La cybersecurity delle reti industriali

I sistemi industriali possono essere bersaglio dello stesso tipo di cyber-attacchi subiti dalle reti general-purpose, e il semplice impiego delle contromisure concepite e sviluppate per queste ultime non può rappresentare una soluzione di sicurezza efficace. Questo articolo illustra alcune metodologie e possibili soluzioni, proposte recentemente nella letteratura scientifica e finalizzate alla riduzione dei rischi sotto soglie predeterminate, nel contesto del processo di gestione della sicurezza contemplato dagli enti di standardizzazione internazionali.

Luca Durante
Adriano Valenzano

Keyword

Sicurezza delle reti, analisi del rischio, contromisure per la sicurezza, comunicazioni industriali

Le reti di comunicazioni industriali (SCAI - sistemi di controllo e automazione industriale) del passato erano ambienti "chiusi" per topologia e tecnologie adottate e, come tali, relativamente protette da attacchi informatici. Il continuo sviluppo di tecniche di comunicazione ha reso facile e conveniente l'interconnessione e l'integrazione dei diversi sottosistemi, tipicamente presenti nei contesti manifatturieri, al prezzo di una loro crescente esposizione agli stessi tipi di minacce che da tempo affliggono le reti d'ufficio (SCUG - sistemi computerizzati da ufficio e/o gestionali).

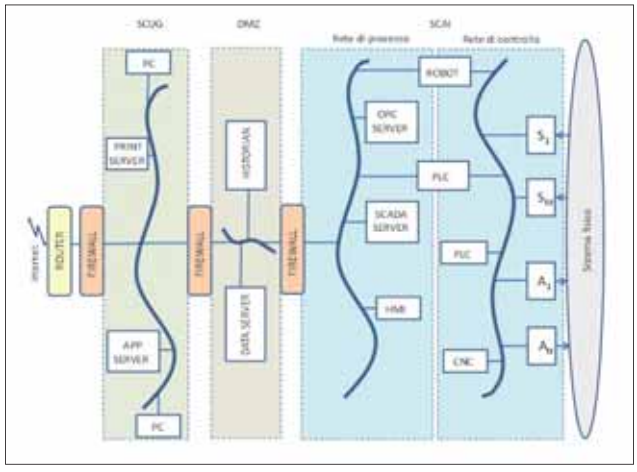

Figura 1 - Interconnessione di reti SCAI, SCUG e Internet

La ►**figura 1** schematizza una comune topologia d'interconnessione di una rete SCAI a una SCUG e a Internet.
L'infrastruttura SCAI è costituita dai due blocchi di destra. Le linee ondulate indicano differenti mezzi di comunicazione e relativi apparati. L'infrastruttura SCAI, a differenza delle SCUG, è connessa direttamente a un sistema fisico (processo, impianto d'automazione ecc.), tramite i suoi sensori e attuatori. La zona demilitarizzata (DMZ) consente la condivisione di risorse tra SCAI e SCUG senza connessioni dirette (tecnica di sicurezza piuttosto comune).
Si considerino ora i tre requisiti di sicurezza principali:

- *availability* cioè la disponibilità all'accesso da parte di altre entità;
- *integrity* cioè la salvaguardia dell'accuratezza e dell'integrità dell'informazione;
- *confidentiality* cioè la garanzia che l'informazione non sia resa disponibile ai non autorizzati.

	SCAI	SCUG
Priorità Crescente	availability	confidentiality
	integrity	integrity
	confidentiality	availability

Tabella 1 - Requisiti fondamentali di sicurezza.

SCAI e SCUG differiscono per le priorità assegnate ai requisiti (►**tabella 1**) e, conseguentemente, per le metodologie che occorre adottare per soddisfare gli stessi.
Se si considera, invece, la criticità dei requisiti,

	SCAI	SCUG
Aggiornamento di hardware e software	critico	non critico
Vincoli di tempo reale	critici	non critici
Conseguenze di guasti e attacchi	critiche	non critiche
Prestazioni e requisiti energetici	critici	non critici

Tabella 2 - Criticità differenti per reti SCAI e SCUG.

GLI AUTORI
L. Durante, A. Valenzano - IEIIT - Consiglio Nazionale delle Ricerche (CNR)

occorre fare riferimento alla ►**tabella 2**.

In particolare si tenga presente che:

- L'aggiornamento di software (s/w) e hardware (h/w) per la protezione da nuove vulnerabilità è frequente nelle SCUG, ma in molte SCAI richiederebbe che il sistema fosse messo temporaneamente in stato di off-line. Purtroppo, questo tipo d'intervento, quando possibile, dev'essere pianificato con anticipo notevole, ma è spesso incompatibile con il requisito di availability.
- I vincoli di tempo reale di molte SCAI rendono difficile/impossibile la pianificazione di attività asincrone come gli aggiornamenti del s/w anti-virus. Firewall e filtri di rete, inoltre, possono introdurre ritardi non predicibili nel controllo dei processi.
- I guasti delle SCUG causano danni economici e/o di reputazione, poiché solo i dati sono oggetto di protezione. Ovviamente ciò è importante anche per le SCAI, dove, tuttavia, le conseguenze possono essere gravi anche per l'ambiente e gli esseri umani (correlazione tra security e safety).
- Prestazioni e consumi sono critici nei sistemi SCAI, dove molti dispositivi hanno capacità computazionali ridotte e/o disponibilità limitata di energia. Ciò rende arduo l'uso di sistemi avanzati di crittografia e di protocolli per la sicurezza, normalmente piuttosto avidi di risorse di calcolo.

Alla luce di queste considerazioni appare evidente come l'utilizzo di contromisure "general-purpose" in reti industriali richieda attenzioni particolari e valutazioni precise.

Le ricerche condotte dalla comunità scientifica seguono due approcci differenti e complementari. Il primo considera il sistema/la rete nel suo insieme, indipendentemente dalla dimensione e complessità, e ne valuta le caratteristiche su un piano globale (livello di sistema). Il secondo affronta aspetti specifici di sicurezza a livello di componente, ove il termine "componente" si riferisce non solo al singolo meccanismo ma, all'occorrenza, anche a un insieme di meccanismi h/w e/o s/w atti a migliorare il grado di sicurezza. Esempi di componenti sono i firewall, i protocolli crittografici, gli intrusion detection system (IDS), gli algoritmi per l'autenticazione ecc. Naturalmente le strategie che operano a livello di sistema si basano o fanno uso di soluzioni che agiscono a livello di componente.

La parte restante di quest'articolo è così strutturata: il paragrafo seguente presenta una breve panoramica delle attività di standardizzazione nel settore della sicurezza delle reti industriali al fine di renderle "security-aware". Successivamente si affronta il problema della sicurezza dei sistemi SCAI a livello di sistema, mentre il paragrafo seguente tratta alcuni aspetti di sicurezza a livello di componente, cioè dei meccanismi che sono utilizzati per prevenire o identificare gli attacchi.

Riferimenti normativi

A prescindere dalla terminologia utilizzata, i principali enti di normazione sono concordi nel considerare l'information security management (ISM) come un processo iterativo che coinvolge tutti gli aspetti di un'organizzazione industriale. I principali documenti normativi che riguardano l'ISM adottano modelli concettuali simili. Un possibile schema riassuntivo è visualizzato nella ►**figura 2**, dove la sequenza dei passi logici necessari è illustrata sul lato sinistro, mentre a destra sono elencati gli eventi che attivano e/o reiterano il processo fino al raggiungimento di una situazione soddisfacente, confermata dal passo di validazione. La validazione è necessaria per verificare che il livello complessivo di rischio sia stato (ri)condotto al di sotto della soglia di accettabilità e solitamente implica attività off-line (risk assessment) e run-time (monitoring).

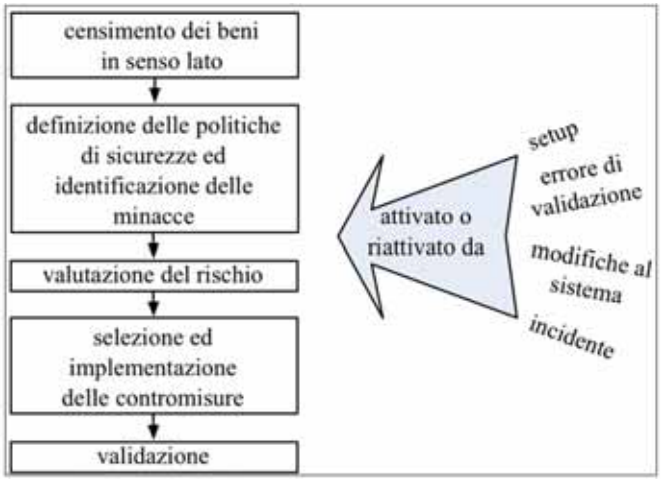

Figura 2 - Principali fasi dell'ISM

L'approccio ANSI/ISA [1] si concentra principalmente sulla sicurezza dei sistemi di automazione industriale e controllo di processo, mentre le norme ISO/IEC [2] e NIST [3] considerano sistemi ICT generici, e possono quindi essere utilizzate e adattate a situazioni diverse. A complemento di ciò, sia ISO/IEC [4] sia NIST [5,6] hanno anche definito linee guida più specifiche per quanto concerne il risk assessment. NIST, infine, affronta anche esplicitamente la sicurezza dei sistemi SCAI [7].

Le contromisure possono invece essere classificate in funzione di come si oppongono alle minacce, cosicché è possibile identificare tre diverse modalità di difesa: prevenzione, identificazione e reazione/recupero. Le proposte in letteratura appartengono anche a più di una di queste categorie contemporaneamente.

Metodologie di analisi e progetto a livello di sistema

La valutazione del rischio (funzione della probabilità di verificarsi di un evento indesiderato e della quantificazione delle sue conseguenze) richiede l'identificazione degli elementi chiave del sistema e delle situazioni potenzialmente dannose. Tali compiti competono ai primi tre passi di qualsiasi ISM (►**figura 2**), e devono essere condotti a livello di sistema, tenendo in conto le interdipendenze tra tutti gli elementi in gioco. Tradizionalmente le conseguenze del rischio sono valutate in termini di danno economico, anche se tale metrica può essere particolarmente riduttiva per le SCAI, dove è frequente l'impatto su vite umane e ambiente.

Le metodologie di risk analysis in letteratura possono essere raggruppate in tre

famiglie principali, che differiscono per il modo con cui il sistema è dapprima modellato e poi analizzato [8]:

- L'approccio Hierarchical Holographic Model (HHM) scompone il sistema con interdipendenze complesse in viste indipendenti tra loro. Le viste, possono essere ricomposte in modo coerente consentendo l'identificazione di tutte le possibili forme di rischio.
- La tecnica Inoperability Input-Output Model (IIOM) supera alcune limitazioni di HHM: quando le interdipendenze sono eccessivamente complesse, occorre modellare le interazioni tra i vari sottosistemi in cui il sistema è scomposto.
- Il Probabilistic Risk Assessment è, invece, l'approccio più utilizzato: il sistema è modellato sotto forma di grafo i cui vertici rappresentano i componenti e gli archi le dipendenze tra i componenti stessi.

È opportuno che i modelli siano analizzati in modo (semi)automatico da strumenti s/w. Per fornire indicazioni efficaci, infatti, il modello deve essere dettagliato e, nel caso di sistemi complessi e/o di ampie dimensioni, la gran mole di dati è generalmente difficile da gestire manualmente. Recentemente in ambito accademico sono state sviluppate alcune metodologie e prototipi di strumenti s/w volti ad automatizzare l'analisi del rischio. In [9], in particolare, è affrontato il problema dell'analisi di vulnerabilità: la descrizione del sistema (topologia, protocolli, moduli s/w installati ecc.) è integrata con quella delle vulnerabilità conosciute, in termini di prerequisiti per il loro sfruttamento e relative conseguenze. Lo strumento di analisi acquisisce la descrizione e identifica gli attacchi che possono essere condotti sfruttando le vulnerabilità presenti.
Il modello, per sua natura, può descrivere anche un sistema ancora in fase d'ideazione. Analogamente, qualora lo strumento evidenzi debolezze nel sistema, è possibile procedere all'analisi di un modello opportunamente modificato, fino al raggiungimento del grado di robustezza desiderato. Allo stesso modo è possibile analizzare e comparare soluzioni diverse per un identico problema, dando luogo a ciò che è comunemente nota come "what if analysis".
Un approccio differente a livello di sistema, specifico per le SCAI e in particolare sistemi di controllo, è stato presentato in [10]. In questo caso le conseguenze indesiderate di un attacco sono integrate nelle equazioni del sistema di controllo. Interessante è il cambio di prospettiva: gli autori, infatti, non si concentrano sulle vulnerabilità sfruttabili da un attaccante, ma sull'obiettivo finale dell'attacco.

Contromisure a livello di componente

Contromisure per la prevenzione
In estrema sintesi si può affermare che la maggior parte delle proposte presenti in letteratura si concentra su meccanismi atti a garantire l'autenticità e la confidenzialità delle informazioni. In quest'ambito si passa dall'impiego di chiavi simmetriche condivise (che hanno varie controindicazioni: ad esempio generare una proliferazione di chiavi diverse o costituire un "single point of failure" quando la chiave è unica per tutti) all'utilizzo delle più moderne tecniche di crittografia asimmetrica, che richiede risorse computazionali non sempre disponibili negli ambienti industriali. Promettente appare l'uso della Elliptic Curve Cryptography (ECC) [11] che è più efficiente delle tecniche tradizionali.

Contromisure per l'identificazione
Le contromisure per l'identificazione sono giustificate dal fatto che non è possibile prevenire tutte le minacce, soprattutto a causa delle vulnerabilità ignote (non ancora scoperte) e del lungo ciclo di vita dei componenti dei sistemi SCAI, che sono obiettivamente meno aggiornati ed attrezzati contro le modalità di attacco più recenti.
In buona sostanza tali contromisure s'identificano spesso con gli IDS, sviluppati dagli anni '80 per le SCUG, che hanno lo scopo di riconoscere situazioni anomale monitorando le attività in corso nel sistema.
Rispetto alla classificazione classica gli IDS per le SCAI sono prevalentemente di tipo network-based (utilizzano cioè informazioni provenienti da più parti della rete) e anomaly detection-based (operano identificando le anomalie rispetto al comportamento atteso del sistema).
Un'altra dicotomia per gli IDS industriali è basata sulla relativa stabilità dei sistemi SCAI e sullo stato globale del sistema in esame [8]. Si parla allora di IDS stateful (da non confondere con i firewall stateful), mentre il termine stateless è riservato agli IDS che non sfruttano tale conoscenza.
Gli IDS stateless richiedono la conoscenza del comportamento atteso del sistema e la capacità di misurare le differenze tra il comportamento ideale e quello effettivo. Le prestazioni, in questo caso, non sono generalmente un elemento critico poiché la distanza tra il comportamento atteso e quello patologico è computata in modo efficiente. Critico è invece l'aspetto del grado di accuratezza raggiunto, che può essere valutato soltanto a posteriori o attraverso simulazioni.
Gli IDS stateful presuppongono di disporre anche di un modello costituito da tutti gli stati del sistema stesso e dalle relative transizioni tra gli stati. Sulla base delle informazioni acquisite dal sistema reale, gli IDS stateful determinano lo stato corrente e stabiliscono se esso rappresenti (o preluda a) una potenziale situazione di pericolo; in questo caso vengono anche attivate le idonee procedure di segnalazione e le contromisure di reazione. Questa metodologia garantisce un livello di accuratezza assoluto in qualsiasi circostanza perché non dipende dai passi effettuati per condurre un attacco, ma solo dal suo obiettivo.

Conclusioni

La gestione della sicurezza delle reti di comunicazioni industriali è universalmente riconosciuta come un processo iterativo da tutti gli enti di normazione attivi nel settore.
Quest'articolo ha presentato, in breve, alcuni aspetti particolarmente rilevanti che costituiscono lo stato dell'arte per quanto riguarda la ricerca scientifica nello scenario della cyber-security dei sistemi industriali.
In particolare è stato posto in evidenza come la realizzazione di un informa-

tion security management system moderno debba prevedere due livelli complementari di intervento. A livello di sistema si collocano, infatti, tutte le tecniche di analisi e gestione del rischio che richiedono, tra l'altro, un grado elevato di astrazione. A tale ambito appartengono anche le metodologie e gli strumenti di definizione delle politiche di sicurezza e le soluzioni concepite per la loro gestione.
A livello di componente si trovano invece le contromisure che possono essere adottate per l'implementazione delle politiche di alto livello, ovvero i meccanismi di prevenzione, identificazione e reazione. L'articolo ha introdotto una classificazione schematica delle soluzioni proposte in letteratura ed ha fatto particolare riferimento agli approcci che, al momento, appaiono più promettenti per il progetto e la realizzazione sistemi security-aware di nuova generazione.

Bibliografia

[1] ANSI/ISA: *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*, ANSI/ISA Std. 99.02.01-2009, 2009.
[2] ISO/IEC: *Information Technology - Security Techniques - Information Security Management Systems – Requirements*, ISO/IEC Std. 27001, 2005.
[3] NIST: *Minimum Security Requirements for Federal Information and Information Systems*, NIST Std. FIPS 200, 2006.
[4] ISO/IEC: *Information Technology - Security Techniques - Information Security Risk Management*, ISO/IEC Std. 27005, 2008.
[5] NIST: *Guide for Applying the Risk Management Framework to Federal Information Systems - A Security Life Cycle Approach*, NIST SP 800-37 rev. 1, 2010.
[6] NIST: *Managing Information Security Risk - Organization, Mission, and Information System View*, NIST SP 800-39, 2011.
[7] K. Stouffer, J. Falco, and K. Scarfone, *Guide to Industrial Control Systems (ICS) Security*, NIST SP 800-82, 2008.
[8] M. Cheminod, L. Durante, and A. Valenzano, "Review of Security Issues in Industrial Networks", *IEEE Trans. Ind. Informat.*, Vol. 9, No. 1, pp. 277-293, 2013.
[9] M. Cheminod, I. Cibrario Bertolotti, L. Durante, P. Maggi, D. Pozza, R. Sisto, and A. Valenzano, "Detecting Chains of Vulnerabilities in Industrial Networks", *IEEE Trans. Ind. Informat.*, vol. 5, no. 2, pp. 181–193, 2009.
[10] A. A. Cárdenas, S. Amin, Z.-S. Lin, Y.-L. Huang, C.-Y. Huang, and S. Sastry, "Attacks Against Process Control Systems: Risk Assessment, Detection, and Response", in *Proc. 6th ACM Symp. on Information, Computer and Communications Security (ASIACCS)*, pp. 355–366, 2011.
[11] D. Hankerson, A. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*. Springer, 2004.