CURRICULUM VITAE DI:

BORTOLOZZO MATTEO

INFORMAZIONI PERSONALI

Nome	BORTOLOZZO MATTEO
Indirizzo	
C.A.P.	30030
Telefoni	
MOBILE:	333 1216735
E-mail	matteo.bortolozzo@libero.it
Sito	http://matteobortolozzo.altervista.org
Nazionalità	ITALIANA
Data di nascita	24 MAGGIO 1982

ISTRUZIONE E FORMAZIONE

LICENZA MEDIA

Licenza di scuola Media conseguita presso l'istituto "Ungaretti" di Spinea (VE) con indirizzo (sperimentale) informatico.
Regolarmente diplomato in 3 anni con valutazione: BUONO

LICENZA SUPERIORE

Licenza di scuola Superiore conseguita presso l'Istituto I.T.I.S. "Primo Levi" di Mirano (VE) con indirizzo ELETTRONICA E TELECOMUNICAZIONI.
Regolarmente diplomato in 5 anni con valutazione: 85/100

CARRIERA UNIVERSITARIA

Laurea **TRIENNALE** in INFORMATICA conseguita nell'anno 2006 presso l'università "Cà Foscari" di Venezia con valutazione 95/110.
Vincitore di una borsa di studio del "Fondo Sociale Europeo" conferita ai 15 migliori studenti del primo anno di corso.
Tesi di Laurea presentata nell'ambito della SICUREZZA dal titolo: "D.R.M.: tecnologie per la tutela del diritto d'autore nell'era digitale". Tale tesi verte nell'analisi critica delle tecnologie di DRM presenti nel mercato.

Laurea **MAGISTRALE** (specialistica) in INFORMATICA conseguita nell'anno 2009 presso l'università "Cà Foscari" di Venezia con valutazione 106/110.
Tesi di Laurea presentata nell'ambito della SICUREZZA dal titolo: "Vulnerabilità dello standard PKCS#11: dalla teoria alla pratica". Tale tesi verte sull'analisi teorica e sperimentale delle debolezze dello standard PKCS#11, finalizzata alla produzione di un software per la verifica degli attacchi sui dispositivi hardware che supportano tale standard.

Più volte assistente di laboratorio per il corso di "Laboratorio di Architettura degli elaboratori" che verte sulla programmazione ASSEMBLY.

Speaker alla conferenza internazionale A.S.A. svoltasi a Port Jefferson (New York) nel Luglio 2009.

ESPERIENZE DI STAGE

Nome: TIM S.p.a.
Tipologia: Telecomunicazioni

Panoramica sui vari settori che compongono una tipica sede TIM:

- ✓ assistenza del cliente
- ✓ installazione e manutenzione delle antenne per la copertura del segnale

Nome: Dal Maschio automazioni
Tipologia: Automazioni industriali

Creazione di robot per processi industriali:

- ✓ assemblaggio della componentistica elettronica che compone il pannello principale di controllo
- ✓ assemblaggio delle parti meccaniche
- ✓ stesura del software per il funzionamento dell'automa
- ✓ collaudo del robot

ESPERIENZE LAVORATIVE

Datore: Università Cà Foscari di Venezia
Tipologia: Ricerca e sviluppo

Approfondimento nello studio dello standard PKCS#11 al fine di creare un prodotto software da inserire nel mercato.
Durante il periodo occupazionale ho partecipato come "speaker" alla conferenza A.S.A. (Analysis of Security APIs) tenutasi a Port Jefferson (New York) nel Luglio 2009 dove ho presentato i risultati della mia ricerca.
Sempre durante il periodo contrattuale ho lavorato in Francia all'INRIA (Institut national de recherche en informatique et automatique) a fianco del Dr. Graham Steel per creare un sistema di verifica e di attacco automatico dei dispositivi PKCS#11 mediante operazioni di reverse engineering.

Datore: Università Cà Foscari di Venezia
Tipologia: Ricerca e sviluppo

Miglioramento, ottimizzazione e sperimentazione su larga scala del software prodotto. Il software finora realizzato è stato testato su un considerevole numero di Token PKCS#11 presenti in commercio con il fine di produrre un articolo scientifico.

Datore: BRB Solutions
Tipologia: Sviluppo software

Da Febbraio 2011 lavoro presso la "BRB Solutions" di Mira come sviluppatore software. La mia principale occupazione è lo sviluppo di un software per studi fotografici che consente l'archiviazione, l'organizzazione e la manipolazione di fotografie digitali. In questo periodo ho anche dato il mio apporto per sviluppo di software per Verona Fiere (Vinitaly), Cà Foscari (digital-week) e altri.

ESPERIENZE DI RILIEVO

Nel Marzo del 2009 ho iniziato lo studio del sistema "iMOB Venezia"e ho partecipato ad un meeting presso la sede dell'ACTV a Mestre dove è stata dimostrata una delle vulnerabilità scoperte nel sistema iMOB.

BORSA DI RICERCA

Vincitore di una borsa di studio della durata di un anno presso l'università degli studi "Cà Foscari" di Venezia, dipartimento di informatica. Il lavoro di ricerca ha riguardato lo studio dei tag RFid, con particolare attenzione alla soluzione introdotta dal sistema di trasporto pubblico locale di ACTV (iMob).
Lo scopo di tale borsa è lo studio della sempre più emergente tecnologia RFid e delle possibili vulnerabilità nella sua sicurezza.

PUBBLICAZIONI E ARTICOLI SCIENTIFICI

- ✓ Secure your PKCS#11 token against API attacks! (presentato alla conferenza ASA a Port Jefferson nel Lugio 2009)
- ✓ Attacking Aladdin eToken PRO
- ✓ Vulnerability Report on Feitian StorePass2000, ePass2000 and ePass2003Auto
- ✓ How Smart is Your Smartcard? (Extracting Keys from PKCS#11 Security Tokens)
- ✓ Remote attacks on PKCS#11 Token
- ✓ CryptokiX: A cryptographic software token with security fixes (in quest'articolo, accettato alla conferenza ASA 2010 e FloC 2010 che si è tenuta ad Edimburgo dal 9 al 12 Luglio 2010 è stata per la prima volta presentata la mia soluzione al problema degli attacchi ai token PKCS#11)
- ✓ How Smart is Your Smartcard? Attacking and Fixing PKCS#11 Security Tokens (presentato alla 17° esima A.C.M. Conference on Computer and Communications Security, a Chicago nell'Ottobre 2010)

CAPACITÀ E COMPETENZE PERSONALI

Certificazioni rilasciate da AISACE (centro di formazione per l'emergenza sanitaria, regione Veneto):

- ✓ PS: Primo Soccorso (Att. 496/V/PS2011). Corso con esame teorico e pratico sulle procedure di primo soccorso, massaggio cardiaco e respirazione artificiale
- ✓ BLSD: Basic Life Support and Defibrillation (Att. 316/V/BLSD2011). Corso con esame teorico e pratico sull'utilizzo del defibrillatore

Abilitazione al maneggio delle armi da fuoco lunghe e corte (Cert. Num. 1425157)
Qualifica di allenatore/educatore rilasciata da "Lions Club" e riconosciuta dal CONI.
Predisposizione alla grafica e alle presentazioni in pubblico.

MADRELINGUA ITALIANO

ALTRE LINGUE INGLESE

Capacità di lettura	buono
Capacità di scrittura	buono
Capacità di espressione orale	buono

CAPACITÀ E COMPETENZE ORGANIZZATIVE

Da sempre designato nell'amministrazione dei gruppi di lavoro universitari per lo sviluppo di software o documenti, nei corsi di Web Design, Ingegneria del Software, Laboratorio di Ingegneria del Software, Sistemi Operativi, Calcolo Parallelo, Linguaggi Logici, Laboratorio di Linguaggi, Basi di Dati e Laboratorio di Basi di Dati.
Per due anni ho svolto l'incarico di assistente di laboratorio per il corso di Laboratorio di Architettura degli elaboratori (programmazione in assembly).
Collaborazione con gli assessori comunali nel 2006 per la realizzazione di alcuni aspetti della "Festa dello Sport" di Salzano.
Nel gruppo sportivo di cui faccio parte svolgo regolarmente la mansione di Web Desing del sito web che ho prodotto e gestisco le relazioni con alcuni fornitori di materiale sportivo. Nel 2007 ho ricevuto dal mio Direttore Tecnico un riconoscimento per la "dedizione e la passione" che ho proferito nello sviluppo di tale gruppo sportivo.
Precedentemente membro di un team di Hacking universitario che ha lo scopo di partecipare alle sfide internazionali di "capture the flag".

CAPACITÀ E COMPETENZE TECNICHE

Realizzazione di alcuni siti web con tecnologia HTML/CSS
Conoscenza dei linguaggi di programmazione/scripting: ASSEMBLY, C, JAVA, PERL, PROLOG, C#, LINQ, XAML, XML.

DataBase conosciuti:

- ✓ MySQL
- ✓ SQL SERVER 2008

Conoscenza di livello avanzato di applicazioni come:

- ✓ MS Office (Microsoft)
- ✓ Vue (e-on software) per lo sviluppo di ambientazioni grafiche 3D
- ✓ Poser (curious Lab) per lo sviluppo di modelli umani 3D
- ✓ PinnacleVideoStudio (Pinnacle) per il montaggio di filmati
- ✓ UnleadMediaStudio (Unlead) per il montaggio di filmati
- ✓ Adobe Premiere Pro (Adobe) per il montaggio di filmati
- ✓ Photoshop (Adobe) per la manipolazione di immagini
- ✓ Adobe Audition (Adobe) per la manipolazione audio

Ambienti di sviluppo conosciuti:

- ✓ Microsoft Visual Studio (C, C++, C#)
- ✓ NetBeans (Java)
- ✓ Dreamweaver (Macromedia) per lo sviluppo di siti Web

Librerie di terze parti finora studiate e utilizzate:

- ✓ IAIK (libreria di interfacciamento tra l'implementazione dello standard PKCS#11 e Java)
- ✓ Aforge (libreria di filtri grafici)
- ✓ XPBurn (libreria per la masterizzazione di file in ambiente Windows)

Linguaggi di programmazione in apprendimento

- ✓ PHP

CAPACITÀ E COMPETENZE ARTISTICO-SPORTIVE

Pratica costante d'attività fisica come:

- ✓ Sollevamento pesi
- ✓ Mountain bike
- ✓ Tiro con l'arco
- ✓ Kick Boxing
- ✓ Taekwon-Do (Campione Italiano nel 2007, Campione regionale nel 2005 e nel 2007, Campione interregionale nel 2007 e nel 2008, Secondo Classificato ai Campionati regionali del 2008, Terzo Classificato in due specialità ai Campionati Italiani nel 2008, diciottesimo posto a pari merito alla Coppa del Mondo nel 2008, Campione Italiano nel 2010 e terzo posto nella specialità "combattimento tradizionale")
- ✓ Kalah - Krav Maga
- ✓ Mixed Martial Arts - Valetudo
- ✓ Knife Combat (Baraw)

Partecipazione a Stage di Taekwon-Do, difesa personale e Military Kraw Maga con Borut Kincl (addestratore delle truppe speciali Serbe) e Peter Weckauf.
Qualifica di istruttore e di arbitro nazionale nell'ambito del Taekwon-Do I.T.F.
Autodidatta di Kobuto
Regolarmente iscritto al "Tiro a segno Nazionale"
Appassionato di fotografia digitale

ATTUALI ATTIVITA'
(extra lavorative)

Istruttore di Taekwon-Do I.T.F. presso la palestra "Fitness Formula" a Mirano (VE).
Frequentatore del corso istruttori di "Tecniche e tattiche di Krav Maga" presso la S.D.T.T. (Self Defence Techniques & Tactics). Il fine di tale corso è la formazione completa di un insegnante per la difesa personale.
Frequentatore del corso istruttori di BARAW (Knife Combat) presso il S.A.M.I. (Vienna - Austria)

PATENTE O PATENTI

Patente acquisita di tipo B