ANDREA BISEGNA

nato a Trento (Italia), il 16 marzo 1979
residente in via della Resistenza 82, 38123 Trento (Italia)
tel. +39 347 5432724 • e-mail a.bisegna@gmail.com

ESPERIENZE LAVORATIVE

RICERCATORE in Cybersecurity 2015 - attuale
Fondazione Bruno Kessler, Trento (Italia)

- Sviluppo e utilizzo di strumenti basati sull'intelligenza artificiale per il security testing, con focus su protocolli di autenticazione e gestione dell'identità.
- Design, sviluppo e attività di analisi di sicurezza per soluzioni di gestione dell'identità digitale attraverso la Carta d'Identità Elettronica (CIE).
- Analisi di sicurezza dell'implementazione SPID (Sistema Pubblico Identità Digitale) e creazione di un test plan per *Service Provider* e *Identity Provider*.
- Analisi, approfondimenti e studi di fattibilità del nuovo regolamento generale sulla protezione dei dati GDPR (*General Data Protection* Regulation).
- Gestione delle attività e responsabile scientifico in diversi progetti di ricerca sia italiani che europei.

RICERCATORE in Cybersecurity 2021 - 2022
Futuro & Conoscenza, Trento (Italia)
[Istituto Poligrafico e Zecca dello Stato & Fondazione Bruno Kessler]

- Progettazione e sviluppo di soluzioni sicure con tecnologie emergenti in materia di identità digitale tramite la Carta d'Identità Elettronica (CIE). Soluzioni di autenticazione tramite CIE con il protocollo *OpenID Connect* e tramite *Digital Wallet* con modello *Self-Sovereign Identity*.
- Progettazione e sviluppo di soluzioni innovative in relazione ai problemi di business individuati nell'ambito della dematerializzazione dei documenti fisici. Nel dettaglio, soluzioni per dematerializzare la *Mobile Driving License* e le *Digital Travel Credentials*.

PROJECT MANAGER 2014 - 2015
TCbit, Trento (Italia) - Brasov (Romania)

- Analisi delle commesse e pianificazione delle idee progettuali.
- Gestione delle fasi progettuali, pianificazione e gestione delle attività di marketing e vendita dei progetti.
- Amministrazione del budget e coordinamento di un gruppo di lavoro internazionale.

PROJECT MANAGER 2013 - 2014
TrentoRise, Trento (Italia)

- Creazione e pianificazione del piano marketing (*executive, audit, SWOT, planning*).
- Organizzazione e gestione delle attività di promo-commercializzazione.
- Gestione e verifica delle attività di progetto con gli *stakeholder* e la Provincia Autonoma di Trento.

QUALITY & ASSURANCE TEAM 2010 - 2013
The Microsoft Research - COSBI, Trento (Italia)

- Organizzazione in sinergia con l'area sales delle attività di marketing e vendita.
- Pianificazione, creazione e gestione dei test di accettazione e del test plan.
- Coordinamento del test esploratorio, d'interfaccia, di sistema e di prestazione.

PROJECT MANAGER 2008 - 2010
Sentieri Vivi S.r.l., Trento (Italia)

- Creazione e pianificazione delle attività progettuali e di marketing.
- Coordinamento di un team internazionale.
- Pianificazione e gestione del budget e delle attività di commercializzazione.

CONSIGLI DI AMMINISTRAZIONE

- Consigliere presso la Famiglia Cooperativa di Povo, eletto nel 2023, con il compito di contribuire alle decisioni strategiche e alla gestione delle attività della cooperativa.

FORMAZIONE

- Dottorato di Ricerca in *Program in Computer Science e Systems Engineering* – Università degli Studi di Genova – Italia.
- Laurea Specialistica in Ingegneria delle Telecomunicazioni (laurea nel 2007) – Università degli Studi di Trento – Italia.
- Socrates-Erasmus Programme (2005) – University of Aberdeen – Scozia.
- Laurea Magistrale in Ingegneria delle Telecomunicazioni (laurea nel 2004) – Università degli Studi di Trento – Italia.

ATTIVITÀ DI RICERCA

Il mio lavoro di ricerca si concentra sulla sicurezza dei sistemi di gestione dell'identità digitale e dell'accesso, che garantisce la sicurezza delle informazioni sensibili in diverse applicazioni online in ambiti come sanità, l'e-commerce e l'e-government. I protocolli di sicurezza sono fondamentali in questi contesti, poiché stabiliscono regole e metodi per l'autenticazione degli utenti e l'accesso a risorse protette.

Il mio focus mira a comprendere le vulnerabilità e i rischi che possono essere presenti nei sistemi di autenticazione online e a sviluppare soluzioni per prevenire eventuali minacce alla sicurezza. Questo lavoro è cruciale per garantire che le informazioni sensibili degli utenti rimangano protette e che i sistemi di autenticazione siano sicuri e affidabili. Sono particolarmente interessato ai protocolli utilizzati nel browser che permettono l'accesso a risorse da parte di utenti autorizzati e rendono più semplice la progettazione e l'implementazione di applicazioni online complesse.

Mi sono concentrato sulla rilevazione automatica delle vulnerabilità logiche e di Cross-Site Request Forgery (CSRF) nei sistemi di gestione dell'identità digitale (per esempio, SPID e CIE a livello italiano mentre eIDAS a livello europeo) e più in generale su sistemi basati sul Single Sign-On. Il focus su queste vulnerabilità è stato sviluppato per creare un approccio più versatile e generale per i test di sicurezza dei sistemi di autenticazione online. I risultati hanno mostrato un alto numero di vulnerabilità critiche presenti in servizi online comunemente utilizzati. Questa scoperta evidenzia la necessità di una maggiore attenzione alla sicurezza nella progettazione e nella implementazione di questi sistemi per garantire che le informazioni sensibili degli utenti

rimangano protette.

Inoltre, durante la ricerca, sono stati identificati nuovi pattern di attacco e scoperte nuove vulnerabilità. Questo ha portato a una maggiore comprensione delle minacce alla sicurezza presenti nei sistemi di autenticazione online e ha fornito informazioni preziose per lo sviluppo di soluzioni di sicurezza più efficaci.

PROGETTI DI RICERCA

- B-Zero – Notarify. Legge Provinciale 6, 2024.
- SPARTA: Strategic programs for advanced research and technology in Europe (finanziato dalla Commissione Europea nell'ambito del progetto H2020).
- Teichos: Technical Environment for Intelligent Cyber Operational Security (nell'ambito delle attività EIT Digital 2019).
- API Assistant 2 (nell'ambito delle attività EIT Digital 2019). Questo è il proseguimento di API Assistant.
- API Assistant: Automated Security Assessment of 3rd party apps for the API economy (nell'ambito delle attività EIT Digital 2018).
- Federated Identity Management System (FIDES 2016) (nell'ambito delle attività EIT Digital 2016).
- Federated Identity Management System (FIDES 2015) (nell'ambito delle attività EIT Digital 2015).
- SmartCampus. Il mio contributo è stato l'analisi degli aspetti di sicurezza della piattaforma SmartCampus. http://www.smartcampuslab.it/
- Cartella Clinica del Cittadino (TreC), finanziato dalla Provincia Autonoma di Trento. www.trec.trentinosalute.net.

RILEVANTI PUBBLICAZIONI SCIENTIFICHE E INTERVENTI IN CONFERENZE

- Andrea Bisegna, Matteo Bitussi, Roberto Carbone, Silvio Ranise. "Enhancing Security Testing for Identity Management Implementations: Introducing Micro-Id-Gym Language and Micro-Id-Gym Testing Tool". Presso: IEEE Security & Privacy.
- Andrea Bisegna, Matteo Bitussi, Roberto Carbone, Luca Compagna, Silvio Ranise, Avinash Sudhodanan. "CSRFing the SSO Waves: Security Testing of SSO-Based Account Linking Process". Presso: 9th IEEE European Symposium on Security and Privacy (EUROS&P 2024).
- A. Bisegna, R. Carbone e S. Ranise. "Integrating a Pentesting Tool for IdM Protocols in a Continuous Delivery Pipeline". Presso: *4th International Workshop on Emerging Technologies for Authorization and Authentication* (ETAA 2021).
- A. Bisegna, R. Carbone e S. Ranise. "Integrating a Pentesting Tool for IdM Protocols in a Continuous Delivery Pipeline". Presso: *Italian Conference on Cybersecurity* (ITASEC 2021).
- A. Bisegna, R. Carbone e S. Ranise. "Integrating a Pentesting Tool for IdM Protocols in a Continuous Delivery Pipeline". Presso: *OWASP Italy Day 2021*.
- A. Bisegna, R. Carbone, G. Pellizzari e S. Ranise. "Micro-Id-Gym: a Flexible Tool for Pentesting Identity Management Protocols in the Wild and in the Laboratory". Presso: *3rd International Workshop on Emerging Technologies for Authorization and Authentication* (ETAA2020).
- A. Bisegna, R. Carbone, M. Ceccato, S. Manfredi, S. Ranise, G. Sciarretta, A. Tomasi e E. Viglianisi. "Automated Assistance to the Security Assessment of API for Financial Services". Presso: *Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures. Ed. by J. Soldatos, J. Philpot, and G. Giunta. Boston-Delft: now publishers, 2020, pp. 94–103*.
- S. M. Nóbrega Gonçalves, A. Tomasi, A. Bisegna, G. Pellizzari e S. Ranise. "Verifiable Contracting". Presso: *25th European Symposium on Research in Computer Security* (DETIPS) (2020).

- A. Bisegna, R. Carbone, I. Martini, V. Odorizzi, G. Pellizzari e S. Ranise. “Micro-Id-Gym: Identity Management Workouts with Container-Based Microservices”. Presso: *International Journal of Information Security and Cybercrime (IJISP), Volume 8, Issue 1* (2019).

SUPERVISORE DI TESI DI LAUREA

- Roberto Savi (Tesi di laurea, Università di Trento, 2024) - Integrating Pentesting Tools for Identity Management Protocols into DevSecOps: The MIG-T Use Case.
- Pier Guido Seno (Tesi di laurea, Università di Trento, 2024) - From Local to Remote: Enhancing MIG-T Pentesting Tool with SaaS for Securing Digital Identity.
- Luigi Dell'Eva (Tesi di laurea, Università di Trento, 2023) - Chatting is Healthy: How Better Cybersecurity Hygiene can be Obtained by Integrating Chatbots with Pentesting Tools.
- Alessandro Biasi (Tesi di laurea, Università di Trento, 2023) - Syntax and Semantics of a Declarative Language for Security Testing of Browser-based Security Protocols.
- Eleonora Marchesini (Tesi di Laurea Magistrale, Università di Trento, 2022) - Design and Implementation of a Cybersecurity Chatbot for Identity Management Protocols: the SAML and Slack Use Case.
- Giuseppe Alessio Sciumè (Tesi di laurea, Università di Trento, 2022) - A Comprehensive Analysis of the OAuth 2.0 Threat Model to Develop a Chatbot Providing Actionable Security Suggestions.
- Michele Zucchelli (Tesi di laurea, Università di Trento, 2022) - Pimp My Micro-Id-Gym: Enhancing the Automation and Usability of a Security Testing Tool for Digital Identity Protocol.
- Matteo Bitussi (Tesi di laurea, Università di Trento, 2022) - Declarative Specification of Pentesting Strategies for Browser-based Security Protocols: the Case Studies of SAML and OAuth/OIDC.
- Sofia Zanrosso (Tesi di laurea, Università di Trento, 2022) - Enlarging the Pen-Test Coverage of SAML Single Sign-On Solutions with Cyber Threat Intelligence.
- Wendy Barreto (Tesi di laurea, Università di Trento, 2021) - Design and implementation of an attack pattern language for the automated pentesting of OAuth/OIDC deployments.
- Luca Bazzanella (Tesi di laurea, Università di Trento, 2021) - Analysis of the State of the Art of DevSecOps: The Gitlab case study.
- Francesco Defilippo (Tesi di laurea, Università di Trento, 2021) - Attack Patterns for Pentesting SAML 2.0 Web Browser Single Sign-On deployments.
- Giulio Pellizzari (Tesi di Laurea Magistrale, Università di Trento, 2020) - Micro-Id-Gym: A Tool to Support Sandboxing and Automated Pentesting of Identity Management Protocols.
- Stefano Facchini (Tesi di laurea, Università di Trento, 2020) - Design and implementation of an automated tool for checking SAML SSO vulnerabilities and SPID compliance.
- Claudio Grisenti (Tesi di laurea, Università di Trento, 2020) - A pentesting tool for OAuth and OIDC deployments.
- Lorenzo Tait (Tesi di laurea, Università di Trento, 2019) - A Customized Threat Modeling for Secure Deployment And Pentesting of SAML SSO Solutions.
- Ivan Martini (Tesi di laurea, Università di Trento, 2018) - An automated security testing framework for SAML SSO deployments.
- Valentina Odorizzi (Tesi di laurea, Università di Trento, 2018) - Progettazione e sviluppo di uno strumento per l'analisi automatica di vulnerabilità "Missing XML Validation" in SAML SSO.
- Giulio Pellizzari (Tesi di laurea, Università di Trento, 2018) - Design and implementation of a tool to detect Login Cross-Site Request Forgery in SAML SSO: G Suite case study.

SOFTWARE TOOL

Micro-Id-Gym (MIG) - https://stfbk.github.io/tools/Micro-Id-Gym) - è uno strumento open source che aiuta gli amministratori di sistema e i tester nella distribuzione e nella verifica della sicurezza delle implementazioni dei protocolli per la gestione dell'identità digitale. MIG fornisce un ambiente controllato (di laboratorio) in cui i

pentester possono configurare facilmente l'ambiente di produzione e sviluppare esperienze pratiche sul funzionamento delle soluzioni di identità digitale, eseguire attacchi ad alto impatto e comprendere meglio i problemi di sicurezza sottostanti. MIG offre inoltre una serie di strumenti per l'analisi automatica della sicurezza dei protocolli per l'identità digitale.

INSEGNAMENTO

- Ho tenuto diversi workshops sui protocolli di autenticazione come parte del corso universitario di "Introduction to Computer and Network Security" presso l'Università di Trento negli anni accademici dal 2019 al 2022.
- Ho tenuto seminari negli anni 2021 e 2022, organizzati all'interno del programma di dottorato presso l'Università di Genova - DIBRIS, intitolato "Digital identity: enrollment, authentication, and all that". Nei seminari ho insegnato l'utilizzo di strumenti di pentesting per i protocolli di gestione delle identità.
- Sono stato docente nel 2021 per alta formazione a Padova presso l'ITS Academy Meccatronico (SMACT ITS) per il corso "ITS Cyber Security". Ho aiutato studenti e lavoratori a crescere nelle competenze di cybersecurity insegnando loro i protocolli di gestione delle identità e l'utilizzo di strumenti di penetration testing.
- Sono stato docente dal 2020 al 2022 alla "CyberChallenge.IT", il primo programma di formazione italiano in cybersecurity per studenti delle scuole superiori e universitari organizzato dal CINI.

LINGUE

- Inglese: fluente, scritto e parlato.
- Spagnolo: fluente, scritto e parlato.
- Tedesco: conoscenza base, scritto e parlato.
- Italiano: madre lingua.

COMPETENZE E CAPACITÀ PERSONALI

Sono una persona seria, affidabile, molto legata al territorio, con ottime capacità nell'organizzazione, nella pianificazione e gestione di progetti e nel *problem solving*. Ho un forte senso di responsabilità e di *ownership* dei progetti e delle attività di cui mi occupo, e mi impegno a raggiungere gli obiettivi stabiliti, cercando di superare le difficoltà con determinazione e spirito di squadra. Ho una formazione solida, acquisita attraverso anni di studi e di esperienza lavorativa, che mi consente di affrontare con competenza le sfide che mi vengono presentate. Nel tempo libero ho progettato e sviluppato alcune app mobile con utenti provenienti da tutto il mondo. Sono infine in possesso di certificazione *Agile* per la gestione di progetti.

Trento, 20 dicembre 2024. Andrea Bisegna