vgl. Beispiel Abbildung 2).

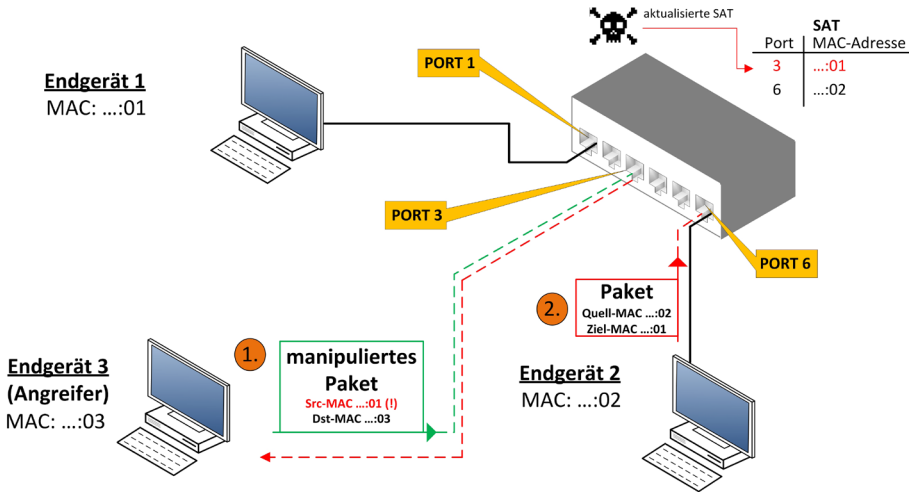


Abbildung 2: Angreifer überschreibt die SAT und erhält die für Endgerät 1 bestimmten Daten.

Mögliche Angriffsszenarien

Werden kontinuierlich derartige Pakete versandt, gelangen die an das Opfer adressierten Daten nicht mehr an ihr eigentliches Ziel – die klassische Denial-of-Service-Attacke. In industriellen Netzwerken können damit wichtige Komponenten vom Netzwerk getrennt werden, was schwerwiegende Folgen haben kann. Doch i. d. R. werden Systeme, die über Profinet IO kommunizieren, so projektiert, dass bei einer vorbestimmten Zeitspanne ohne Paketeingang eine Alarmmeldung gegeben wird. Das betroffene Gerät wird in einen sicheren Zustand versetzt und der Operator beginnt mit der Fehlersuche.

Ein gefährlicheres Szenario ist der Man-in-the-Middle-Angriff (MITM-Angriff). Dabei positioniert sich der Angreifer zwischen zwei Netzwerkteilnehmern und kann dadurch übertragene Daten mitlesen oder manipulieren. Dies stellt sowohl aus datenschutzrechtlicher Sicht, als auch aus Gründen der Betriebssicherheit ein hohes Risiko dar.

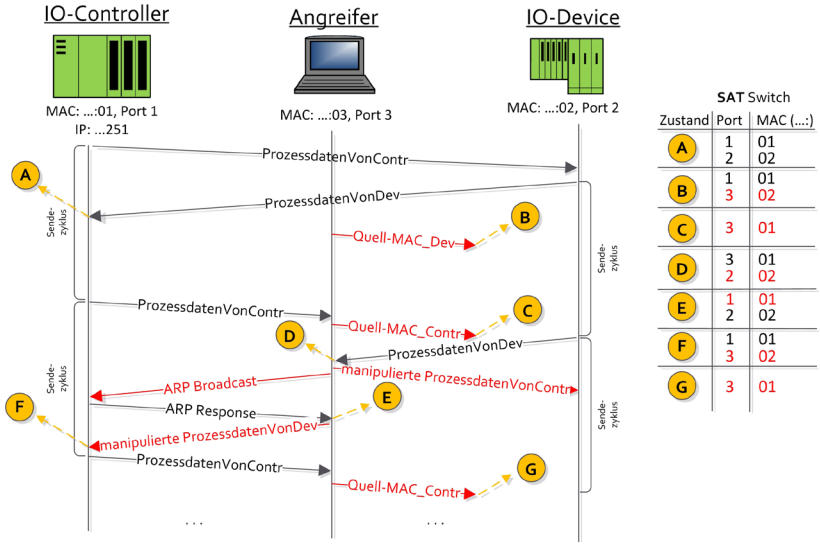
Datenübertragung bei Profinet IO

Bei Profinet IO werden die Prozessdaten zwischen der Baugruppe, in der das Automatisierungsprogramm abläuft (IO-Controller) und dem Feldgerät (IO-Device) zyklisch übertragen. Der Datenaustausch erfolgt in einem parametrisierbaren Takt (abhängig von Gerät und Anlagengröße), die Zykluszeit liegt im ms-Bereich (typischer Wert: 4 ms).
Beim Prozessdatenaustausch wird zur Identifizierung der Teilnehmer nur die MAC-Adresse verwendet. Konfigurations- und Diagnoseinformationen werden azyklisch über einen separaten Kanal versandt. Hierzu benötigt jeder Teilnehmer eine IP-Adresse.

MITM bei Profinet IO

Ein Angreifer gelangt an die für ihn relevanten Informationen (MAC-/IP-Adressen, Geräterolle, d. h. Controller oder Device) über das Discovery and Configuration Protocol (DCP). Dabei schickt dieser einen DCPIdentifyRequest an alle Teilnehmer eines Netzwerkssegements (Broadcast) und erhält von jedem eine DCPIdentifyResponse-Nachricht mit den benötigten Informationen. Anschließend kann er das in Tabelle und Abbildung 3 beschriebene Szenario ausführen und besitzt die volle Kontrolle über den Datenverkehr.

Schritt	Beschreibung	SAT Zustand
0	Ausgangszustand	A
1	Der Angreifer „stiehlt“ den Port des Controllers, indem er ein gefälschtes Paket mit der Quell-MAC des Devices sendet (Quell-MAC_Dev).	B
2	Damit erhält er die für das Device bestimmten Prozessdaten (ProzessdatenVonContr).	B
3	Anschließend sendet er ein Paket mit der Quell-MAC des Controllers (Quell-MAC_Contr).	C
4	Der Angreifer erhält die Prozessdaten des Devices (ProzessdatenVonDev).	D
5	Weiterleitung der geänderten Prozessdaten vom Controller (manipulierte ProzessdatenVonContr) an das Device.	D
6	Um die geänderten Daten des Devices (manipulierte ProzessdatenVonDev) an den Controller senden zu können, muss die SAT des Switches wieder umprogrammiert werden. Hierzu nutzt der Angreifer das Address Resolution Protocol (ARP), dass zur MAC-/IP-Adresszuordnung verwendet wird. Dabei wird mithilfe eines ARP Broadcasts nach der IP-Adresse des Controllers gefragt.	D
7	Antwort des Controllers mit einem ARP Response.	E
8	Weiterleitung der geänderten Prozessdaten vom Device (manipulierte ProzessdatenVonDev) an den Controller.	F
9	Anschließend erhält der Angreifer die Daten vom Controller (ProzessdatenVonContr).	F
10	Anschließend sendet er ein Paket mit der Quell-MAC des Controllers (Quell-MAC_Contr) um das MITM-Szenario aufrechtzuerhalten.	G



SAT Switch

Zustand	Port	MAC (...:)
A	1 2	01 02
B	1 3	01 02
C	3	01
D	3 2	01 02
E	1 2	01 02
F	1 3	01 02
G	3	01

Tabelle und Abbildung 3: Port-Stealing-Algorithmus bei Profinet IO.

Auswahl an Schutzmaßnahmen

Um einen effektiven Schutz zu gewährleisten, sollte ein mehrstufiges Sicherheitskonzept implementiert werden. Basis dieses Konzepts ist ein wirksamer Zugriffsschutz. Mit Hilfe von Zutrittskontrollen muss Unbefugten der unmittelbare, physische Zugang zu Steuerungskomponenten und Netzwerkhardware verwehrt bzw. erschwert werden.
Moderne Switches bieten zudem ein Sicherheitsfeature (MAC-Locking), dass es ermöglicht, die SAT statisch zu schalten und an eine MAC-Adresse zu binden. Meist erlauben diese auch die ungenutzten Ports zu deaktivieren. Sollte ein Angreifer trotz Zutrittskontrollen sich physischen Zugang zum System verschaffen, müsste dieser ein angeschlossenes Gerät vom Netz trennen und mit dessen MAC-Adresse das Angriffsszenario ausführen. Im Regelfall wird das (wenn auch nur kurzzeitige) Entfernen eines Geräts protokolliert. Damit lässt sich ein Angriff zwar nicht verhindern, aber besser zurückverfolgen.
Ist zusätzlich portbasierte Authentifizierung nach IEEE 802.1X konfiguriert, setzt man eine hohe Hürde für den Angreifer. Mit Hilfe dieser Technologie wird ein Port vom Switch erst dann für die Kommunikation freigegeben, nachdem sich das angeschlossene Gerät authentisiert hat. Hierzu übermittelt das Gerät vor dem Verbindungsaufbau vorher festgelegte

Authentisierungsdaten an ein zentrale Instanz, die diese Informationen überprüft. Ist die Verifizierung nicht erfolgreich, verwehrt der Switch den Zugriff zum Netzwerk. Gelangt ein Angreifer nicht an die Authentisierungsdaten, erhält er keinen Zugang und kann damit das Port-Stealing-Szenario nicht ausführen.
Eine Möglichkeit Angriffe zu erkennen, ist der Einsatz eines Intrusion Detection Systems (IDS). Das IDS wird mittels Sensoren in das industrielle Netzwerk integriert und überwacht kontinuierlich den Datenverkehr. Dabei nimmt ein Sensor einzelne Pakete im Netzwerkfluss auf und untersucht diese mit geeigneten Algorithmen auf Abweichungen. Im beschriebenen MITM-Szenario werden fortlaufend ARP-Pakete verschickt. Diese stellen eine Anomalie dar und sind ein Angriffsindikator. Tritt eine derartige Abweichung im System auf, wird dies dem Operator gemeldet und er kann entsprechenden Gegenmaßnahmen einleiten.

Eine weitere Schutzmöglichkeit ist die Absicherung der Kommunikationswege. Hierzu wird das im IEEE 802.1AE-Standard beschriebene MACsec-Verfahren angewandt und bietet neben erweiterten Integritätsschutzmechanismen, zudem die Möglichkeit den Datenverkehr auf Layer 2 zu verschlüsseln.

Wird ein Automationssystem mit den erläuterten Methoden abgesichert, bietet es einem potentielle Angreifer eine recht geringe Angriffsfläche. Port-Stealing-Szenarien werden damit deutlich erschwert.

Peter Semmelbauer, M.Eng.

Peter Semmelbauer hat an der Technischen Hochschule Deggendorf (THD) ein Bachelorstudium in Angewandter Informatik/Infotronik mit dem Studienschwerpunkt Embedded Systems absolviert. Anschließend war er als Projektingenieur am Institut ProtectIT beschäftigt. In verschiedenen Forschungsprojekten befasste er sich mit der Sicherheit von industriellen Anlagen und Gebäudeautomationssystemen. Er absolvierte ein Master-Studium in „Applied Research in Engineering Sciences“ und schloss dieses Anfang 2018 ab.

Peter Semmelbauer studied “Applied Computer Sciences” (BA) with a focus on Embedded Systems at Deggendorf Institute of Technology (DIT) and was later employed as a project engineer at the institute ProtectIT at DIT. In several research projects he analyzed cyber security risks of industrial plants and building automation systems. He recently successfully finished the master programme “Applied Research in Engineering Sciences”.

Nachdruck von / Reprint from:

Semmelbauer, Peter
Industrial-Ethernet-Protokolle: Sicherheitsrisiko Layer-2-Switch
In: Industrie 4.0-Magazin - Zeitschrift für die vierte industrielle Revolution, TeDo Verlag GmbH, 35043 Marburg (Heft 1/2017)
Online verfügbar unter http://www.i40-magazin.de/allgemein/industrial-ethernet-protokolle-sicherheitsrisiko-layer-2-switch/