Studio delle problematiche di sicurezza e sostenibilità delle architetture di rete per contesti industriali e infrastrutture critiche

Progetto

Il progetto di ricerca proposto si colloca nell'ambito della Sicurezza Informatica, in particolare sulla sicurezza delle reti.
La sicurezza delle reti è un processo che coinvolge sempre di più tutti i livelli logici e architetturali, e ha implicazioni anche sul consumo di risorse associate all'esecuzione dei compiti di monitoraggio e reazione agli attacchi.
Nello specifico settore delle reti per contesti industriali e infrastrutture critiche è quindi necessario studiare in modo coerente:

- gli aspetti legati alle tecnologie proprie dei suddetti settori, in termini di protocolli e architetture di connessione
- di integrazione tra le reti collocate sugli impianti e l'architettura cloud che oggigiorno costituisce un elemento imprescindibile per l'elaborazione dei dati raccolti

L'obiettivo del progetto proposto è di affrontare le due tematiche in modo da identificare i problemi più rilevanti, e di proporre soluzioni che salvaguardino le proprietà di sicurezza tenendo in considerazione vincoli di minimizzazione dell'impatto eneregetico.
A questo fine si può considerare come quadro di riferimento quello delle SDN (Software Defined Network) in cui il comportamento complessivo della rete è pilotato tramite un*control plane* che dialoga da un lato con applicazioni di qualsivoglia complessità, da utilizzarsi per diagnosticare il funzionamento della rete e per definire le politiche di riconfigurazione dinamica,e dall'altro con il *data plane* formato dai dispositivi che materialmente smistano i flussi di traffico.
Il modello consolidato di SDN ha però alcuni limiti che ne pregiudicano le prestazioni e l'integrabilità con reti che utilizzino protocolli particolari come quelli del contesto industriale. Risulta opportuno indagare possibili modalità di arricchimento delle funzionalità standard, introducendo il concetto di data-plane programmabile (ad esempio con *switch P4-enabled*) e riadattando lo stack logico e protocollare per consentire un salto di efficacia ed efficienza in termini di informazioni raccolte a livello data-plane, interazione tra data- e control-plane, e attuazione di meccanismi di gestione dei flussi dati.

Piano di attività

Nell'arco dell'anno allocato per la realizzazione del progetto si prevedono le seguenti attività:

- Studio delle architetture di rete per contesti industriali e infrastrutture critiche (field bus di maggiore diffusione, reti time-sensitive, e simili)
- Studio delle architetture SDN e delle evoluzioni basate su data-plane programmabile con P4
- Caratterizzazione delle proprietà di sicurezza di tali architetture
- Individuazione di eventuali vulnerabiliità e indicazione delle possibilità di mitigazione
- Sviluppo di ambienti di simulazione per reti industriali basati su dispositivi data-plane programmabili
- Progetto di architetture di integrazione tra dispositivi data-plane e reti software-defined, per delineare un modello di sistema che si estenda dal'impianto al cloud computing center, valutando l'impatto in termini di sicurezza e di utilizzo delle risorse conseguente all'impiego degli strumenti di monitoraggio e riconfigurazione implementabili

Study of the safety and sustainability issues of network architectures for industrial contexts and critical infrastructures

Project

The proposed research project addresses the field of Information Security, in particular network security.
Network security is a process that increasingly involves all logical and architectural levels, and also has implications on the consumption of resources associated with the execution of monitoring tasks and response to attacks.
In the specific sector of networks for industrial contexts and critical infrastructures, it is therefore necessary to study in a coherent way:

- the aspects related to the technologies of the aforementioned sectors, in terms of connection protocols and architectures
- the integration between the networks located on plants and the cloud architecture, which today constitutes an essential element for the processing of collected data.

The objective of the proposed project is to study the two issues in order to identify the most relevant problems, and to propose solutions that safeguard the security properties while taking into account the minimization of the energy impact.
To this end, the SDN (Software Defined Network) framework can be considered as a reference. In SDN, the overall behavior of the network is driven by a control plane that communicates on one side with applications of any complexity, to be used to diagnose the functioning of the network and to define dynamic reconfiguration policies, and on the other side with the data plane formed by the devices that physically dispatch the traffic flows.
However, the consolidated SDN model has some limitations that affect its performance and integration with networks that use particular protocols, such as those of the industrial context. It is appropriate to investigate possible ways of enriching its standard functions, by introducing the concept of programmable data-plane (for example with P4-enabled switch) and readjusting the logical model and the protocol stack, to allow a leap in effectiveness and efficiency in terms of information collected at the data-plane, interaction between data and control planes, and implementation of data flow management mechanisms.

Activity plan

During the year allocated for the realization of the project, the following activities are planned:

- Study of network architectures for industrial contexts and critical infrastructures (most widespread field buses, time-sensitive networks, and similar technologies)
- Study of SDN architectures and its evolutions based on programmable data-plane with P4
- Characterization of the security properties of such architectures
- Identification of any vulnerabilities and indication of possible mitigations
- Development of simulation environments for industrial networks based on programmable data-plane devices
- Design of integration architectures between data-plane devices and software-defined networks, to outline a system model that extends from the plant to the cloud computing center, evaluating the impact in terms of security and use of resources resulting from using the monitoring and reconfiguration tools enabled by the same model