Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

IL RETTORE

VISTO lo Statuto della Scuola IMT Alti Studi Lucca, emanato con Decreto Direttoriale n. 05973(214).I.2.02.07.19, pubblicato nella Gazzetta Ufficiale, Serie Generale - n. 163 del 13 luglio 2019, modificato con Decreto Direttoriale n. 03610(160).I.2.22.04.21 pubblicato sulla Gazzetta Ufficiale, Serie Generale, n. 108 del 7 maggio 2021 e con Decreto Direttoriale n. 04794(145).I.2.22.04.22 - Pubblicato sulla Gazzetta Ufficiale della Repubblica Italiana – Serie Generale – n. 105 del 6 maggio 2022;

VISTO il Decreto MUR prot. n. 1148 del 12 ottobre 2021 con il quale il Prof. Rocco De Nicola è nominato Direttore (ora Rettore) della Scuola IMT Alti Studi Lucca per la durata di tre anni a decorrere dal 1° novembre 2021;

VISTA la legge 30 dicembre 2010, n. 240 "Norme in materia di organizzazione delle Università, di personale accademico e reclutamento, nonché delega al Governo per incentivare la qualità e l'efficienza del sistema universitario", e in particolare l'art. 19, "Disposizioni in materia di dottorato di ricerca";

VISTO l'art. 4 della Legge 3 luglio 1998, n. 210, che prevede che le Università, con proprio regolamento, disciplinino l'istituzione dei corsi di Dottorato di Ricerca, le modalità di accesso e di conseguimento del titolo, gli obiettivi formativi ed il relativo programma di studi, la durata, il contributo per l'accesso e la frequenza, le modalità di conferimento e l'importo delle borse di studio, nonché le convenzioni con soggetti pubblici e privati;

VISTA la Legge 30 novembre 1989, n. 398 "Norme in materia di borse di studio universitarie", e s.m.i.;

VISTO il D.M. 40/2018 (trasmesso con nota del 25 gennaio 2018) con il quale il Ministero dell'Istruzione, dell'Università e della Ricerca modifica il D.M. del 18 giugno 2008 relativo all'importo annuale delle borse di studio per la frequenza ai corsi di dottorato;

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);

VISTO il Decreto Legislativo 30 giugno 2003, n. 196 – Codice in materia di protezione dei dati personali (recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE);

VISTO il Decreto 14 dicembre 2021, n. 226 - Regolamento recante modalità di accreditamento delle sedi e dei corsi di dottorato e criteri per la istituzione dei corsi di dottorato da parte degli enti accreditati, pubblicato sulla Gazzetta Ufficiale, Serie generale - n. 308 del 29 dicembre 2021;

VISTO il Decreto Ministeriale n. 117 del 2 marzo 2023 con il quale sono state attribuite, per l'anno 2023/2024, a valere sul PNRR, Missione 4 "Istruzione e ricerca", Componente 2 "Dalla Ricerca all'Impresa" - Investimento 3.3 "Introduzione di dottorati innovativi che rispondono ai fabbisogni di innovazione delle imprese e promuovono l'assunzione dei ricercatori dalle imprese", incluse le economie resesi disponibili a valere sulle dotazioni finanziarie di cui all'art. 3, comma 2, del decreto del Ministro dell'università e della ricerca n. 352 del 9 aprile 2022, borse di dottorato di durata triennale per la frequenza di percorsi per dottorati innovativi accreditati ex DM 45/2013 XXXVII ciclo – Anno Accademico 2021/2022 e da accreditare ex DM 226/2021 XXXIX ciclo – Anno Accademico 2023/2024;

VISTO il Decreto Ministeriale n. 118 del 2 marzo 2023 con il quale sono state attribuite, per l'anno 2023/2024, a valere sul PNRR, Missione 4, componente 1 "Potenziamento dell'offerta dei servizi di istruzione: dagli asili nido all'Università" - Investimento 3.4 "Didattica e competenze universitarie avanzate" e Investimento 4.1 "Estensione del numero di dottorati di ricerca e dottorati innovativi per la pubblica amministrazione e il patrimonio culturale", incluse le economie resesi disponibile a valere sulle dotazioni finanziarie di cui all'art. 3, comma 2 e all'art. 3, comma 3 del

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

decreto del Ministro dell'università e della ricerca n. 351 del 9 aprile 2022, borse di dottorato di durata triennale per la frequenza di percorsi di dottorato accreditati ex D.M. n. 45/2013 ed ex D.M. n. 226/2021 e da accreditare ex D.M. n. 226/2021 in programmi dedicati a dedicati alle transizioni digitali e ambientali, per dottorati di ricerca PNRR, per dottorati per la Pubblica Amministrazione e per dottorati per il patrimonio culturale;

VISTE le convenzioni per l'attivazione e il funzionamento del corso di Dottorato di Ricerca di Interesse Nazionale in Cybersicurezza che la Scuola IMT ha sottoscritto nel 2022;

VISTI gli addendum alle convenzioni sopra citate sottoscritti per il finanziamento di borse di dottorato per il XXXIX ciclo;

VISTO il Regolamento del Dottorato di Ricerca della Scuola IMT Alti Studi Lucca, emanato con Decreto del Rettore n. 6729(181).I.3.04.05.23 (Rep. Albo on line n. 6730(170).I.7.04.05.23);

VISTO il Regolamento del Dottorato di interesse nazionale in "Cybersicurezza", allegato alle sopracitate convenzioni;

VISTO il Codice di comportamento della Scuola IMT, emanato con Decreto Direttoriale n. 01053(095).I.3.24.03.14;

VISTO l'IMT *Code of Conduct and Ethics*, emanato con Decreto Direttoriale n. 01408(99).11.05.11;

ACCERTATA la disponibilità a bilancio sul capitolo CG.04.46.05.04.01 - Borse di studio dottorato di ricerca;

ACQUISITO il parere favorevole del Senato Accademico della Scuola espresso durante la seduta del 28 marzo 2023 relativamente al progetto formativo e all'istituzione del XXXIX ciclo dei Programmi di Dottorato della Scuola;

VISTA la delibera del Consiglio di Amministrazione della Scuola adottata durante la seduta del 29 marzo 2023 con la quale è stato approvato il progetto formativo e istituito il XXXVIII ciclo dei Programmi di Dottorato della Scuola;

ACQUISITO il parere favorevole del Nucleo di Valutazione della Scuola espresso durante la seduta del 11 aprile 2023 relativamente al progetto formativo e all'istituzione del XXXIX ciclo del Programma di Dottorato di interesse nazionale in "Cybersicurezza";

TENUTO CONTO che l'attivazione del XXXIX ciclo del Programma di Dottorato di Ricerca di interesse nazionale in "Cybersicurezza" è subordinata alla verifica dei requisiti richiesti per l'accreditamento secondo le modalità definite dagli organismi competenti, ai sensi del DM 226/2021

DECRETA

l'emanazione del bando di concorso pubblico per l'accesso al XXXIX ciclo del Programma di Dottorato di Ricerca di interesse nazionale in "Cybersicurezza" allegato al presente decreto.

Lucca, data della firma digitale

Rocco De Nicola
Rettore
Scuola IMT Alti Studi Lucca
(f.to digitalmente Rocco De Nicola)

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

BANDO DI CONCORSO PER L'ACCESSO AL XXXIX CICLO DEL PROGRAMMA DI DOTTORATO DI RICERCA DI INTERESSE NAZIONALE IN "CYBERSICUREZZA" DELLA SCUOLA IMT ALTI STUDI LUCCA

ARTICOLO 1 - DESCRIZIONE DEL PROGRAMMA E POSTI A CONCORSO

La Scuola IMT Alti Studi Lucca (nel seguito "Scuola IMT" o "Scuola") indice un concorso pubblico per l'accesso al Programma di Dottorato di Ricerca di interesse nazionale in "Cybersicurezza" (XXXIX ciclo):

Descrizione	Proteggere da attacchi informatici gli ambienti ibridi a cui molte organizzazioni sono passate è diventato sempre più difficile. L'adozione del cloud, il lavoro da remoto, la mobilità stanno mettendo a dura prova le capacità di difesa delle aziende e delle amministrazioni pubbliche di tutto il mondo. Per fronteggiare attacchi sempre più sofisticati, sotto forma di zero-day e nuovi malware, serve un mix di tecnologia e best practice, ma soprattutto servono persone con ottime conoscenze tecniche, legali e organizzative, in grado di limitare il divario tra le competenze necessarie e quelle disponibili nel campo della cybersicurezza, visto che questa sta sempre più incorporando il valore della tutela dei diritti nel cyberspazio. Anche se il campo della cybersicurezza si è espanso esponenzialmente nell'ultimo decennio, il fatto che la forza lavoro nel campo non sia aumentata adeguatamente è ormai evidente. Il numero di lavoratori specializzati e qualificati non è sufficiente a soddisfare la domanda, e i mercati del lavoro nazionali sono sconvolti in tutto il mondo, Europa compresa, come conseguenza. Il corso di dottorato di ricerca di interesse nazionale in Cybersicurezza (Ph.D.-CySec) prepara ad analizzare e risolvere un ampio spettro di problemi relativi a diversi aspetti della cybersicurezza, tutti con un elevato interesse istituzionale, sociale e industriale, con l'obiettivo primario di identificare, di volta in volta, le soluzioni più efficaci in funzione dell'obiettivo e del dominio di applicazione. Le opportunità sono quindi sia in ambito accademico, in varie discipline (ingegneria, informatica, economia, legale e gestionale), sia nel settore pubblico, ivi compresa l'Agenzia per la Cybersicurezza Nazionale, sia nei laboratori di ricerca, nei centri di studio e nei centri di competenza, sia nei settori privati per servizi, sicurezza industriale e consulenze professionali. L'obiettivo principale del dottorato di interesse nazionale Ph.D.-CySec è quello di formare una nuova generazione di studiosi, e futuri responsabili, che possano supportare e aumentare la resilienza di cittadini, istituzioni pubbliche e imprese rispetto ad attacchi informatici, sviluppando e implementando correttamente processi e infrastrutture digitali più sicure e affidabili. Durante il percorso dottorale, gli allievi/le allieve impareranno ad affrontare i problemi di sicurezza informatica da diverse prospettive, all'interno di un team inter- e multi-disciplinare di esperti di altri campi e avranno la possibilità di affrontare casi di studio reali proposti da attori e stakeholder sia del settore privato sia di quello pubblico. Al termine del dottorato, gli allievi/le allieve saranno in grado di affrontare la crescente complessità degli attacchi informatici, grazie a un approccio olistico che abbraccia aspetti tecnologici, economici, umani, sociali e legali. Gli sbocchi professionali comprendono, oltre alla carriera accademica, ruoli manageriali nel settore privato e nella pubblica amministrazione, in enti governativi, nonché l'inserimento in organismi di ricerca di vario tipo che richiedono professionisti, esperti e dirigenti caratterizzati da solide competenze scientifiche, background tecnologico e metodologico in cybersicurezza. Per raggiungere tali obiettivi, il dottorato di interesse nazionale Ph.D.-CySec propone un forte

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

Descrizione	approccio multidisciplinare e interdisciplinare fornendo una formazione di base di ampio respiro e concentrandosi su alcuni ambiti di specializzazione. Saranno ammessi al dottorato studenti con diverso background formativo che va dall'informatico, all'ingegnere dell'informazione, al matematico, al fisico fino all'esperto legale, all'economista e allo scienziato sociale. Il piano didattico, grazie alla numerosità e alla diversificazione culturale del collegio docenti, prevederà percorsi specializzati ritagliati sulle competenze in ingresso che punteranno ad offrire una visione olistica della cyber sicurezza ma allo stesso tempo a specializzare in diversi ambiti chiave attraverso i quattro diversi curriculum descritti di seguito. Il curriculum in **Foundational Aspects in Cybersecurity** offre un background scientifico per l'avanzamento della ricerca in materia di sicurezza informatica, che include elementi di crittografia, intelligenza artificiale, programmazione sicura, calcolo distribuito, metodi formali e linguaggi, e ulteriori contributi innovativi alla ricerca sulla sicurezza informatica. A conclusione del percorso dottorale, l'allievo sarà in grado di collaborare con gruppi di ricerca nel mondo accademico e in centri di ricerca privati o pubblici. Il curriculum in **Software, System, and Infrastructure Security** mira a fornire le conoscenze scientifiche, tecnologiche e metodologiche necessarie per affrontare, in modo appropriato e proattivo, i principali problemi posti dalla sicurezza di sistemi e infrastrutture di varia natura e complessità, inclusi software, hardware e sistemi di comunicazione, caratterizzati da requisiti di sicurezza e resilienza diversi, a seconda del loro specifico campo di applicazione. A conclusione del percorso dottorale, l'allievo sarà in grado di collaborare con team multidisciplinari per affrontare, dal punto di vista sia tecnologico sia operativo, i vari aspetti di sicurezza dei sistemi e delle infrastrutture, comprese quelle critiche. Il curriculum in **Data Governance & Protection** affronta temi relativi alla necessità di archiviare ed elaborare i dati in modo efficace ed efficiente, di fare affidamento su piattaforme di elaborazione scalabili, efficienti e affidabili e altre questioni relative alla riservatezza e all'integrità dei dati e dell'elaborazione. A conclusione del percorso dottorale, l'allievo padroneggerà i metodi e le tecnologie per il controllo dell'accesso ai dati e la regolamentazione del loro utilizzo, riducendo al minimo l'impatto sull'utente finale e garantendo riservatezza, integrità e disponibilità dei dati in tutto il ciclo di vita dei dati stessi, dalla creazione alla elaborazione, alla trasmissione e alla memorizzazione. Il curriculum in **Human, Economic, and Legal Aspects in Cybersecurity** è rivolto principalmente a candidati/e con un background non STEM, a cui fornisce una solida conoscenza degli aspetti tecnici della sicurezza informatica utilizzati per comprendere e affrontare i rischi potenziali o esistenti per la sicurezza informatica e padroneggiare le strategie necessarie per ridurli e proteggere le informazioni sensibili. I profili in uscita possiederanno le necessarie conoscenze e competenze tecniche nell'ambito delle tecnologie dell'informazione, saranno in grado di comprendere il quadro socio-giuridico generale in cui operano e di progettare processi operativi in linea con gli standard di tutela dei diritti fondamentali, gli obblighi normativi, le politiche internazionali e le implicazioni economiche. Gli sbocchi professionali comprendono, oltre alla carriera accademica, ruoli manageriali nel settore privato e nella pubblica amministrazione, in enti governativi, nonché l'inserimento in organismi di ricerca di vario tipo che richiedono professionisti, esperti e dirigenti caratterizzati da solide competenze scientifiche, background tecnologico e metodologico in cybersicurezza.

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

La Scuola IMT applica il principio di pari opportunità e rifiuta ogni discriminazione basata su stati e qualità personali quali il sesso, l'identità di genere, l'identità nazionale o etnica, la fede religiosa, l'orientamento sessuale, lo stato di salute e qualunque altro stato o qualità non rilevanti in relazione al procedimento di cui al presente bando.

Durata del Programma di Dottorato: tre anni.

Inizio del Programma di Dottorato: 1 dicembre 2023

Coordinatore del Programma: Prof. Rocco De Nicola.

Lingua ufficiale dei Programmi di Dottorato: inglese.

Borse di dottorato: 30, da assegnare nell'ambito dei progetti riportati in allegato.

I posti possono essere aumentati a seguito di finanziamenti erogati da soggetti pubblici o privati che si rendessero disponibili anche dopo l'emanazione del presente bando. Di tale evenienza è data comunicazione mediante pubblicità sul sito web e all'Albo on line della Scuola o con altri mezzi ritenuti idonei.

Importo lordo delle borse di dottorato: 16.243,00 euro annuali (per i dettagli si veda il successivo art. 8).

Ulteriori *benefit* per i vincitori della presente selezione:

- totale esenzione dal pagamento delle tasse di iscrizione. Tale esenzione non comprende il pagamento della tassa regionale per il diritto allo studio (attualmente pari a 140€/anno);
- possibilità di usufruire di *benefit* aggiuntivi, come indicato nelle schede dei progetti allegate al presente bando.

ARTICOLO 2- REQUISITI DI AMMISSIONE AL CONCORSO

Possono partecipare al concorso coloro che, entro la data di scadenza per la presentazione della domanda di partecipazione, siano in possesso dei seguenti requisiti:

1. **Titolo di studio** (per la documentazione necessaria si veda il successivo art. 3) in alternativa tra i seguenti:
   - Laurea magistrale o specialistica, ai sensi del D.M. n. 509 del 3 novembre 1999, e successive modifiche, o laurea quadriennale o quinquennale conseguita ai sensi del previgente ordinamento, o titolo di studio conseguito all'estero e dichiarato equipollente;
   - titolo di studio conseguito all'estero che non sia già stato dichiarato equipollente ai titoli sopra citati, purché dia accesso al Dottorato di Ricerca nel Paese in cui è stato conseguito e sia riconosciuto idoneo dalle Commissioni di Concorso ai soli fini dell'ammissione al concorso.

Ai candidati/Alle candidate si chiede di allegare online i documenti come descritti all'articolo 3, "Tabella 2 – Allegati" del presente bando.

2. **Conoscenza della lingua inglese:** i candidati/le candidate devono dichiarare la conoscenza della lingua inglese selezionando uno dei livelli previsti nella sezione dedicata del modulo d'iscrizione online.

Possono altresì partecipare al concorso coloro che prevedano di conseguire un titolo accademico valido per l'ammissione entro il giorno **31 ottobre 2023**. In tal caso l'ammissione al concorso è disposta "con riserva" e il candidato/la candidata è tenuto/a a presentare, entro e non oltre il giorno dell'immatricolazione, una

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

autocertificazione del conseguimento del titolo (per i titoli conseguiti in Italia) o una copia del certificato del conseguimento del titolo (per i titoli conseguiti all'estero) a pena di esclusione. È possibile anticipare il documento sopraindicato via e-mail all'indirizzo phdapplications@imtlucca.it.

ARTICOLO 3- DOMANDA DI AMMISSIONE

La domanda di ammissione deve essere obbligatoriamente **compilata in lingua inglese** e **confermata** utilizzando esclusivamente la procedura on line resa disponibile dalla Scuola IMT, **a pena di esclusione**, entro e non oltre le **ore 13:00 (ora italiana)** del giorno **21 agosto 2023**.

Non sono ammesse domande di partecipazione pervenute con modalità diverse, salvo espressa autorizzazione da parte della Scuola IMT a fronte di richiesta motivata del candidato/della candidata in relazione a eventuali impedimenti di carattere tecnico.

Si precisa che gli allegati devono essere caricati esclusivamente tramite l'apposito modulo disponibile online. Non sono ammessi documenti pervenuti con modalità diverse da quella descritta, salvo espressa autorizzazione da parte della Scuola IMT a fronte di richiesta motivata del candidato/della candidata in relazione a eventuali impedimenti di carattere tecnico. **Ogni allegato deve essere un unico documento in formato .pdf** e non deve superare la **dimensione massima** di **30 MB**.

La Commissione di Concorso (in seguito anche "Commissione") prende in considerazione ai fini della valutazione solo i documenti prodotti in lingua **italiana e/o inglese** (salvo laddove diversamente specificato nelle tabelle seguenti).

Informazioni		
Dati personali	Obbligatorio	In questa sezione i candidati/le candidate devono inserire i propri dati personali (nome, indirizzo, contatti, ecc.).
Livello di conoscenza della lingua inglese	Obbligatorio	I candidati/le candidate devono dichiarare la conoscenza della lingua inglese selezionando uno dei livelli previsti nella sezione dedicata del modulo d'iscrizione online.
Informazioni aggiuntive/ Preferenza sulla modalità di svolgimento dell'esame	Obbligatorio	I candidati/Le candidate devono indicare la modalità con cui intendono svolgere l'esame (qualora ammessi al termine della preselezione): • presso la sede della Scuola IMT a Lucca, con spese di viaggio a carico del candidato/della candidata; • in videoconferenza o con altra tecnologia che consenta la visualizzazione del candidato/della candidata: in tal caso il documento di riconoscimento utilizzato nella *online application form* deve essere esibito prima dell'inizio della prova al fine di consentire l'identificazione del candidato/della candidata; • telefonicamente presso un'Ambasciata o un Consolato Italiano dove il funzionario competente provvederà all'identificazione del candidato/della candidata.
Informazioni aggiuntive/Eventuali disabilità per le quali sia necessario un ausilio all'esame	Opzionale	I portatori/Le portatrici di handicap che intendano usufruire di un ausilio sono tenuti a richiederlo.

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

Informazioni aggiuntive/Modalità con cui i candidati/le candidate sono venuti a conoscenza di IMT	Obbligatorio	I candidati/Le candidate devono indicare le modalità con cui sono venuti a conoscenza della Scuola IMT.
Titoli di studio	Obbligatorio	I candidati/Le candidate devono attestare i titoli di studio, indicati come requisito per l'ammissione al concorso all'art. 2 del presente bando, di durata complessiva minima di quattro anni in regime di tempo pieno, relativa media degli esami sostenuti ed eventuale votazione finale.
Titoli di studio aggiuntivi	Opzionale	In questa sezione i candidati/le candidate possono specificare qualsiasi altra qualifica considerata rilevante in relazione alla domanda.
Elenco pubblicazioni	Opzionale	I candidati/Le candidate possono indicare propri articoli pubblicati, libri o altro materiale che possa essere considerato rilevante per il Dottorato e le attività di ricerca.

Allegati			
1	**Copia di un documento di riconoscimento**	Obbligatorio	I candidati/Le candidate devono allegare copia di un documento di riconoscimento in corso di validità: - per cittadini italiani e della UE: carta di identità o passaporto - per cittadini non-UE: carta di identità o passaporto (il passaporto è altamente preferibile) Sulla copia devono essere apposti **la data, il luogo e la firma del candidato/della candidata**. In particolare, il documento deve contenere la/e pagina/e con la fotografia, i dati anagrafici, il numero del documento, il luogo e la data di rilascio. Non sarà considerato valido qualsiasi altro documento che non abbia tutte le informazioni predette. Nel caso in cui il documento non sia in lingua **italiana** o **inglese**, ai fini della corretta identificazione del candidato/della candidata, è richiesta una **traduzione** nelle suddette lingue a cura del candidato stesso/della candidata stessa. Nel caso in cui il documento allegato sia poco leggibile, è facoltà della Commissione di Concorso, qualora il candidato/la candidata risulti ammesso/a all'esame, chiederne una nuova produzione.
2	**Curriculum vitae et studiorum**	Obbligatorio	I candidati/Le candidate devono allegare il proprio curriculum vitae et studiorum, redatto in lingua **italiana** o **inglese (quest'ultima è altamente preferibile)**, con indicazione dei titoli di livello universitario posseduti, delle esperienze di lavoro e di ricerca più significative e di eventuali pubblicazioni.

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

3	**Titoli di studio** (indicati come requisito per l'ammissione al concorso)	Obbligatorio	I candidati/Le candidate devono allegare uno dei seguenti documenti in lingua **italiana** o **inglese**: - per i **titoli conseguiti in Italia** e/o in **Francia**, **Belgio**, **Irlanda**, **Danimarca** e **Germania:** una **autocertificazione** attestante il possesso dei titoli di studio di cui all'art. 2 del presente bando, la data e l'Università di conseguimento, l'eventuale votazione finale; - per i **titoli conseguiti in tutti gli altri Paesi UE ed Extra-UE:** una **certificazione** attestante il possesso dei titoli di studio di cui all'art. 2 del presente bando, la data e l'Università di conseguimento e l'eventuale votazione finale.
4	**Academic transcript/Diploma supplement**	Obbligatorio	Per ogni titolo di studio inserito ai fini dell'ammissione al concorso (art. 2), i candidati/le candidate devono allegare uno dei seguenti documenti redatti in lingua **italiana** o **inglese (quest'ultima è altamente preferibile)**: - un certificato, *Academic transcript* o un'autocertificazione contenente **l'elenco degli esami sostenuti e la relativa votazione conseguita**, <u>o, in alternativa,</u> - il *Diploma Supplement*, certificazione rilasciata dall'università contestualmente al titolo di studio e recante tutte le informazioni previste dalla normativa europea (https://ec.europa.eu/education/diploma-supplement_en).
5	**Progetto di ricerca**	Obbligatorio	Ai candidati/Alle candidate è richiesto di esprimere la preferenza per uno o più progetti di ricerca (massimo 4) di cui all'articolo 1 del presente bando. Tale preferenza non ha valore vincolante in sede di assegnazione del progetto ai vincitori/alle vincitrici (si veda l'art. 5).
6	**Research Statement**	Obbligatorio	Al fine di valutare l'attitudine dei candidati/delle candidate alla ricerca, con specifico riferimento all'inserimento nel Programma di Dottorato di interesse nazionale in "Cybersicurezza" della Scuola IMT, si richiede la compilazione di un *research statement* **redatto obbligatoriamente in lingua inglese, di lunghezza massima pari a 10.000 caratteri, spazi inclusi**, in cui siano descritte: – le competenze ed esperienze acquisite in metodi e ambiti di studio rilevanti per il/i progetto/i prescelto/i e come si ritiene che possano essere impiegate per affrontarlo/i; – le motivazioni relative alla domanda di ammissione alla Scuola IMT ed in particolare rispetto al progetto scelto/ai progetti scelti; – progetti futuri.

Nel caso in cui la domanda risulti mancante di una informazione o di un allegato definiti come "obbligatori", le Commissioni possono decidere di ammettere il candidato/la candidata alla valutazione con riserva e la domanda sarà considerata valida solo ove lo stesso/la stessa produca i documenti richiesti entro il giorno previsto per l'esame.

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

Le informazioni e gli allegati definiti come "opzionali" sono comunque ritenuti utili al fine di consentire alle Commissioni una più approfondita valutazione dei candidati/delle candidate.

La **corretta conclusione** della procedura è **confermata dall'invio automatico di un messaggio di posta elettronica** all'indirizzo email indicato nella domanda dal candidato/dalla candidata; il suddetto messaggio di conferma certifica esclusivamente l'avvenuta ricezione della domanda e la data della stessa. La Scuola IMT non è tenuta ad effettuare alcuna verifica di validità e completezza delle domande nel periodo antecedente la scadenza del termine per la presentazione delle stesse.

Una volta chiusa la domanda di ammissione al concorso non sarà possibile modificare i dati inseriti nel sistema.

I candidati/le candidate devono altresì accedere alla **seconda sezione della domanda online** dedicata ai referee:

Referee	Obbligatorio	I candidati/Le candidate devono **indicare i nominativi e i dati di contatto di due *referee***. I *referee* riceveranno una notifica automatica via email e potranno far pervenire le **lettere di referenza in lingua inglese entro il giorno 28 agosto 2023 alle ore 13:00 (ora italiana)** esclusivamente attraverso la piattaforma online. I candidati/Le candidate riceveranno una notifica automatica via email per ciascuna lettera pervenuta, ma non potranno accedere alle referenze fornite.

La Scuola IMT non assume alcuna responsabilità per la dispersione di comunicazioni dipendente da inesatta indicazione del recapito o dell'indirizzo di posta elettronica da parte dei candidati/delle candidate o da mancata o tardiva comunicazione del cambiamento degli stessi, né per eventuali disguidi informatici o comunque imputabili a fatto di terzi, a caso fortuito o forza maggiore.

ARTICOLO 4 - COMMISSIONE DI CONCORSO

La Commissione di Concorso è nominata dal Rettore della Scuola IMT con proprio Decreto ed è composta da esperti nelle aree di riferimento dei progetti in cui si articola il Programma, anche appartenenti ad altre istituzioni e alle aziende partner, secondo quanto previsto dal Regolamento del Dottorato di interesse nazionale in "Cybersicurezza" e dal Regolamento del Dottorato di Ricerca della Scuola IMT.

ARTICOLO 5 - CRITERI DI VALUTAZIONE E PROCEDURA DI SELEZIONE

Criteri di valutazione

Prima di procedere alla valutazione dei titoli, la Commissione definisce i criteri riferiti ai titoli e più in generale all'intera procedura di valutazione. In ogni caso la Commissione valuta i seguenti elementi:

- percorso di studi, conoscenze, competenze e valore scientifico del candidato/della candidata;
- attitudine del candidato/della candidata alla ricerca e possibilità di inserimento nelle attività di ricerca specifiche del progetto selezionato/dei progetti selezionati nella domanda;
- grado di interdisciplinarietà del profilo, conoscenze e competenze del candidato/della candidata in relazione alla multidisciplinarietà del Programma di Dottorato e al progetto prescelto/ai progetti prescelti.

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

Preselezione

L'esame di concorso è preceduto da una preselezione per titoli. La valutazione dei titoli è effettuata in relazione alle specifiche del Programma di Dottorato e dei progetti in cui si articola ai soli fini dell'ammissione all'esame.

In fase di preselezione, la valutazione del candidato/della candidata è effettuata dalla Commissione, di cui all'art. 4 del presente bando, sulla base delle dichiarazioni rese nella domanda, dei documenti allegati alla stessa (secondo le modalità di cui al precedente articolo 3) e delle lettere di referenza pervenute.

Sulla base della valutazione dei titoli, la Commissione individua i candidati/le candidate da ammettere alla fase successiva (esame) mediante la stesura di una *shortlist*, senza graduatoria di merito.

L'elenco degli ammessi all'esame sarà pubblicato sul sito web e all'Albo On Line della Scuola IMT. Tale comunicazione ha valore di notifica a tutti gli effetti. Non vengono effettuate comunicazioni personali ai singoli candidati/alle singole candidate.

Esame

I candidati ammessi/Le candidate ammesse all'esame dovranno confermare la loro partecipazione inviando una email all'indirizzo phdapplications@imtlucca.it entro 2 giorni dalla pubblicazione della lista degli ammessi all'esame. Essi/e dovranno altresì confermare la preferenza, già indicata in sede di domanda di ammissione alla partecipazione al concorso, circa la modalità di svolgimento dell'esame (come definito all'articolo 3 del presente bando).

L'esame consiste in un colloquio in lingua inglese, volto ad approfondire la valutazione delle conoscenze e delle competenze del candidato/della candidata in relazione alle specifiche del progetto/dei progetti per cui è stata presentata la candidatura.

La Commissione avrà a disposizione 100 punti per la valutazione dell'esame e il punteggio minimo per il superamento dell'esame è fissato in 70/100.

Ogni informazione sulla procedura e il calendario di svolgimento dell'esame saranno pubblicati sul sito web e all'Albo on line della Scuola IMT. Tale pubblicazione ha valore di notifica a tutti gli effetti. Non verranno effettuate comunicazioni personali ai singoli candidati/alle singole candidate.

Graduatoria finale

Al termine dell'esame, per i candidati risultati idonei/le candidate risultate idonee, la Commissione procede alla stesura di una graduatoria di merito per ciascun progetto in base alla votazione riportata all'esame. La preferenza espressa dal candidato/dalla candidata in fase di domanda non è vincolante per la Commissione, la quale può assegnare il candidato/la candidata alla graduatoria del progetto a bando che sia ritenuto maggiormente corrispondente al profilo.

A parità di punteggio, la preferenza è determinata dalla minore età del candidato/della candidata.

In caso di rinuncia, si scorrerà la graduatoria fino alla copertura delle posizioni previste (come indicato all'art. 1 del presente bando).

La graduatoria, approvata con provvedimento del Rettore, è immediatamente efficace e pubblicata sul sito web nonché all'Albo on line della Scuola IMT. Dell'avvenuta pubblicazione è dato avviso sulla Gazzetta Ufficiale.

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

ARTICOLO 6 - IMMATRICOLAZIONE DEI CANDIDATI AMMESSI/DELLE CANDIDATE AMMESSE

La domanda di immatricolazione, il cui modello sarà trasmesso via e-mail ai candidati ammessi/alle candidate ammesse, deve pervenire alla Scuola **entro il termine di 5 giorni** decorrente **dalla data di pubblicazione della graduatoria finale di merito**.

La domanda è considerata valida solo se corredata di tutta la documentazione richiesta dagli uffici competenti.

La domanda deve essere consegnata secondo una delle seguenti modalità: a mano presso la Scuola IMT, spedita tramite servizio postale (in tal caso farà fede la data del timbro postale) o tramite servizio di posta elettronica certificata ai recapiti sottoelencati:

- Scuola IMT Alti Studi Lucca
  Ufficio Dottorato e Alta Formazione
  Piazza S. Ponziano 6,
  55100 Lucca – Italy
- Posta elettronica certificata: imtlucca@postecert.it

La mancata consegna della domanda con le modalità ed entro i termini sopradetti si intende quale rinuncia alla partecipazione al Programma di Dottorato e implica la perdita del diritto all'immatricolazione e lo scorrimento della graduatoria secondo quanto previsto dal Regolamento del Dottorato di Ricerca della Scuola IMT Alti Studi Lucca e dal presente bando.

Nel caso in cui uno o più documenti allegati alla domanda di ammissione non corrispondano a quelli inviati in fase di immatricolazione rivelando dichiarazione falsa e mendace, il candidato/la candidata perderà automaticamente il diritto all'immatricolazione.

L'immatricolazione avviene di norma il giorno di inizio dei corsi, salvo eventuali casi particolari gestiti dall'Amministrazione, previa autorizzazione del Rettore, ferma restando la necessaria acquisizione del titolo di studio. Assenze ingiustificate il giorno di inizio dei corsi possono annullare la procedura di immatricolazione.

ARTICOLO 7 - INCOMPATIBILITÀ

Coloro che risultano già iscritti a un corso di Dottorato di Ricerca possono accedere al Programma di Dottorato della Scuola IMT a seguito del superamento del relativo concorso, purché rinuncino al corso frequentato e inizino dal primo anno del Programma per cui sono stati ammessi.

ARTICOLO 8 - BORSE DI DOTTORATO

L'importo annuale della borsa di dottorato è di euro 16.243,00, al lordo degli oneri previdenziali a carico dell'allievo/a previsti dalla normativa vigente.

La borsa di dottorato è corrisposta in rate mensili, ad eccezione di quanto previsto dall'art. 15 del Regolamento del Dottorato di Ricerca della Scuola IMT Alti Studi Lucca.

Per il soggiorno fuori sede all'estero per attività di formazione e/o ricerca, l'importo della borsa è incrementato del 50% fino ad un massimo di 12 mesi.

Alle borse di dottorato per la frequenza dei Programmi di Dottorato di Ricerca si applicano le disposizioni in materia di agevolazioni fiscali di cui all'art. 4 della Legge del 13 agosto 1984, n. 476.

La borsa di dottorato del dottorato di ricerca è soggetta al versamento dei contributi previdenziali INPS (Gestione Separata), ai sensi dell'articolo 2, comma 26, della Legge 8 agosto 1995, n. 335 e successive modificazioni, nella misura di due terzi a carico dell'Amministrazione e di un terzo a carico del beneficiario.

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

Chi abbia già usufruito di una borsa di dottorato per un corso di Dottorato di Ricerca in Italia non può beneficiarne nuovamente in caso di iscrizione ad un nuovo corso di Dottorato.

Le borse di dottorato non sono cumulabili con assegni di ricerca o altre borse, a qualsiasi titolo conferite, tranne che con quelle concesse da istituzioni nazionali o straniere utili ad integrare, con soggiorni all'estero, l'attività di ricerca dell'allievo/a.

La borsa di dottorato ha durata di tre anni ed è soggetta a conferma annuale, previa verifica, secondo quanto stabilito dagli artt. 15 e 16 del Regolamento del Dottorato di Ricerca della Scuola IMT. Eventuali estensioni della durata del percorso di studio non implicano l'ampliamento del periodo di fruizione della borsa di dottorato.

L'erogazione della borsa è sospesa nei casi previsti dal Regolamento del Dottorato di Ricerca della Scuola IMT.

Gli allievi/Le allieve con borsa di dottorato che rinunciano o sono esclusi dal Programma entro i primi 45 giorni dall'inizio dello stesso o dall'immatricolazione, non maturano il diritto alla fruizione della borsa. In tale caso, si procede con lo scorrimento della graduatoria, scorrimento da chiudersi entro la scadenza fissata annualmente dal Ministero dell'Università e della Ricerca per il monitoraggio dei dottorati accreditati e la registrazione dei dati degli allievi immatricolati/delle allieve immatricolate nell'anno accademico di riferimento.

In caso di rinuncia alla sola borsa di dottorato, il Collegio Docenti può deliberare l'assegnazione della borsa al primo/alla prima dei candidati idonei/delle candidate idonee, ove ve ne siano.

Il diritto alla borsa di dottorato, per gli/le aventi diritto immatricolati/e oltre 45 giorni dopo l'inizio del Programma, matura dal giorno dell'immatricolazione e si conclude allo scadere del periodo di svolgimento del Programma (durata di tre anni).

ARTICOLO 9 - TRATTAMENTO DEI DATI PERSONALI

Il trattamento dei dati personali è effettuato dalla Scuola IMT Alti Studi Lucca in attuazione e nel rispetto del Regolamento UE 2016/679 General Data Protection Regulation (di seguito anche "GDPR"), con particolare riferimento a quanto previsto dall'art. 5, e del D. Lgs. 196/03 ("Codice in materia di protezione dei dati personali) e ss.mm.ii..

Il Titolare del trattamento dei dati è la Scuola IMT Alti Studi Lucca, in persona del Rettore, Professor Rocco De Nicola, sede legale Piazza San Ponziano, 6 - 55100 – Lucca. I dati di contatto del Titolare del trattamento dei dati personali sono: imtlucca@postecert.it.

Il Responsabile della protezione dei dati (DPO) della Scuola IMT è il Dott. Giulio Bolzonetti. I dati di contatto del DPO sono i seguenti: e-mail dpo@imtlucca.it; indirizzo PEC imtlucca@postecert.it.

La Scuola IMT si impegna, come Titolare del trattamento dei dati personali forniti dal candidato/dalla candidata, a trattare tali dati unicamente per permettere l'espletamento delle procedure di selezioni, ai sensi di quanto previsto dall'art. 6, comma 1, lett. e) del GDPR.

Il conferimento dei dati è necessario per il conseguimento delle finalità sopra indicate. In assenza di tali dati il candidato/la candidata non sarà ammesso/a alla selezione.

Ai dati personali oggetto del trattamento potranno accedere esclusivamente soggetti autorizzati debitamente istruiti, anche con riguardo al rispetto delle misure di sicurezza e agli obblighi di riservatezza.

I dati personali potranno essere comunicati a soggetti terzi (pubblici e/o privati) nell'ambito dei rapporti istituzionali, per l'adempimento di obblighi di legge, di regolamento o di contratto.

I dati personali saranno conservati negli archivi informatici e/o cartacei della Scuola IMT per il tempo necessario al conseguimento delle finalità per le quali sono trattati e conformemente ai tempi di conservazione previsti dalla normativa vigente.

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

Si precisa che i dati sono trattati con o senza l'ausilio di strumenti elettronici, specifiche misure di sicurezza sono osservate per prevenire la perdita dei dati, usi illeciti o non corretti ed accessi non autorizzati.

L'interessato/a ha il diritto di accedere ai propri dati personali e ottenere le informazioni rilevanti sul trattamento, ai sensi dell'art. 15 del GDPR.

L'interessato/a ha diritto di esercitare i diritti di cui alla sezione 2, 3 e 4 del Capo III del Regolamento UE 2016/679, ove applicabile.

L'interessato/a ha inoltre il diritto di proporre reclamo al Garante per la Protezione dei Dati se ritiene che il trattamento che lo riguarda violi il Regolamento UE 2016/679, ai sensi e nelle modalità dell'art. 77 di detto Regolamento o di adire le opportune sedi giudiziarie (art. 79).

La partecipazione alla selezione implica la pubblicazione dei nominativi dei candidati/delle candidate e dei dati relativi all'esito della stessa sul sito web e all'Albo on Line della Scuola IMT.

ARTICOLO 10- RESPONSABILE DEL PROCEDIMENTO

A tutti gli effetti del bando, è individuata quale responsabile del procedimento la Dott.ssa Serena Argentieri, presso l'Ufficio Dottorato e Alta Formazione, sito in Piazza S. Ponziano, 6 - 55100 Lucca (tel. 0583-4326530 – indirizzo di posta elettronica: phdapplications@imtlucca.it).

Per maggiori informazioni relative al presente bando e alla procedura di selezione, è possibile contattare l'Ufficio Dottorato e Alta Formazione sia per posta elettronica, scrivendo all'indirizzo phdapplications@imtlucca.it, sia per telefono, al numero +39 0583 4326530.

Ulteriori informazioni sul Programma di Dottorato e, in generale, sulla Scuola IMT sono disponibili sul sito web www.imtlucca.it.

ARTICOLO 11 - RINVIO AD ALTRE NORME E NORME FINALI

Per tutto quanto non previsto dal presente bando si fa riferimento alle disposizioni vigenti, al Regolamento del Dottorato di Ricerca di interesse nazionale in "Cybersicurezza", al Regolamento del Dottorato di Ricerca della Scuola IMT Alti Studi Lucca e a quant'altro compatibile con la disciplina di settore.

L'attivazione del Programma è subordinata alla verifica dei requisiti richiesti per l'accreditamento secondo le modalità definite dagli organismi competenti, ai sensi del DM 226/2021.

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

NATIONAL PHD PROGRAM IN "CYBERSECURITY" - RESEARCH PROJECTS

1. Keeping Systems, Data, and Your Identity Secure

Curriculum: Software, System, and Infrastructure Security

University: Università della Calabria

Funds: DM MUR 118/2023

Additional benefits: University canteen

Website: https://angelo.furfaro.dimes.unical.it, https://people.dimes.unical.it/andreapugliese

Contact persons: Angelo Furfaro, Andrea Pugliese

Description
The project aims at studying various problems related to different aspects of cybersecurity,
with the aim of (i) identifying methodological and technological approaches and solutions to the issues that currently present the greatest interest, also through the study of real cases proposed by public and private actors and stakeholders) and (ii) defining and developing more secure and reliable processes and infrastructures. The main topics of the project include (i) methods, techniques and tools for the protection of systems, infrastructure and data and (ii) methods, techniques and tools for digital identity and accountability. The student will study and identify, in the above areas, appropriate solutions for the benefit of individual citizens, public institutions and other complex organizations. The student will also develop knowledge and skills that will allow him/her a wide range of professional possibilities, in the public sector (including the National Cybersecurity Agency), research laboratories, centers of study and expertise, private
sectors, and other complex organizations, including through collaboration with inter- and multi-disciplinary teams in cybersecurity - in general, in those settings that require professionals with solid scientific, methodological, and technological skills in cybersecurity.

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

2. Cross-Layer Design of Secure Systems

Curriculum: Software, System, and Infrastructure Security

University: Alma Mater Studiorum - Università di Bologna

Funds: DM MUR 118/2023

Additional benefits: -

Website: https://disi.unibo.it/en/research/research-areas/computer-security-biometric-systems-and-legal-issues

Contact person: Marco Prandini

Description
The research project will investigate the interplay between the different layers and methodologies involved in the design of secure systems. Security is an intrinsically interdisciplinary field, and the proposed challenge is to take into account aspects that are traditionally independent such as hardware design (e.g. trusted cores, reference monitors), software architectures (e.g. novel virtualization approaches), networking models (e.g. interplay between network programmability and security), formal methods (e.g. analysis, automatic generation of code from provably secure design descriptions), and the human element (e.g. sensitivity to attack vectors).

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

3. Machine Learning for Threat Detection

Curriculum: Software, System, and Infrastructure Security

University: Università di Palermo

Funds: DM MUR 118/2023Università di Palermo

Additional benefits: -

Website: https://www.unipa.it/persone/docenti/d/alessandra.depaola

Contact person: Alessandra De Paola

Description
In many cybersecurity contexts, it is crucial to timely recognize ongoing events by analyzing information provided by different sensing nodes. Intrusion detection and malware recognition, for instance, are two common scenarios in which heterogeneous data/features are evaluated together to extract the peculiarities of different attacks. Most approaches exploit supervised classifiers to identify known attacks; however, these are not effective in the case of new threats, i.e., zero-day attacks, where unforeseen patterns may occur. The research activity aims to address this challenge by proposing new solutions that conjugate anomaly detection algorithms with the most recent artificial intelligence methods in order to identify potential cybersecurity breaches at an early stage. To this aim, the candidate should exploit a combination of various techniques, such as statistical analysis, unsupervised learning, classification algorithms and other artificial intelligence methods, to overcome the limitations of single approaches. The research activity should address several challenges, such as the need to perform detection of anomalies and potential threats in real time, also minimizing resource consumption, especially in those scenarios where resource-limited devices are used.

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

4. Usable and Secure Authentication Mechanisms

Curriculum: Software, System, and Infrastructure Security

University: Università Ca' Foscari, Venezia

Funds: DM MUR 118/2023

Additional benefits: Access to extensive research funds for participation to conferences and schools.

Website: https://www.unive.it/data/people/5590985

Contact person: Flaminia Luccio

Description
Authentication is preliminary to access control and authorization since it allows for identifying users and programs into a system. Authentication is often based on multi-factor approaches, such as passwords, OTPs and biometrics, and typically tend to reduce usability. It is thus important to explore trade-offs between usability and security in order to make users accept the proposed mechanism and prevent abuses such as the selection of weak passwords, the sharing of OTP devices, etc. The PhD student will analyze existing authentication solutions and classify them based on their security, usability and compliance to existing regulations. Then, the student will investigate innovative solutions that balance usability and security with respect to various threat models and regulatory/administrative domains, also considering real case studies.

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

5. Formal Analysis of Trusted Execution Environments

Curriculum: Foundational Aspects of Cybersecurity

University: Università Ca' Foscari, Venezia

Funds: DM MUR 118/2023

Additional benefits: Access to extensive research funds for participation to conferences and schools.

Website: https://www.unive.it/data/people/5590470

Contact person: Riccardo Focardi

Description
Hardware and software systems drive the digital transformation. They are a pervasive aspect of our daily lives and we rely upon them for a growing number of critical tasks. The ever-growing complexity of these system raises concerns about their security. This project aims at rigorously studying which are the security guarantees that some of these emerging systems provide to their users. The PhD student will use the techniques and methodologies provided by the field of language-based security to study the design and implementation of trusted execution environments (TEEs) in different contexts. The student will investigate innovative solutions to formally prove the security of a system based on the properties of the underlying TEEs. These solutions might be implemented directly in hardware or as IDE/compiler plugins helping the programmer to develop secure-by-design software.

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

6. Towards Effective Strategies for Monitoring, Analyzing, and Mitigating Information Disorder

Curriculum: Foundational Aspects in Cybersecurity

University: Istituto di Informatica e Telematica -CNR di Pisa

Funds: Istituto di Informatica e Telematica

Additional benefits: -

Website: https://cyb.iit.cnr.it/

Contact person: Maurizio Tesconi

Description
This project focuses on the development of techniques for monitoring, analysing and mitigating Information Disorder. Information disorder refers to the dissemination of false or misleading information that can cause confusion, harm or even social and political destabilization. The project aims to identify and develop effective methods to detect and address two specific problems: coordinated behavior and the use of manipulated content such as DeepFake. Coordinated Behaviour refers to groups of users performing synergic actions in pursuit of a common intent. One objective will be to identify and characterize this type of behavior on social networks by identifying indices to measure it. The use of manipulated content is another major problem of information disorder. The project will focus on identifying and developing effective methods to detect and mitigate the use of DeepFake content. To achieve these objectives, the project will use a combination of qualitative and quantitative research methods with a multidisciplinary approach, ranging from computer science to social sciences. The expected results of this project are the development of effective techniques and strategies to detect and mitigate the coordinated behavior and use of DeepFake content in online information ecosystems. The results of the project will contribute to the broader effort to combat information disorder and its impact on society and democracy.

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

7. Study of Secure Off-Chain Protocols for Controlling IoT Devices

Curriculum: Software, Systems and Infrastructure Security

University: Università di Camerino

Funds: FFO Ateneo

Additional benefits: -

Website: https://computerscience.unicam.it/

Contact person: Leonardo Mostarda, Michele Loreti

Description
The main goal of this research project is to advance the off-chain protocol state of the art by building a novel approach that can run-on battery-operated sensor and actuator IoT devices. Off-chain solutions are second layer approaches that can be used in the context of Distributed Ledger Technology (DLT) in order to improve scalability. This research project aims at conceiving secure protocols that allow the implementation of a novel off-chain system that is scalable and energy efficient. In particular, this off-chain system must be conceived to be executed on IoT devices that are battery powered, have low computation capabilities (in terms of memory and CPU power) and have limited communication range. These limitations pose the main challenges in order to devise off-chain secure protocols. The goal is to investigate security provable techniques that can guarantee off-chain system security. This will be done by adapting the existing modelling and formal analysis approaches. More precisely, the project aims at developing tools and methodologies that support the specification and verification of security properties. These tools must allow the formalization of security requirements that can be verified at design time and monitored during the system execution. The tools and methodologies developed in the project will be applied to smart city scenarios.

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

8. Cryptographic Tools and Protocols for Quantum-Safe Networks

Curriculum: Foundational Aspects in Cybersecurity

University: Università Politecnica delle Marche

Funds: DM MUR 118/2023

Additional benefits: -

Website: https://www.univpm.it

Contact person: Marco Baldi

Description
The availability of the first quantum computers motivates the need to study, design, analyze, implement, integrate, validate, and test new cryptographic tools and primitives capable of withstanding both attacks performed with classical computers and future quantum computer-based attacks. The hosting research group has already been active for many years in designing and implementing post-quantum cryptographic primitives and participating in their standardization process coordinated by NIST. The research project is aimed at investigating, designing, and validating new approaches for finding new solutions to major open problems in
this research area, such as: devising new efficient and secure post-quantum digital signature schemes, integrating post-quantum cryptographic into existing applications (such as Internet security protocols, space communications, etc.), identify new cryptographic protocols to perform advanced functions and for use in decentralized cryptography-based infrastructures, such as those leveraging blockchain and distributed ledger technology.

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

9. AI-based Botnet Classification and Categorization Through Behavior Analysis

Curriculum: Software, System, and Infrastructure Security

University: IIT-CNR

Funds: Altro

Additional benefits: -

Website: https://ccn.iit.cnr.it/en/

Contact persons: Abraham Gebrehiwot and Filippo Lauria

Description
Botnets represent one of the most serious cybersecurity threats faced by organizations today. While a significant amount of research has been accomplished on botnet analysis and detection, several challenges remain unaddressed, such as the ability to design detectors which can cope with new forms of botnets. The goal of the project is to use artificial intelligence-based techniques to classify and categorize botnets by analyzing the commands executed and the malware used to infect devices. A network infrastructure implementing honeypots will be used to interact with bots and collect useful data. Using artificial intelligence-based behavior analysis of bots attempting to infect new victim devices, the project aims to identify patterns and signatures that can be used to classify and categorize botnets. The ultimate goal of the project is to use this information to prevent future botnet attacks.

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

10. Cybersecurity of RISC-V-based Cyber-Physical Systems in Embedded Scenarios

Curriculum: Software, System, and Infrastructure Security

University: Politecnico di Torino

Funds: DM MUR 118/2023

Additional benefits: -

Website: -

Contact person: Alessandro Savino

Description
Embedded computing systems (ECS) at the base of several application domains (CPS, IoT, transportation, autonomous driving, etc.) must be designed with security in mind from their design phase in a measurable manner. Security must be considered at all layers of an ECS design, including:

- Embedded hardware vulnerabilities
- Memory Access Protection (MMU & MPU)
- Secure Debugging (HSM and Host)
- Runtime Manipulation Detection
- Secure Feature Activation (Switch Over)

In particular, the hardware is the root of trust of a full ECS; with jeopardized hardware, the whole system is at stake. Thus, it is imperative to enhance the control and trust of hardware across the supply chain and during its operation, and this is the global objective of this Ph.D. project.
This Ph.D. project aims to investigate new RISC-V-based CPU-centric architectures protected against the significant hardware security threats observed across different computing domains: from low-end embedded to High-Performance Computing (HPC) systems. Such an investigation should also exploit security features from external accelerators, either implemented with standard CMOS or with emerging technologies.
The research aims to create an all-encompassing analysis framework and implementation strategy to ensure security in the hardware supply chain and system operation. This involves integrating dedicated monitoring and countermeasure hardware and software to mitigate the effects of attacks that can compromise information or disrupt services.
Solutions will be considered at all stages of the system design process, including simulation, architectural design, and Register Transfer Level (RTL) design, working mainly on open hardware architectures such as RISC-V.

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

11. Detection and Characterization of Fake Media Content

Curriculum: Data Governance and protection

University: University of Siena

Funds: ex DM 118 co-funded with research funds available at the Department

Additional benefits:

Website: -

Contact person: Mauro Barni

Description
The diffusion of fake media and the ease with which end-users can create fake media is raising increasing concern, due to the impact that the diffusion of fake media can have on our society. It is essential that public entities develop tools to detect fake media, monitor their diffusion on social media and within our society, and investigate the reason behind the creation and diffusion of fake media.

In the last years, multimedia forensic researchers have developed several tools to distinguish genuine media from fake ones and to identify several forms of media manipulations. Yet, detecting fake media and media manipulations is not enough to combat the use of manipulated media for disinformation campaigns; it is necessary that the malevolent use of the manipulations is identified. At the same time, the integrity of a media asset does not ensure that the use of the asset is a benign one: the inclusion of a pristine image in a wrong context may lead to user disinformation as much as the use of a manipulated image.

The next challenge in media forensics, then, is to characterize media manipulation within the context and discourse wherein the media is used and link the manipulation to the intended goal of the counterfeiter.

The goal of this research is twofold:

1. to build suitable, multimodal, models to study the contextual impact of media manipulations;
2. to develop a pool of automatic techniques working under different modalities (images, videos, text), linking the manipulations of a media asset to the intended meaning of the manipulation.

The expected research is a truly multidisciplinary one, touching both the cognitive and technological aspects of the addressed problem.

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

12. Cryptographic Algorithms and Protocols for Satellite Telecommunication Applications

Curriculum: Software, System, and Infrastructure Security

Institution: Istituto di Calcolo e Reti ad Alte Prestazioni (Cnr-ICAR)

Funds: CNR-ICAR

Additional benefits: -

Website: www.icar.cnr.it

Contact person: Giovanni Schmid

Description
The emergence of quantum computers has triggered the development of new solutions for future secured communications by major security agencies and standardization bodies. This project aims to identify, investigate, and trade off the best candidate quantum cryptography (QC) and post-quantum cryptography (PQC) algorithms and protocols for secure satellite telecommunication missions. The project will focus on the following three main activities:

1. Identification of satellite telecommunication scenarios requiring protection from quantum computers, with the definition of a complete set of functional and security requirements for each scenario;
2. Selection of QC and PQC algorithms and their implementation in networking protocols compliant with the functional and security requirements previously identified;
3. Development of a testbed to evaluate in a laboratory environment the usability and performance of the above protocols within their use cases.

The above-selected algorithms and protocols will comply with open cryptography and satellite communications standards.

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

13. Assessing and Improving Security of AI Code Generators

Curriculum: Foundational Aspects of Cybersecurity

University: Federico II University of Naples

Funds: University

Additional benefits: -

Website: http://www.dessert.unina.it/

Contact person: Domenico Cotroneo

Description
Nowadays, AI code generators are a valuable solution to help programmers and developers automate coding tasks and reduce the time and effort needed to create software applications. Since they are founded on deep neural networks, AI-based code generators are inevitably exposed to adversarial inputs, i.e., inputs with subtle perturbations that can mislead the models. This issue has several implications also in security applications. Poisoning of AI code generators refers to the malicious act of intentionally feeding the generator with malicious code or data with the intent of causing it to generate flawed or vulnerable code. These vulnerabilities can be exploited by attackers to gain unauthorized access to systems, steal sensitive data, or cause other types of damage.
This project will focus on the assessment of the data used to feed the AI code generators to ensure that only high-quality code (i.e., free from biases, errors, or vulnerabilities) can be used as a source of information for the models. To fulfill this goal, the Ph.D. candidate will develop solutions based on ML, or that leverage static and dynamic analysis, to assess the code correctness and vulnerabilities. More specifically, the candidate will adopt these solutions to:

1. assess whether the AI code generators are poisoned, i.e., whether the code generated by the models adheres to best practices and industry standards for security, reliability, maintainability, and other quality metrics; and
2. heal the poisoned models by fine-tuning them on data free from vulnerability, i.e., to let the generator learn from examples of code that have already been tested and verified to meet certain standards.

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

14. Malware Detection for Edge-based Computing and Edge-AI

Curriculum: Software, System, and Infrastructure Security

University: Università degli Studi dell'Insubria (Varese)

Funds: DM MUR 118/2023

Additional benefits: -

Website: -

Contact person: Elena Ferrari

Description
Edge computing allows faster computation and better support for real-time applications than pure cloud-based architectures. However, the rapid increase in the size of edge computing networks and their heterogeneity raise new security issues and challenges. This project aims to address some of the most relevant ones, that is, those related to malware detection, with a focus on the challenging use case of edge-AI. The Ph.D. student will work on the definition of innovative lightweight decentralized solutions for early-stage malware detection at the edge. Learning approaches, such as deep learning, will be investigated, where edge devices are responsible for the learning process without any central observer or coordinator. The challenge is to achieve good accuracy and competitive efficiency even if participating devices lack a global view of the network to feed their learning process.

One of the reference scenarios of the Ph.D. research activity is the challenging Edge-AI use case. Edge-AI services can run under different architectures (e.g., federated learning, decentralized, federated learning, or hybrid solutions), characterized by various advantages and drawbacks, and different security threats. Part of the Ph.D. activity will be devoted to understanding and analyzing the rapidly evolving threat class represented by malware for edge-AI under the most challenging attack scenarios and learning architectures. Detection techniques will be designed, able to cope with different kinds of poisoning attacks, either performed individually or collaboratively (i.e., Sybil attacks).

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

15. Assessing Risks and Mitigating Harm in AI Systems: Towards the Development of a Trustworthy and Secure AI

Curriculum: Software, System, and Infrastructure Security

University: University of Bari

Funds: DM MUR 118/2023

Additional benefits: -

Website: https://serlab.di.uniba.it/people/danilo-caivano/

Contact person: Danilo Caivano

Description
The proliferation of intelligent systems in our society has revolutionized various fields. At the same time, the widespread adoption of such systems has led to a corresponding increase in risks associated with cybersecurity.

Intelligent systems must be built with reference to "trust by design" and "security by design" principles to ensure that they are trustworthy and generate results that do not cause harm or unnecessary risk. The advent of Generative AI has further enhanced these risks that must be addressed to ensure that these systems are designed with the appropriate safeguards from cyberattacks.

Cybersecurity and trustworthiness are interlinked as the principles of trustworthiness complement and sometimes overlap the ones of AI cybersecurity.

Trustworthiness features such as robustness, accuracy, traceability, explainability, data quality, and fairness inherently complement cybersecurity.

The objective of this Ph.D. project is to investigate such issues and propose novel solutions for a Trustworthy and Secure AI, identify potential risks and vulnerabilities of AI models and algorithms, and provide actions for remediation. Proposed solutions and approaches should help organizations develop and validate their intelligent systems and ensure they meet the necessary standards for safety, security, robustness, and privacy protection while also promoting transparency, accountability, and ethical behavior. Finally, intelligent systems should be validated to make them compatible with current regulations.

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

16. Protection of Data in Use via Trusted Execution Environment (Tee) Technology

Curriculum: Software, System, and Infrastructure Security

University: University of Naples "Parthenope"

Funds: Research funds of the FITNESS research group.

Additional benefits: Additional research contract within the context of the active project(s), to be negotiated on an individual basis.

Websites: http://www.fitnesslab.eu/, https://certify-project.eu/, https://encrypt-project.eu/, https://cyberseas.eu/, https://incisive-project.eu/

Contact person: Luigi Romano

Description
Even the most secure algorithm is vulnerable, if the computing environment where it is executed is not adequately protected (ENISA Annual Report on Cybersecurity Research and Innovation Needs and Priorities). Effective protection is needed not only when data is "in transfer" (e.g. exchanged over a network connection) or "at rest" (e.g. stored on a disk) but also when it is "in use" (e.g. loaded in the RAM or in the CPU). While the protection of data in transfer and at rest is relatively easy to achieve, protection of data in use is still - to a large extent - an open issue. The main challenge is that data must be protected even from attacks by privileged users (e.g. system administrators or cloud providers) and software (e.g. the OS or the hypervisor). The availability of effective mechanisms for the protection of data in use is a key enabler of a number of application domains, such as Industrial Control Systems, Smart Grids, eHealth, and more. Also importantly, it is the prerequisite for the real take-up of cloud computing. Some of the big players in the cloud market already offer solutions (e.g. Microsoft ACC) which provide protection of data in use via TEE. The PhD program will focus on techniques for the protection of data in use via TEE, and apply them to challenging use cases in realistic setups, within the context of research projects funded by the European Commission, including CERTIFY, ENCRYPT, CyberSEAS, and INCISIVE.

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

17. Software and Infrastructure Security: Analysis and Verification of Properties

Curriculum: Software, System, and Infrastructure Security

University: University of Pisa

Funds: DM MUR 118/2023

Additional benefits: -

Websites: https://di.unipi.it/

Contact person: Gian-Luigi Ferrari

Description
The overall aim of the PhD project is concerned with defining methodologies and tools to govern the design, development, and maintenance of secure ICT infrastructures. The project involves the design of innovative solutions to govern both the management process and the development of secure ICT infrastructure, through the use of a variety of techniques ranging from static analysis to dynamic analysis, from probabilistic to symbolic methods, to the adoption of digital twin and distributed ledger with the goal of detecting possible malicious activities, preventing or limiting their impact, according to a self-defence and autonomic paradigm. The PhD project aims to significantly extend the power and scalability of currently available techniques to make them applicable to real-world infrastructure in several application fields.

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

18. Unsupervised and Continuous Learning for Intrusion Detection Systems

Curriculum: Software, System and Infrastructure Security

University: University of Udine

Funds: University

Additional benefits: -

Website: -

Contact persons: Gian Luca Foresti, Marino Miculan

Description
Nowadays, Intrusion Detection Systems represent a fundamental research subject in the field of cyber security. To overcome the problem of recognizing new types of attacks, increasingly frequent in recent years, it is important to design and develop new unsupervised machine learning models capable of detecting anomalies in computer networks. Among other issues, a problem is that most attacks to computer networks are rare events, with respect to the whole (legit) traffic; moreover, attackers constantly change the pattern of their actions, in order to hide from IDSs. The PhD research activities will be focalized on new unsupervised approaches with continuous learning capabilities for anomaly detection; in particular, the proposed study should consider recent neural network architectures such as SF-SOINN for efficient continuous learning. The proposed systems must be tested on important benchmark datasets (e.g., NSL-KDD, etc.) in order to demonstrate its ability in detecting new attacks, learning them and imtevolving its knowledge to increase system robustness to multiple attacks.

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

19. Methods and Tools for the Security Assessment of Critical Information Infrastructures

Curriculum: Software, System and Infrastructure Security

University: IMT School for Advanced Studies Lucca

Funds: DM MUR 118/2023

Additional benefits: Students are offered free on-campus housing and free meals at the IMT canteen for three years

Website: https://sysma.imtlucca.it/

Contact persons: Letterio Galletta

Description
Information and communications technologies (ICT) form a vital part of our society, providing essential goods and services. Critical information infrastructures (CIIs) are ICT platforms that enable other critical infrastructures whose disruption may affect the safety of citizens. Security engineering for CIIs is a multidisciplinary field involving various topics, from secure software development and cryptography to embedded systems and network security. Formal modelling and verification techniques have the potential to provide strong security guarantees and support vulnerability detection. However, developing effective formal methods-based tools for CIIs is still open. This project aims to provide new methodologies and tools for the security assessment of CIIs that could support Macro-regional CSIRT in their activities. The research could focus on different aspects, such as network security, protocol security, and application security, and can consider different verification techniques.

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

20. Tools and Techniques for Scalable and Usable Cyber Ranges

Curriculum: Software, System and Infrastructure Security

University: IMT School for Advanced Studies Lucca

Funds: DM MUR 118/2023

Additional benefits: Students are offered free on-campus housing and free meals at the IMT canteen for three years

Website: https://sysma.imtlucca.it/

Contact persons: Gabriele Costa

Description
Cyber ranges are highly sophisticated infrastructures that serve as battlegrounds for cybersecurity activities including, e.g., training, testing, and incident simulation. Although modern virtualization and simulation technologies provide the building blocks for cyber ranges, scalability, re-usability, and affordability are still open issues. As a matter of fact, the access to cyber ranges is today limited and the benefit for the society at large is only marginal.
The goal of this project is to investigate state-of-the-art technologies and methodologies for making cyber ranges accessible to a wider class of users. The candidate will have access to cyber range technologies currently available and will have to investigate innovative approaches to improve their usability and scalability. These approaches include (but are not limited to): infrastructure design languages, orchestration, vulnerability testing, red team automation, exploitability, gamification techniques, attack strategies generation and execution.

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

21. Machine Learning Models for the Analysis and Detection of Stealth Threats and Latent Vulnerabilities

Curriculum: Foundational Aspects in Cybersecurity

University: University of Cagliari

Funds: DM MUR 118/2023

Additional benefits: -

Website: www.unica.it, www.pralab.diee.unica.it

Contact person: Giorgio Giacinto

Description
The trend in the development of cyber threats is characterised by the exploitation of latent vulnerabilities and by the stealthiness of the techniques used to attack systems and sensors, designed to evade sensing and detection tools. This research project is aimed at devising effective machine learning models based on the recent advances in other fields such as image and natural language understanding. The goal is to spot even small signals of suspicious activities while keeping the rate of false alarms small. Recent advances in deep learning models, as well as the use of ensemble methods, will be leveraged to build a novel framework. In particular, a huge effort will be spent in investigating different models to represent either source code or binaries that can reveal potential vulnerabilities or malicious actions. To this end, recent advances in machine learning models for language modelling and multimedia processing will be analysed and tailored to the computing environment.

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

22. Harnessing Societal Infrastructures. Formally

Curriculum: Foundational Aspects of Cybersecurity

University: Gran Sasso Science Institute

Funds: DM MUR 118/2023

Additional benefits: -

Website: https://cs.gssi.it

Contact person: Emilio Tuosto

Description
Modern societies rely on infrastructures that are more and more connected through digital networks. This creates complex cyber-physical ecosystems that are vulnerable to many different types of attacks. A source of weakness is that this integration possibly involves systems that were originally designed to operate in (closed) trustworthy settings. In fact, some systems may not provide strong security guarantees (or satisfy only basic security requirements) because they are conceived to operate in non-hostile environments. Therefore, their integration with other systems, nowadays hardly negotiable, could easily introduce security breaches if done naively. This could possibly compromise sub-systems, including those designed to guarantee strong security requirements. This project aims to develop formal approaches to harness existing systems with security guarantees. The main idea is to analyse existing systems and identify weaknesses that could expose them to attacks. The project considers a case study involving a platform developed at Actyx (https://developer.actyx.com/) to support the coordination of factory production. The platform has been designed and implemented assuming a non-adversarial context. A crucial part of the project is to develop approaches to enforce security in systems that rely on the Actyx platform, whose formal modelling and analysis have been initiated in a recent publication.

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

23. Methodologies and Techniques for Countering and Mitigating the Impact of GenAI and LLM on Information Disorder

Curriculum: Software, System, and Infrastructure Security

University: Università degli Studi di Salerno

Funds: DM MUR 118/2023 - M4C1-PNRR

Additional benefits: -

Website: https://www.unisa.it/

Contact person: Vincenzo Loia

Description
Generative Artificial Intelligence (GenAI) is a branch of Artificial Intelligence aimed at creating complex data, such as images, videos, audio, text, etc., from scratch, mimicking human creativity. The capabilities of emulating human language and interaction skills of Open AI ChatGPT and Bing Sydney are particularly impressive examples. The Large Language Models (LLMs) are revolutionizing the writing approach of journalists, writers, and researchers. However, LLMs are affected by two different issues: (1) biased data adopted for the training task can lead to demographic stereotypes and imprecise information; (2) the generated results can arbitrarily be true or not. As a consequence, the risk of spreading imprecise or false information is high with unchecked generated text. Moreover, presented weaknesses can be easily adopted in disinformation campaigns or political propaganda by, for example, fake persona creation, AI-generated imagery, deep fake for discrediting adversaries, etc.
This project aims to find methodologies able to identify and monitor disinformation phenomena nourished by LLMs. The objective is to let users use and exploit advantages associated with the employment of such innovative technologies, and work for their optimization in order to study solutions that could mitigate the negative effects of LLMs. Moreover, solutions to unmask voluntary or involuntarily generated disinformation content without censorship will be approached.

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

24. XAI Methodologies and Techniques for Countering Information Disorder

Curriculum: Software, System, and Infrastructure Security

University: Università degli Studi di Salerno

Funds: DM MUR 118/2023 - M4C1-PNRR

Additional benefits: -

Website: https://www.unisa.it/

Contact person: Giuseppe Fenza

Description
Explainable AI (xAI) refers to strategies and procedures employing Artificial Intelligence technology (AI) that allow human experts to gain insight into the AI model outcomes. xAI is a powerful approach for spotting model defects and data biases, contributing to an increase in user trust. The interpretability achieved through xAI models can be exploited for generalization independently from training data issues, such as limited availability of labeled data and lack of domain-specific or multi-language information. In addition, the application of xAI can be a double-edged sword. It substantially improves cybersecurity practices but leaves, at the same time, the system vulnerable to adversary attacks. In this regard, xAI can be adopted to study the vulnerabilities of a system and, consequently, guide its strength or protection. Insights from cybersecurity can be studied to approach threats of the infodemic era, where disinformation attempts can undermine the role of institutions, national security, and democracy itself.
This project aims at studying xAI methodologies that support the definition of more powerful, robust, and generalizable models (in terms of propaganda, fake news, hate speech detection, etc.). The objective is to identify information disorder counterfeiting solutions where models
must be capable of dealing with ever-new challenges due to continuous technological evolution.

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

25. Automating Risk Assessment of Infrastructure with AI/ML Components

Curriculum: Software, System, and Infrastructure Security

University: Universita' degli studi di Trento

Funds: DM 118/2023 - M4C1- Inv. 3.4

Additional benefits: The students will be trained in the industrial methodologies used by the industry partners and spend 6 months at Vrije Universiteit Amsterdam

Website: https://securitylab.disi.unitn.it

Contact persons: Fabio Massacci, Marco Rocchetto

Description
Several methodologies exist for cybersecurity risk assessment of IT/OT infrastructures (such as ISO 27001, ISO 27002, ISO 27005, NIST SP 800-53, CIS Control v8). However, they are hardly automated and even less account for the presence of artificial intelligence or machine learning components. To date, risk analysis is done by exploiting the experience of technical personnel and is based on beliefs and opinions rather than scientific theories. The result is that risk analysis, which should be a central activity of IT/OT infrastructures management, is found on the margins of corporate GRC (Governance, Risk, Compliance), being almost always evaluated as not very informative. The purpose of the research is the definition of an automatic or semi-automatic process for risk assessment (which includes the identification of threats with a relative estimate of impact and probability). The project will be in cooperation with an innovative start-up company (https://www.v-research.it/) that will support the student in the concrete case studies and the activities for the technological transfer of the results of the project.

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

26. Countering fake contents and malicious activities

Curriculum: Software, System and Infrastructure Security

University: Università degli Studi di Catania

Funds: DM MUR 118/2023

Additional benefits:

Website: https://web.dmi.unict.it/it/content/dottorato-informatica

Contact persons: Giampaolo Bella, Sebastiano Battiato

Description
Common media such as digital images, audio and video clips could be fake, namely generated by computer programs to resemble genuine ones, with the aim of offering altered contents to unaware users. At an extreme, such contents and the services delivering them could become fully malicious, so as to actively engage with other computer programs as well as with the users to craft cunning attack vectors. Even whole devices could be malicious, including modern Voice Personal Assistants and, more in general, widespread IoT devices – and the role itself of the user could be exploited, for example by mounting a self-issue attack on a voice channel.

The overarching goal of this research is to liberate the IoT from fake contents as well as from malicious activity. The technical objectives are: to promote a precise understanding of the scope and aims of fake contents and malicious activity in the IoT; to devise scalable approaches to thwart fake contents and malicious activity at all architectural layers of the IoT; to define algorithms to detect fake media and deep fakes in the context of the IoT; to implement such algorithms as viable and practical tools that are applicable to real-world scenarios; to tailor the novel algorithms and tools to the particular problem of user privacy preservation so as to make them fully compliant with the General Data Protection Regulation.

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

27. Explainable and robust AI solutions for malware detection and analysis

Curriculum: Software, system and infrastructure security

University: CNR

Funds: CNR

Additional benefits: -

Contact person: Fabio Martinelli

Description
Design and implementation of techniques for detecting intrusions on mobile devices and IoT, through the use of federated machine learning techniques. Particular importance will be given to the explainability of the proposed models, in order to integrate the techniques developed in a real context, where they can be of support to the malware analyst. Solutions will also be designed for assessing the risk of being attacked by malware, also providing ad-hoc best practices to protect mobile/IoT devices from cyberattacks.

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

28. Security policy management for digital sovereignty

Curriculum: Data governance and protection

University: CNR

Funds: CNR

Additional benefits: -

Contact person: Fabio Martinelli

Description
The project focuses on the management of policies for digital sovereignty starting from regulations and laws till producing machine understandable, enforceable and verifiable policies. This entails the adoption of methodologies for automated policy generation from natural language, also including large language models. Such security policies will be used for data usage control and data sovereignty solutions that are main instruments of digital sovereignty. The policy management framework could be also adopted in several contexts from compliance to standards to fine grained and continuous control of data and systems in accordance to regulations, usage control policies and privacy preferences. Policy models may include
obligation management frameworks.

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

29. Preventing, investigating and fighting cybercrimes: substantial and procedural issues

Curriculum: Human, Economic, and Legal Aspects in Cybersecurity

University: Sant'Anna School of Advanced Studies - Pisa

Funds: DIRPOLIS INSTITUTE and prof. Gaetana Morgante

Additional benefits: Additional research contract within the context of the active project(s), to be negotiated on an individual basis.

Websites: https://www.santannapisa.it/en/istituto/dirpolis-institute

Contact person: Gaetana Morgante

Description
Investigating, preventing and fighting cybercrimes is challenging the traditional categories of criminal law and procedure. The building of an efficient legal framework at a domestic, European and international level needs a strong multidisciplinary approach to the juridical, ethical, economical, political, social and human profiles of cybersecurity. The PhD program will concern the different forms of cybervictimization (individual and collective, public and private up to the CyberWar) and take into account the studies on Digital Criminology. The different models of prevention and repression of cybercrimes will also be studied in the light of the international obligations and cooperation (so-called Cyber-Diplomacy). The PhD program will also cover the procedural issues of Cybersecurity from the analysis of the multileveled legal framework up to the collection of the best investigative practices to balance cybersecurity and protection of the fundamental rights in cyberspace (so-called Digital forensics), and the questions related to the jurisdiction on crimes committed in the cyber- and transnational dimension.

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

30. Advanced solutions for data security and privacy in emerging scenarios

Curriculum: Data Governance and Protection

University: Università degli Studi di Milano

Funds: DM MUR 118/2023

Additional benefits: -

Websites: https://samarati.di.unimi.it/

Contact person: Pierangela Samarati

Description
Data are the central resource for any modern society. Also, the availability of highly performing systems and services (e.g., cloud/fog/edge/IoT) for gathering, storing, and processing data, as well as of efficient machine learning and AI-based solutions operating on large data collections, brings great benefits on a personal, business, economic and social level. On the other hand, data may be sensitive or company-confidential and cannot be shared openly, and their confidentiality, as well as their integrity, should be guaranteed even when non fully trusted parties are involved in data storage or processing. The goal of the project is to contribute to the development of advanced scientific and technological solutions enabling the different actors (e.g., individuals, companies, institutions) with control over their data in the various data release, sharing, and analysis scenarios. The research is in the area of computer science and can entail investigation of different scientific and technological issues contributing to solving the problem of protecting data in emerging scenarios. Technological aspects that can be investigated include: data modeling for enforcing security and privacy restrictions; access control languages and models; data protection in release, storage, or computation by untrusted parties; data integrity; data security and privacy in artificial intelligence scenarios; and AI-based security and privacy solutions.

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

31. Methodologies and Methods for Quantitative Risk Assessment with reference to European and Domestic Regulations and Frameworks

Curriculum: Software, system and infrastructure security

University: CINI Cybersecurity National Lab

Funds: DM 117/2023

Additional benefits: -

Websites: https://cybersecnatlab.it/

Contact person: Paolo Prinetto

Description
A few years after the first European cybersecurity directive came into operation, a new directive (NIS 2) was published in January 2023, effectively replacing the first one. NIS 2 was the result of a major improvement process of the previous directive, with the goal of strengthening the security measures required and necessary for the protection of critical infrastructure. In fact, new application areas were added, in addition to those previously identified as critical, and the risk management measures to be taken by operators and providers of essential services were better detailed.
In the Italian context the "*Framework Nazionale per la Cybersecurity e la Data Protection*", which outlines guidelines for the proper and effective cybersecurity management of systems. Accompanying this document is also the identification of a set of "*essential controls*", that is, minimum security measures that are easily implemented that refer to the guidelines expressed within the Italian Cybersecurity Framework.
In both contexts, it becomes crucial to be able to provide tools that can enable a rigorous, objective, and quantitative approach to the assessment process that can be applicable not only by large organizations but also by small and medium-sized enterprises.

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

32. Implementation of acoustic jammers for privacy protection - technical, ethical, and legal issues

Curriculum: Software, system and infrastructure security

University: CINI Cybersecurity National Lab

Funds: DM 117/2023

Additional benefits: -

Websites: https://cybersecnatlab.it/

Contact person: Paolo Prinetto

Description
Microphones are commonly installed in many devices, not just phones but also IoT and wearable devices. Most microphones are today based on MEMS sensors.

Several cases have been reported in which microphones are used to violate privacy in order to fraudulently record private conversations.

Many papers have been published about attack techniques that resort to ultrasonic waves to prevent these attacks by creating a DoS on a microphone (i.e., the microphone cannot record any sound at all or the sound is extremely distorted and not intelligible).

In addition, other attack techniques exploit ultrasonic waves to activate voice commands on smart devices (e.g., SIRI, Google, Alexa): these commands cannot be heard by humans but can still be picked up by common microphones.

During the proposed thesis, we want to deeply analyze DoS attacks against microphones, from both red-teaming and blue-teaming perspectives, in different thread scenarios. In addition, we need to deeply investigate how different sound frequencies might affect electronic devices (i.e., disturbing them and creating unwanted DoS) and people (i.e., possible Impacts on health and safety).

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

33. Evaluation of Resilient and Secure Cyber-Physical and Distributed Systems

Curriculum: Software, System, and Infrastructure Security

University: Università degli Studi di Firenze

Funds: DM MUR 118/2023

Additional benefits: -

Website: http://rcl.dimai.unifi.it/, https://www.unifi.it/p-doc2-0-0-A-3f2b342f372e2b.html

Contact person: Andrea Ceccarelli

Description

As systems are becoming massively distributed, interconnected, and evolutionary, the complexity of threats and attack paths is increasing. Models for the security and dependability assessment must take into consideration the multiplicity of components, which often share similarities, but at the same time exhibit variations due to different configurations or roles. Further, due to dynamicity and evolution, changes to configurations are introduced over time, and system models need to be updated to reflect such changes.

The proposed research focuses on selected aspects of the design and especially the evaluation of resilient and secure cyber-physical systems, with a particular preference for the security of critical infrastructures and systems of systems. The research shall investigate qualitative and/or quantitative methods for the identification, analysis, classification, and mitigation of threats and hazards, for example aiming to analyze and rank the most probable attack paths, identify the most critical components to be protected, or compare different architectural solutions with different defensive mechanisms.

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

34. Cybersecurity of Complex Systems

Curriculum: Software, System, and Infrastructure Security

University: University of Genova

Funds: Serics - D.D. n. 341 del 15 marzo 2022

Additional benefits: -

Website: https://www.csec.it/

Contact person: Alessandro Armando, Luca Verderame

Description

This research project focuses on the study of automated or semi-automated methodologies to assess the cyber risk exposure of complex application ecosystems. The candidate will explore emerging scenarios such as Mobile, Cloud, Fog, IoT (Internet of Things), and combinations thereof. Furthermore, all the solutions developed in the project will be evaluated in real-world industrial scenarios.
In detail, the project will be included in one of the following lines of research:
- the design of effective methods for analyzing and quantifying potential cyber risks exposure of complex application environments and the associated supply chain, with specific attention to CI/CD scenarios and the DevSecOps paradigms;
- the identification of proper digital twin technologies to create multi-domain scenarios for testing cyber risk resilience, identifying vulnerabilities, evaluating countermeasures against potential cyber-attacks, and assessing the effectiveness of existing procedures.

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

35. Towards a Regulatory Sandbox on Cybersecurity

Curriculum: Human, Economic, and Legal Aspects in Cybersecurity

University: University of Florence

Funds: DM 118/2023

Additional benefits: -

Website: -

Contact person: Andrea Simoncini

Description

The project aims to develop a new 'regulatory sandbox' for cybersecurity using a forward-looking approach to regulation, allowing minimal barriers by creating a controlled regulatory testing environment. The 'regulatory sandbox' is a way to connect innovators and regulators, providing a controlled environment for them to cooperate. It facilitates the development, testing and validation of innovative digital tools to ensure compliance with the requirements of existing regulations. The PhD candidate will focus her/his project on studying regulatory sandboxes as a way to co-regulate technological tools and participate in implementing a real regulatory sandbox on cybersecurity in Italy. For these purposes, the candidate will be asked to develop strong state of the art on regulatory sandboxes in Europe and be able to analyse and study relevant European use cases that serve as best practices in operational terms. Activities should also include analysis of legal issues, regulatory compliance and rules on technology. The research activities will be conducted within the Department of Legal Studies of the University of Florence.

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

36. New generation malware detection through artificial intelligence

Curriculum: Software, System, and Infrastructure Security

University: University of Sannio

Funds: DM 118/2023

Additional benefits: -

Website: -

Contact person: Aaron Visaggio

Description

The research aims to develop novel techniques for the detection of new-generation malware that leverage artificial intelligence techniques.

Decreto del Rettore n. 8516(214).V.2.30.05.23
Rep. albo on line n. 8517(199).I.7.30.05.23
Ufficio Dottorato e Alta Formazione
Responsabile Serena Argentieri
Autore Serena Argentieri
Classificazione I.7

37. Securing digital identities, authentication and communication in a distributed context

University: Università degli Studi Mediterranea di Reggio Calabria

Funds: DM MUR 118/2023

Website: https://www.diies.unirc.it/scheda_persona.php?id=576

Contact persons: Francesco Buccafurri

Description:

The project focuses on the context of cybersecurity and aims to secure services provided to citizens and organizations. In this scenario, securing communication and protecting digital identity deserve in-depth study. This requires (1) designing distributed solutions not to rely on trusted third parties, (2) guaranteeing that the service applicant is really who claims to be, (3) allowing an entity to communicate anonymously when admitted, (4) allowing disclosing the minimum personal data when required, and (5) providing accountability even if a service is accessed anonymously. The first requirement implicates the adoption of Distributed Ledger Technologies, requirements 2 and 3 involve network security, whereas the last two aspects address the data protection requirements imposed by the GDPR. The student will develop knowledge and skills useful for a wide range of
professional possibilities. Furthermore, the student will acquire professionals with solid scientific, methodological, and technological skills in cybersecurity.