Mauro Andreolini	
Indirizzo	Dipartimento di Scienze Fisiche, Informatiche e Matematiche Università di Modena e Reggio Emilia Via Campi, 213/A 41125 - Modena
Tel. E-mail Home page	+39 059 2055192 mauro.andreolini@unimore.it https://secloud.ing.unimore.it/people/andreolini

Dati Anagrafici e Formazione

Mauro Andreolini, nato a Roma l'8 febbraio 1973, è Ricercatore Universitario presso l'Università di Modena e Reggio Emilia (Gruppo Scientifico Disciplinare attuale 01/INFO-01, Settore Scientifico Disciplinare attuale INFO-01/A) dal 18 gennaio 2005 e afferisce al Dipartimento di Scienze Fisiche, Informatiche e Matematiche dal settembre 2012.

Posizioni Precedenti

dicembre 2023: Conseguimento dell'Abilitazione Scientifica Nazionale alle funzioni di professore universitario di seconda fascia nel Settore Concorsuale 01/B1 (INFORMATICA). La validità dell'Abilitazione è di dodici anni a decorrere dal 12/12/2023 e avrà scadenza il 12/12/2035.

dicembre 2023: Conseguimento dell'Abilitazione Scientifica Nazionale alle funzioni di professore universitario di seconda fascia nel Settore Concorsuale 09/H1 (SISTEMI DI ELABORAZIONE DELLE INFORMAZIONI). La validità dell'Abilitazione è di dodici anni a decorrere dal 17/12/2023 e avrà scadenza il 17/12/2035.

settembre 2012-maggio 2026: Ricercatore (Settore Scientifico Disciplinare INF/01) presso il Dipartimento di Scienze Fisiche, Informatiche e Matematiche dell'Università di Modena e Reggio Emilia.

gennaio 2005-settembre 2012: Ricercatore (Settore Scientifico Disciplinare INF/01) presso il Dipartimento di Ingegneria dell'Informazione dell'Università di Modena e Reggio Emilia.

luglio 2003-dicembre 2003: Visiting researcher per sei mesi presso l'IBM T.J. Watson Research Center, Yorktown Heights, NY, USA, ospite del Dr. Philip Yu.

novembre 2001-novembre 2004: Dottorato di ricerca (XVII ciclo) in Automazione e Ingegneria dell'Informazione presso l'Università di Roma "Tor Vergata".

maggio 2001-ottobre 2001: Collaborazione coordinata e continuativa presso il Dipartimento di Informatica e Si-stemistica dell'Università di Roma "La Sapienza", svolta

sotto la guida del Prof. Bruno Ciciani. Titolo: *Implementazione di un server Web fault-tolerant ad alte prestazioni*.

gennaio 2001: Laurea con il punteggio di *110/110 e lode* presso l'Università di Roma "Tor Vergata" nel gennaio 2001. Titolo della tesi: *Meccanismi content-aware per il Web dispatching*, relatori Prof. Salvatore Tucci, Prof. Michele Colajanni.

Attività di Ricerca

Nell'ambito della attività di ricerca, Mauro Andreolini ha pubblicato 55 lavori su conferenze e riviste internazionali negli ambiti seguenti.

Sicurezza informatica

Crittografia. In [46] si affronta il problema dell'integrità dei dati nei database cloud proponendo Bloom filter cifrati che permettono all'utente di rilevare modifiche non autorizzate ai dati esternalizzati. Si propone inoltre un modello analitico per ottimizzare i costi di storage e rete in funzione della struttura del database e del workload. La soluzione viene valutata tramite micro-benchmark e TPC-C, mostrando miglioramenti rispetto alle alternative esistenti. Il contributo unisce robustezza dell'integrità e riduzione dell'overhead operativo. In [47] si mette in luce il divario tra modelli teorici e implementazioni concrete nella sicurezza dei database cifrati. Nello specifico, si analizza la sicurezza offline dello schema di Order-Revealing Encryption proposto inizialmente da Lewi e Wu, evidenziando il fatto che quest'ultimo, pur garantendo sicurezza semantica, richiede l'ordinamento dei ciphertext per efficienza. Si mostra come la costruzione degli indici, ignorata nel paper originale, può introdurre gravi fughe di informazioni ("information leak´) quali la presenza di valori duplicati, la distribuzione statistica dei valori e la storia delle transazioni nel DBMS. Analizzando due implementazioni open source, si individuano vulnerabilità dovute all'uso di alberi di ricerca standard. Si propongono infine le condizioni necessarie e alcune soluzioni pratiche per strutture di indicizzazione sicure.

Schemi di autenticazione. In [45] si propone una critica al modello di sicurezza perimetrale (ritenuto inadeguato per sistemi Web dinamici caratterizzate dall'aggiunta e rimozione repentina e continua di utenti e host host), e abbraccia l'approccio "zero trust", che applica controlli ad ogni richiesta senza basarsi sulla posizione fisica di utenti e dispositivi. Gli autori osservano che le architetture zero trust esistenti presumono in modo poco realistico l'inviolabilità di alcuni componenti. Propongono quindi una nuova architettura zero trust "sopravvivibile" ("survivable"), pensata per ambienti cloud. Questa architettura garantisce robustezza, è capace di tollerare compromissioni e può recuperare da fallimenti software e attacchi andati a segno.

Side channel. In [51] si studia la possibilità di condurre attacchi temporali ad alta precisione su dispositivi embedded USB, come smart card, utilizzando un normale PC. Nello specifico si adotta eBPF per misurare in kernel space i tempi di esecuzione delle firme digitali, ottenendo dati più accurati rispetto alle misurazioni in user space proposte nei lavori precedenti. Gli autori testano l'approccio su una smart card vulnerabile e valutano l'impatto delle misurazioni sulla riuscita di un attacco noto per il recupero delle chiavi private. I

risultati mostrano miglioramenti significativi sia nella precisione dei tempi raccolti sia nella probabilità di compromissione.

Rilevazione e contrasto alle anomalie. L'attività di ricerca nell'ambito della rilevazione delle anomalie (motivata dal desiderio di contrastare in modo efficace l'attività degli attaccanti) si è evoluta nell'arco di venti anni, passando da semplici euristiche di riconoscimento di attacchi a veri e propri modelli basati su intelligenza artificiale euristica. In [2] è presentato HoneySpam, un framework basato su honeypot nato per contrastare le attività degli spammer. L'idea principale alla base del prototipo è quella di contrastare lo spamming alla sorgente, piuttosto che in fase di ricezione dei messaggi come nella maggior parte degli approcci presenti in letteratura. Le tecniche usate nelle attività di contrasto spaziano dal rallentamento del processo di collezionamento degli indirizzi di posta, all'avvelenamento delle basi di dati di indirizzi di posta, alla tracciabilità dei responsabili attraverso proxy civetta aperti. In [23] si presenta una nuova tipologia di attacco, la mobility-based evasion, che sfrutta la mobilità dei dispositivi per frammentare un payload malevolo e aggirare anche gli intrusion detection system più avanzati. Si mostra come i protocolli mobili, progettati senza adeguate misure di sicurezza, siano particolarmente vulnerabili. Infine si propone un framework cooperativo di rilevamento delle intrusioni che ricompone e analizza le informazioni distribuite durante la mobilità. Un prototipo su Mobile IPv4, Mobile IPv6 e WiFi dimostra l'efficacia e la praticabilità dell'approccio. In [53] si propone DAGA, un algoritmo di anomaly detection per reti veicolari basato su n-gram che analizza solo le sequenze degli ID dei messaggi CAN, risultando leggero e adatto a microcontrollori con risorse limitate. Il framework permette di generare modelli con diversi footprint di memoria, adattabili a piattaforme hardware con requisiti di miniaturizzazione differenti. I test effettuati su tre prototipi mostrano che DAGA può superare lo stato dell'arte sui microcontrollori più potenti e rimanere comunque operativo su dispositivi molto semplici. Il dataset e il codice sono stati rilasciati pubblicamente per favorire ulteriori ricerche. In [52] si propone DOLOS, un'architettura che integra in modo armonico Moving Target Defense e Cyber Deception direttamente nei sistemi di produzione, superando i limiti delle soluzioni esistenti. DOLOS unisce randomizzazione, diversità e ridondanza con tecniche di inganno, rendendo più difficile per gli attaccanti distinguere tra componenti reali e falsi. La valutazione sperimentale contro malware e penetration tester mostra un rallentamento significativo degli attacchi ed una migliore protezione contro gli attacchi perpetrati dai gruppi di cyber criminali.

In [36] si affronta la debolezza dei sistemi di rilevazione delle intrusioni basati su machine learning di fronte ad attacchi adversarial mirati. Si propone una nuova metodologia di difesa pensata per modelli di tipo random forest, particolarmente adatti alla cyber security. La tecnica viene integrata in un rilevatore di traffico di rete e testata su milioni di flussi. I risultati mostrano che il sistema è più resistente agli attacchi e mantiene buone prestazioni anche in condizioni normali, superando i rilevatori esistenti. In [39] si introduce un framework basato su deep reinforcement learning per difendere rilevatori di botnet dagli attacchi adversarial. Il sistema genera automaticamente esempi di evasione realistici e li usa per irrobustire i modelli, senza degradarne le prestazioni in assenza di attacchi. Il framework è validato su vari algoritmi e dataset pubblici, mostrando miglioramenti consistenti rispetto alle soluzioni esistenti. Il risultato è un approccio generalizzabile che rende più resilienti i sistemi di rilevamento basati su machine learning contro attacchi presenti e futuri. In [55] si introduce il primo dataset pensato per valutare la resilienza dei rilevatori di botnet contro

attacchi adversarial. Esso contiene migliaia di campioni generati automaticamente tramite tecniche di deep reinforcement learning, capaci di eludere rilevatori machine/deep learning allo stato dell'arte. I campioni derivano da flussi di botnet reali e includono modifiche realistiche che non alterano la natura malevola del traffico. Il dataset consente ai ricercatori di testare difese in condizioni realistiche e offre insight utili per comprendere e contrastare meglio gli attacchi adversarial. In [37] si criticano i modelli di minaccia usati nella ricerca sugli attacchi adversarial ai sistemi di rilevazione delle intrusioni, ritenuti spesso irrealistici per scenari concreti. Si propone un nuovo modello che descrive capacità e vincoli realistici degli attaccanti contro Network Intrusion Detection System (NIDS) basati su machine learning. Applicando il modello a vari attacchi noti, si mostra quali siano davvero praticabili e quali no. Il contributo aiuta a rafforzare i sistemi difensivi e a guidare la ricerca verso attacchi adversarial più aderenti alle condizioni reali.

Automazione delle operazioni cyber. In [48, 49] viene proposta una distribuzione GNU/Linux innovativa, CAINE (Computer Aided INvestigative Environment), orientata alle indagini forensi off-line. La specifica novità di CAINE risiede nell'ambiente operativo che integra strumenti di analisi eterogenei e produce un unico report personalizzabile.

In [1] si introduce un framework di supporto ai security assessment basato su un sistema esperto in Prolog che tratta l'attività di valutazione come la dimostrazione di un teorema. Il framework può inferire nuovi fatti, eseguire azioni e aggiornare dinamicamente la base di conoscenza, superando limiti tipici degli strumenti tradizionali. I test su scenari jeopardy e boot-to-root mostrano che l'approccio consente di individuare obiettivi non standard, trattare sistemi isomorfi (ovvero strutturalmente simili e con lo stesso percorso di sfruttamento delle vulnerabilità) senza riconfigurazioni e scoprire vulnerabilità emergenti dalla combinazione di più debolezze.

In [17] si propone un sistema avanzato per valutare le performance degli allievi partecipanti alle esercitazioni di cybersecurity nei cyber range. La soluzione proposta combina un'architettura di monitoraggio distribuito, una modellazione delle attività tramite grafi orientati e nuovi algoritmi di scoring basati su grafi. Questo consente di misurare con precisione velocità e accuratezza degli allievi, individuando anche gli errori specifici. Rispetto alle piattaforme attuali, il metodo permette una valutazione molto più dettagliata e oggettiva del percorso svolto dal partecipante. In [40] si propone una valutazione dell'efficacia del sistema proposto su scenari di esercitazione grandi ed eterogenei, evidenziandone alcune anomalie negli score (perdite di precisione e punteggi distorti). Si propone una correzione al modello attuale che scompone l'esercizio in grafi locali (per sfide intermedie) e un grafo globale, permettendo valutazioni più accurate e pesature specifiche. I test svolti con un simulatore Python mostrano che il nuovo approccio scala meglio e produce punteggi più affidabili sia localmente che globalmente.

Privacy. In [41] si studia l'identificazione delle traiettorie degli utenti in movimento (equipaggiati di dispositivi IoT) in presenza di contromisure di privacy come geohashing e clustering K-means. Anche con forti generalizzazioni, le traiettorie rimangono spesso uniche e quindi facilmente identificabili, confermando la riduzione della privacy insita nel collezionamento di dati geografici. Le tecniche testate soffrono inoltre di importanti problemi di usabilità, soprattutto quando riducono drasticamente la risoluzione spaziale. I risultati confermano che la protezione della privacy in un contesto di mobilità è un problema estremamente complesso, che richiede soluzioni più sofisticate.

Sistemi ad alte prestazioni

Web server distribuiti. Con riferimento a sistemi distribuiti localmente e geograficamente, sono stati proposti algoritmi di dispatching di primo e di secondo livello. I risultati sperimentali hanno mostrato l'efficacia degli algoritmi proposti content-aware rispetto alle politiche tradizionali, in presenza di scenari di carico realistici. L'analisi, che conferma alcuni risultati noti nella teoria del load sharing, pone inoltre nuovi interrogativi, come ad esempio l'utilità nell'adottare aggiornamenti periodici dello stato dei nodi rispetto a notifiche asincrone di sovraccarico [24, 28]. Si è inoltre proceduto con il progetto di architetture di clustering a livello locale innovative. La scalabilità e le prestazioni ottenute sono risultate comparabili a quelle di analoghi prodotti commerciali [25, 26]. In [20] sono caratterizzate le principali proprietà di un moderno sistema di e-commerce performante ed affidabile anche in presenza di picchi di carico. In [4] sono dettagliati i principali strumenti e metodi di benchmarking per sistemi Web e viene valutata la loro applicabilità ai sistemi Web distribuiti.

Lo sviluppo di algoritmi di dispatching efficaci richiede una conoscenza approfondita delle caratteristiche del carico interno ed esterno al sistema. Per quanto riguarda il carico esterno, si è proceduto con una modellazione del workload Web, tenendo conto delle proprietà statistiche del traffico, della dinamicità dei servizi e degli effetti geografici tra i client ed i server [M2, C28]. Per quanto riguarda la caratterizzazione del carico interno, è stata proposta una nuova metodologia di analisi delle prestazioni che, operando a livelli di granularità più fine, consente di individuare in maniera precisa i colli di bottiglia presenti nel sistema [R4]. Tale metodologia è stata in seguito adottata per studiare la sensibilità delle prestazioni di un sistema distribuito localmente in funzione di diversi parametri hardware, quali ad esempio la disponibilità di memoria e di connettività [R2, C20]. I risultati preliminari si sono rivelati di primaria importanza per lo studio delle proprietà statistiche dei modelli di carico interno di un sistema [R1, C16, C18]. In particolare, si è evidenziato come, in presenza di scenari di carico realistici, i modelli tradizionali di rappresentazione del carico non sono adeguati alla complessità dei nuovi sistemi distribuiti connessi ad Internet. Sono stati, pertanto, proposti modelli stocastici di rappresentazione del carico lineari e non lineari che hanno dimostrato caratteristiche di precisione e rapidità.

Un interessante spunto di ricerca ha riguardato l'integrazione dello stato di carico di una risorsa con una ulteriore informazione legata all'andamento della stessa (trend). Tale informazione permette di anticipare eventi indesiderati e, applicata a contesti di bilanciamento del carico per cluster Web [C1], ha dimostrato migliorare sensibilmente i tempi di risposta rispetto agli algoritmi esistenti. In [C14], il concetto di trend viene applicato ad un modello di regressione lineare per la predizione dello stato futuro del carico.

NIDS distribuiti localmente. In [13] sono proposte e confrontate diverse politiche di ridistribuzione del carico nel contesto di Network Intrusion Detection System (NIDS) distribuiti localmente. I risultati sperimentali mostrano l'efficacia di alcune delle soluzioni proposte in termini di bilanciamento del traffico di rete su diverse istanze di SNORT, un NIDS molto popolare.

Sistemi distribuiti a qualità del servizio garantita

Il Web ha assunto il ruolo di interfaccia preferenziale anche nel contesto di servizi altamente critici, che necessitano di un trattamento privilegiato rispetto ad altri. Di riflesso, le architetture dei sistemi Web si sono spostati da semplici sistemi di tipo *best effort* a strutture in grado di differenziare il proprio comportamento in funzione di una data tipologia di utente. La ricerca in questo contesto ha mirato al progetto ed alla valutazione delle prestazioni di sistemi Web distribuiti localmente, content-aware, arricchiti con funzionalità per la fruizione di servizi con livelli di prestazione garantiti contrattualmente. Tali funzionalità, ben note nell'ambito della teoria sulla QoS, sono state integrate al livello applicativo, al fine di garantire la qualità dei servizi end-to-end.

I meccanismi proposti si basano su *classificazione delle richieste*, *controllo di ammissione*, *isolamento delle prestazioni* ed *elevato utilizzo di risorse*. Sono stati integrati in un prototipo ed i risultati sperimentali ne confermano la buona stabilità e robustezza rispetto agli obiettivi [6]. Sono stati proposti anche diversi algoritmi di scheduling che integrano tutti i principi della QoS sopra menzionati [5].

In [8] si affronta il problema della "graceful degradation", ossia il degrado graduale e voluto delle prestazioni in presenza di un volume di carico tale da saturare la capacità di un server Web. A tal scopo le richieste pervenute al server sono classificate e gestite in ordine di importanza. In [31] viene proposto un nuovo meccanismo di admission control per cluster Web, in grado di garantire graceful degradation in presenza di sovraccarico. A differenza di altri approcci esistenti in letteratura, caratterizzati da un rifiuto incondizionato delle richieste in presenza di sovraccarico, lo schema proposto ha permesso di ridurre sensibilmente il numero di richieste rifiutate, al prezzo di sporadiche violazioni dei Service Level Agreement.

Sistemi operativi

Budget Fair Queueing (BFQ) è uno scheduler del disco di tipo "proportional share" per il kernel Linux. In [54] si presentano alcune euristiche di BFQ atte a ridurre sensibilmente il ritardo di risposta per i processi interattivi e ad aumentare il throughput complessivo per un'ampia gamma di dischi (rotazionali e SSD). Una estesa analisi sperimentali mostra la superiorità di BFQ sullo scheduler del disco ufficiale (Completely Fair Queueing, CFQ) in diversi scenari di uso.

Monitoraggio di sistemi complessi

Algoritmi. I sistemi informatici odierni sono sempre più spesso caratterizzati da una elevata complessità in termini di risorse hardware/software utilizzate ed interazioni non banali fra molteplici componenti. La gestione di un siffatto sistema è problematica in assenza di strumenti di monitoraggio opportuni. In tale contesto la ricerca, volta ad aumentare la scalabilità di un sistema di monitoraggio, è stata condotta in due direzioni distinte: una algoritmica ed una architetturale. In [42] sono stati proposti algoritmi di monitoraggio delle risorse di un sistema a partire da campionamenti continui effettuati con strumenti standard. Il fine principale è l'estrazione di una rappresentazione interna stabile e predicibile su diverse scale temporali, anche in presenza di alta variabilità, dispersione e rumore dei singoli campioni.

I risultati sperimentali mostrano come sia possibile migliorare l'accuratezza della predizione fornita dagli algoritmi standard (basati su modelli lineari ed autoregressivi), limitando nel contempo il consumo di risorse richiesto per il calcolo della rappresentazione. In [28] viene inoltre studiata la possibilità di adattare dinamicamente l'intervallo di campionamento delle risorse con l'obiettivo di abbattere i costi di gestione legati al monitoraggio, cercando allo stesso tempo di non alterare le proprietà statistiche delle serie temporali campionate. L'efficacia della soluzione proposta è evidenziata mediante diverse tracce sintetiche e reali.

Architetture. Uno studio preliminare ha evidenziato la non scalabilità delle basi di dati relazionali quali supporto di memorizzazione di massa per le informazioni legate al monitoraggio dei sistemi [21]. Per tale motivo, in [16] [C8] è proposta una architettura innovativa per il monitoraggio di data center di grandi dimensioni ospitanti applicazioni multi-tenant. L'approccio proposto permette di superare i limiti di soluzioni centralizzate (incapaci di scalare con il numero di risorse) e puramente gerarchiche (incapaci di supportare applicazioni distribuite su diversi data center). Il prototipo è stato in seguito arricchito con diversi algoritmi di monitoraggio [30, 27]. In [34] è dettagliato uno studio di scalabilità del prototipo che ne mostra l'efficacia.

Cloud Computing

Nel contesto di sistemi Cloud eroganti servizi virtualizzati è stato proposto un algoritmo di (ri)allocazione delle macchine virtuali sui nodi fisici dell'infrastruttura [14, 15]. L'algoritmo, pensato per sistemi di grandi dimensioni, è adattativo, non fa uso di soglie e robusto con rispetto al carico applicato sui nodi. Un risultato importante osservato nelle sperimentazioni è la capacità dell'algoritmo di ridurre in maniera sensibile il numero di migrazioni live, abbassando pertanto il costo di gestione dell'infrastruttura cloud.

In [50] è stato studiato un algoritmo di redirezione delle richieste per sistemi Web distribuiti su infrastrutture cloud. Nella letteratura precedente, il server più adatto a servire la richiesta è scelto tenendo in considerazione al più lo stato di carico del server stesso e la latenza di rete. L'algoritmo proposto cerca, invece, di predire il costo di redirezione (includendo anche aspetti specifici dovuti all'infrastruttura cloud) ed il corrispettivo tempo di risposta, optando per la redirezione solo in caso favorevole. In tal senso, il lavoro rappresenta uno dei primi tentativi di integrazione di informazioni di carico relative all'infrastruttura, all'utente e alla rete.

Sistemi autonomici

La ricerca ha preso spunto dall'osservazione che la grande maggioranza dei sistemi Internet-based critici opera su architetture distribuite geograficamente su vasta scala, tipicamente attraverso l'esecuzione a run-time di un gran numero di algoritmi decisionali, orientati a risolvere problemi di load balancing, overload ed admission control, ridirezione geografica. Il considerevole numero di componenti e di parametri in gioco ha suggerito la possibilità adottare modelli basati su "self-* properties" per orientarsi verso veri e propri sistemi autonomici. La ricerca in tale contesto ha proposto algoritmi e meccanismi innovativi di self-inspection e self-decision nei sistemi Internet-based tradizionali, con lo scopo di aumentarne la scalabilità e la robustezza.

I modelli di aggregazione del carico considerati sono stati valutati tramite un supporto modulare di self-inspection, applicabile in generale ai sistemi Internet-based. Tale meccanismo permette di misurare lo stato di carico di una risorsa in maniera efficiente e robusta per diversi scenari applicativi realistici, caratterizzati da proprietà statistiche molto diverse [44, 9]. Inoltre, è stato dimostrato come l'uso di tali modelli di aggregazione riesca ad aumentare la scalabilità e la disponibilità del sistema evitando, nel contempo, il degrado delle prestazioni ed il sovraccarico dei singoli componenti [34, 13].

In [11] sono stati proposti algoritmi autonomici per il dispatching e la ridirezione delle richieste nel contesto di sistemi Web distribuiti su scala geografica che hanno dimostrato diversi vantaggi rispetto alle politiche tradizionali: il rapido adattamento a variazioni repentine del carico che favorisce la stabilità del sistema, l'uso di informazioni locali che minimizza l'aggravio computazionale legato all'aggiornamento degli stati di carico fra i nodi, l'assenza di parametri di configurazione ad-hoc, la robustezza nei casi di eventi inattesi.

Sistemi peer-to-peer

Alcuni studi hanno evidenziato come il traffico peer-to-peer (P2P) sia caratterizzato da forti località negli accessi alle risorse, e hanno proposto l'uso di tecniche di caching per limitare l'impatto del traffico P2P sulle infrastrutture di rete. Tuttavia, si è osservato come la non considerazione degli effetti di temporalità negli accessi e l'adozione di alcune assunzioni semplificative portano ad inesattezze nelle stime della porzione di traffico P2P suscettibile di caching. In [18] si propone un'analisi del traffico P2P finalizzata a due scopi. Da un lato viene proposto il primo modello analitico di workload P2P che evidenzia le caratteristiche del traffico, dall'altro si valuta l'efficacia di soluzioni di caching alla luce dei risultati ottenuti. Per ciascuna categoria di risorse tipicamente disponibili in una rete di file sharing si sono fornite le distribuzioni probabilistiche di dimensione e popolarità delle risorse, il traffico istantaneo e la sua evoluzione temporale con pattern stagionali, settimanali e orari. Il modello di workload ottenuto dalle analisi è stato usato per stime più attendibili sulle quali può essere valutata con maggior precisione l'efficacia del caching di traffico legato al file sharing, ridimensionando alcuni risultati precedentemente proposti in letteratura.

In [33] viene presentata una classificazione delle tecniche comunemente utilizzate per la caratterizzazione del traffico P2P. In particolare, si confrontano i risultati ottenibili mediante analisi di campioni di traffico e mediante probing attivo su una overlay network per file sharing. Vengono evidenziate alcune discrepanze in risultati ottenuti con i due metodi e si dimostra che solo un uso combinato delle due tecniche consente di avere una visione completa dei pattern di traffico associati alle applicazioni P2P.

In [32] è proposto un nuovo meccanismo di ricerca di risorse basato su Distributed Hash Table (DHT) fuzzy. Il meccanismo proposto risolve uno dei problemi legati all'uso delle DHT nell'ambito delle funzionalità di ricerca, ossia l'impossibilità di effettuare ricerche per wildcard (per via della necessità di adoperare un identificatore univoco). Le proprietà esibite nella valutazione sperimentale sono le seguenti: flessibilità nella ricerca, efficacia nel recuperare le risorse, efficienza d'uso delle risorse di sistema, robustezza rispetto al malfunzionamento dei nodi.

Attività didattiche

Mauro Andreolini ha svolto le seguenti attività di docenza universitaria presso l'Ateneo di Modena e Reggio Emilia, suddivise per anno accademico.

- Titolare del corso **Vulnerability Research** (12 ore, 3 ECTS) nell'ambito del Corso di Dottorato in "Computer and Data Science for Technological and Social Innovation (CDS-TSI)" (2023-).
- Titolare del corso di **Sviluppo di Software Sicuro** (9 CFU) nel Corso di Laurea Magistrale di Informatica (2018-)
- Titolare del modulo introduttivo (6 CFU) del corso di **Sistemi Operativi** (6+3 CFU) nel Corso di Laurea Triennale di Informatica (2024-).
- Titolare del corso di **Programmazione Sicura** (6 CFU) nel Corso di Laurea Magistrale di Informatica (2016-2017)
- Titolare del corso di **Tecnologie innovative per il Web** (9 CFU) nel Corso di Laurea Magistrale di Informatica (2009).
- Titolare del corso di **Linguaggi Dinamici** (9 CFU) nel Corso di Laurea Triennale di Informatica (2008, 2010).
- Titolare del corso di **Metodologie per il progetto del software** (6 CFU) nel Corso di Laurea di Informatica (2006-2007).
- Docente del corso di **Applicazioni Informatiche** (2 CFU) nel Corso di Laurea di Scienze Geologiche (2005-2007).
- Titolare del corso di **Sistemi Operativi** (9 CFU) nel Corso di Laurea Triennale di Informatica (2004-2023).

È inoltre stato relatore o correlatore di 80 tesi di Laurea. È tutor scientifico di due dottorandi presso il Corso di Dottorato in "Computer and Data Science for Technological and Social Innovation (CDS-TSI)" dell'Università di Modena e Reggio Emilia. È membro del collegio docenti del Corso di Dottorato in "Computer and Data Science for Technological and Social Innovation (CDS-TSI)" dal 2023.

Attività di Terza Missione

Mauro Andreolini ha svolto le attività didattiche seguenti nell'ambito della Terza Missione.

- Titolare del Corso di Perfezionamento **Penetration Tester Avanzato** (40 ore) (2025).
- Lezione plenaria "Hacker, questo illustre sconosciuto!" presso l'evento "A tu per tu con la Scienza" (2024-).
- Titolare del Corso di Perfezionamento **Penetration Tester** (40 ore) (2022-2023).

- Titolare del modulo didattico **Exploitation** (24 ore) del Corso di Perfezionamento "Cyber Academy" (2018).
- Titolare del modulo didattico **Programmazione Sicura** (24 ore) del Corso di Perfezionamento "Cyber Academy" (2016-2018).
- Titolare del modulo didattico **Vulnerability Assessment e Penetration Testing** (24 ore) del Corso di Perfezionamento "Cyber Academy" (2016-2018).
- Titolare del modulo didattico **Sistemi Operativi** (24 ore) del Corso di Perfezionamento "Cyber Academy" (2016-2017).
- Titolare del modulo didattico **Vulnerability Assessment** (24 ore) del Master in CyberDefense presso la Scuola di Telecomunicazioni delle Forze Armate di Chiavari (2014-2018).
- Titolare del modulo didattico **Sistemi Operativi** (24 ore) del Master in CyberDefense presso la Scuola di Telecomunicazioni delle Forze Armate di Chiavari (2013-2017).
- Titolare dei moduli didattici **Sistemi Operativi** e **Penetration Testing** del Master di II livello in "Sicurezza dei Sistemi Informatici: Normative e Tecniche Avanzate di Protezione" (2010-2014).

Mauro Andreolini ha svolto le attività di public engagement seguenti nell'ambito della Terza Missione.

- Responsabile dello stand "CyberChallenge.IT" presso l'evento "Notte della Ricerca" (2023-).

Servizi per la Comunità Scientifica

Comitati scientifici

Mauro Andreolini ha fatto parte del comitato scientifico delle seguenti conferenze internazionali:

- International IEEE Symposium on Network Computing and Applications (IEEE NCA 2014-2024).
- International Workshop on Emerging Technologies for Next-generation GRID (ETN-GRID 2006-2014).
- IEEE Workshop on Dependable Parallel, Distributed and Network-Centric Systems (IEEE DPDNS 2013-2013).
- IEEE International Symposium on Parallel and Distributed Processing with Applications (IEEE ISPA 2012).

Comitati organizzativi

Mauro Andreolini ha fatto parte del comitato organizzativo delle seguenti conferenze internazionali:

- Responsabile finanziario (Financial Chair) della conferenza internazionale internazionale International IEEE Symposium on Network Computing and Applications (NCA 2023).
- Presidente del Comitato di Programma (Program Chair) della conferenza internazionale International IEEE Symposium on Network Computing and Applications (NCA 2022).
- Componente del Comitato Organizzatore dell'IFIP WG7.3 International Symposium on Computer Performance Modeling, Measurement and Evaluation (PERFORMANCE 2002).

Attività di Revisore

Mauro Andreolini è stato revisore per le seguenti riviste internazionali: IEEE Transactions on Parallel and Distributed Systems, ACM Performance Evaluation Review, Computer Journal, IEEE Computer Networks, Journal of Systems and Software, Journal of Network computing and Applications, Int'l Journal of Web Engineering and Technology, Pervasive computing. Mauro Andreolini è stato revisore per le seguenti conferenze internazionali: World Wide Web Int'l Conference (2002, 2003, 2004, 2005, 2006, 2007, 2009), AAA-Idea (2006, 2007), Europar (2007), DISC (2005), Globe-comm (2007), HotP2P (2004, 2005, 2006, 2007), IEEE MASCOTS (2004, 2005), MP2P (2005), Perf 2002, PE-WASUN(2005), ACM SIGMETRICS 2007, UIC 2007, WTAS 2006, COOPIS (2007), NCA (2008-2025).

Responsabilità scientifiche

Mauro Andreolini è stato Responsabile Scientifico per i seguenti progetti di ricerca per l'Università degli Studi di Modena e Reggio Emilia:

2017-2021 PNRM A2016.099bis "UNAVOX";

2016-2017 PNRM E.F. 2015 A2013.060 "Smart Environment Area Firing RangE (SEAFIRE)";

2015-2021 PNMR E.F. 2014 A2012.154 "Digital Trunk Communication in Hostile Environment (DTCHE)";

2008-2010 Capo unità locale di ricerca UNIMORE nel PRIN AUTOSEC "Autonomic Security".

Premi e riconoscimenti

Nell'ambito della sua attività di ricerca il Dott. Mauro Andreolini ha conseguito i seguenti premi e riconoscimenti in ambito internazionale.

- **Best paper award** per Mauro Andreolini, Sara Casolari, Stefania Tosi, "A hierarchical architecture for on-line control of private cloud-based systems", *Proc. of 10th World Wide Web Internet Conference*, Timisoara, Romania, October 2010.
- **Best paper award** per Mauro Andreolini, Sara Casolari, Michele Colajanni, "Self-inspection mechanisms for the support of autonomic decisions in Internet-based systems", *Proc. of 3rd International Conference on Autonomic and Autonomous Systems*, Athens, Greece, June 2007.
- **Candidate best paper award** per Mauro Andreolini, Marcello Pietri, Stefania Tosi, Andrea Balboni, "Monitoring Large Cloud-Based Systems", *Proc. of the International Conference on Cloud Computing and Services Science*, Barcelona, Spain, 3-5 April 2014.

Responsabilità organizzative

- Responsabile del progetto CyberChallenge.IT per l'Università di Modena e Reggio Emilia (2023-).

Prodotti della ricerca

- Autore originario della distribuzione GNU/Linux CAINE (Computer Aided INvestigative Environment) per attività di computer forensics.
- Contributore di una modifica allo scheduler del disco del kernel Linux BFQ (Budget Fair Queueing) finalizzata al miglioramento del throughput in scenari di carico interlacciato.

Modena, lì 21 maggio 2026

MAURO
ANDREOLINI
19.05.2026
12:24:06
GMT+02:00

Bibliografia

Riferimenti bibliografici

[1] Mauro Andreolini, Andrea Artioli, Luca Ferretti, Mirco Marchetti, Michele Colajanni, Claudia Righi, et al. A framework for automating security assessments with deductive reasoning. In *CEUR WORKSHOP PROCEEDINGS*, volume 3488. CEUR-WS, 2023.

[2] Mauro Andreolini, Alessandro Bulgarelli, Michele Colajanni, and Francesca Mazzoni. Honeyspam: Honeypots fighting spam at the source. *SRUTI*, 5:11–11, 2005.

[3] Mauro Andreolini, Claudia Canali, and Riccardo Lancellotti. Impact of request dispatching granularity in geographically distributed web systems. In *Sixth IEEE International Symposium on Network Computing and Applications (NCA 2007)*, pages 45–52. IEEE, 2007.

[4] Mauro Andreolini, Valeria Cardellini, and Michele Colajanni. Benchmarking models and tools for distributed web-server systems. In *IFIP International Symposium on Computer Performance Modeling, Measurement and Evaluation*, pages 208–235. Springer, 2002.

[5] Mauro Andreolini, Emiliano Casalicchio, Michele Colajanni, and Marco Mambelli. A cluster-based web system providing differentiated and guaranteed services. *Cluster Computing*, 7(1):7–19, 2004.

[6] Mauro Andreolini, Emiliano Casalicchio, Michele Colajanni, Marco Mambelli, et al. Qos-aware switching policies for a locally distributed web system. In *Proc. of the 11th Int'l World Wide Web Conf.* Honolulu, Hawaii, May, 2002.

[7] Mauro Andreolini and Sara Casolari. Load prediction models in web-based systems. In *Proceedings of the 1st international conference on Performance evaluation methodolgies and tools*, pages 27–es, 2006.

[8] Mauro Andreolini, Sara Casolari, and Michele Colajanni. A distributed architecture for gracefully degradable web-based services. In *Fifth IEEE International Symposium on Network Computing and Applications (NCA'06)*, pages 235–238. IEEE, 2006.

[9] Mauro Andreolini, Sara Casolari, and Michele Colajanni. Self-inspection mechanisms for the support of autonomic decisions in internet-based systems. In *Third International Conference on Autonomic and Autonomous Systems (ICAS'07)*, pages 53–53. IEEE, 2007.

[10] Mauro Andreolini, Sara Casolari, and Michele Colajanni. Trend-based load balancer for a multi-tier distributed system. In *2007 15th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems*, pages 288–294. IEEE, 2007.

[11] Mauro Andreolini, Sara Casolari, and Michele Colajanni. Autonomic request management algorithms for geographically distributed internet-based systems. In *2008 Second IEEE International Conference on Self-Adaptive and Self-Organizing Systems*, pages 171–180. IEEE, 2008.

[12] Mauro Andreolini, Sara Casolari, and Michele Colajanni. Models and framework for supporting runtime decisions in web-based systems. *ACM Transactions on the Web (TWEB)*, 2(3):1–43, 2008.

[13] Mauro Andreolini, Sara Casolari, Michele Colajanni, and Mirco Marchetti. Dynamic load balancing for network intrusion detection systems based on distributed architectures. In *Sixth IEEE International Symposium on Network Computing and Applications (NCA 2007)*, pages 153–160. IEEE, 2007.

[14] Mauro Andreolini, Sara Casolari, Michele Colajanni, and Michele Messori. Dynamic load management of virtual machines in cloud architectures. In *International Conference on Cloud Computing*, pages 201–214. Springer, 2009.

[15] Mauro Andreolini, Sara Casolari, Marcello Pietri, Stefania Tosi, et al. Resilient and adaptive networked systems., 2014.

[16] Mauro Andreolini, Sara Casolari, Stefania Tosi, et al. A hierarchical architecture for online control of private cloud based systems. In *Proc. of 10th World Wide Web Internet Conference (WWWCONF2010), Timisoara, Romania*, 2010.

[17] Mauro Andreolini, Vincenzo Giuseppe Colacino, Michele Colajanni, and Mirco Marchetti. A framework for the evaluation of trainee performance in cyber range exercises. *Mobile Networks and Applications*, 25(1):236–247, 2020.

[18] Mauro Andreolini, Michele Colajanni, and Riccardo Lancellotti. Peer-to-peer workload characterization: techniques and open issues. In *2004 International Workshop on Hot Topics in Peer-to-Peer Systems*, pages 66–71. IEEE, 2004.

[19] Mauro Andreolini, Michele Colajanni, and Riccardo Lancellotti. Impact of memory technology trends on performance of web systems. In *International Conference on Next Generation Web Services Practices (NWeSP'05)*, pages 7–pp. IEEE, 2005.

[20] Mauro Andreolini, Michele Colajanni, and Riccardo Lancellotti. Web system reliability and performance. In *Web Engineering*, pages 181–218. Springer, 2006.

[21] Mauro Andreolini, Michele Colajanni, and Riccardo Lancellotti. Assessing the overhead and scalability of system monitors for large data centers. In *Proceedings of the First International Workshop on Cloud Computing Platforms*, pages 1–7, 2011.

[22] Mauro Andreolini, Michele Colajanni, Riccardo Lancellotti, and Francesca Mazzoni. Fine grain performance evaluation of e-commerce sites. *ACM Sigmetrics Performance Evaluation Review*, 32(3):14–23, 2004.

[23] Mauro Andreolini, Michele Colajanni, and Mirco Marchetti. A collaborative framework for intrusion detection in mobile networks. *Information Sciences*, 321:179–192, 2015.

[24] Mauro Andreolini, Michele Colajanni, and Ruggero Morselli. Performance study of dispatching algorithms in multi-tier web architectures. *ACM SIGMETRICS Performance Evaluation Review*, 30(2):10–20, 2002.

[25] Mauro Andreolini, Michele Colajanni, and Marcello Nuccio. Kernel-based web switches providing content-aware routing. In *Second IEEE International Symposium on Network Computing and Applications, 2003. NCA 2003.*, pages 25–32. IEEE, 2003.

[26] Mauro Andreolini, Michele Colajanni, Marcello Nuccio, et al. Scalability of content-aware server switches for cluster-based web information systems. In *The Twelfth International World Wide Web Conference-WWW 2003: proceedings of the tracks education, global community, industrial practice and experience, web services*, pages 200–208. World Wide Web Conference Committee., 2003.

[27] Mauro Andreolini, Michele Colajanni, and Marcello Pietri. A scalable architecture for real-time monitoring of large information systems. In *2012 Second Symposium on Network Cloud Computing and Applications*, pages 143–150. IEEE, 2012.

[28] Mauro Andreolini, Michele Colajanni, Marcello Pietri, and Stefania Tosi. Real-time adaptive algorithm for resource monitoring. In *Proceedings of the 9th International Conference on Network and Service Management (CNSM 2013)*, pages 67–74. IEEE, 2013.

[29] Mauro Andreolini, Michele Colajanni, Marcello Pietri, and Stefania Tosi. Adaptive, scalable and reliable monitoring of big data on clouds. *Journal of Parallel and Distributed Computing*, 79:67–79, 2015.

[30] Mauro Andreolini, Michele Colajanni, and Stefania Tosi. A software architecture for the analysis of large sets of data streams in cloud infrastructures. In *2011 IEEE 11th International Conference on Computer and Information Technology*, pages 389–394. IEEE, 2011.

[31] Mauro Andreolini, Michele Colajanni, and Paolo Valente. Design and testing of scalable web-based systems with performance constraints. In *2005 Workshop on Techniques, Methodologies and Tools for Performance Evaluation of Complex Systems (FIRB-PERF'05)*, pages 15–25. IEEE, 2005.

[32] Mauro Andreolini and Riccardo Lancellotti. A flexible and robust lookup algorithm for p2p systems. In *2009 IEEE International Symposium on Parallel & Distributed Processing*, pages 1–8. IEEE, 2009.

[33] Mauro Andreolini, Riccardo Lancellotti, and Philip S Yu. Analysis of peer-to-peer systems: workload characterization and effects on traffic cacheability. In *The IEEE Computer Society's 12th Annual International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunications Systems, 2004.(MASCOTS 2004). Proceedings.*, pages 95–104. IEEE, 2004.

[34] Mauro Andreolini, Marcello Pietri, Stefania Tosi, Andrea Balboni, et al. Monitoring large cloud-based systems. In *CLOSER 2014-Proceedings of the 4th International Conference on Cloud Computing and Services Science*, pages 341–351. SciTePress, 2014.

[35] Mauro Andreolini, Marcello Pietri, Stefania Tosi, and Riccardo Lancellotti. A scalable monitor for large systems. In *International Conference on Cloud Computing and Services Science*, pages 100–116. Springer, 2014.

[36] Giovanni Apruzzese, Mauro Andreolini, Michele Colajanni, and Mirco Marchetti. Hardening random forest cyber detectors against adversarial attacks. *IEEE Transactions on Emerging Topics in Computational Intelligence*, 4(4):427–439, 2020.

[37] Giovanni Apruzzese, Mauro Andreolini, Luca Ferretti, Mirco Marchetti, and Michele Colajanni. Modeling realistic adversarial attacks against network intrusion detection systems. *Digital Threats: Research and Practice (DTRAP)*, 3(3):1–19, 2022.

[38] Giovanni Apruzzese, Mauro Andreolini, Mirco Marchetti, Vincenzo Giuseppe Colacino, and Giacomo Russo. Appcon: Mitigating evasion attacks to ml cyber detectors. *Symmetry*, 12(4):653, 2020.

[39] Giovanni Apruzzese, Mauro Andreolini, Mirco Marchetti, Andrea Venturi, and Michele Colajanni. Deep reinforcement adversarial learning against botnet evasion attacks. *IEEE Transactions on Network and Service Management*, 17(4):1975–1987, 2020.

[40] Andrea Artioli, Mauro Andreolini, Luca Ferretti, Mirco Marchetti, et al. Evaluating trainees in large cyber exercises. In *CEUR WORKSHOP PROCEEDINGS*, volume 3731. CEUR-WS, 2024.

[41] Andrea Artioli, Luca Bedogni, and Mauro Andreolini. Effects of geohashing and k-means clustering on uniqueness in a mobility dataset. In *2024 IEEE/ACM Symposium on Edge Computing (SEC)*, pages 389–394. IEEE, 2024.

[42] Sara Casolari, Mauro Andreolini, and Michele Colajanni. Runtime prediction models for web-based system resources. In *2008 IEEE International Symposium on Modeling, Analysis and Simulation of Computers and Telecommunication Systems*, pages 1–8. IEEE, 2008.

[43] Michele Colajanni, Mauro Adreolini, and Valeria Cardellini. Benchmarking of locally and geographically distributed web-server systems. *World Wide Web, Budapest*, 2003.

[44] Michele Colajanni, Mauro Andreolini, Riccardo Lancellotti, et al. Open issues in self-inspection and self-decision mechanisms for supporting complex and heterogeneous information systems. *Proceedings of. Int'l SELF-STAR*, page 13, 2004.

[45] Luca Ferretti, Federico Magnanini, Mauro Andreolini, and Michele Colajanni. Survivable zero trust for cloud computing environments. *Computers & Security*, 110:102419, 2021.

[46] Luca Ferretti, Mirco Marchetti, Mauro Andreolini, and Michele Colajanni. A symmetric cryptographic scheme for data integrity verification in cloud databases. *Information Sciences*, 422:497–515, 2018.

[47] Luca Ferretti, Mattia Trabucco, Mauro Andreolini, Mirco Marchetti, et al. How (not) to index order revealing encrypted databases. In *CEUR WORKSHOP PROCEEDINGS*, volume 3488. CEUR-WS, 2023.

[48] G Giustini, Mauro Andreolini, Michele Colajanni, et al. Caine: A new open-source live distribution for digital forensics. In *First Workshop on Open Source software for computer and network forensics (OSSCONF2008)*, pages 51–61. Springer, 2008.

[49] Giancarlo Giustini, Mauro Andreolini, and Michele Colajanni. Open source live distributions for computer forensics. In *Open source software for digital forensics*, pages 69–82. Springer, 2009.

[50] Riccardo Lancellotti, Mauro Andreolini, Claudia Canali, and Michele Colajanni. Dynamic request management algorithms for web-based services in cloud computing. In *2011 IEEE 35th Annual Computer Software and Applications Conference*, pages 401–406. IEEE, 2011.

[51] Gianmarco Lusvardi, Luca Ferretti, Mauro Andreolini, et al. Timing side-channel attacks on usb devices using ebpf. In *CEUR WORKSHOP PROCEEDINGS*, volume 3731. CEUR-WS, 2024.

[52] Giulio Pagnotta, Fabio De Gaspari, Dorjan Hitaj, Mauro Andreolini, Michele Colajanni, and Luigi V Mancini. Dolos: A novel architecture for moving target defense. *IEEE Transactions on Information Forensics and Security*, 18:5890–5905, 2023.

[53] Dario Stabili, Luca Ferretti, Mauro Andreolini, and Mirco Marchetti. Daga: Detecting attacks to in-vehicle networks via n-gram analysis. *IEEE Transactions on Vehicular Technology*, 71(11):11540–11554, 2022.

[54] Paolo Valente and Mauro Andreolini. Improving application responsiveness with the bfq disk i/o scheduler. In *Proceedings of the 5th Annual International Systems and Storage Conference*, pages 1–12, 2012.

[55] Andrea Venturi, Giovanni Apruzzese, Mauro Andreolini, Michele Colajanni, and Mirco Marchetti. Drelab-deep reinforcement learning adversarial botnet: A benchmark dataset for adversarial attacks against botnet intrusion detection systems. *Data in Brief*, 34:106631, 2021.