Principali informazioni sull'insegnamento	
Denominazione dell'insegnamento	**Sicurezza in Ambienti Mobile**
Corso di studio	Sicurezza Informatica
Anno Accademico	2024/25
Crediti formativi universitari (CFU) / European Credit Transfer and Accumulation System (ECTS)	6 CFU
Settore Scientifico Disciplinare	INF/01
Lingua di erogazione	Italiano
Anno di corso	Secondo
Periodo di erogazione	1^ semestre, le date esatte sono riportate nel manifesto/regolamento
Obbligo di frequenza	No, ma la frequenza è fortemente raccomandata
Sito web del corso di studio	https://www.uniba.it/it/corsi/cdl-sicurezza-informatica-taranto/corso-di-laurea-in-sicurezza-informatica-sede-di-taranto

Docente/i	
Nome e cognome	Paolo Buono
Indirizzo mail	paolo.buono@uniba.it
Telefono	080 544 2239
Sede	Dipartimento di Informatica, Via Orabona 4, 70125, Bari. Stanza n. 571, 5° piano.
Sede virtuale	Piattaforma e-learning UNIBA - https://elearning.uniba.it/
Sito web del docente	https://ivu.di.uniba.it/people/buono.html
Ricevimento (giorni, orari e modalità, es. su appuntamento)	Mercoledì 13:00-15:00 presso la stanza docenti, al primo piano della sede di Taranto

Docente/i	
Nome e cognome	Giuseppe Desolda
Indirizzo mail	giuseppe.desolda@uniba.it
Telefono	080 544 3289
Sede	Dipartimento di Informatica, Via Orabona 4, 70125, Bari. Stanza n. 573, 5° piano.

Sede virtuale	Piattaforma e-learning UNIBA - https://elearning.uniba.it/
Sito web del docente	https://ivu.di.uniba.it/people/desolda.html
Ricevimento (giorni, orari e modalità, es. su appuntamento)	Mercoledì, 14.00-15.00 in presenza presso la sede di Taranto. Telematicamente previo appuntamento da richiedere via mail.

Syllabus	
Obiettivi formativi	Obiettivo di questo corso è essere in grado di effettuare un'analisi della sicurezza delle app installate in uno smartphone, con specifico riferimento all'architettura Android. Il corso si inserisce e integra gli insegnamenti della sicurezza nelle applicazioni e della sicurezza nelle reti e nei sistemi distribuiti focalizzandosi sulle applicazioni per dispositivi mobili.
Prerequisiti	Prerequisiti preferenziali: - architettura Android - sviluppo su app Android - sistemi crittografici - protocolli di rete
Contenuti di insegnamento (Programma)	Fondamenti sulla sicurezza in ambienti mobile. (4h). Ecosistema e modello di sicurezza di Android. (4h). Architettura Android, Dalvik e ART, ambiente di sviluppo Android (4h). Manifest, Activity, Fragment e ciclo di vita di app. Permessi. (4h). Package Android, utenti. Memorizzazione delle credenziali e persistenza. Sicurezza del dispositivo. SELinux. Rooting. Supporto multiutente, OTA. (4h) OWASP mobile: V1-V8. (4h) Usable Security (8h). Sistemi host. Linux Tamer, Genymotion. Analisi statica e dinamica del codice. Penetration testing. Protocollo OWASP. (15h)
Testi di riferimento	Riferimento principale del corso è costituito dai due libri disponibili sul sito OWASP: Mobile Application Security Verification Standard (MASVS) e Mobile Application Security Testing Guide (MASTG), che sono curati dalla OWASP foundation, che si pone come missione la promozione del software sicuro. In aggiunta ci sono le slide del docente relative allo sviluppo su Android. Testi di approfondimento per l'architettura Android sono: - Nikolay Elenkov, Android. Guida alla sicurezza per hacker e sviluppatori, Apogeo. 2015 - J. J. Drake, P. O. Fora, Z. Lanier et al. Android Hacker's Handbook, Wiley. 2014 Gli studenti che lo desiderano possono ottenere i testi in prestito dalla Biblioteca. Può convenire verificarne la disponibilità mediante il Sistema Bibliotecario di Ateneo

	https://opac.uniba.it/easyweb/w8018/index.php? e contattare la biblioteca per concordare il prestito.
Note ai testi di riferimento	Data la natura altamente tecnologica dei contenuti del corso i testi per approfondimento sono datati, la loro consultazione serve solo per ampliare la conoscenza anche all'evoluzione storica dei sistemi in esame. Per qualsiasi dubbio consultare il docente.

Organizzazione della didattica

Ore

Totali	Didattica frontale	Esercitazioni	Studio individuale
150 ore	32 ore	15 ore	103 ore

CFU/ETCS

6 CFU	4 CFU	1 CFU	

Metodi didattici

L'erogazione della didattica avviene prevalentemente tramite lezioni frontali.
Sono previste sessioni di esercitazioni da svolgere in aula relative all'indagine della sicurezza di applicazioni mobile.
Le attività sono prevalentemente individuali, così come lo studio a casa relativa alla parte di progetto. Non si escludono attività in piccoli gruppi durante il periodo di lezione.
Nelle ore di esercitazione è prevista la presentazione di casi di studio presentati precedentemente e loro discussione in aula.
Eventuali nuovi elaborati realizzati in aula saranno inseriti in piattaforma di e-learning per memoria storica e per agevolare i non frequentanti.

Risultati di apprendimento previsti

Conoscenza e capacità di comprensione	Gli studenti acquisiscono competenze relative ai principi fondamentali della sicurezza in ambienti mobile, dei paradigmi fondativi di questa disciplina, delle sue evoluzioni, nonché delle applicazioni delle tecniche e modalità per realizzare ambienti mobile dotati di un buon grado di sicurezza.
Conoscenza e capacità di comprensione applicate	Gli studenti acquisiscono competenze per lo sviluppo e la realizzazione di tecniche per la verifica del livello di sicurezza degli ambienti mobile. Esercitazioni guidate ed individuali contribuiscono all'applicazione di quanto studiato in teoria.
Competenze trasversali	**Autonomia di giudizio** Gli studenti acquisiscono una significativa autonomia di giudizio e di gestione delle problematiche relative alle tecniche di attacco e di difesa rispetto ai sistemi operativi

	mobile e alle app ivi residenti. Discussioni di gruppo incentivano l'argomentazione del proprio giudizio nell'ambito di un gruppo di lavoro. **Abilità comunicative** Gli studenti acquisiscono abilità di illustrare in modo appropriato le caratteristiche di tecniche, strumenti e metodologie proprie dell'ambito della sicurezza in ambienti mobile. Sono previste presentazioni dello stato di avanzamento dello studio, da fare con l'ausilio di slide e ambienti di sviluppo di app. **Capacità di apprendere in modo autonomo** Gli studenti sviluppano capacità di apprendere e di orientarsi agilmente nelle problematiche della progettazione di app sicure. A fine lezione si assegnano esercizi da svolgere a casa e da consegnare entro la lezione successiva, al fine di rafforzare l'autovalutazione dell'apprendimento di quanto presentato e discusso.

Valutazione	
Modalità di verifica dell'apprendimento	L'esame si espleta in una sola prova orale. Gli studenti presentano un caso di studio relativo alla valutazione della sicurezza di una app e presentano una relazione scritta che illustra la parte di teoria necessaria alla realizzazione dell'analisi di sicurezza e la documentazione relativa. Durante la presentazione sono chieste domande di chiarimento e accertamento delle competenze acquisite degli studenti. In piattaforma e-elearning UNIBA sono riportati esempi di relazioni precedenti, per dare agli studenti un parametro di confronto su cosa e come realizzare per l'esame.
Criteri di valutazione	La verifica dell'apprendimento prevede lo svolgimento di esercitazioni durante il corso al fine di sviluppare strategie di problem solving nell'ambito della sicurezza in ambienti mobile. Saranno valutate le capacità di scelta di adeguatezza delle tecniche per la sicurezza rispetto al problema specifico.
Criteri di misurazione dell'apprendimento e di attribuzione del voto finale	La valutazione finale è in trentesimi ed è effettuata durante la prova d'esame. L'esito è comunicato seduta stante. Se compatibile con il calendario delle lezioni si terrà conto delle esercitazioni svolte durante le lezioni per attribuire un punteggio aggiuntivo che comunque non può superare i tre punti.
Altro	Si suggerisce agli studenti di affidarsi esclusivamente alle informazioni/comunicazioni fornite sui siti ufficiali del Dipartimento di Informatica, ovvero sui gruppi social solo se costituiti e amministrati esclusivamente dai docenti dei relativi insegnamenti: • https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea • https://www.uniba.it/it/ricerca/dipartimenti/informatica • https://elearning.uniba.it/ Le informazioni che tutti gli studenti dovrebbero conoscere sono scritte nei regolamenti didattici e manifesti degli studi disponibili nel sito: • https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea Si suggerisce agli studenti di diffidare delle informazioni e dei materiali circolanti su siti o gruppi social non ufficiali, poiché spesso sono risultati non affidabili, non corretti o incompleti. Per ogni dubbio, chiedere un incontro al docente secondo le modalità previste per il ricevimento.

	Il link al corso sulla piattaforma e-learning UNIBA è il seguente: https://elearning.uniba.it/course/view.php?id=4957 Eventuali link a forum di collaborazione saranno concordati con gli studenti all'inizio del corso e riportati nella piattaforma di e-learning UNIBA. La registrazione in piattaforma è libera previa approvazione da parte del docente.

Main information on the course		
Course name	**Sicurezza in Ambienti Mobile (Mobile Security)**	
Degree	Sicurezza Informatica (Computer Science Security)	
Academic year	2024/25	
European Credit Transfer and Accumulation System (ECTS), in Italian Crediti Formativi Universitari (CFU)		6 CFU (each CFU corresponds to 25 hours (h) of student's time); CFU are of type T1, T2 or T3 T1 = 8 h lecture + 17 h individual study T2 = 15 h practice + 10 h individual study T3 = 25 h individual study
Settore Scientifico Disciplinare		
Course language	Italian	
Course year	Second	
Course period	First Semester - exact dates can be found in the didactic regulations	
Course attendance requirement	None, but it is highly recommended to attend classes	
Website of the Degree	https://www.uniba.it/it/corsi/cdl-sicurezza-informatica-taranto/corso-di-laurea-in-sicurezza-informatica-sede-di-taranto	

Teacher(s)	
Name and Surname	Paolo Buono
email	paolo.buono@uniba.it
phone	080 544 2239
office	Dipartimento di Informatica, Via Orabona 4, 70125, Bari. Room 571, 5th floor
e-learning platform	Piattaforma e-learning UNIBA - https://elearning.uniba.it/
Teacher's homepage	https://ivu.di.uniba.it/people/buono.html
Office hours	Wednesday 13:00-15:00. Lecturer room 1st floor, Taranto venue.

Teacher(s)	
Name and Surname	Giuseppe Desolda
email	giuseppe.desolda@uniba.it
phone	080 544 3289
office	Dipartimento di Informatica, Via Orabona 4, 70125, Bari. Room n. 573, 5th floor.
e-learning platform	Piattaforma e-learning UNIBA - https://elearning.uniba.it/
Teacher's homepage	https://ivu.di.uniba.it/people/desolda.html
Office hours	Wednesday 13:00-15:00. Lecturer room 1st floor, Taranto venue.

Syllabus	
Course goals	The objective of this course is to be able to perform a security analysis of apps installed in a smartphone, with specific reference to the Android architecture. The course fits in and integrates the arguments of application security and security in networks and distributed systems and focuses on mobile applications.
Prerequisites/requirements	Preferred prerequisites: - Android architecture - development on Android apps

	- cryptographic systems - network protocols
Course program	Fundamentals of security in mobile environments. (4h). Android ecosystem and security model. (4h). Android architecture, Dalvik and ART, Android development environment (4h). Manifest, Activity, Fragment and app lifecycle. Permissions. (4h). Android packages, users. Credential storage and persistence. Device security. SELinux. Rooting. Multiuser support, OTA. (4h) OWASP mobile: V1-V8. (4h) Usable Security (8h). Host systems. Linux Tamer, Genymotion. Static and dynamic code analysis. Penetration testing. OWASP protocol. (15h)
Books of reference	The main reference of the course are the two books available on the OWASP website: Mobile Application Security Verification Standard (MASVS) and Mobile Application Security Testing Guide (MASTG), which are edited by the OWASP foundation, whose mission is to promote secure software. In addition, there are the lecturer's slides related to development on Android and to the usable security. In order to deeper the knowledge, texts for Android architecture are also available: - Nikolay Elenkov, Android. A security guide for hackers and developers, Apogeo. 2015 - J. J. Drake, P. O. Fora, Z. Lanier et al. Android Hacker's Handbook, Wiley. 2014 Students who wish to do so can obtain the texts on loan from the University library. It may be convenient to check their availability through the University Library System https://opac.uniba.it/easyweb/w8018/index.php? and contact the library to arrange borrowing.
Notes to the books	Due to the highly technological nature of the course content, the texts for in-depth study are dated; their reference is only to broaden knowledge to include the historical evolution of the systems under study. Please ask the lecturer for any doubts.

Organization of the didactic activities

Hours			
Total	Lectures	Practice sessions	Individual study
150 hours	32 hours	15 hours	103 hours
CFU/ETCS			
6 CFU	4 CFU	1 CFU	

Teaching methods

	Teaching delivery is mainly through face-to-face lectures. Exercise sessions are planned to be conducted in the classroom related to the investigation of mobile application security. The activities are mainly individual, as well as home study related to the project part. Small group activities are not excluded during the class period. During the practice sessions, the presentation of previously presented case studies and their discussion in the classroom is planned. Any new papers produced in the classroom will be posted on the e-learning platform for historical memory and to facilitate students that cannot attend the lectures.

Expected learning outcomes	
Knowledge and understanding	Students acquire skills related to the fundamentals of security in mobile environments, the foundational paradigms of this discipline, its evolutions, and the applications of techniques and ways to realize mobile environments with a good degree of security.
Applying knowledge and understanding	Students gain skills in developing and implementing techniques for testing the security level of mobile environments. Guided and individual exercises contribute to the application of what is studied in theory.
Other skills	*Making judgements* Students gain significant autonomy in judgment and management of issues related to attack and defense techniques with respect to mobile operating systems and the apps residing therein. Group discussions encourage the argumentation of one's own judgment within a working group. *Communication* Students acquire skills to appropriately illustrate the characteristics of techniques, tools and methodologies specific to the field of security in mobile environments. Presentations of the progress of the study are planned to be made using slides and app development environments. *Learning skills* Students develop skills to learn and nimbly navigate the issues of secure app design. At the end of class, exercises are assigned to be done at home and turned in by the next class in order to reinforce self-assessment of learning of what was presented and discussed.

Assessment	
Assessment methods	The assessment is conducted in a single oral test. Students present a case study related to the security evaluation of an app and submit a written report outlining the part of theory required to carry out the security analysis and related documentation. Questions are asked to the students during the presentation to clarify and ascertain their acquired skills.

	Examples of previous reports are provided in the UNIBA e-elearning platform to give students a parameter for comparison on what and how to accomplish for the exam.
Evaluation criteria	The learning assessment will involve conducting exercises during the course in order to develop problem solving strategies in the area of security in mobile environments. The ability to choose appropriateness of techniques for security with respect to the specific problem will be assessed.
Measurements and final grade	The final evaluation is in thirtieths and is made during the examination. The outcome is announced on the spot. If compatible with the lecture schedule, the exercises carried out during the lectures will be taken into account to award an additional mark, which, however, may not exceed three points.
Further information	It is suggested that students rely exclusively on the information/communication provided on the official websites of the Department of Computer Science, or on social groups only if they are established and administered exclusively by the faculty members of the relevant subjects: ● https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea ● https://www.uniba.it/it/ricerca/dipartimenti/informatica ● https://elearning.uniba.it/ Information that all students should be aware of is written in the teaching regulations and study manifestos available on the website: - https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea Students are suggested to be wary of information and materials circulating on unofficial sites or social groups, as they are often found to be unreliable, incorrect or incomplete. If you have any doubts, ask for a meeting with the lecturer in accordance with the reception arrangements. The link to the course on the e-learning UNIBA platform is as follows: https://elearning.uniba.it/course/view.php?id=4957 Any links to collaborative forums will be agreed with students at the beginning of the course and reported in the UNIBA e-learning platform. Registration on the platform is free upon approval by the lecturer.