

Allegato A

Progetto:

**Metodologie e strumenti innovativi a supporto dei
test di sicurezza software di sistemi e componenti
ordinari ed embedded di interesse per le attività
del CVCN**

Indice

| | |
|---|--------------------|
| 1. Amministrazione proponente | 2 |
| 2. Denominazione del progetto | 2 |
| 3. Contesto di inquadramento | 3 |
| 4. Descrizione dell'obiettivo generale del progetto | 4 |
| 5. Descrizione degli obiettivi specifici | 55 4 |
| 6. Formazione | 5 |
| 7. Durata temporale del progetto | 66 5 |
| 8. Area geografica di localizzazione dell'intervento | 6 |
| 9. Descrizione delle attività per il conseguimento dei risultati attesi | 6 |
| 10. Impegno delle risorse | 8 |
| 11. Piano di finanziamento del progetto | 12 |
| 11.1 Risorse per strumentazione | 12 |
| 11.2 Risorse per il personale | 1313 12 |
| 11.3 Risorse totali | 13 |
| 12. Riferimenti bibliografici | 13 |

1. Amministrazione proponente

Il proponente del presente progetto è il Ministero per lo Sviluppo Economico (MISE) / Direzione Generale per le Tecnologie delle Comunicazioni e per la Sicurezza Informatica - Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione.

2. Denominazione del progetto

Il progetto, denominato " Metodologie e strumenti innovativi a supporto dei test di sicurezza software di sistemi e componenti ordinari ed embedded di interesse per le attività del CVCN ", è incentrato sul supporto alle attività del Centro di Valutazione e Certificazione Nazionale (CVCN) focalizzandosi sullo sviluppo di nuovi strumenti e metodologie per l'esecuzione di test software anche per sistemi embedded.

3. Contesto di inquadramento

Le disposizioni del DL 105/2019 convertito nella legge 133/2019 richiedono che il CVCN possa condurre con un **termine di 60 giorni** test su apparati software e hardware, con criteri di **gradualità** legati al rischio e al settore di attività. Questo scenario operativo si presta all'utilizzo di un ventaglio di tecniche, in modo combinato e incrementale in base alla profondità e complessità dell'accertamento. Il presente progetto si focalizza sul test del software per sistemi e componenti ordinari ed embedded. Questi ultimi sono di particolare interesse per il CVCN considerato il loro sempre più diffuso impiego e la carenza di strumenti di analisi maturi che ne consentano i test di sicurezza.

L'utilizzo di tecniche di estrazione automatica di informazioni statiche da firmware permette di identificare alcune **vulnerabilità note** osservate in altri firmware anche di natura diversa, permettendo una caratterizzazione iniziale, seppur non approfondita, in termini rapidi [sec14]. La verifica dell'operatività e delle funzionalità di un firmware comporta invece la necessità di analizzare dinamicamente l'esecuzione, facendo ricorso a tecniche di emulazione whole-system [asiaccs16, ndss14]. In funzione della disponibilità dell'apparato hardware su cui il firmware opera, si può procedere a intercettare le interazioni con l'hardware durante l'emulazione per riprodurle sul dispositivo stesso [ndss14], o viceversa definire dei componenti software in grado di simulare le interazioni con l'hardware [acsac16].

Quando si rende necessario effettuare test corrispondenti al grado di affidabilità elevato descritto nel Regolamento (UE) 2019/881, ovvero nei confronti di complessi attacchi cyber perpetrati da persone che dispongono di abilità e risorse significative, proponiamo di integrare innanzitutto le verifiche descritte in precedenza con due metodologie di program analysis ben note nella comunità scientifica di sicurezza informatica. La prima riguarda l'esecuzione simbolica del codice [ndss15, csur18], una tecnica che permette di esplorare possibili esecuzioni alternative di una porzione di un software, alla ricerca di vulnerabilità da sfruttare o comportamenti non previsti. La seconda riguarda il fuzzing [sec19, ndss19], ad oggi la tecnica più efficace che un attaccante può impiegare per individuare errori nel software, e successivamente analizzarli manualmente per valutare se e come possono essere sfruttati per un attacco. Inoltre, potranno essere esplorate tecniche introspettive (e.g., debugger@sw/JTAG@hw) per poter osservare gli effetti sul sistema tramite tecniche white-box. Il lavoro di analisi del software embedded necessario alla definizione di metodologie e strumenti innovativi per l'esecuzione di test di sicurezza potrà a sua volta ispirare nuove tecniche di analisi, avanzando lo stato dell'arte.

La complessità delle tecniche elencate e la difficoltà di guidare il processo di analisi ad esse associato portano a individuare come scenario di possibili soluzioni l'integrazione di queste proposte in soluzioni di Visual Analytics [ieee05, gosl10]. L'utilizzo congiunto di visualizzazioni e tecniche automatiche di calcolo è, difatti, sempre più utilizzato nel contesto della cybersecurity, come dimostrato dalla crescita di conferenze internazionali di settore quali IEEE VizSec (Visualization for

Cyber Security)¹, giunta alla sua sedicesima edizione in concomitanza con l'evento mondiale più significativo sulla visualizzazione, IEEE VIS. Esempi di soluzioni di Visual Analytics proposte in tale contesto e pertinenti alle finalità di questo documento sono relative alla ricerca di minacce presenti nel bytecode Java [vizsec16], a metodi per il controllo di soluzioni per la ricerca di vulnerabilità basate sull'esecuzione simbolica del codice [vizsec19] o alla visualizzazione delle vulnerabilità presenti all'interno del codice [vizsec16a].

Qualora le attività del CVCN siano relative a una rete di dispositivi appare significativo prevedere l'utilizzo di tecniche di Visual Analytics basate sull'analisi delle vulnerabilità presenti sui vari elementi della rete per individuare i possibili cammini di attacco multi-step (attack graph) e valutarne il loro impatto rispetto al rischio che inducono sui servizi e dispositivi target della rete [cdcn18, jvlc2019], anche allo scopo di individuare delle priorità di intervento sulle vulnerabilità secondo differenti funzioni obiettivo [tvcg18]

4. Descrizione dell'obiettivo generale del progetto

Il progetto si focalizza sullo sviluppo di tecniche e prototipi a supporto del CVCN in modo da consentire test sul software che pilota dispositivi ordinari ed embedded, fornendo indicazioni su eventuali elementi di vulnerabilità che ne possano compromettere la sicurezza. Diversamente dai dispositivi ordinari, per i quali esistono tecniche di test più mature, i **sistemi embedded** sono sistemi di calcolo progettati per svolgere esclusivamente compiti specifici, tipicamente in tempo reale. Esempi di sistemi embedded sono dispositivi medici come pace maker, pompe insuliniche e apparati per la diagnostica per immagini, sistemi di controllo e attuazione per la guida di veicoli e sistemi industriali, apparati di rete come router e switch, modem, controllori e attuatori in ambito domotico, e in generale tutti quei sistemi che si basano su attività programmabili. Il comportamento dei sistemi embedded è governato dal **firmware**, un software che determina il funzionamento del sistema stesso e si occupa dell'interfacciamento con elementi hardware specifici come sensori e attuatori.

La difficoltà principale nell'analisi e nel test di questi dispositivi è l'**alto livello di eterogeneità**, ad esempio nel set di istruzioni del microprocessore e nell'interfaccia con i dispositivi esterni, e la **carenza di standard comuni**. Il progetto dovrà pertanto investigare tecniche per adattare metodologie e strumenti di uso generale per l'esecuzione di test di sicurezza sul software a famiglie specifiche di firmware per sistemi embedded.

I lavori saranno effettuati dal Centro di Ricerca di Cyber Intelligence and Information Security (CIS) di Sapienza Università di Roma (CIS-Sapienza) di concerto e in collaborazione con il MISE.

L'obiettivo generale del progetto sarà la definizione di una collezione di metodologie e strumenti (nella forma di prototipi) per l'esecuzione di test di sicurezza. Tale definizione sarà guidata da almeno tre casi di studio di interesse in ambito CVCN e si avvarrà della esperienza decennale del CIS in

¹ <https://vizsec.org/vizsec2019/#cfp>

materia, integrata dagli studi ed approfondimenti che saranno necessari per applicare metodologie e strumenti anche a sistemi e componenti di tipo embedded.

5. Descrizione degli obiettivi specifici

Attività a breve termine (entro la data in cui dovrà essere operativo il CVCN)

Come obiettivi specifici, il progetto individuerà innanzitutto le tipologie di dispositivi di particolare rilevanza per il CVCN, studiandone le caratteristiche hardware e software e individuando almeno tre casi di studio. Le famiglie così selezionate verranno analizzate alla luce degli strumenti esistenti, verificandone criticamente il grado di applicabilità.

L'analisi si concentrerà anche su tecniche preliminari per il monitoraggio e test non invasivo dei dispositivi nel loro sistema di utilizzo, esplorando possibili strategie per verificarne il corretto funzionamento (ostacoli a tale attività sono la riservatezza dei dati che il dispositivo gestisce, l'accesso al dispositivo per inserire i casi di test, e il mantenimento del livello di operatività del sistema). L'attività sarà inoltre relativa alla sperimentazione per l'adattamento di tecniche e prototipi per la gestione delle vulnerabilità nel contesto attack graph alle specifiche esigenze del CVCN.

Come secondo obiettivo, il progetto si propone di collaborare alla definizione di procedure operative CVCN, basandosi sui casi di studio individuati.

Il terzo obiettivo è la realizzazione da parte di CIS-Sapienza di prototipi per l'esecuzione di test di sicurezza sul software, basati anche sull'utilizzo di piattaforme open-source, coprendo aspetti legati all'analisi statica e dinamica del software e formando gli analisti CVCN sulle soluzioni esistenti e quelle sviluppate ad hoc nell'ambito del progetto.

Attività a lungo termine (nei rimanenti due anni di progetto)

Ottemperati gli obblighi iniziali legati all'operatività del CVCN, il progetto si concentrerà sulla validazione di quanto messo in opera e sull'arricchimento e miglioramento delle tecniche di test e degli strumenti forniti, alla luce delle specificità di nuovi dispositivi, delle attività di ricerca svolta dal personale CIS-Sapienza e dell'analisi di quanto verrà prodotto nei prossimi anni dalla comunità scientifica internazionale.

Per maggiori dettagli sulle attività, la loro realizzazione e la corrispondente tempistica si rimanda al paragrafo 9.

6. Formazione

Attività di formazione del personale MISE sulle soluzioni esistenti e su metodologie e prototipi sviluppati nell'ambito del progetto

7. Durata temporale del progetto

Tre anni

8. Area geografica di localizzazione dell'intervento

Il progetto si sviluppa in ambito nazionale.

9. Descrizione delle attività per il conseguimento dei risultati attesi

Il CIS-Sapienza supporta il CVCN nelle seguenti attività:

| Attività | Descrizione |
|----------|---|
| A | <p>Acquisizione casi di studio:</p> <ul style="list-style-type: none">Il MISE identifica le tipologie di dispositivi di interesse con riferimento alle attività previste per il CVCN, prendendo in considerazione sia sistemi o componenti ICT ordinari di larga diffusione (e.g., router) sia sistemi o componenti ICT particolari utilizzati in specifici contesti applicativi (e.g., antenna 5G, funzionalità di rete realizzate in <i>software</i>, dispositivi nel contesto del controllo e dell'automazione industriale, ecc.). Il MISE e CIS-Sapienza identificano le architetture hardware e software più comunemente utilizzate nelle tipologie di dispositivi di interesse.MISE e CIS-Sapienza individuano almeno tre casi di studio rappresentativi delle tipologie di hardware e software di interesse per il presente progetto. Il MISE otterrà l'oggetto dei casi di studio, definendo con CIS-Sapienza il materiale di supporto (documentale, ambiente di esercizio e test) da richiedere per poter procedere a sperimentazioni congiunte. |
| B | <p>Studio soluzioni di test software per sistemi e componenti anche di tipo embedded presenti in letteratura rispetto ai casi di studio. Sperimentazione sui casi di studio:</p> <ul style="list-style-type: none">CIS-Sapienza realizza uno studio approfondito della letteratura sul test del software anche in ambito embedded, analizzando criticamente le soluzioni liberamente disponibili ("open source"). Ne verifica quindi l'applicabilità al software dei casi di studio individuati nell'attività A. CIS-Sapienza studia e implementa un adattamento alla specificità delle attività del CVCN delle tecniche e dei prototipi sviluppati per la gestione delle vulnerabilità e dei cammini di attacco multi-step (attack graph). |
| C | <p>Supporto stesura metodologie CVCN:</p> <ul style="list-style-type: none">Valutando i riscontri dalle attività A e B, il MISE individua, con il supporto di |

Prof. Camil Demetrescu

Camil Demetrescu (professore ordinario in ingegneria informatica) conduce ricerca all'intersezione di diverse aree che spaziano da sicurezza informatica, linguaggi di programmazione e sistemi, algoritmi e strutture dati e ingegneria del software. I suoi risultati sono apparsi in riviste (fra cui IEEE Transactions on Software Engineering, ACM Transactions on Programming Languages and Systems e Journal of the ACM) e congressi internazionali di primo piano (inclusi PLDI, OOPSLA, STOC, FOCS, SODA, ICALP). Ha svolto attività pionieristica nell'ambito degli algoritmi incrementali e ha partecipato ai comitati di programma di conferenze ammiraglie come PLDI, SODA e OOPSLA. Fa parte del comitato scientifico della Dagstuhl Artifacts Series (DARTS) e dell'editorial board della rivista Mathematical Programming Computation. Ha coordinato inoltre a livello nazionale il programma di selezione di talenti CyberChallenge.IT che ha formato gli atleti della squadra nazionale italiana cyber patrocinata dal Ministero dello Sviluppo Economico, dal Ministero della Difesa e dal Sistema di Informazione per la Sicurezza della Repubblica della Presidenza del Consiglio dei Ministri.

Dr. Emilio Coppa

Emilio Coppa ha conseguito il Dottorato di Ricerca in Informatica presso Sapienza Università di Roma nel 2015, specializzandosi su tecniche di analisi del software per ottimizzazione e predizione del tempo di computazione. Nel 2015 è stato Visiting Scholar presso la Technische Universität di Darmstadt nel gruppo di ricerca del Prof. Patrick Eugster. La sua ricerca post-dottorale ha riguardato l'analisi del software applicato al contesto della cybersecurity, sfruttando tecniche di analisi come symbolic execution e software fuzzing per attività di reverse engineering e vulnerability detection. E' stato istruttore ed organizzatore sia locale che nazionale per l'iniziativa CyberChallenge.IT nelle edizioni 2017-2019. E' stato prima allenatore nel 2017-2018 e poi responsabile nel 2019 del team nazionale di cybersecurity per l'European Cyber Security Challenge organizzata dall'ENISA.

Dr. Daniele Cono D'Elia

Daniele Cono D'Elia ha conseguito il Dottorato di Ricerca in Ingegneria Informatica presso Sapienza Università di Roma nel 2016, specializzandosi su tecniche di costruzione e trasformazione del software per ottimizzazione e debugging. Nel 2014 è stato Visiting Scholar presso la Purdue University. La sua ricerca post-dottorale si svolge nell'ambito della sicurezza del software, studiando tecniche di analisi dei programmi (quali symbolic execution e taint analysis) per reverse engineering, trasformazioni per offuscamento e deoffuscamento, e tecniche di analisi per codice malevolo. E' stato istruttore ed organizzatore locale per l'iniziativa CyberChallenge.IT nelle edizioni 2017-2019. E' stato speaker a congressi non accademici di rilevanza internazionale nell'area dell'information security quali Black Hat.

Ing. Pietro Borrello

Pietro Borrello ha conseguito la Laurea Magistrale in Ingegneria Informatica presso Sapienza Università di Roma nel 2019 con una tesi sulla protezione del software attraverso l'impiego di avanzate tecniche di *code reuse*. Attualmente è al primo anno del Dottorato in Ingegneria Informatica

con indirizzo Cybersecurity presso Sapienza Università di Roma. Ha partecipato nel 2017 alla prima edizione della CyberChallenge. IT come studente, e dal 2018 è un istruttore per questa iniziativa sui temi di binary exploitation presso il nodo locale Sapienza. Ha fatto parte della nazionale di cybersecurity per l'European Cyber Security Challenge 2017 organizzata dall'ENISA, partecipa abitualmente a competizioni Capture-the-Flag (CTF) con i team TheRomanXpl0it e mHACKeroni, ed ha partecipato con quest'ultimi alla più prestigiosa competizione di hacking DEF CON CTF nel 2018 e 2019.

Pubblicazioni attinenti dei ricercatori coinvolti

- "SoK: Using dynamic binary instrumentation for security (and how you may get caught red-handed)". D'Elia et al, 2019. ACM ASIA Conference on Computer and Communications Security.
- "WEIZZ: Automatic grey-box fuzzing for structured binary formats". Fioraldi et al, 2019. Technical report <https://arxiv.org/abs/1911.00621>
- "SymNav: Visually Assisting Symbolic Execution". Angelini et al, 2019. IEEE Symposium on Visualization for Cybersecurity.
- "Reconstructing C2 Servers for Remote Access Trojans with Symbolic Execution". Coppa et al, 2019. International Conference on Cybersecurity Cryptography and Machine Learning.
- "A survey of symbolic execution techniques". Baldoni et al, 2018. ACM Computing Surveys.
- "Rethinking pointer reasoning in symbolic execution". Coppa et al, 2017. ACM/IEEE International Conference on Automated Software Engineering.
- "Assisting malware analysis with symbolic execution: a case study". Coppa et al, 2017. International Conference on Cyber Security Cryptography and Machine Learning.

Il secondo gruppo di ricerca, AWARE³, coordinato dal Prof. Giuseppe Santucci, vanta una esperienza di 15 anni nel settore della visualizzazione e di Visual Analytics con applicazioni specifiche nel contesto della cybersecurity.

I ricercatori del gruppo che saranno coinvolti nelle attività sono:

Prof. Giuseppe Santucci

Giuseppe Santucci è professore associato presso il DIAG (Dipartimento di Ingegneria Informatica Automatica e Gestionale Antonio Ruberti) della "Sapienza" Università di Roma, dove tiene i corsi di Fondamenti di Informatica e Visual Analytics e partecipa al centro di ricerca CIS-Sapienza (Cyber Intelligence and Information Security) situato presso il DIAG. Ha svolto attività di ricerca principalmente nei settori interfacce per Basi di Dati, linguaggi di interrogazione visuali, Visualizzazione dell'Informazione e Visual Analytics, pubblicando oltre 200 articoli su riviste e congressi internazionali di rilievo. E' membro degli steering committee delle principali conferenze mondiali relative a visualizzazione (Eurovis) e Visual Analytics (VAST).

³ <http://www.dis.uniroma1.it/~santucci/AWARE/aware-website/index.html>

Negli ultimi 6 anni la ricerca si è concentrata su aspetti relativi alla cyber security, sviluppando metodologie e soluzioni di Visual Analytics per, e.g., sicurezza di infrastrutture critiche, analisi delle vulnerabilità software, gestione dei cammini di attacco, sistemi di classificazione di malware, analisi del codice sorgente per individuazione di vulnerabilità.

Ing. Simone Lenti

Simone Lenti ha conseguito la Laurea Magistrale in Ingegneria Informatica presso Sapienza Università di Roma nel 2017 con una tesi sul supporto all'analisi di scenari di attacco in fase proattiva e reattiva nel contesto di Network Security. Attualmente è al terzo anno del Dottorato in Ingegneria Informatica presso Sapienza; la sua attività di ricerca si concentra sullo sviluppo di tecniche di Visual Analytics nel contesto di Cybersecurity, focalizzandosi in particolare sulla gestione del rischio in infrastrutture complesse, sulla gestione e implementazione di framework e direttive legate al rischio cyber, e sull'analisi di codice malevolo.

Pubblicazioni rilevanti del personale scientifico:

- "SymNav: Visually Assisting Symbolic Execution" Angelini M., Blasilli G., Borzacchiello L., Coppa E., D'Elia D. C., Demetrescu C., Lenti S., Nicchi S. & Santucci G. (2019). In *Proceedings of the IEEE Symposium on Visualization for Cyber Security (VizSec 2019)*. Vancouver, Canada.
- "MAD: A visual analytics solution for Multi-step cyber Attacks Detection". Angelini, M., Bonomi, S., Lenti, S., Santucci, G., Taggi, S., (2019) *Journal of Computer Languages*, 52, pp. 10-24.
- "ROPMate: Visually Assisting the Creation of ROP-based Exploits". Angelini, M., Blasilli, G., Borrello, P., Coppa, E., Drelia, D.C., Ferracci, S., Lenti, S., Santucci, G., 2018 *IEEE Symposium on Visualization for Cyber Security, VizSec 2018*.
- "Vulnus: Visual vulnerability analysis for network security". Angelini, M., Blasilli, G., Catarci, T., Lenti, S., Santucci, G. (2019) *IEEE Transactions on Visualization and Computer Graphics*, 25 (1), art. no. 8443131, pp. 183-192.
- "A review and characterization of progressive visual analytics". Angelini, M., Santucci, G., Schumann, H., Schulz, H.-J. (2018) *Informatics*, 5 (3)
- "Visual exploration and analysis of the Italian cybersecurity framework". Angelini, M., Blasilli, G., Lenti, S., Santucci, G. Visual exploration and analysis of the Italian cybersecurity framework (2018) *Proceedings of the Workshop on Advanced Visual Interfaces AVI*
- "An attack graph-based on-line multi-step attack detector". Angelini, M., Bonomi, S., Borzi, E., Del Pozzo, A., Lenti, S., Santucci, G. (2018) In *Proceedings of the 19th International Conference on Distributed Computing and Networking (ICDCN 2018)*. Varanasi, India .
- "The goods, the bads and the uglies: Supporting decisions in malware detection through visual analytics". Angelini, M., Aniello, L., Lenti, S., Santucci, G., Ucci, D.
- (2017) *IEEE Symposium on Visualization for Cyber Security, VizSec 2017*, 2017-October, pp. 1-8.
- "CRUMBS: A cyber security framework browser". Angelini, M., Lenti, S., Santucci, G. (2017) *2017 IEEE Symposium on Visualization for Cyber Security, VizSec 2017*

- “Cyber situational awareness: from geographical alerts to high-level management”. Angelini, M., Santucci, G. (2017) Journal of Visualization, 20 (3), pp. 453-459.
- “PERCIVAL: Proactive and reactive attack and response assessment for cyber incidents using visual analytics”. Angelini, M., Prigent, N., Santucci, G. (2015) 2015 IEEE Symposium on Visualization for Cyber Security, VizSec 2015, Chicago, IL, 2015, pp. 1-8.

11. Piano di finanziamento del progetto

11.1 Risorse per strumentazione

Nella tabella seguente sono indicate le spese sostenute dalla DGTCISI-Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione per la realizzazione del progetto, relative all'acquisto di apparecchiature e strumentazione, che costituiranno proprietà esclusiva del MISE.

| Obiettivo | Descrizione | Costo complessivo |
|--|---|-------------------|
| Sperimentazione e analisi del software | Licenze prodotti software per analisi necessari per la costruzione dei prototipi (si riporta il costo per singola licenza) <ul style="list-style-type: none"> • Hex-Rays: IDA Pro (2819 USD), ARM64 Decompiler (3944 USD), ARM32 Decompiler (3944 USD), x64 Decompiler (3944 USD). Ulteriori prodotti Decompiler potranno rendersi necessari in base ai dispositivi da analizzare. • Binary Ninja: 600-2000 USD (in funzione delle caratteristiche offerte) • Riserva di 5000€ per acquisto di prodotti per l'analisi del codice (es. CodeSurfer, rev.ng) in funzione delle necessità che emergeranno. • | € 22.950 |
| IVA 22% | | € 5049 |
| Totale | | € 28.000 |

11.2 Risorse per il personale

Nella tabella seguente sono indicate le spese relative all'impegno di ricercatori finanziate dalla Direzione Generale per le Tecnologie delle Comunicazioni e per la Sicurezza Informatica-ISCTI per la realizzazione del progetto.

| Obiettivo | Descrizione | Costo complessivo |
|-------------------------------|---|-------------------|
| Acquisizione personale senior | 3 assegni di ricerca RTD-A | € 471.203 |
| Acquisizione personale junior | 4 borse di studio junior | € 84.800 |
| Acquisizione personale junior | 2 borse di dottorato triennali | € 147.472 |
| Attività di ricerca | Partecipazione a conferenze internazionali di settore e organizzazione/finanziamento di eventi scientifici collegati alla ricerca | € 66.525 |
| Totale | | € 770.000 |

11.3 Risorse totali

Nella tabella seguente viene riportato il totale delle risorse impegnate nel progetto, incluso il costo della gestione CIS del progetto:

| Sintesi delle risorse | Costo complessivo |
|----------------------------|-------------------|
| Risorse per strumentazione | € 28.000 |
| Risorse per il personale | € 770.000 |
| Costo totale | € 798.000 |

12 Riferimenti bibliografici

[asiaccs16] “Automated Dynamic Firmware Analysis at Scale: A Case Study on Embedded Web Interfaces”. Costin, Andrei et al. ACM ASIA Conference on Computer and Communications Security, 2016.

- [cdcn18] Angelini, M., Bonomi, S., Borzi, E., Pozzo, A. D., Lenti, S., & Santucci, G. (2018, January). An Attack Graph-based On-line Multi-step Attack Detector. In Proceedings of the 19th International Conference on Distributed Computing and Networking (pp. 1-10).
- [csur18] "A Survey of Symbolic Execution Techniques". Baldoni, Roberto et al. ACM Computing Surveys, 2018.
- [gosl10] Keim, Daniel. "Mastering the Information age: solving problems with visual analytics." Goslar: Eurographics Association 2010.
- [ieee05] Thomas, James J. *Illuminating the path:[the research and development agenda for visual analytics]*. IEEE Computer Society, 2005.
- [jvlc 2019] Angelini, M., Bonomi, S., Lenti, S., Santucci, G., & Taggi, S. (2019). MAD: A visual analytics solution for Multi-step cyber Attacks Detection. Journal of Computer Languages , 52 ,10-24.
- [ndss14] "Avatar: A Framework to Support Dynamic Security Analysis of Embedded Systems' Firmwares". Zaddach, Jonas et al. Network and Distributed System Security Symposium, 2014.
- [ndss15] "Firmalice - Automatic Detection of Authentication Bypass Vulnerabilities in Binary Firmware". Shoshitaishvili, Yan et al. Network and Distributed System Security Symposium, 2015.
- [ndss19] "REDQUEEN: Fuzzing with Input-to-State Correspondence". Aschermann, Cornelius et al. Network and Distributed System Security Symposium, 2019.
- [sec14] "A Large-Scale Analysis of the Security of Embedded Firmwares," Costin, Andrei et al. USENIX Security Symposium, 2014.
- [sec19] "Firm-AFL: High-Throughput Greybox Fuzzing of IoT Firmware via Augmented Process Emulation," Zheng, Yaowen et al. USENIX Security Symposium, 2019.
- [tvcg18] Angelini, M., Blasilli, G., Catarci, T., Lenti, S., & Santucci, G. (2018). Vulnus: Visual vulnerability analysis for network security. IEEE transactions on visualization and computer graphics , 25 (1), 183-192.
- [vizsec16] "J-Viz: Finding algorithmic complexity attacks via graph visualization of Java bytecode," M. J. Alam, M. T. Goodrich and T. Johnson, *2016 IEEE Symposium on Visualization for Cyber Security (VizSec)*, Baltimore, MD, 2016, pp. 1-8.
- [vizsec16a] "Cesar: Visual representation of source code vulnerabilities," H. Assal, S. Chiasson and R. Biddle, *2016 IEEE Symposium on Visualization for Cyber Security (VizSec)*, Baltimore, MD, 2016, pp. 1-8.
- [vizsec19] "SymNav: Visually Assisting Symbolic Execution," Angelini, M., Blasilli, G., Borzacchiello, L., Coppa, E., D'Elia, D. C., Demetrescu, C., Simone Lenti, Simone Nicchi, Santucci, G. " *2019 IEEE Symposium on Visualization for Cyber Security (VizSec)*, Vancouver, Canada, 2019.