Umberto Morelli

ESPERIENZA PROFESSIONALE

Giu. 22 - Lug.22 **Sviluppatore**
Futuro & Conoscenza SRL

Implementazione prototipale della soluzione di **voto elettronico** proposta nel progetto E-voting.

Mag. 16 – Mag.22 **Tecnologo**
Fondazione Bruno Kessler - Unità di Security & Trust, Trento

Design e sviluppo di una soluzione di **voto elettronico** anti-coercizione a supporto degli italiani all'estero nell'ambito del progetto Futuro & Conoscenza E-Voting.

Security Code Review del *middleware* utilizzato per l'autenticazione e l'interazione dell'utente con la Carta d'Identità Elettronica (CIE 3.0) in ambienti Windows, Linux e Mac OS.

Analisi dell'applicazione mobile Android CieID con metodologia OWASP nell'ambito dell'aggiornamento sulla conformità della CIE 3.0 al regolamento UE eIDAS.

Security Testing della piattaforma Cartella Clinica del Cittadino (TreC): analisi del *backend* e delle applicazioni mobile a supporto della piattaforma secondo le linee guida OWASP e NIST.

- Analisi dei rischi e *Threat Modelling* nell'implementazione di nuove funzionalità.
- Supporto al gruppo di sviluppo per realizzare soluzioni sicure *by-design* e *by-default*: analisi delle applicazioni mobile *OTP PAT* e *TreC Referti*; design e analisi dell'applicazione mobile *TreC FSE* e supporto alle implementazioni pilota (es., TreC Diabete).

Analisi di vulnerabilità web di tipo *Cross-site Request Forgery* nella classifica Alexa Top 1500, nei processi che precedono e seguono la fase di autenticazione dell'utente.

Attività di ricerca e analisi di sicurezza relative all'uso della **Carta d'Identità Elettronica** (CIE 3.0):

- Analisi dell'implementazione del protocollo SAML nel flusso di autenticazione con la CIE 3.0 (nell'ambito del gruppo di lavoro DigiMat Lab). Analisi degli ambienti preproduzione e produzione; verifica del traffico.
- Supporto al design e implementazione di una soluzione di ***pull printing*** open-source, basata su OpenID Connect (OIDC), che usa la CIE 3.0 come secondo fattore per l'invio in stampa di documenti sensibili. Estensione verso un ecosistema di servizi aziendali.
- Uso della CIE 3.0 per rilasciare un'identità derivata, univoca e sicura, ai dispositivi IoT (caso d'uso *automotive*).

Collaborazione con un noto consorzio bancario italiano:

- Identificazione e verifica del fornitore più adatto di ***Threat Intelligence***.
- Valutazione dei requisiti di sicurezza nello sviluppo di un'**architettura a microservizi**.

Due Diligence per un *exchange* italiano di criptovalute.

Sviluppo di SecurePG, uno strumento per la generazione e valutazione locale di politiche di controllo degli accessi in ambienti **cloud** (piattaforme Amazon AWS e OpenStack); e per la migrazione di identità e permessi da/verso il cloud.

- Estensione del meccanismo di controllo degli accessi di AWS in ambito ***Internet of Things*** (IoT) e sua valutazione nel cloud e in locale (elaborazione su dispositivi ***edge***).
- Utilizzo dei servizi AWS IAM (gestione delle identità), S3 (memorizzazione dati), RDS (database relazionale), Lambda (funzioni *serverless*), IoT e GreenGrass (*Edge processing*).

Supporto allo sviluppo di MQTTSA, strumento per rilevare errori di configurazione con alto impatto sulla sicurezza e possibili vulnerabilità in architetture IoT basate sul protocollo **MQTT**.

- Analisi delle prestazioni e funzionalità di sicurezza nelle implementazioni di MQTT open-source più utilizzate; anche considerando l'ultima versione del protocollo (MQTT 5).
- Analisi postura di sicurezza dei server MQTT catalogati dal motore di ricerca Shodan;
- Utilizzo di MQTTSA per la formazione e durante gli eventi divulgativi *Notte dei Ricercatori 2021 e 2019*; e durante *Isaca Community Day 2019* con uno scenario di domotica che usa la CIE 3.0 per comandare un modellino di porta via MQTT, un lettore carte e un'applicazione Android.

Supporto allo sviluppo di un'interfaccia per configurare in maniera sicura un servizio MQTT e valutarne le prestazioni in diverse condizioni operative, in ambienti reali o simulati.

- Verifica dei cifrari utilizzati in Mosquitto, una delle implementazioni più diffuse di MQTT, mediante simulazione con container **Docker**.

Sviluppo di un laboratorio per approfondire, mediante l'uso delle schede *Raspberry PI* e *Arduino*, le problematiche di sicurezza derivanti dall'unione di **IT e OT**; e suo utilizzo durante un corso e un workshop presso l'I.T.T. Buonarroti di Trento e durante l'evento ProM 2019.

Didattica in ambito sicurezza, cloud e IoT presso l'I.T.T. Buonarroti di Trento (corso *Digital Security*, A.A. 2019/20 e 2020/21) e l'istituto di formazione Fòrema (*corso ITS Industrial Cyber Security Specialist*, A.A. 2021/22).

- Utilizzo dei servizi Azure AD (gestione delle identità), Azure Blob Storage (memorizzazione dati), Azure IoT ed IoT Edge.

Approfondimento e uso delle tecnologie **Blockchain** e **Distributed Ledger**.

- Supporto alla creazione di un modello di controllo degli accessi basato su attributi con Hyperledger Fabric; sperimentazione con la piattaforma IOTA.
- Analisi potenzialità e possibili applicazioni in ambito sanitario durante l'evento sponsorizzato dalla Fondazione Bruno Kessler WebValley 2018; focus sulla conformità normativa - seminario per il corso di Comparative Private Law alla Facoltà di Giurisprudenza di Trento.
- Confronto tra le diverse tipologie durante l'attività di tutoraggio curriculare per studenti triennali dell'Università degli Studi di Trento.

Pubblicazioni:

- R. Longo, U. Morelli, C. Spadafora, A. Tomasi. *Adaptation of an i-voting scheme to Italian Elections for Citizens Abroad* [inviato a E-Vote-ID 2022].
- A. Tahir, M. Umberto, R. Silvio. *Distributed Enforcement of Access Control policies in Intelligent Transportation System (ITS) for Situation Awareness* [accettato ad ARES FARES 2022].
- S. Berlato, M. Umberto, C. Roberto, R. Silvio. *End-to-End Protection of IoT Communications Through Cryptographic Enforcement of Access Control Policies* [accettato a DBSEC 2022].

- U. Morelli, I. Vaccari, S. Ranise, E. Cambiaso. *DoS Attacks in Available MQTT Implementations: Investigating the Impact on Brokers and Devices, and supported Anti-DoS* Protections [accettato ad ARES IoT SecFOR 2021].
- M. Leonelli, U. Morelli, G. Sciarretta, S.Ranise. *Secure Pull Printing with QR Codes and National eID Cards: A Software-oriented Design and an Open-source Implementation* [accettato a CODASPY 2021].
- A. Tahir, M. Umberto, R. Silvio, Z. Nicola. *Extending access control in AWS IoT through event-driven functions: an experimental evaluation using a smart lock system* [accettato a IJIS 2021].
- A. Tahir, M. Umberto, R. Silvio. *Deploying Access Control Enforcement for IoT in the Cloud-Edge Continuum with the help of the CAP Theorem* [accettato a SACMAT 2020].
- M. Leonelli, U. Morelli, S. Ranise, G. Sciarretta. *Pull Printing with National eID Cards: An Open-source and Software-oriented Implementation* [accettato a ITASEC 2020].
- U. Morelli, L. Nicolodi, S. Ranise. *An Open and Flexible CyberSecurity Training Laboratory in IT/OT Infrastructures* [accettato a MSTEC 2019].
- U. Morelli, S. Ranise, D. Sartori, G. Sciarretta, A. Tomasi. *Audit-Based Access Control with a Distributed Ledger: Applications to Healthcare Organizations* [accettato a STM 2019].
- P.Prem, A.Palmieri, S.Ranise, U.Morelli and T.Ahmad. MQTTSA: *A Tool for Automatically Assisting the Secure Deployments of MQTT brokers[accettato a IEEE WKSP CSR-IoT 2019]*
- A. Tahir, M. Umberto, R. Silvio, Z. Nicola. *A Lazy Approach to Access Control as a Service (ACaaS) for IoT: An AWS Case Study* [accettato a SACMAT 2018].
- M. Umberto, R. Silvio. *Assisted Authoring, Analysis and Enforcement of Access Control Policies in the Cloud* [accettato a IFIPSEC 2017].
- S. Avinash, C. Roberto, C. Luca, D. Nicolas, A. Alessandro, M. Umberto. *Large-scale Analysis & Detection of Authentication Cross-Site Re*quest Forgeries [accettato a EURO S&P 2017]

Lug. 15 – Gen.16

Tirocinio universitario – Università degli studi di Genova

Fondazione Bruno Kessler - Unità di Security & Trust, Trento

Creazione di un'applicazione *web-based* per la gestione delle promozioni e l'aumento della fidelizzazione dei clienti utilizzando i framework di sviluppo Spring e i servizi cloud Amazon AWS.

Nell'analisi è stato valutato il problema del controllo degli accessi analizzando il modello basato su attributi, quello supportato da AWS e la soluzione implementata (basata su OpenID Connect).

Ambito: Gestione, traduzione ed *enforcement* di politiche di controllo degli accesi.

Set. 12 – Dic.12

Tirocinio universitario – Università degli studi di Napoli

SESM Soluzioni Evolute per la Sistemistica e i Modelli, Giugliano in Campania (NA)

Analisi dei principali *controller* in una SDN implementata con OpenFlow allo scopo di ricercare la migliore soluzione per la gestione del traffico dati in una *Enterprise Private Cloud*. La campagna sperimentale è stata condotta valutando prestazioni, isolamento e corretto funzionamento.

Ambito: Protocollo di rete OpenFlow.

ISTRUZIONE E FORMAZIONE

Ott. 17 – Mar. 22

Corsi di formazione

Fondazione Bruno Kessler, Trento

- MS - *AZ-900: Microsoft Azure Fundamentals*; MS - *Security Virtual Training Day: Security, Compliance, and Identity Fundamentals*.
- MS - *AZ-220: Microsoft Azure IoT Developer*; MS - *AZ-500: Microsoft Azure Security*.
- *Cloud-ready Architectures and Applications*; Piattaforme e strumenti per Cloud Native Apps.
- *Introduction to Python II*.

- *Let's be.. Agile!* - Pensiero, manifesto Agile e principali approcci.
- *Clean Code & Test Driven Development*.
- Comunicare la ricerca - Strumenti teorici e pratici; *Super-short science talk*.
- *Public Speaking*; Ingredienti per un *Pitch* di successo.
- *Infographics & data visualization* - Come (rap)presentare i dati in maniera efficace.
- Autoproduzione di video-tutorial e videolezioni.
- Gestire e coordinare un gruppo di lavoro/team di progetto.
- *Team working*; Le relazioni all'interno di un gruppo di lavoro, anche virtuale.
- *Mentoring WebLAB.*
- *Business English*; *English Conversation B2+.*

Sett. 13 – Mar. 16 **Laurea Magistrale in Ingegneria Informatica**
Università degli studi di Genova, Genova
Valutazione conseguita 107/110

Tesi dal titolo: "Condivisione sicura dei dati personali in ambiente Cloud".

Dic. 14 **Certificazione Ericsson IP Technology**
Ericsson Education Center, Genova

Conoscenza completa della suite TCP/IP, differenze IPv4-v6, servizi IP e multicast. Protocollo ethernet, VLAN-tag, IPRouting, protocolli appartenenti alle tipologie Link State e Distance Vector, Atonomous Systems e Classless Routing. Necessità e uso di MPLS e IP-QoS.

Set. 13 **Certificazione Cambridge English (ESOL) - Council of Europe Level B2**
British Council, Napoli

COMPETENZE TECNICHE

Gestione dell'identità e di risorse sensibili *on-premise*, nel cloud e mediante tecnologie basate su Blockchain e Distributed Ledgers; requisiti e responsabilità a livello normativo e implementativo per la corretta gestione dei dati.

Architettura e problematiche di sicurezza nelle reti e in ambienti desktop e mobile: analisi statica e dinamica del codice sorgente; utilizzo dei tool OWASP Zap, Burp e Fiddler per intercettare il traffico e interagire con il sistema dalla prospettiva di un attaccante. Utilizzo delle metodologie OWASP e delle linee guida NIST ed ENISA per la valutazione della postura di sicurezza e del rischio.

Requisiti e problematiche dell'ecosistema *Internet of Things*: implementazione di un meccanismo di controllo degli accessi su dispositivi RaspberryPi che incoraggia l'espressività delle policy e un singolo punto di amministrazione, la portabilità ed estensibilità dei permessi; affronta le problematiche di latenza, affidabilità e scalabilità. Approfondimento delle infrastrutture basate sul protocollo di comunicazione MQTT.

Esperienza con i protocolli di autenticazione e autorizzazione OpenID Connect (anche attraverso il servizio cloud Amazon AWS Cognito), OAuth e SAML.

Containerizzazione e paradigma di programmazione *stateless*: utilizzo di Docker e del servizio Amazon AWS Lambda.

Padronanza del linguaggio Python:

- Sviluppo (in corso) dell'infrastruttura che supporta una soluzione di voto elettronico anti-coercizione.
- Estensione di MQTTSA per il supporto a MQTT 5 e a nuovi test verificare vulnerabilità di tipo *Denial of Service*.
- Sviluppo dei prototipi per le sperimentazioni in ambito IoT e con la Carta d'Identità Elettronica (CIE 3.0).

Sviluppo in ambito mobile:

- Supporto alla realizzazione di un'applicazione Android per la stampa sicura in ambito aziendale con la CIE 3.0.
- Creazione di un'applicazione Android per l'uso della CIE in ambito IoT.

Padronanza del linguaggio Java:

- Utilizzo dei framework Spring, Spring MVC e Spring Security per creare un'applicazione web-based e Android con specifici requisiti di sicurezza; validazione dei parametri mediante le annotazioni di Java, Spring e Hibernate.
- Utilizzo di Java Swing e ANTLR per lo sviluppo di SecurePG.

Buona conoscenza dei linguaggi C++ e C#:

- Analisi e interazione con il Middleware della Carta d'Identità Elettronica in ambienti Windows e Mac OS.
- Progettazione di un *parser* di file PMML per importare dati in Microsoft Sql Server.

Conoscenza di SQL/PLSQL e utilizzo dei database MySQL, SqlServer 2014 e OracleDBMS (mediante connettore JDBC).

Attività di *subreviewer* per le conferenze ITASEC 2017, 2020 e 2021, SACMAT 2019, FPS 2017 e 18, PST 2017.

ALTRE COMPETENZE

Competenze comunicative	Presentazione del corso e workshop IT/OT all'I.T.T. Buonarroti di Trento e del modulo *Identity Access Management* presso l'istituto di formazione Fòrema di Padova; presentazione dei seminari FBK *Internet of Things* e *Sensitive Data Sharing*. Presentazione dei progetti sviluppati nell'Unità di Security & Trust della Fondazione Bruno Kessler (FBK) durante gli eventi e le demo a carattere divulgativo; approfondimenti interni ed esterni in tema Blockchain e Distributed ledger.
Competenze organizzative e gestionali	Collaborazione con l'unità FBK *eHealth* e, nell'ambito del gruppo di lavoro Trentino Salute 4.0, con l'Azienda Provinciale per i Servizi Sanitari (APSS). Coordinamento e gestione in tema di sicurezza dei progetti che coinvolgono le Unità di ricerca eHealth e Security & Trust di FBK. Partecipazione ai gruppi di lavoro FBK Cloud, EHDS e ZeroTrust. Supporto all'ottenimento della ISO 9001 del Centro di Cybersecurity come Responsabile Sistema Gestione Qualità (RSGQ). Attività di mentoring e tutoraggio degli studenti tirocinanti e con progetto di ricerca dell'Università degli Studi di Trento. Premio Best Innovation Idea Award assegnato per l'Elevator Pitch durante l'evento SECENTIS PhD Symposium (Luglio 2016).
Patente di guida	A, B