Curriculum vitae

INFORMAZIONI PERSONALI

Sinigaglia Federico

via G. Acerbi 10/18, 16148, Genova

3331602010

federico.sinigaglia.ge@gmail.com

ESPERIENZA PROFESSIONALE

Dicembre 2018 – Alla data attuale

Funzionario Sistemi Informativi – Capoprogetto

Direzione Sistemi Informativi - Comune di Genova

2017–Novembre 2018

Designer soluzioni di autenticazione

Security and Trust Research unit - FBK & Istituto Poligrafico e Zecca dello Stato

Nell'ambito del **progetto** per realizzare uno scenario d'uso della nuova Carta di Identità digitale ho provveduto a:

- Analisi delle normative
- Analisi delle caratteristiche della CIE come SmartCard
- Design del protocollo di autenticazione
- Design delle fasi preliminari

2016–2017

Analista della sicurezza di protocolli

Security and Trust & E-Health research units, FBK

Nell'ambito del **progetto TreC**, ho eseguito:

- Analisi dei protocolli di autenticazione
- Analisi dei rischi e vulnerabilità dei protocolli
- Design di nuove procedure di attivazione utenti

Nell'ambito del progetto legato all'analisi di sicurezza di **PosteID** ho eseguito:

- Valutazione della sicurezza dei meccanismi di autenticazione implementati
- Analisi di rischi e vulnerabilità
- Design di nuove procedure di attivazione utenti

03/2015–10/2015

Analista protocolli di sicurezza

Fondazione Bruno Kessler, Trento

Nell'ambito di un progetto di ricerca, ho eseguito analisi di determinati protocolli di autenticazione forte forniti da una azienda italiana di medie dimensioni.

In particolare, ho adottato tecniche di specifica formale e model checking per verificare la presenza di attacchi ai vari protocolli da me analizzati.

Il lavoro ha portato alla redazione di un documento di analisi che è stato apprezzato dall'azienda commissionante il lavoro.

2013–2015 **Freelance Web Designer**

- Meeting con clienti
- Design e realizzazione di siti web

02/2014–07/2014 **User Interface Designer**

Ianuatech S.r.l., Genova

ISTRUZIONE E FORMAZIONE

11/2015–alla data attuale **Dottorando di Ricerca**

Università degli studi di Genova, Fondazione Bruno Kessler

Il dottorato di ricerca verte sull'analisi di sicurezza di protocolli per l'autenticazione forte.

Il lavoro ha visto un iniziale impegno nello studio dello stato dell'arte, diviso in:

- Identificazione scenari applicativi
- Analisi e approfondimenti su implementazioni reali
- Studio di normative Europee nell'ambito degli scenari rilevanti
- Studio di documentazione e linee guida fornite da istituzioni ed entità di notevole rilevanza nell'ambito (es, NIST)

Una seconda parte del lavoro ha portato alla specifica di una metodologia di analisi per soluzioni di autenticazione forte, costituita da:

- Identificazione di caratteristiche rilevanti per la sicurezza di un protocollo di autenticazione forte
- Estensione dell'analisi sulle fasi preliminari all'utilizzo del protocollo
- Specifica di un linguaggio semi-formale per la rappresentazione dei protocolli
- Specifica di un insieme di modelli di attaccante per la verifica della sicurezza
- Specifica del metodo di analisi

Gli studi hanno anche permesso la realizzazione di un prototipo per l'automatizzazione parziale della procedura di analisi

09/2013–03/2015 **Laurea Magistrale in Ingegneria Informatica (110/110)**

Università degli Studi di Genova, Genova (Italia)

TESI: *Analisi di Sicurezza di Protocolli per l'Autenticazione Forte.*
Nel mio lavoro di tesi ho analizzato la sicurezza di alcuni protocolli di autenticazione forte. A tal fine, ho impiegato metodi di specifica formale e di model checking per verificare la presenza di possibili vulnerabilità nei protocolli proposti.

Esami sostenuti:

SISTEMI E INTERFACCE MULTIMEDIALI
• Basic interaction types
• Modal and multimedia environments
• Affordance and Gesthalt concepts
• Human body actions and reactions
• Human senses modeling (Card-Moran-Newell, Fitt's Law, etc)
• KLM modeling
• Testing (Anova, ecc)

GESTIONE DEI SISTEMI DI PRODUZIONE
• Petri Networks
• Can-Bus

• Scheduling (EDD, SDD, etc)

SISTEMI OPERATIVI E SICUREZZA INFORMATICA
• Criptography (Block, stream, etc)
• Public and Private Keys
• Smart Cards and Authentication Protocols
• Security Protocols and Practical examples (Needham–Schroeder, etc)
• Access Control (Access Control List, Role-Based, Mandatory)
• Mobile Security on Android OS

METODI E MODELLI PER L'INGEGNERIA DEL SOFTWARE
• Developing Methods (Agile, V, etc.)
• Testing Basic Concepts
• Model Checking (Bounded, LTL formulas, CTL, etc)
• SPIN & PROMELA testing

SISTEMI TRANSAZIONALI E DATA MINING
• OLAP
• Data Mining Techniques
• Advanced queries

CONTROLLO DIGITALE
• Z Transform
• Analog signal Conversion
• Digital Control in Closed Loop

RICERCA OPERATIVA
• Simplex
• Ordinary Least Squares
• Gradient Descent

TECHNOLOGIES FOR WIRELESS NETWORKS
• Wi-Fi specifications
• Wi-Fi basic functioning and protocols
• Wi-Fi security
• Bluetooth basic functioning and transmission protocols
• GSM basic functioning and transmission protocols
• UMTS basic functioning and transmission protocols

REAL-TIME OPERATING SYSTEMS
• Real Time Policies
• Real Time Scheduling
• RTAI and basic linux driver programming

AMBIENT INTELLIGENCE
• Sensors types and peculiarities
• Localization protocols (triangulation, ecc)
• Intelligent Environment design
• Knowledge representation
• OWL language and class-individual relationship

SOFTWARE ARCHITECTURES
• Java language
• Thread scheduling
• Parallel program execution
• Shared resources problems

TECHNOLOGIES FOR INDUSTRIAL AUTOMATION
• Basic instruments in industrial applications (Valve, Indicators, magnetic flow meter, etc)

• Fieldbus
• Power supply and safety problems
• Profinet
• Smart Devices

09/2009–09/2013

Laurea Triennale in Ingegneria Informatica

Università degli Studi di Genova, Genova (Italia)

COMPETENZE PERSONALI

Lingua madre: italiano

Lingue straniere

	COMPRENSIONE		PARLATO		PRODUZIONE SCRITTA
	Ascolto	Lettura	Interazione	Produzione orale	
inglese	C1	C1	C1	C1	C1

Livelli: A1 e A2: Utente base - B1 e B2: Utente autonomo - C1 e C2: Utente avanzato
Quadro Comune Europeo di Riferimento delle Lingue

Competenze comunicative

- Buone competenze comunicative, dovute alla mia naturale propensione al dialogo e all'interazione con altre persone
- Buon livello di comunicazione in pubblico e propensione all'insegnamento

Competenze professionali

- Buone competenze in tutoring, visto il mio impegno nel seguire con successo un tesista durante il suo percorso di laurea triennale

Competenze digitali

AUTOVALUTAZIONE				
Elaborazione delle informazioni	Comunicazione	Creazione di Contenuti	Sicurezza	Risoluzione di problemi
Utente avanzato	Utente avanzato	Utente autonomo	Utente avanzato	Utente autonomo

Competenze digitali - Scheda per l'autovalutazione

Patente di guida: A, B

ULTERIORI INFORMAZIONI

Pubblicazioni

- F. Sinigaglia, R. Carbone, G. Costa, **Strong Authentication for e-Banking: A Survey on European Regulations and Implementations**, SECRYPT 2017
- G. Costa, F. Sinigaglia, R. Carbone, **PolEnA: Enforcing Fine-grained Permission Policies in Android**, SAFECOMP 2017

Conferenze

- **Feb 2018-** Attività di disseminazione delle conoscenze riguardante un'estensione del lavoro su *Strong Authentication for e-Banking: A Survey on European Regulations and Implementations*, presso ITASEC 2018.
- **Set 2017 -** Presentazione del lavoro *PolEnA: Enforcing Fine-grained Permission Policies in Android*, presso SAFECOMP 2017.
- **Lug 2017 -** Presentazione del lavoro *Strong Authentication for e-Banking: A Survey on European Regulations and Implementations*, presso SECRYPT 2017.

Presentazioni

- **Feb 2018 -** Seminario introduttivo su *Sicurezza informatica e all'internet delle cose*, presso Fondazione Bruno Kessler
- **Dec 2016 -** Seminario di approfondimento su *Tecnologie per virtualizzazione di smart card - ArcotID*, presso Università di Genova

Corsi

- **Bertinoro International Spring School 2016**
  - Advanced topics in programming languages, Giuseppe Castagna
  - Models and Languages for Service-Oriented and Cloud Computing, Gianluigi Zavattaro
- **Comparative ICT Law**, Paolo Guarda, Mark Perry, Thomas Margoni, presso Università degli Studi di Trento - Facoltà di Giurisprudenza, Feb-Apr 2017
- **Mobile security**, Alessandro Armando, 2016
- **Security Analysis Techniques based on SMT Solving**, Silvio Ranise, Nov 2016
- **SECENTIS Winter School**, Nov 2016
- **MOVEP Summer School**, May 2017