Controllo di accesso
in sistemi industriali distribuiti

La definizione e l'analisi di politiche di controllo d'accesso (access policy) sono elementi cardine su cui basare qualsiasi schema di protezione per sistemi industriali di controllo e di automazione distribuiti, contro attacchi informatici condotti sia a livello locale sia attraverso il cyberspazio. Quest'articolo mostra come l'uso di opportune tecniche di modellazione e di verifica, condotte con l'ausilio di strumenti software automatici, possa essere di aiuto nel raccordare le policy specificate a un alto livello di astrazione con i meccanismi elementari di sicurezza di basso livello, presenti nell'implementazione del sistema fisico reale. L'approccio utilizzato per raggiungere tale obiettivo è basato su un tipo di modello innovativo che integra due diverse viste dello stesso sistema, indicate nel seguito rispettivamente con i termini di specifica e implementazione. Le capacità descrittive del modello sono presentate tramite un semplice esempio derivato da un prototipo reale d'impianto progettato per la riparazione, lo smontaggio e il riciclaggio di circuiti stampati.

Manuel Cheminod
Luca Durante
Lucia Seno
Adriano Valenzano

Keyword

Sicurezza dei sistemi industriali, role-based access control (RBAC), policy per il controllo di accesso, strumenti automatici di analisi, model checking

GLI AUTORI
M. Cheminod, L. Durante, L. Seno, A. Valenzano - IEIIT, Consiglio Nazionale delle Ricerche (CNR), Corso Duca degli Abruzzi 24, 10129 Torino, Italy

La protezione da attacchi informatici, sferrati contro sistemi industriali di controllo e automazione (industrial control systems - ICS) e infrastrutture critiche attraverso il cyberspazio, impone di doversi misurare con sfide ardue e sempre nuove senza soluzione di continuità. La sicurezza degli ICS, infatti, è ormai universalmente considerata un processo in continua evoluzione e non un prodotto da utilizzarsi all'occorrenza [1]. Alla base di tale processo si trovano inevitabilmente opportune strategie e tecniche per il controllo d'accesso che rendono possibile la realizzazione di sistemi di protezione di qualsivoglia complessità.

In termini molto semplificati un insieme di access policy definisce "chi può fare cosa e su quali oggetti" del sistema. Nella quasi totalità dei casi le access policy sono definite a un livello elevato di astrazione, perché ciò offre vantaggi rilevanti in termini di verifica della loro coerenza e dell'indipendenza delle strategie adottate dall'effettiva implementazione del sistema. Purtroppo i benefici sono spesso attenuati dalle difficoltà che s'incontrano nel verificare che la configurazione del sistema reale (in particolare per quanto riguarda l'impostazione di meccanismi di base quali password, diritti di accesso, regole di filtraggio dei dispositivi di rete ecc.) corrisponda esattamente e correttamente a quanto richiesto per soddisfare le policy di alto livello.

L'approccio seguito frequentemente in altri settori applicativi dell'information technology (IT), cioè il disporre di sistemi software e hardware in grado di garantire il rispetto (enforcement) delle policy, non è quasi mai applicabile al caso degli ICS a causa delle peculiarità di questi ultimi. Molti ICS, ad esempio, adottano dispositivi hardware speciali e/o software dedicato e ciò rende semplicemente impossibile il procedere alla loro sostituzione con elementi "policy-aware". La scarsa sensibilità ai problemi di sicurezza, tipica del recente passato, ha inoltre fatto in modo che un gran numero di ICS sia alquanto carente, ancora oggi, di quei meccanismi di protezione a basso livello (per esempio account diversificati, gestione dei diritti ecc.) che rappresentano spesso l'unica opzione disponibile per "costringere" l'utente al rispetto delle policy di accesso. Da questo punto di vista assume quindi cruciale importanza la disponibilità di tecniche e strumenti che consentano di verificare se la configurazione del sistema e dei suoi dispositivi realizzi correttamente quanto specificato dalle policy di alto livello.

La soluzione proposta in quest'articolo si basa su un modello innovativo del sistema da analizzare che permette di coniugare due diversi punti di vista. Il primo (specifica) consente di descrivere le policy di accesso a livello astratto, come solitamente avviene, tramite l'uso di un opportuno formalismo (nel nostro caso, in particolare, si fa uso della diffusa metodologia

role based access control - RBAC [2,3]). Il secondo (implementazione) tiene in considerazione l'effettiva configurazione dei componenti del sistema reale. La definizione del modello a due viste permette di concepire e sviluppare diversi tipi di analisi di sicurezza e, in particolare, il confronto tra le access policy e la configurazione dei dispositivi che le devono supportare [4]. Per meglio chiarire tale concetto, nel seguito si farà riferimento a un esempio di sistema reale.

Modello di impianto prototipale

Il caso di studio preso in esame, illustrato nella ►figura 1 e schematizzato nella ►figura 2, è quello di un impianto flessibile per la riparazione e il riciclaggio di circuiti stampati (PCB) composto da quindici moduli di trasporto che interconnettono varie celle di produzione e buffer di ingresso/uscita.

Figura 1 - Impianto per la riparazione, lo smontaggio e il riciclaggio di circuiti stampati

L'elettronica per la gestione e il coordinamento delle funzioni di ogni modulo è contenuta in un cabinet, indicato dalla freccia nella ►figura 1 e schematizzato in tre esemplari nella ►figura 2, facente parte del modulo stesso. La ►figura 2 indica anche che in ogni cabinet sono presenti due moduli slave ModBus/TCP, uno switch e un PC industriale.

Gli slave ModBus/TCP, oltre alle consuete operazioni con il master dell'impianto, consentono l'amministrazione remota tramite web server. L'accesso a ogni slave è controllato tramite password. I PC industriali, invece, offrono funzionalità tipiche dei PLC tramite l'impiego di due server software (IsaGraf e OPC-UA): le interazioni con tali servizi avvengono remotamente via rete. I dispositivi dedicati all'amministrazione, configurazione e supervisione dell'impianto sono situati nell'area di controllo di processo (connessa via rete a quella di campo) come mostrato nella ►figura 2 (Area 1).

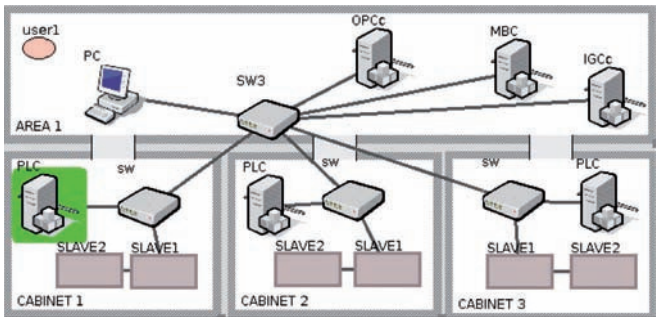

Figura 2 - Schema dell'impianto

Modello del sistema: specifica

La descrizione di una specifica si basa sul noto framework RBAC (Role Based Access Control) [2,3] e sui suoi elementi fondamentali (ruoli, permessi, utenti e relazioni tra questi tre insiemi). I permessi, ad esempio, sono definiti tramite coppie di valori ciascuna delle quali individua un'azione e la risorsa/servizio cui l'azione stessa è associata (per esempio <amministra, web_server>, <opera, web_server>). I permessi sono associati ai diversi ruoli, che tengono conto delle varie responsabilità, e, infine, ogni utente (per esempio Carneade) è assegnato a uno o più ruoli (per esempio "operatori"). I ruoli sono anche inseriti in una relazione gerarchica che, solitamente, rispecchia quella esistente tra le diverse figure operanti nell'impianto reale.

Nel nostro caso, ad esempio, il ruolo "operatori", che può agire sui moduli slave, ha privilegi prettamente operativi e non di configurazione; questi ultimi diritti, infatti, sono riservati agli "amministratori". A più alto livello nella gerarchia si trovano i "responsabili di cella" e i "responsabili d'impianto". I primi hanno in gestione gli slave e i PC/PLC dei diversi moduli, mentre i secondi coordinano e gestiscono operazioni che coinvolgono interazioni tra i PC/PLC delle diverse celle e tra questi e i server OPC e di più alto livello nell'area di controllo di processo.

Modello del sistema: implementazione

La parte di modello identificata come implementazione si basa su due elementi essenziali: la descrizione statica delle risorse del sistema (ad esempio locazioni fisiche, dispositivi, servizi ecc.) e quella delle possibili interazioni tra gli utenti e le risorse stesse. Nel nostro modello, ad esempio, gli ambienti sono risorse dotate di porte che consentono, agli utenti dotati delle opportune credenziali, l'accesso alle varie aree dell'impianto (la ►figura 2 mostra i vari cabinet come aree fisiche distinte, ciascuna collegata ad Area1 mediante opportuno varco/sportello).

I servizi offerti dai PC/PLC sono altri esempi di risorse su cui gli utenti possono compiere azioni condizionate dall'essere in possesso o meno di opportune credenziali. La descrizione dei vari dispositivi dell'impianto (PC, switch, server ecc.), dei servizi da essi offerti, e delle loro interconnessioni in rete costituisce la vista statica del sistema.

La descrizione di ogni risorsa prevede anche quella delle azioni a essa associate. L'esecuzione di un'azione, in genere, richiede il soddisfacimento di opportune precondizioni (per esempio avere accesso al dispositivo che offre il servizio) e l'eventuale possesso di credenziali (per esempio conoscere una password). Il modello contempla tre diverse tipologie di precondizioni riguardanti l'accessibilità fisica, locale e remota. L'accessibilità fisica, ad esempio, è utile per modellare l'interazione con un pannello touch-screen, mentre quella locale consente di tener conto dell'accesso a un dispositivo tramite procedura di login per poterne invocare

i servizi. L'accessibilità remota, infine, permette di considerare l'esecuzione di quelle azioni che sono invocate via rete su risorse situate su nodi differenti.
Nel nostro modello gli effetti dell'esecuzione di un'azione su una risorsa sono tenuti in conto tramite opportune post-condizioni. Un esempio di post-condizione è l'acquisizione di un accesso locale alle risorse ospitate da un dispositivo dell'impianto a seguito dell'esecuzione con successo di un'operazione di login sul dispositivo stesso.
Nel modello d'impianto prototipale gli slave Modbus ospitano la risorsa "web_server" che consente la configurazione remota del dispositivo tramite l'azione "amministra". La stessa risorsa consente di avviare il funzionamento convenzionale dello slave tramite l'azione "opera". L'operazione "amministra" è soggetta al soddisfacimento di una precondizione di tipo "remoto" con specifici parametri di comunicazione (porta/protocollo). L'operazione richiede inoltre una credenziale e non ha particolari post-condizioni. L'azione "opera", è descritta in modo simile ma prevede differenti parametri di comunicazione e non richiede il possesso di credenziali.
Un altro esempio è costituito dalla risorsa "sistema operativo" di ogni PC collocato nell'area di processo. L'operazione "login", per essa definita (<login, sistema_operativo>), richiede quale precondizione l'accesso fisico al PC e il possesso di una password appropriata (credenziale) al fine di far ottenere all'utente che la esegue con successo un accesso locale alle risorse del dispositivo (post condizione).

Verifica delle policy di accesso

La costruzione delle due viste del modello, consente di condurre un'analisi semi-automatica del corretto mapping tra le policy di alto livello e la configurazione dei dispositivi. L'analizzatore software, infatti, utilizza la vista specifica (descrizione dei ruoli, loro gerarchia, utenti, permessi associati ecc.) per enumerare tutti i permessi in possesso di ogni utente del sistema in base ai ruoli assegnati.
La vista implementazione, invece, è utilizzata per costruire l'insieme di tutte le possibili azioni da parte di tutti gli utenti sulle risorse del sistema. Il procedimento seguito in questo caso è più complesso, dovendosi considerare la situazione del sistema e delle sue interazioni con gli utenti, da un punto di vista sia statico sia dinamico. Senza entrare in dettagli, lo strumento software costruisce un diagramma esaustivo di tutte le possibili sequenze di azioni che ogni utente può compiere sulle risorse del sistema utilizzando, per far ciò, la descrizione statica del sistema stesso e un insieme di regole (regole di inferenza) che dettano il comportamento dell'utente e le sue modalità di interazione con i vari oggetti a cui può accedere. In pratica, l'analisi di ciascuna vista produce un insieme di triple del tipo <oggetto, operazione, utente> relative alle sole azioni permesse rispettivamente dalla specifica e dall'implementazione. Il confronto dei due insiemi di triple permette quindi di evidenziare eventuali differenze (violazioni) tra ciò che è definito come "lecito" nella specifica e quello che invece è realmente consentito nel sistema reale.
Ad esempio un comune utente Carneade, che a livello di specifica non è previsto possegga i permessi <amministra, web_server> e <opera, web_server> relativi agli slave Modbus del sistema reale, potrebbe riuscire ad eseguire le suddette operazioni utilizzando legittimamente il nodo PC in Area1. La prima condizione sarebbe resa possibile se l'accesso al servizio "web_server" utilizzasse la password di default, cioè una credenziale nota a tutti (le password di default sono note a tutti gli utenti per definizione). La seconda violazione potrebbe verificarsi in assenza di idonei filtri di comunicazione tra l'area di processo (Area1) e l'area di campo (Cabinet X). L'utente Carneade, infatti, può accedere lecitamente al PC di Area1 e, conseguentemente, agli slave Modbus tramite il canale di comunicazione diretto con l'area di campo che non è esplicitamente filtrato. Per correggere simili violazioni, identificabili dall'analizzatore, è possibile modificare le configurazioni dei servizi coinvolti, ad esempio cambiando la password di default per "web_server" e/o introducendo dispositivi filtranti (firewall) per impedire le comunicazioni tra il nodo PC e i dispositivi ospitati nei cabinet. In ogni caso, tuttavia, l'effetto di una modifica deve essere preventivamente verificato con un nuovo passo di analisi.

Conclusioni

La sicurezza dei sistemi distribuiti di controllo e automazione richiede lo sviluppo di soluzioni tecniche innovative, in grado di tenere in considerazione le peculiarità e i requisiti tipici delle applicazioni industriali. Quest'articolo ha introdotto le caratteristiche salienti di un nuovo modello in grado di descrivere contemporaneamente le due possibili viste (specifica e implementazione) di un sistema ICS per quanto attiene la definizione delle policy di controllo d'accesso. Su tale modello si fonda lo sviluppo di strumenti software di analisi automatica che operano mediante opportuno confronto delle viste. In questo modo è possibile evidenziare e correggere possibili differenze (violazioni) tra la definizione delle policy di accesso ad alto livello e la configurazione dei meccanismi di sicurezza a basso livello presenti nel sistema reale.

Bibliografia

[1] M. Cheminod, L. Durante, and A. Valenzano, "Review of Security Issues in Industrial Networks," *IEEE Trans. Ind. Informat.*, Vol. 9, n. 1, pp. 277-293, 2013.
[2] Ansi Incits, "Role Based Access Cotnrol", *Ansi Incits,* 359/2012, 2012.
[3] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-Based Access Control Models," *IEEE Computer*, vol. 29, n. 2, pp. 38–47, 1996.
[4] M. Cheminod, L. Durante, L. Seno, and A. Valenzano, "On the Description of Access Control Policies in Networked Industrial Systems", *Proc. of the 10th IEEE Int. Workshop on Factory Communication Systems* (WFCS 2014), pp. 1-10, 2014

RINGRAZIAMENTI
Questo lavoro è stato svolto nell'ambito del Progetto Bandiera CNR "Fabbrica del Futuro" - sottoprogetto "Generic Evolutionary Control Knowledge-based mOdule" (GECKO).