Analisi e rilevamento intelligente di processi di attacco alle Smart-Grid

Davide Cerotti[1], Daniele Codetta-Raiteri[1], Giovanna Dondossola[2], Lavinia Egidi[1], Giuliana Franceschinis[1], Luigi Portinale[1], Roberta Terruggia[2]

[1]Istituto di Informatica, DiSIT, Univ. del Piemonte Orientale, Alessandria, Italia

[2]RSE: Ricerca sul Sistema Energetico, Milano, Italia

{davide.cerotti, daniele.codetta, lavinia.egidi, giuliana.franceschinis, luigi.portinale}@uniupo.it

{giovanna.dondossola, roberta.terruggia}@rse-web.it

Abstract

Proponiamo una metodologia basata sulle Reti Bayesiane come strumento di supporto all'analisi della sicurezza di Smart Grid, ed in particolare per la previsione di intrusioni e attività ostili.

1 Introduzione

La protezione delle piattaforme digitali utilizzate da infrastrutture critiche viene individuata come una priorità a livello internazionale in quanto negli ultimi anni si sono verificati attacchi a sistemi energetici, quali Stuxnet, Drangonfly, Black Energy e Industroyer. Per rispondere in modo adeguato alla Direttiva Europea 2016/1148 - Network and Information Security (NIS) indirizzata agli operatori di servizi essenziali, è fondamentale sviluppare strumenti evoluti orientati alla valutazione della sicurezza in scenari dove le possibili minacce sono in continua evoluzione. In primo luogo occorre valutare l'efficacia di misure di sicurezza già disponibili per la protezione degli asset e delle comunicazioni nei sistemi energetici. Esiste poi la necessità di gestione degli incidenti cyber: lo stato delle tecnologie di monitoraggio e rilevamento di anomalie giocano un ruolo fondamentale nell'intercettare tempestivamente azioni ostili, interrompere l'avanzamento dei processi di attacco ed implementare rimedi efficaci. Il grado di maturità delle tecnologie di *anomaly detection* attualmente disponibili è considerato insufficiente. Un obiettivo dello strumento di valutazione è prevenire nuovi possibili scenari di attacco, per anticipare potenziali azioni offensive.

La metodologia di modellazione e valutazione che proponiamo è basata sulle *Reti Bayesiane* (BN) [Portinale e Codetta, 2015], modello di riferimento per sistemi di ragionamento in presenza di incertezza in IA. La costruzione della BN parte dall'analisi di dati di attacchi reali su un'architettura di riferimento per sistemi di controllo industriale (ICS). I dati provengono in parte dal progetto MITRE ATT&CK (attack.mitre.org) e sono ispirati al progetto MITRE ICS ATT&CK non ancora disponibile. Per la parte di monitoraggio ci basiamo sul progetto MITRE Cyber Analytic Repository (car.mitre.org/wiki/Main_Page).

Il tool securiCAD (www.foreseeti.com/securicad) utilizza una metodologia simile, che permette di generare automaticamente grafi di attacco e difesa, in ambito ICT, i quali prendono la forma di modelli grafico-probabilistici. Quindi calcola la probabilità di successo di attacchi e il Time To Compromise degli asset di una data architettura di rete. In securiCAD i passi di attacco e le loro dipendenze logiche sono cablati nel sistema, rendendo difficile sia l'analisi del modello, sia la valutazione dei risultati. Il nostro approccio si propone di superare tali limitazioni, sviluppando una metodologia aperta, estendibile e orientata alle piattaforme dei sistemi energetici. [Rahimi *et al.*, 2018] descrive un lavoro recente che studia la sicurezza delle power grid ed è basato su tecniche e analitiche dei progetti MITRE. A differenza del nostro approccio, è ristretto alla valutazione del livello di sicurezza della rete in esame in un dato intervallo di tempo.

2 Strumenti e metodologia

La nostra metodologia è costruita su un'architettura di riferimento [Stouffer *et al.*, 2015] per ICS, caratterizzata dalla compresenza di due sottoreti molto diverse sia per i protocolli utilizzati sia per i requisiti operativi e di sicurezza. La prima, la *corporate network*, è una classica rete di computer che obbedisce alle regole della Information Technology (IT). L'altra rete, nella quale si concentrano i processi di ICS, è una rete Operational Technology (OT). Le due reti devono comunicare, pertanto le best practices raccomandano di interporre tra le due aree una DMZ per imporre la segregazione del traffico. I processi di attacco sono generalmente costituiti da più passi distribuiti in un arco temporale ampio, anche di diversi mesi [Hutchins *et al.*, 2011]. Molto spesso gli attacchi ad un ICS iniziano con la compromissione di una macchina nell'area IT, utilizzando tecniche standard (ad esempio, spear phishing) e poi procedono con movimenti laterali che portano l'attaccante attraverso la DMZ alla rete OT. Da qui vengono sferrati attacchi specifici al dominio di applicazione (nel nostro caso il sistema energetico). La nostra ricerca è incentrata su questa ultima fase, ma pone attenzione anche alla fase intermedia di movimento laterale.

La modellazione passa attraverso un formalismo intermedio, i *grafi di attacco* (AG), i cui nodi sono stati e i cui archi sono etichettati con passi di attacco che derivano dai progetti MITRE che propongono matrici che contengono tutti gli attacchi "atomici" identificati nell'analisi dei rapporti dei casi reali noti, in ambito IT, OT e ICS. Tali passi prendono il nome di *tecniche* e sono raggruppati in base ai loro obbiettivi a breve termine (accesso iniziale, movimento laterale, ecc.). Nel progetto MITRE ATT&CK sono suggerite delle misu-

Tabella 1: Risultati della valutazione della BN

Evidenze	Compromis. DMZ	Compromis. SCADA	Instabilità Sistema
nessuna	0.00529	2.80133e-05	2.82830e-06
tutte An. off	0.00476	1.91003e-05	1.25377e-06

a) Monitoraggio del sistema di sicurezza

Analitiche	A priori	Compromissione
NICS	0.04834	0.05221
MASQ	0.05648	0.06031

b) Valutazione rischi per pianificazione difese

Analitiche	ON	OFF	Riduzione
CD	0.69623	0.06708	90.36%
SBM	0.26001	0.06564	74.75%

c) Pianificazione del sistema di monitoraggio

Legenda: CD = Coherence with Device; SBM = Service Binary Modification; NICS = New ICS Service; MASQ = Masquerading;

re di frequenza delle tecniche basate sul numero di gruppi avversariali che le hanno utilizzate, sul numero di software (malware e utility di sicurezza) in cui sono implementate e sulla frequenza con cui compaiono in letteratura. Tali dati non erano disponibili per le tecniche specifiche dell'ambito ICS, per cui abbiamo derivato delle stime di frequenze da dati estratti dal database ICS-CERT Vulnerability Advisory (ics-cert.us-cert.gov/advisories), basandoci sul Common Vulnerability Scoring System (CVSS, www.first.org/cvss). In aggiunta, nel nostro lavoro utilizziamo le *analitiche* (ancora da un progetto del MITRE) che sono evidenze del fatto che siano stati fatti degli attacchi: se un'analitica è associata ad una tecnica, implementando il sensore corrispondente nel sistema di monitoraggio si ottiene lo scatto di un allarme nel caso la tecnica venga utilizzata dagli attaccanti.

3 Analisi

Abbiamo costruito un AG per il generico movimento laterale e uno per un generico attacco contro un servizio della rete OT, e a partire da questi abbiamo costruito la BN. Le Fig. 1 e 2 mostrano rispettivamente il secondo AG e la BN corrispondente. In realtà la BN utilizzata per l'analisi è più ampia perché considera tutto lo scenario di attacco (IT, OT, ICS), e consente di calcolare la distribuzione di probabilità di qualunque nodo, data l'osservazione dei valori di altri nodi. Usiamo *GeNIe* (download.bayesfusion.com) a questo scopo.

La Tab. 1a mostra le probabilità di compromettere la DMZ, lo SCADA, e di rendere il sistema instabile, nel caso in cui non siano state implementate analitiche, e nel caso in cui invece siano state implementate ma non rilevino nulla. Il modello considera analitiche imperfette, cioè la possibilità di falsi positivi e falsi negativi. La Tab. 1b mostra le probabilità a priori di due tecniche assieme alle probabilità condizionate dall'aver osservato il sistema in stato instabile. Infine assumiamo di osservare la compromissione dello SCADA e lo stato di una sola analitica per volta: la Tab. 1c mostra la criticità di due analitiche confrontando le probabilità di avere il sistema instabile, ottenute osservando l'analitica attiva o meno.

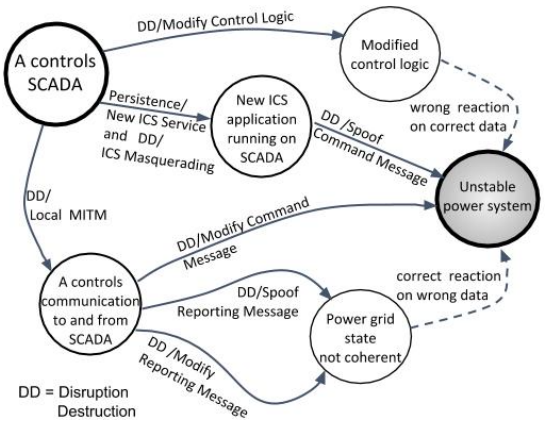

Figura 1: AG dell'attacco all'ICS

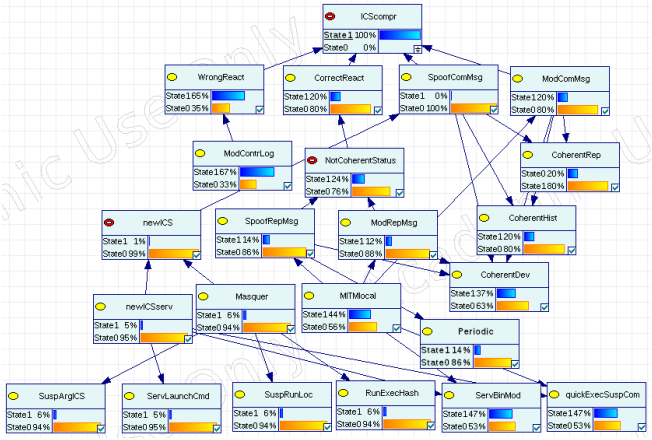

Figura 2: BN derivata dall'AG in Fig. 1

4 Conclusioni

Il nostro approccio basato su BN valuta il livello di sicurezza di una smart grid, considerando i livelli IT, OT e ICS, e calcolando misure basate sulla probabilità condizionata. Sviluppi futuri saranno la modellazione di maggiori dettagli nello scenario di attacco e l'inclusione di ulteriori dati reali.

Riferimenti bibliografici

[Hutchins *et al.*, 2011] E.M. Hutchins, M.J. Cloppert, e M.R. Amin. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research*, 1, 01 2011.

[Portinale e Codetta, 2015] L. Portinale e D. Codetta. *Modeling and Analysis of Dependable Systems: A Probabilistic Graphical Model Perspective*. World Scientific Pub., 2015.

[Rahimi *et al.*, 2018] A. Rahimi, A. Hahn, e M. Merrick. Continuous security monitoring techniques for energy delivery systems, 2018. cred-c.org/videos/continuous-security-monitoring-techniques-energy- delivery-systems.

[Stouffer *et al.*, 2015] K. Stouffer, V. Pillitteri S. Lightman, M. Abrams, e A. Hahn. SP800-82Rev2, NIST, Guide to industrial control systems (ICS) security, 2015.