ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Master Universitario di II livello in Homeland Security

Tecniche avanzate per l'analisi e la protezione delle infrastrutture di trasporto pubblico

Anno Accademico 2008/2009

Relatore
Ing. Concetta Pragliola

Correlatore
Ing. Francesco Flammini

Candidato
Alfio Pappalardo

Introduzione

Nel mondo globalizzato lo sviluppo di un territorio appare sempre più legato alla capacità di garantire alle persone e alle strutture che su di esso risiedono un sufficiente livello di sicurezza rispetto ad atti criminosi, compresi gli attacchi terroristici, gli incidenti e gli eventi naturali avversi. Negli ultimi anni, in tutti i Paesi occidentali si è diffusa la consapevolezza che alcune delle infrastrutture che assicurano lo sviluppo, la sicurezza e la qualità della vita sono altamente vulnerabili, sia nei confronti di minacce antropiche, sia a seguito di eventi naturali. Il benessere e il mantenimento delle funzioni vitali di un Paese dipendono sempre più dal funzionamento, continuo e coordinato, di tali infrastrutture che, per la loro importanza, sono definite *Infrastrutture Critiche*.

Con il termine infrastruttura critica (CI, *Critical Infrastructure*) si intende un sistema, una risorsa, o un processo, la cui distruzione, interruzione (anche parziale) o momentanea indisponibilità ha l'effetto di indebolire in maniera significativa l'efficienza e il normale funzionamento di un Paese, oppure il suo livello di sicurezza, e il sistema economico-finanziario e sociale. Tali infrastrutture, quindi, devono essere protette in modo adeguato.

La protezione di infrastrutture critiche (CIP, *Critical Infrastructure Protection*) è diventata un'attività sempre più importante e delicata, che richiede lo sviluppo di approcci innovativi per l'identificazione e la mitigazione delle relative vulnerabilità, rischi o minacce. L'introduzione di efficaci tecniche di valutazione di quest'ultime si è dimostrata

impegnativa, soprattutto a causa della dinamicità e interconnettività delle CI.

Nell'ambito delle infrastrutture critiche, i sistemi di trasporto di massa giocano un significativo ruolo sociale ed economico nella connessione di diverse città o di diverse zone di una stessa città, non solo in termini di trasporto di passeggeri. Data la stratetigicità di queste infrastrutture è indiscussa l'esigenza di ridurre, a livelli socialmente ed economicamente sostenibili, il rischio connesso agli effetti sia di eventi tipo naturale e catastrofico, che di azioni intenzionali gravi - come atti di microcriminalità, vandalismo, furti, sabotaggi, fino ad arrivare agli attacchi terroristici - rispondendo in modo adeguato e preventivo alle minacce.

In particolare, la minaccia terroristica ha fatto emergere il problema della vulnerabilità dei passeggeri, come dimostrato dai numerosi episodi di diversa gravità che si sono susseguiti negli ultimi anni, tra cui gli attentati di Madrid e Londra. Un'accurata analisi del rischio nei confronti di atti di natura dolosa e l'impiego di tecnologie di protezione sempre più avanzate rappresentano la strada da seguire per fronteggiare tali minacce.

Da parte degli operatori è sempre più sentita l'esigenza di dotarsi di meccanismi che consentano di proteggere il sistema da tutte le minacce che provengono in qualche modo dall'esterno (problematica che rientra tra quelle di *security*) e quelle che riguardano la garanzia dell'integrità del sistema e degli utenti nei confronti di malfunzionamenti di origine non intenzionale (tematica che rientra tra quelle di *safety*). L'interesse per la security, da parte del mondo della ricerca e dell'industria, è cresciuto di pari passo con il mutato clima socio-politico internazionale. La strada da percorrere per arginare i diversi fenomeni in grado di minacciare i sistemi di trasporto parte senz'altro dall'adozione di adeguate metodologie e tecnologie.

I fenomeni da fronteggiare richiedono prima di tutto un'attività di analisi del rischio che si pone l'obiettivo di valutare in maniera rigorosa le minacce a cui il sistema è esposto al fine di pianificare gli interventi di protezione più adatti, in termini di rapporto costi/benefici, per la riduzione del rischio. Tale attività viene spesso indicata con la denominazione anglosassone di *Risk Analysis*. Tecniche avanzate di analisi sono possono garantire

importanti benefici all'intero processo di protezione, indirizzandolo in maniera puntuale verso la giusta direzione.

Dal punto di vista tecnologico, la security di infrastrutture critiche è stata spesso gestita adottando sistemi di allarme basati su sensoristica anti-intrusione, controllo degli accessi e sistemi TVCC (TeleVisione a Circuito Chiuso). Le nuove tecnologie possono innovare in maniera significativa i meccanismi di protezione, garantendo funzioni e capacità impensabili in passato. L'evoluzione tecnologica dei sistemi di sicurezza è un processo tanto auspicabile, quanto necessario se si vuole garantire una protezione sempre "proporzionata" all'abilità degli attaccanti.

Tradizionalmente, l'uso delle diverse tecnologie di protezione è spesso disomogenea. La soluzione per sfruttarle in maniera efficiente è quella di integrare dispositivi di rilevamento eterogenei utilizzando sistemi hardware e software che diano una visione coesa dello stato dell'intero sistema di security, consentendo di ottenere una superiore conoscenza della situazione (*situational awareness*), oltre che un adeguato supporto alle decisioni da intraprendere. Uno dei vantaggi più rilevanti dell'integrazione consiste nella possibilità di definire meccanismi di correlazione tra gli eventi elementari rilevati da reti sensoriali eterogenee, nelle quali è possibile sfruttare le potenzialità delle nuove tecnologie, come videosorveglianza intelligente, audiosorveglianza intelligente, sistemi per lo screening di massa e sensori CBRNe (Chimico Batteriologico Radiologico Nucleare Esplosivo).

Minacce particolarmente complesse richiedono l'adozione di sistemi che riescano a correlare gli eventi non solo in base ad una logica elementare (di tipo booleano), ma anche in funzione di attributi spaziali e temporali degli eventi (ad esempio per il rilevamento di particolari sequenze di azioni in siti specifici). Un ulteriore passo in avanti è costituito dalla possibilità di adottare modelli di rilevamento non deterministici, con l'importante scopo di prevedere l'accadimento di determinati eventi, riconoscere in anticipo gli scenari di attacco e di conseguenza anticipare l'adozione di contromisure. Il perseguimento di questo obiettivo consente di rilevare precocemente i pattern di attacco definiti in sede di

Risk Analysis.

I capitoli che seguiranno sono stati organizzati in questo nel modo seguente:

- **Capitolo 1 - Protezione di Infrastrutture Critiche: concetti, definizioni e ciclo di vita**. Espone i concetti base di Infrastruttura Critica e di Protezione di Infrastrutture Critiche, presentando anche i principali settori interessati. Sono riportate le definizioni impiegate nelle direttive europee in merito alle ECI (*European Critical Infrastructure*). Viene inoltre presentato il ciclo di vita che descrive le attività richieste – prima, durante e dopo un evento indesiderato – per garantire la protezione di tali infrastrutture.
- **Capitolo 2 - Sicurezza dei sistemi di trasporto pubblico: stato dell'arte**. Nell'ambito delle infrastrutture critiche l'attenzione è qui focalizzata sulle reti di trasporto pubbliche. Vengono presentate le principali criticità dei sistemi, così come le principali minacce e vulnerabilità. Si descrivono le principali strategie di protezione e i relativi effetti. Infine vengono elencate le contromisure convenzionalmente adottate.
- **Capitolo 3 – Tecniche avanzate di analisi**. Vengono presentate le metodologie in grado di valutare i diversi fenomeni che minacciano i sistemi di trasporto, il cui impiego permette di coprire la prima fase del ciclo di vita per la protezione delle infrastrutture critiche. Il capitolo descrive le attività principali previste dall'analisi del rischio, e specifica il ruolo della modellazione nella valutazione del rischio e nell'analisi delle infrastrutture.
- **Capitolo 4 – Tecniche avanzate di protezione**. Il capitolo descrive alcune delle principali tecnologie innovative per la security dei sistemi di trasporto pubblico. Inoltre sono presentati i vantaggi di un sistema in grado di integrare i dati provenienti dai diversi sottosistemi sensoriali. In particolare, opportuni meccanismi di correlazione migliorano l'affidabilità del rilevamento e permettono il riconoscimento di pattern di attacco più complessi.