Security-Demonstrator Industrie 4.0

Kevin Lamshöft · Robert Fischer · Jana Dittmann

Otto-von-Guericke University of Magdeburg
AMSL Research Group
kevin.lamshoeft@st.ovgu.de · robert.fischer@ovgu.de
jana.dittmann@iti.cs.uni-magdeburg.de

Zusammenfassung

Der fortschreitende Wandel von isolierten IT-Systemen, Netzwerken und Produktionsanlagen hin zu komplexen Verbünden von interagierenden Industrie 4.0 Umgebungen führt zu neuen Herausforderungen u.a. im Bereich der IT-Sicherheit. Durch Vernetzung komplexer, heterogener Systemlandschaften vergrößert sich die Angriffsfläche und es ergeben sich erweiterte Möglichkeiten für potentielle Angreifer. Die Erforschung von Verfahren zur Schwachstellen- und Angriffsmodellierung sowie Durchführung systematischer, reproduzierbarer Sicherheitsanalysen für komplexe Industrie 4.0 Anlagen stellen daher aktuell wichtige Forschungsfelder dar. Der vorliegende Beitrag adressiert drei zentrale Forschungsfragen, erstens, die Erarbeitung von einheitlichen Ansätzen zur technischen Abbildung und detaillierten Beschreibung von komplexen, heterogenen Zielinfrastrukturen, zweitens, die Erarbeitung von Ansätzen zur Ermöglichung systematischer, reproduzierbarer Sicherheitsuntersuchungen und drittens, die Erforschung von Möglichkeiten zum experimentellen / praktischen Security-Testing. Unter Berücksichtigung der identifizierten Forschungsfragen führt der Beitrag Konzept und initiale Realisierung eines so genannten Security-Demonstrators ein, der ein systematisches, experimentelles Security-Testing von Industrie 4.0 Systemen vorbereiten soll. Die technische Abbildung der Demonstrator-Umgebung erfolgt unter Verwendung eines existierenden Ansatzes zur Komponenten-basierten Modellierung. Unter Verwendung des vorgestellten Security-Demonstrators erfolgt die demonstrative Umsetzung und experimentelle Auswertung von fünf exemplarisch ausgewählten Basisangriffen, die auf die Kommunikation zwischen den einzelnen Komponenten abzielen.

1 Einleitung

Der fortschreitende Wandel von isolierten IT-Systemen, Netzwerken und Produktionsanlagen hin zu vernetzten, interagierenden Industrie 4.0 Umgebungen, ist gekennzeichnet durch eine zunehmende Anzahl von heterogenen Hardware- und Software-Komponenten sowie einer ansteigenden Komplexität der individuellen Komponenten und der daraus resultierenden vernetzten Umgebungen. Dieser grundlegende Wandel von einzelnen IT-Systemen hin zu Verbünden von interagierenden Produktionsanlagen führt zu neuen Herausforderungen u.a. in der IT-Sicherheit. Durch die Vernetzung komplexer, heterogener Systeme vergrößert sich die Angriffsfläche und es ergeben sich erweiterte Möglichkeiten für potentielle Angreifer (z.B. Erpressung, Sabotage und Industriespionage). Die Erforschung von Verfahren zur Schwachstellen- und Angriffsmodellierung sowie Durchführung systematischer, reproduzierbarer Sicherheitsanalysen für komplexe Industrie 4.0 Anlagen, stellen daher aktuell wichtige Forschungsfelder, in den Bereichen Sicherheit von Industrie 4.0, sichere Steuerung von Industrieprozessen und Schutz kritischer Infrastrukturen, dar.

P. Schartner · N. Pohlmann (Hrsg.) · D•A•CH Security 2018 · syssec (2018) 264-275.

Als zentrale Forschungsfragen für den vorliegenden Beitrag wurden folgende Herausforderungen identifiziert. Erstens die Erarbeitung von einheitlichen Ansätzen zur technischen Abbildung und detaillierten Beschreibung von komplexen, heterogenen Zielinfrastrukturen und eine systematische Identifikation von Zugriffsmöglichkeiten und Angreiferfähigkeiten. Zweitens, die Erarbeitung von Ansätzen zur Ermöglichung systematischer, reproduzierbarer Sicherheits-Untersuchungen und Umsetzung von praktischen / experimentellen Security-Testing für komplexe, vernetzte Industrie 4.0 Umgebungen (unter Berücksichtigung von Hardware, Software, Protokollen, Kontroll- und Steuerprozessen). Drittens, die Erforschung von Möglichkeiten zum experimentellen Security-Testing basierend auf einer systematisch kombinierten Anwendung von Komponenten-basierter Modellierung und den fünf Basisangriffen.

Den Vorschlag zu solch einer flexiblen Testumgebung stellt unsere Konzeption und initiale Inbetriebnahme eines Security-Demonstrators dar, der ein systematisches, experimentelles Security-Testing von Industrie 4.0 Systemlandschaften vorbereiten soll. Der Security-Demonstrator realisiert eine vereinfachte Ampelsteuerung mit drei üblichen Komponenten: eine Speicherprogrammierbare Steuerung (SPS) mit angeschlossenen Sensoren und Aktoren, die den Ampelprozess steuern, ein Projektierungsportal zur Programmierung und Administration der SPS, sowie ein Human-Machine-Interface zur Überwachung der Ampelsteuerung. Die technische Abbildung und detaillierte Beschreibung des Security-Demonstrators erfolgen unter Anwendung eines existierenden Komponenten-basierten Ansatzes. Unter Verwendung des vorgestellten Security-Demonstrators erfolgt im zweiten Teil des Beitrages die demonstrative Umsetzung und experimentelle Auswertung von fünf exemplarisch ausgewählten Basisangriffen, die auf die Kommunikation zwischen den drei Komponenten SPS, HMI und Projektierungssoftware abzielen.

Der vorliegende Beitrag gliedert sich wie folgt. Die Zusammenfassung des Stands der Technik im zweiten Abschnitt umfasst u.a. wesentliche Grundlagen der IT-Security, wie Sicherheitsaspekte und Basisangriffe, die verwendeten Vorarbeiten zu technischer Abbildung und Beschreibung von Zielinfrastrukturen, eine Zusammenfassung bekannter Angriffe und die Beschreibung der für die experimentelle Umsetzung notwendigen Werkzeuge. Im dritten Abschnitt erfolgt die detaillierte Beschreibung des vorgestellten Security-Demonstrators unter Berücksichtigung von Hardware, Software, Vernetzung, Protokollen, Kontroll- und Steuerprozessen. Im vierten Abschnitt werden die fünf exemplarisch ausgewählten Basisangriffe detailliert beschrieben. Die Ergebnisse der demonstrativen Umsetzung und ersten experimentellen Auswertung werden im fünften Abschnitt vorgestellt. Den Abschluss bilden eine Zusammenfassung des Beitrages, ein Fazit hinsichtlich der formulierten Forschungsfragen und Vorschläge für mögliche zukünftige Arbeiten im sechsten Abschnitt.

2 Stand der Technik

Die Zusammenfassung des Stands der Technik umfasst wesentliche Grundlagen der IT-Security, wie Sicherheitsaspekte [CH13] und Basisangriffe [LDKH07], die verwendeten Vorarbeiten hinsichtlich Angriffs- und Analysezielen aus der Schwachstellenanalyse [FG14, SPL+15], die verwendeten Vorarbeiten zu technischer Abbildung und Beschreibung von Zielinfrastrukturen [CFDD16, FCDD16], eine Zusammenfassung bekannter Angriffe und die Vorstellung der für die experimentelle Umsetzung notwendigen Werkzeuge. Für eine Beschreibung von Auswirkungen von Angriffen auf die Sicherheit von industriellen Kontrollsystemen werden die von Cherdantseva und Hilton [CH13] zusammengefassten Sicherheitsaspekte verwendet. Diese umfassen die fünf Aspekte der Integrität, Authentizität, Vertraulichkeit, Nicht-

Abb. 1: Abbildung des vorgestellten Security-Demonstrators Industrie 4.0

Abstreitbarkeit/Verbindlichkeit, Verfügbarkeit, sowie den zusätzlichen Aspekt der Privatsphäre. Für eine systematische Ermittlung von Angriffsvektoren werden die fünf Basisangriffe Lesen, Modifizieren, Unterbrechen, Stehlen und Erzeugen [LDKH07] auf die Kommunikation in industriellen Steuernetzwerken übertragen. Die technische Abbildung und Modellierung des Security-Demonstrators erfolgt auf Basis vorangegangener Arbeiten, die eine umfassende Modellierung von Zielinfrastrukturen mittels Komponenten-basierter Modellierung vorschlagen [CFDD16, FCDD16]. Für die Komponenten des Security-Demonstrators sind wenige Angriffe umfassend dokumentiert, wie Stuxnet [FMC11] und PLCBlaster [SBS16] sowie Replay- und Authentication-Bypass Angriffe [Ber11]. Diese dokumentierten Fälle und Angriffe sowie in Schwachstellendatenbanken veröffentlichte Exploits [MIT18] sind bei den aktuellen Hardware- und Softwareversionen nicht mehr anwendbar. Ende 2017 ist jedoch bekannt geworden, dass sich die Funktionsweise der Integritätssicherung durch Reverse-Engineering ermitteln lässt [LDL17]. Um die Komponenten vor Replayangriffen und manipulierten Paketen zu schützen, verwendet Siemens im aktuellen Kommunikationsprotokoll S7CommPlus einen verschlüsselten Integritätswert. Ist jedoch die Funktionsweise des Algorithmus bekannt, kann ein Angreifer aufgezeichnete Pakete verändern, den Integritätswert berechnen und das manipulierte Paket einspielen. Für die demonstrative Umsetzung von Angriffen werden Tools zur Netzwerkanalyse und Manipulation verwendet, wie Wireshark [WF18] und Scapy [Sec18], sowie für den Aufbau spezifische Tools, die eine Kommunikation mit Siemens Komponenten unterstützen, wie der S7Comm Dissector [Wie18] für Wireshark sowie NodesS7 [PLC18] und Snap7 [Nar18], zwei Bibliotheken zur Kommunikation mit S7 PLCs.

3 Beschreibung des Security-Demonstrators

In den folgenden Abschnitten findet sich eine detaillierte Beschreibung des in Abbildung 1 dargestellten Security-Demonstrators unter Berücksichtigung von Hardware, Software, Vernetzung, Protokollen, Kontrollprozessen und Steuerprozessen. In Abbildung 3 ist der vorgestellte

Security-Demonstrator unter Verwendung des gewählten Komponenten-basierten Ansatzes aus [CFDD16, FCDD16] dargestellt.

Für die Umsetzung eines Demonstrators für Industriesteueranlagen bedarf es zwei übergeordneter Komponenten: Einen physikalischen Prozess, der gesteuert wird und eine Steuerungsanlage, die mittels Sensoren den Prozess beobachtet und mit Aktoren den Prozess beeinflusst. Für die erste Umsetzung unseres Demonstrators wählen wir einen Prozess, der leicht zu realisieren ist, jedoch genug Möglichkeiten bietet, um Sicherheitstests durchzuführen.

Der vorgestellte Security-Demonstrator realisiert eine Ampelsteuerung, die eine Fußgängerampel simuliert. Der gesamte Demonstrator ist auf einer Spanplatte verschraubt und besteht aus zwei Komponenten, der Steuerungsanlage sowie der simulierten Ampelanlage. Die Ampelanlage besteht aus verdrahteten LEDs, die in einem eigenen Holzgehäuse verbaut sind. Es sind zwei Ampeln für jede Fahrtrichtung der Fahrzeuge vorhanden (oben links und unten rechts, siehe Abbildung 1), sowie zwei Ampeln auf jeder Seite der imaginären Straße für Fußgänger. Die Ampeln werden durch farbige LEDs dargestellt, für Fahrzeuge entsprechend grün, gelb, rot, für Fußgänger grün und rot. Zur Schaltung der Fußgängerampel ist ein Taster vorhanden (unten links, siehe Abbildung 1), der bei Druck den Prozess zum Schalten der Ampel auslöst. Wird der Schalter gedrückt, werden nach einigen Sekunden die Ampeln der Fahrzeuge auf gelb, kurz danach auf rot geschaltet und entsprechend die Fußgängerampeln grün geschaltet. Nach einigen Sekunden wird die Fußgängerampel rot geschaltet, kurz darauf die der Fahrzeuge gelb, anschließend wieder grün. Die Steuerungsanlage hat entsprechend einen Sensor, den Taster, sowie zehn Aktoren (2x 3 LEDs Fahrzeugampel, 2x 2 LEDs Fußgängerampel).

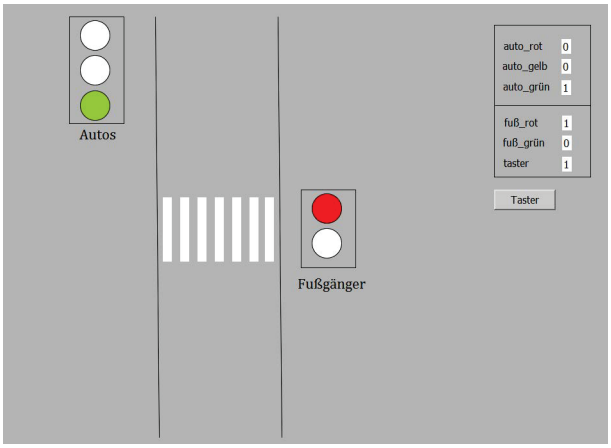

Abb. 2: Abbildung der HMI Oberfläche inklusive Aktualwerten der einzelnen Variablen

Für die Realisierung des Steuerprozesses des Demonstrators werden Hardware- und Softwarekomponenten von Siemens verwendet. Abbildung 3 zeigt eine detail-reduzierte technische Abbildung der Komponenten. Die Siemens Simatic S7-1500 SPS (1516-3 PN/DP) mit direkt angeschlossenen analogen und digitalen I/O Modulen übernimmt die Steuerung der Ampel. Für Projektierung und Verwaltung der S7 wird das Totally Integrated Automation Portal (V13 SP2, inklusive STEP7 und WinCC), verwendet. Das Human-Machine-Interface wird mit dem TIA-Portal erstellt und projektiert und mittels der WinCC Runtime Advanced auf einem weiteren Computer dargestellt. Das HMI zeigt eine vereinfachte Darstellung der Ampelsteuerung sowie eine Tabelle mit aktuellen Variablenwerten, die Oberfläche wird in Abbildung 2 dargestellt. Die

Siemens S7, die Engineering-Workstation mit TIA-Portal und das HMI sind angeschlossen an einen Switch und kommunizieren via PROFINET.

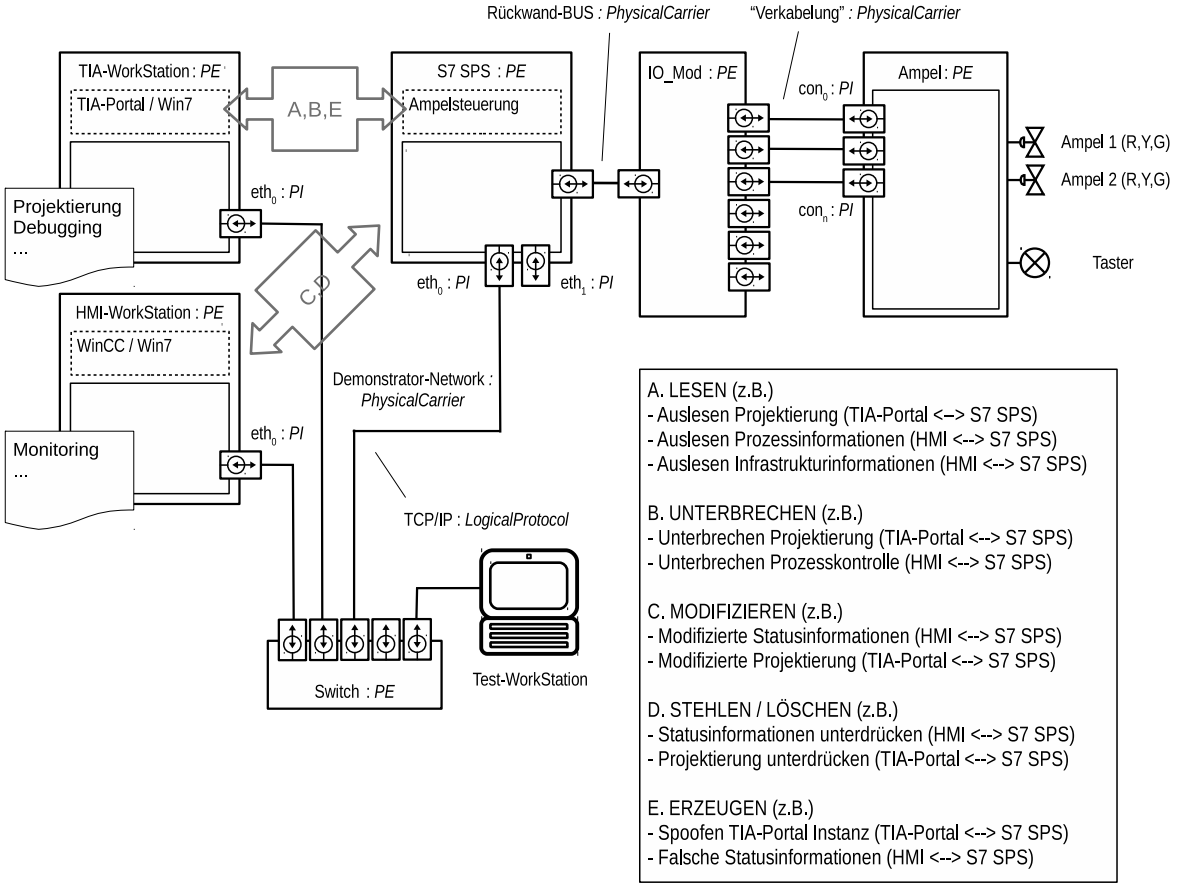

Abb. 3: Komponenten-basierte Modellierung des Security-Demonstrators

4 Die Basisangriffe

Um ein Verständnis für die möglichen Angriffsvektoren zu entwickeln, werden die bekannten fünf Basisangriffe [FCDD16] auf die Kommunikation im Umfeld von industriellen Steueranlagen übertragen und vorgestellt. Hierzu wird die Kommunikation zwischen Speicherprogrammierbaren Steuerungen, Projektierungsportalen und Human-Machine Interfaces betrachtet.

4.1 Lesen

Der Basisangriff Lesen ist für weitere, insbesondere gezielte Angriffe, eine notwendige Grundlage. Beim Lesen wird passiv der Netzverkehr beobachtet und/oder aufgezeichnet. Dies ermöglicht zum einen ein grundsätzliches Verständnis für das Zielsystem entwickeln zu können, wie zum Beispiel Kommunikationsabläufe zwischen Geräten, verwendete Protokolle oder Sicherheitsmaßnahmen. Zum anderen ist es möglich, spezifische Architektur- und Konfigurationsinformationen zu einem konkreten Zielsystem zu erhalten, wie zum Beispiel Art und Anzahl der Geräte, IP-/MAC Adressen und Firmware/Software Versionen. Bei der Beobachtung des

Netzverkehrs von Industriellen Kontrollsystemen ist es möglich, Rückschlüsse auf den physikalischen Prozess, der von dem System gesteuert wird, zu ziehen. Anhand der Kommunikation ist ersichtlich, welche Geräte miteinander kommunizieren, zum Beispiel interagierende SPSs oder Interaktionen zwischen HMIs und SPSs und zudem wie sie kommunizieren. Einerseits kann hierbei nach dem zeitlichen Aspekt des Sendens von Nachrichten differenziert werden, beispielsweise ob die Kommunikation zyklisch, Anfragen-basiert oder als Abonnement verläuft. Andererseits lässt sich die Kommunikation nach der Art der Adressierung unterscheiden, ob eine Nachricht an einen einzelnen Partner (unicast), an mehrere Partner (multicast) oder ohne konkrete Adressierung an alle versendet (broadcast) wird. Anhand dieser Informationen lassen sich bereits Teilnehmer, Struktur und Prozesse ermitteln. Verläuft die Kommunikation zudem nicht verschlüsselt, können Angreifer anhand von Variablen- und Funktionsnamen, die sich in den einzelnen Paketen befinden, auf konkrete I/Os, Prozesse und Steuerfunktionen des Gesamtsystems schließen. Die einzelnen Komponenten eines industriellen Kontrollsystems sind darauf ausgelegt mit anderen Komponenten zu kommunizieren und zu interagieren. Daher bieten die einzelnen Komponenten weitere wichtige Informationen für Angreifer.

Kommunikation zwischen HMI und SPS

Human-Machine Interfaces werden verwendet, um Statusinformation der SPS zu visualisieren und enthalten gegebenenfalls Steuerfunktionen, um den Prozess, der durch die SPS gesteuert wird, zu beeinflussen. Für Angreifer sind insbesondere Statusveränderungen von Variablen sowie Steuerbefehle an SPSen von Interesse. Statusveränderungen geben Auskunft über verwendete Variablen und deren Werte, welche für weiterführende Angriffe benötigt werden. Zudem können sie dem Angreifer Hinweise auf den Prozess geben, der durch die SPS gesteuert wird. Steuerbefehle beeinflussen direkt die SPS oder die Outputs der SPS, wodurch der dahinter stehende Prozess beeinflusst wird. Diese Informationen sind insbesondere für Angreifer von Interesse, die eben diesen physikalischen Prozess manipulieren wollen.

Kommunikation zwischen Projektierungsportal und SPS

Das Projektierungsportal ist zuständig für die Konfiguration, Projektierung und das Monitoring der SPS. Dies umfasst Start-/Stop Kommandos, Debugging Nachrichten sowie die Projektierung. Findet ein Monitoring statt, können so auch verwendete Variablen und deren Zustände ausgelesen werden. Das Mitlesen der Projektierung kann insbesondere im Kontext von Industriespionage relevant sein.

4.2 Unterbrechen

Industrielle Kontrollsysteme steuern in Echtzeit physikalische Prozesse. Sollten Elemente dieses Systems ausfallen, hat dies Auswirkungen auf den physikalischen Prozess. In vielen Fällen kann dies zu ungewollten, gefährlichen, Zuständen führen und im schlimmsten Fall Menschenleben gefährden. Verfügbarkeit ist somit ein zentraler Schutzaspekt von industriellen Kontrollsystemen. Der Basisangriff Unterbrechen zielt auf die (Nicht-)Verfügbarkeit von Nachrichten beziehungsweise Kommunikation und verhindert die korrekte Kommunikation zwischen zwei oder mehreren Partnern. Im industriellen Umfeld finden eine Vielzahl an Kommunikationsabläufen statt, die für Angreifer lohnenswert sein können. Ein interessantes Angriffsziel für den Basisangriff Unterbrechen ist der Prozess der Projektierung, da ein Fehlschlagen der Projektierung zu möglichen Fehlerzuständen der SPS führen kann – und schränkt somit die Verfügbarkeit der SPS ein. Eine weitere Möglichkeit ist die Unterbrechung zwischen HMIs und den SPSen –

insbesondere im Kombination mit weiteren Angriffen. Ist die Kommunikation zwischen HMIs und den SPSsen gestört, können fehlerhafte Zustände der SPS oder des gesteuerten Prozess verschleiert werden, beispielsweise das Überhitzen eines Heizkessel. Die Unterbrechung zwischen Projektierungsportal/Engineering Workstation und SPS kann ebenfalls dazu führen, dass kritische Zustände verschleiert werden oder die Behebung ebendieser verhindert wird.

4.3 Modifizieren

Beim Basisangriff Modifizieren wird eine Nachricht von einem Angreifer während der Übermittlung zwischen den Kommunikationspartnern verändert. In dem Kontext von industriellen Kontrollsystemen sind insbesondere Veränderungen von Variablenwerten von Interesse. Durch die Manipulation von Statusinformationen der SPS an HMIs und Engineering Workstations kann ein Angreifer ein falsches Bild über den aktuellen Status der SPSen und des gesteuerten Prozesses erzeugen. Eine weitere Möglichkeit ist das Abfangen und Modifizieren einer Projektierung. Hierbei könnte beispielsweise Schadcode in die Projektierung eingefügt werden.

4.4 Stehlen/Löschen

Ähnlich zu Modifizieren, lässt sich der Basisangriff Stehlen/Löschen auf die Kommunikation zwischen SPS und HMI anwenden, um Statusinformation von der SPS zu unterdrücken und so kritische Systemzustände zu verschleiern. Eine weitere Möglichkeit besteht im Stehlen der Projektierung – hierzu wird der Netzverkehr und somit die Projektierung vom Projektierungsportal an die SPS an den Angreifer umgeleitet. Die Herausforderung liegt hierbei darin, dass der andere Kommunikationspartner die erwarteten Pakete nicht (mehr) erhält und so gegebenenfalls Fehlermeldungen entstehen, die Aufmerksamkeit erregen.

4.5 Erzeugen

Bei dem Basisangriff Erzeugen werden vom Angreifer gefälschte Nachrichten erzeugt und gesendet. Im Kontext industrieller Systeme ist hier insbesondere die Kommunikation zwischen SPS und Projektierungsportal / Engineering Workstations interessant, da diese umfassende Zugriffsrechte auf die SPS haben. So kann ein Angreifer scheinbar legitime Nachrichten erzeugen, wie zum Beispiel das Starten/Stoppen der Steuereinheit oder die Übertragung einer manipulierten Projektierung.

5 Demonstrative Anwendung und Auswertung

Zur demonstrativen Anwendung werden die zuvor vorgestellten Basisangriffe anhand von exemplarisch gewählten Beispielen auf den Security-Demonstrator übertragen und evaluiert. Dabei kommt die Standard-Konfiguration zur Anwendung, es sind keine zusätzlichen Sicherheitsmaßnahmen im Einsatz und es wird die Kommunikation zwischen Speicherprogrammierbarer Steuerung, Projektierungsportal und Human-Machine Interface betrachtet.

In diesem Aufbau sind das die Siemens S7-1500, das TIA-Portal und das WinCC HMI. Die Kommunikation wird permanent zwischen dem Switch und der S7 mittels eines passiven LAN Taps und eines Raspberry Pis überwacht. Der Rasperry Pi ist vom restlichen Netzwerk getrennt, damit der Netzwerkstrom nicht verändert wird. Die Kommunikation wird mittels eines passiven Netzwerktaps Integritäts-gesichert aufgezeichnet. Für die Aufzeichnung wird tshark verwendet, die Analyse erfolgt in Wireshark [WF18]. Das S7Comm und S7CommPlus Protokoll können mittels eines Plugins [Wie18] in Wireshark dissektiert werden.

Die Aufzeichnungen helfen einerseits ein Verständnis für die Kommunikation und Prozesse zu entwickeln und andererseits die Angriffe zu dokumentieren. Für die Angriffe wird ein Netzwerkzugriff auf den Switch vorausgesetzt. Die Kommunikation zwischen den Geräten findet über PROFINET [PNeP18] statt.

Für die Angriffe werden zwei Bibliotheken (nodeS7 [PLC18] und snap7 [Nar18]) verwendet, die in der Lage sind mit der Simatic S7 zu kommunizieren. Zudem wird scapy [Sec18] verwendet, um abgefangene Nachrichten zu verarbeiten und manipulieren.

5.1 Lesen

Eine Verbindung mit einem Switch ermöglicht bereits eine Vielzahl an Informationen über weitere angeschlossene Geräte des selben Subnetzes zu erlangen. Geräte von Siemens (SPS, TIA, HMI) senden in regelmäßigen Abständen einen Broadcoast in Form des Link Layer Discovery Protokolls. Diese Pakete beinhalten Informationen über Hardware- und Software Konfiguration der Geräte. Damit ist es einem Angreifer zum einen möglich, zu identifizieren, welche Geräte im Netz erreichbar sind, und zum anderen detaillierte Informationen über das Gerät zu sammeln, die für weitere Angriffe verwendet werden können.

Im Falle der S7 sind dies u.a. statische Informationen wie Modell, CPU, Seriennummern, Hardware- und Firmware Versionen, MAC-Adressen, sowie dynamische Information wie etwa die zugeordnete IP Adresse und PROFINET ID.

Die Kommunikation zwischen den Siemens Geräten der ersten Generation (S7-300 und S7-400) findet unverschlüsselt auf dem Application Layer mittels des S7Comm [Ber11] Protokolls statt. In der zweiten Generation (S7-1200 und S7-1500) wird ein neues Protokoll verwendet (S7Comm Plus) [LDL17], das im Header über einen Integritätswert verfügt, der Replay Angriffe verhindern soll. Dieser Integritätswert wird über die PDU gebildet und mittels eines nicht veröffentlichten, proprietären Algorithmus verschlüsselt [LDL17]. Bei Erhalt eines Paketes wird der Integritätswert geprüft und das Paket gegebenenfalls verworfen. Die PDU selbst jedoch bleibt auch im neueren Protokoll unverschlüsselt, so dass ein Angreifer sämtliche Kommunikation zwischen den Geräten mitlesen kann. Aufgrund fehlender Verschlüsselung ist es einem Angreifer möglich Befehle des TIA-Portals an die S7 mitzulesen. Hier müssen zusätzliche Schutzmaßnahmen umgesetzt werden, der Hersteller empfiehlt u.a. eine konsequente Netzwerk-Segmentierung und den Einsatz von Firewalls zur Abschirmung des Automatisierungsnetzes [Sie18].

Mittels ARP-Spoofing / ARP Cache Poisoning [Wha01] ist es möglich den Netzverkehr an den Computer des Angreifers umzuleiten, sodass dieser den Netzverkehr zwischen Geräten, die am gleichen Switch angeschlossen sind, mitlesen kann. Hierbei ist zu beachten, dass die Pakete an den Angreifer geleitet werden und dieser die Pakete an den eigentlichen Adressaten weiterleiten muss damit Verbindungen nicht unterbrochen werden.

5.2 Unterbrechen

Da PROFINET auf dem TCP/IP Protokollstack, ist ein Ansatz zur Unterbrechung die Nutzung bekannter Angriffe auf dem OSI Layer 3 wie zum Beispiel ARP Spoofing / Poisoning. Der Hersteller empfiehlt u.a. eine konsequente Netzwerk-Segmentierung und den Einsatz von Firewalls zur Abschirmung des Automatisierungsnetzes [Sie18]. Die Pakete werden hierbei an den Angreifer geleitet (Basisangriff Lesen), dieser leitet jedoch die erhaltenen Pakete nicht weiter. Die anderen Teilnehmer erhalten somit nicht die erwarteten Pakete und es kommt zu einem Verbin-

dungsverlust. Dabei muss auf genaues Timing geachtet werden, so dass die Unterbrechung zur korrekten Zeit stattfindet. Bei einem vorhergehenden Basisangriff Lesen kann auf bestimmte Pakete, zum Beispiel die Initialisierung der Projektierung gewartet werden, um dann die Verbindung zu unterbrechen. Dies kann insbesondere nützlich sein, wenn ein Angreifer zuvor eine S7 manipuliert hat und verhindern will, dass die S7 wieder korrekt projektiert wird. Auf OSI Layer 4 kann ein Verbindungsabbruch mittels tcpkill [Son18] erreicht werden, welches RST Packete sendet, wodurch gezielt TCP Verbindung unterbrochen werden können. Eine weitere Möglichkeit stellt auf Layer 7 das PROFINET DCP Discovery and Basic Configuration Protocol dar, welches Adressen und Namen in PROFINET Netzwerken vergibt. Hierüber kann die IP-Adresse der S7 geändert werden, was ebenfalls in einem Verbindungsabbruch resultiert.

5.3 Modifizieren

Die Integritätsprüfung des S7CommPlus Protokolls verhindert zunächst ein einfaches Abfangen und Weitersenden eines manipulierten Paketes, da die Berechnung des Integritätswerts nicht bekannt ist. Die Pakete können zwar abgefangen und verändert werden, der Empfänger bemerkt jedoch die Verletzung der Integrität und verwirft das Paket. Erste Versuche deuten darauf hin, dass eine direkte Manipulation möglich ist, wenn die Siemens S7 einen Kompatibilitätsmodus verwendet, der aktiviert werden muss, um Dritt-Anbieter Soft- und Hardware mit der S7 nutzen zu können. Hierbei wird auf das ältere S7Comm Protokoll zurückgegriffen, welches keine Integritätssicherung implementiert. Zudem ist im Dezember 2017 gezeigt worden, dass die Berechnung des Integritätswerts mittels Reverse Engineerings ermittelt werden kann [LDL17], so dass auch ein Modifizieren von Integritäts-gesicherten Paketen möglich ist.

Das absichtliche Verletzen der Integrität kann jedoch auch als Angriff genutzt werden. In unseren Versuchen verwenden wir arpspoof [Son18], um ein Man-in-the-Middle Angriffen zwischen S7 und HMI zu realisieren. Somit werden sämtliche Pakete an den Angreifer-Computer weitergeleitet. Mittels iptables [Net18a] werden die Pakete in nfqueue [Net18b] eingereiht. Ein Python Skript greift auf die Paketqueue zu und die Pakete werden mit der scapy [Sec18] Bibliothek gefiltert, manipuliert und anschließend an den eigentlichen Adressaten weitergeleitet. Das Skript wartet auf Pakete, die aktuelle Statusinformation der S7 an das HMI enthalten. Diese Statusinformation werden beliebig verändert. Aufgrund des Integritätschecks bemerkt das HMI die Inkorrektheit des Pakets und verwirft es. Das HMI gibt jedoch keinerlei Fehlermeldung oder Feedback darüber. Stattdessen verbleibt das HMI bei den zuletzt korrekt erhaltenen Variablen, bzw. Statusinformationen. Das ermöglicht dem Angreifer einen falschen Systemstatus vorzutäuschen.

5.4 Stehlen/Löschen

Ähnlich zu Modifizieren, lässt sich der Basisangriff Stehlen/Löschen auf die Kommunikation von S7 und dem HMI anwenden, um Statusinformation von der S7 zu unterdrücken und so kritische Systemzustände zu verschleiern. Dies kann durch eine Variation des Unterbrechen Angriffs geschehen, indem die Pakete durch das ARP Spoofing oder durch eine Änderung der IP-Adressen an den Angreifer umgeleitet werden, so dass das HMI keine Nachrichten mehr empfängt.

5.5 Erzeugen

Für den Basisangriff Erzeugen sind insbesondere Möglichkeiten zur Re-Programmierung der S7 interessant. Werden die vom Hersteller empfohlenen Sicherheitsmechanismen [Sie18] nicht

konsequent umgesetzt, ist es unter Umständen möglich eine weitere TIA-Portal Instanz in das Netz einzufügen, die die S7 neu projektiert. Da die Kommunikation zwischen den Geräten unverschlüsselt verläuft, ist ein Reverse Engineering der Kommunikationsprotokolle möglich. Eine Umsetzung ist beispielsweise mit Scapy [Sec18] möglich, um eigene Nachrichten zu erstellen und interaktiv mit der S7 zu kommunizieren und diese zu steuern.

6 Resümee und Ausblick

Bezüglich der eingangs formulierten Forschungsfragen kann der vorliegende Beitrag wie folgt zusammengefasst werden. Hinsichtlich der Erarbeitung von einheitlichen Ansätzen zur technischen Abbildung und detaillierten Beschreibung von komplexen, heterogenen Zielinfrastrukturen und einer systematischen Identifikation von Zugriffsmöglichkeiten und Angreiferfähigkeiten, erfolgte die erfolgreiche Anwendung eines existierenden Ansatzes zur technischen Abbildung von komplexen Zielinfrastrukturen auf die vorgestellte Demonstrator Umgebung. Dabei zeigt sich, dass dieses auf Schnittstellen fokussierte Vorgehen die gezielte Suche nach Schwachstellen in vernetzten Umgebungen unterstützen kann.

Hinsichtlich der Erarbeitung von Ansätzen zur Ermöglichung systematischer, reproduzierbarer Sicherheits-Untersuchungen und Umsetzung von praktischen / experimentellen Security-Testing für komplexe, vernetzte Industrie 4.0 Umgebungen, erfolgt die Vorstellung eines Konzeptes sowie initiale Umsetzung eines Security-Demonstrators. Dieser flexible Realaufbau ist Anlagen-unabhängig, leicht erweiterbar und Hersteller-unabhängig, da das vorgestellte Vorgehen für beliebige Hersteller angewendet werden kann. Für die demonstrative Testumsetzung und Vorbereitung weiteren Security-Testings wurden notwendige Programme und Werkzeuge zum Lesen und Manipulieren von Netzwerkpaketen im Laboraufbau umgesetzt.

Hinsichtlich der Erforschung von Möglichkeiten zum experimentellen Security-Testing basierend auf einer systematisch kombinierten Anwendung von Komponenten-basierter Modellierung und Basisangriffen, erfolgte eine demonstrative Umsetzung von fünf exemplarisch gewählten Basisangriffen die auf die Netzwerkkommunikation zielen. Der vorgestellte Security-Demonstrator realisiert einen repräsentativen Kontrollprozess und ermöglicht durch Vielfältigkeit und Konfigurierbarkeit die Betrachtung angepasster und erweiterter Angriffsrealisierungen, die Umsetzung von praktischem Security-Testing und eine reproduzierbare experimentelle Validierung. Die exemplarische Anwendung des vorgeschlagenen Ansatzes unter Laborbedingungen deutet darauf hin, dass die angestrebte Kombination von Basisangriffen und Komponenten-basierter Modellierung, ein hierarchisches Attack-Testing über verschiedene Layer und damit ein gezieltes / smartes Testen ermöglicht.

Die identifizierten Einschränkungen des vorgestellten Ansatzes ergeben sich vor allem durch die proprietären Bestandteile des S7Comm Protokolls und der HMI-/Projektierungssoftware die bisher nur unzureichend nachvollzogen werden konnten. Darüber hinaus konnten eine detaillierte Untersuchung und der Vergleich unterschiedlicher Zugriffsstufen / Sicherheitseinstellungen noch nicht abgeschlossen werden. Die für den vorliegenden Beitrag exemplarisch ausgewählten Basisangriffe sind bisher beschränkt auf die Netzwerkkommunikation zwischen den Komponenten. Zusätzlich existiert bisher keine programmiertechnische Umsetzung zur Unterstützung des vorgestellten Ansatzes. Die manuelle Anwendung, Auswertung und Dokumentation ist zeitintensiv und erlaubt bisher keine Generierung von Angriffssequenzen.

Für zukünftige Arbeiten sollten vor allem die programmiertechnische Umsetzung und die Automatisierbarkeit der einzelnen Schritte in den Mittelpunkt gestellt werden. So könnte z.B. durch

automatische Exploration, Dokumentation und Unterstützung bei der technischen Abbildung von Ziellandschaften komplexere Angriffsszenarien und vielfältigere Angriffssequenzen realisiert werden. Dies beinhaltet u. a. die Berücksichtigung weiterer Protokolle, zusätzlicher Hard- und Softwarekomponenten und erweiterte Kontroll- und Steuerprozesse. Eine weitere Herausforderung für zukünftige Arbeiten stellen die auf eine spezifische Systemlandschaft abgestimmte automatische Generierung von vielfältigen Angriffssequenzen eine mögliche Automatisierbarkeit der Tests dar.

Danksagung

Diese Veröffentlichung wird durch das Bundesministerium für Wirtschaft und Energie (BMWi, SMARTEST, Projekt-Nr. 1501502B), im Rahmen des Deutschen Reaktor-Sicherheits-Forschungsprogramms gefördert. Die Autoren bedanken sich bei den Projektpartnern der Universität Erlangen, der Hochschule Magdeburg-Stendal und der AREVA/Framatome GmbH für die fruchtbaren Diskussionen und den Ideenaustausch.

Literatur

[Ber11] D. Beresford: Exploiting siemens simatic s7 plcs. *Black Hat USA 2011*, 2011.

[CFDD16] R. Clausing, R. Fischer, J. Dittmann, Y. Ding: *Your Industrial Facility and Its IP Address: A First Approach for Cyber-Physical Attack Modeling*, volume 9922, chapter Computer Safety, Reliability, and Security, pages 201–212. Springer International Publishing, September 2016.

[CH13] Y. Cherdantseva, J. Hilton: A reference model of information assurance & security. In *Proceedings of the 2013 International Conference on Availability, Reliability and Security*, ARES '13, pages 546–555, Washington, DC, USA, 2013. IEEE Computer Society.

[FCDD16] R. Fischer, R. Clausing, J. Dittmann, Y. Ding: Industrie 4.0 schwachstellen: Basisangriffe und szenarien. In *Proceedings of D-A-CH Security 2016*, pages 350–362, 2016.

[FG14] C. Freckmann, U. Greveler: It-sicherheitsaspekte industrieller steuerungssysteme. In *Sicherheit 2014: Sicherheit, Schutz und Zuverlässigkeit, Beiträge der 7. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI), 19.-21. März 2014, Wien, Österreich*, pages 149–156, 2014.

[FMC11] N. Falliere, L.O. Murchu, E. Chien: W32. stuxnet dossier. *White paper, Symantec Corp., Security Response*, 5(6):29, 2011.

[LDKH07] A. Lang, J. Dittmann, S. Kiltz, T. Hoppe: Future perspectives: The car and its ip-address – a potential safety and security risk assessment. In Francesca Saglietti and Norbert Oster, editors, *Computer Safety, Reliability, and Security*, pages 40–53, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg.

[LDL17] C. Lei, L. Donghong, M. Liang: The spear to break the security wall of s7commplus. *DEF CON 25, Black Hat EU17*, 2017.

[MIT18] MITRE: Cve common vulnerabilities and exposures database, keyword siemens s7. https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=siemens+s7, 2018.

[Nar18] D. Nardella: Snap7. http://snap7.sourceforge.net, 2018.

[Net18a] Netfilter: Man page of iptables. http://ipset.netfilter.org/iptables.man.html, 2018.

[Net18b] Netfilter: Man page of libnetfilter queue. https://www.netfilter.org/projects/libnetfilterqueue/doxygen, 2018.

[PLC18] PLCPeople: nodes7. https://github.com/plcpeople/nodeS7, 2018.

[PNeP18] PROFIBUS Nutzerorganisation, e.V: Profinet – the leading industrial ethernet standard. https://www.profibus.com/technology/profinet/, 2018.

[SBS16] R. Spenneberg, M. Brüggemann, H. Schwartke: Plc-blaster: A worm living solely in the plc. *Black Hat Asia (p. N/A)*, 2016.

[Sec18] SecDev: Scapy. https://scapy.net/index.html, 2018.

[Sie18] SiemensAG: Industrial security, network security. https://w3app.siemens.com/mcms/infocenter/dokumentencenter/sc/ic/Documentsu20Brochures/Brochure-Network-Security-EN.pdf, 2018.

[Son18] D. Song: dsniff. https://www.monkey.org/ dugsong/dsniff/, 2018.

[SPL+15] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, A. Hahn: Guide to Industrial Control Systems (ICS) Security. Technical Report NIST SP 800-82r2, National Institute of Standards and Technology, June 2015.

[WF18] Wireshark Foundation: Wireshark. https://www.wireshark.org/, 2018.

[Wha01] S. Whalen: An introduction to arp spoofing. *Node99 [Online Document], April*, 2001.

[Wie18] T. Wiens: S7comm wireshark dissector. https://sourceforge.net/projects/s7commwireshark, 2018.