Sicurezza dei Dati

Alfredo De Santis

Dipartimento di Informatica
Università degli Studi di Salerno

ads@unisa.it

http://www.di-srv.unisa.it/~ads/pages/

Settembre 2017

Progetto 1

- **Titolo:** Quantum Key Distribution: Protocolli ed Applicazioni Commerciali.

- **Tipologia:** Progetto Teorico.
- **Prerequisiti richiesti:** Conoscenze di base in ambito crittografico.
- **Descrizione ed obiettivi del progetto:** L'obiettivo dell'attività progettuale è innanzitutto quello di analizzare il problema della Quantum Key Distribution (QKD) dal punto di vista teorico/concettuale, mettendo in evidenza i principi su cui essa si basa. In questa prima fase, lo studente dovrà esporre e contestualizzare il problema, fornendo al lettore tutta la conoscenza pregressa necessaria a comprendere l'argomento trattato (quantum mechanics, etc). Successivamente, lo studente dovrà analizzare lo stato dell'arte relativo alla QKD, soffermandosi su alcuni recenti lavori proposti in questo particolare campo di ricerca. Infine, lo studente dovrà contestualizzare, analizzare e comparare in maniera opportuna, alcuni prodotti commerciali presenti sul mercato che permettono di realizzare Quantum Key Distribution.
- **Numero Partecipanti:** 1.

Progetto 2

- **Titolo:** Uno Strumento Automatico per Attacchi a RSA.
- **Tipologia:** Progetto Pratico.
- **Prerequisiti richiesti:** Conoscenze di base in ambito crittografico, buona familiarità con il sistema operativo Linux e con i linguaggi di programmazione.
- **Descrizione ed obiettivi del progetto:** L'obiettivo dell'attività progettuale è quello di realizzare uno strumento completamente automatico (dotato di interfaccia grafica) che, presa in input una chiave pubblica RSA in formato PKCS #1, restituisca in output la relativa chiave privata, nel medesimo formato, oltre al tempo di esecuzione richiesto per tale calcolo. Il suddetto strumento dovrà utilizzare il YAFU come "engine" per la fattorizzazione, oppure altri strumenti a scelta dello studente. Anche eventuali ottimizzazioni prestazionali fornite dallo studente andranno a rappresentare un contributo per l'attività progettuale. Lo studente dovrà opportunamente documentare lo strumento realizzato, sia per quanto riguarda la fase di realizzazione (progettazione, sviluppo, testing) che di utilizzo.
- **Numero partecipanti:** Max. 2.

Progetto 3

- **Titolo:** Un Framework per l'Implementazione ed il Testing di Schemi di Assegnamento Chiavi Gerarchico.

- **Tipologia:** Progetto Pratico.
- **Prerequisiti richiesti:** Conoscenze di base in ambito crittografico. Conoscenza del linguaggio di programmazione Java.
- **Descrizione ed obiettivi del progetto:** Il controllo degli accessi si occupa di assicurare che solo agli utenti autorizzati di un sistema sia dato accesso a determinate risorse. In base alle loro competenze e responsabilità, gli utenti sono organizzati in una gerarchia, formata da un certo numero di classi disgiunte. In questa gerarchia valgono politiche di accesso di tipo gerarchico, vale a dire che gli utenti appartenenti ad una determinata classe hanno accesso alle risorse delle classi dei livelli inferiori, ma non è vero il viceversa. Gli schemi di Assegnamento Chiavi Gerarchico permettono di implementare le [...]

Progetto 3

- […] suddette politiche di accesso mediante tecniche crittografiche. L'obiettivo dell'attività progettuale è la realizzazione di un framework, scritto in linguaggio Java, che permetta l'implementazione di Schemi di Assegnamento Chiavi Gerarchico. Tale framework dovrà essere realizzato seguendo una logica di programmazione Object Oriented e dovrà avere un'architettura modulare, che permetta l'implementazione ed il testing (anche in termini prestazionali) di un qualsiasi Schema di Assegnamento Chiavi Gerarchico. Lo studente dovrà opportunamente documentare lo strumento realizzato, sia per quanto riguarda la fase di realizzazione (progettazione, sviluppo, testing) che di utilizzo.
- **Numero partecipanti:** Max. 3.

Progetto 4

- **Titolo:** Un Modulo Software per il Controllo degli Accessi Gerarchico e Condiviso ai Log di Sistema.
- **Tipologia:** Progetto Pratico.
- **Prerequisiti richiesti:** Buona familiarità con il sistema operativo Linux e con i linguaggi di programmazione.
- **Descrizione ed obiettivi del progetto:** L'obiettivo dell'attività progettuale è quello di realizzare un modulo (componente), preferibilmente integrata nel sistema operativo, che permetta la memorizzazione cifrata dei file di log del sistema. L'accesso a tali log dovrà inoltre essere garantito in base alle politiche di accesso regolate dalle vigenti norme in materia di protezione dei dati. Per l'implementazione di tali politiche di accesso dovranno essere utilizzate tecniche crittografiche, quali ad esempio Schemi di Assegnamento Chiavi Gerarchico o similari. Lo studente dovrà opportunamente documentare il modulo realizzato, sia per quanto riguarda la fase di realizzazione (progettazione, sviluppo, testing) che di utilizzo.
- **Numero partecipanti:** Max. 3.

Progetto 5

- **Titolo:** Automotive Safety and Security.
- **Tipologia:** Progetto Teorico/Pratico.
- **Prerequisiti richiesti:** Conoscenze di base in ambito crittografico.
- **Descrizione ed obiettivi del progetto:** L'obiettivo dell'attività progettuale è quello di analizzare le principali problematiche di sicurezza relative al settore dell'Automotive. In particolare, lo studente dovrà innanzitutto fornire un quadro d'insieme su quali sono le principali categorie di vulnerabilità a cui possono essere soggetti gli autoveicoli, soprattutto in base alla sempre crescente diffusione di sistemi informatici all'interno di essi. Lo studente dovrà inoltre analizzare le soluzioni proposte allo stato dell'arte per porre rimedio alle suddette vulnerabilità, o almeno per mitigarle, fornendo anche un'analisi comparativa di tali soluzioni. Infine, lo studente dovrà analizzare almeno un caso reale di sicurezza in ambito Automotive, fornendo come caso di studio l'analisi delle problematiche di sicurezza (e relative soluzioni) per un determinato veicolo, basandosi preferibilmente sulle specifiche tecniche fornite dal produttore.
- **Numero partecipanti:** Max. 2.

Progetto 6

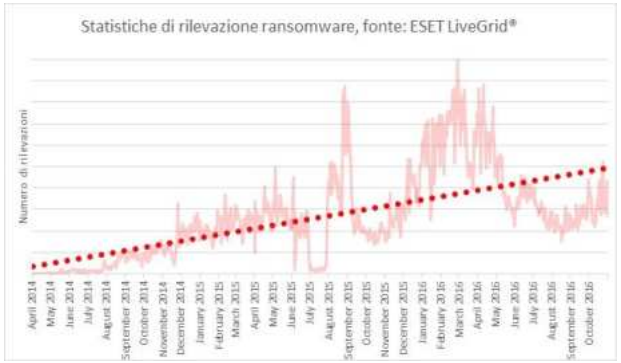
- **Titolo:** Sicurezza e Privatezza in ambito Genomico.
- **Tipologia:** Progetto Teorico.
- **Prerequisiti richiesti:** Conoscenze di base in ambito crittografico.
- **Descrizione ed obiettivi del progetto:** Al giorno d'oggi è sempre crescente il numero di aziende che vendono servizi “direct-to-consumer” di sequenziamento ed analisi del DNA. È facile osservare come tutto ciò possa rappresentare una seria minaccia per l'individuo che si sottopone a tale analisi. Di conseguenza, negli ultimi anni si sta dedicando un grande sforzo di ricerca alla sicurezza e privatezza in ambito genomico. L’obiettivo dell’attività progettuale è innanzitutto quello di definire cosa si intende per sicurezza e privatezza in ambito genomico, enfatizzando quali sono i rischi a cui può essere soggetto un utente che si sottopone a test genomici. Lo studente dovrà inoltre analizzare e categorizzare i principali strumenti crittografici comunemente utilizzati per garantire la sicurezza e privatezza in ambito genomico, fornendo una loro comparazione critica. Infine, lo studente dovrà analizzare uno (o più) strumento specifico a sua scelta, eventualmente anche uno strumento software, proposto in letteratura durante l’ultimo triennio, per garantire la sicurezza e privatezza in ambito genomico.
- **Numero partecipanti:** 1.

Progetto 7

- **Titolo:** Studio ed analisi del malware Wanna Cry.
- **Tipologia:** Progetto Teorico/Pratico.
- **Prerequisiti richiesti:** Nessuno.
- **Descrizione ed obiettivi del progetto:** Mediante il malware *Wanna Cry* è stato di recente perpetrato un importante cyber-attacco su scala mondiale (maggio 2017). Infatti, tale attacco ha infettato oltre 200mila macchine in circa 150 stati, con importanti conseguenze e notevoli danni, prevalentemente dovuti al malfunzionamento di diverse infrastrutture gestite da PC infetti. L'obiettivo principale dell'attività progettuale è lo studio e l'analisi di Wanna Cry, oltre alle sue implicazioni dal punto di vista della sicurezza.
- **Numero partecipanti:** Max. 3.

Progetto 8

- **Titolo:** I Ransomware in Ambito Mobile.
- **Tipologia:** Progetto Teorico/Pratico.
- **Prerequisiti richiesti:** Nessuno.
- **Descrizione ed obiettivi del progetto:** Nell'ultimo periodo la tendenza degli attacchi perpetrati mediante malware di tipo ransomware è aumentata notevolmente, e non solo per quanto riguarda gli attacchi "convenzionali" a danno di elaboratori e workstation. Infatti, una notevole e crescente diffusione è stata rilevata anche in ambito mobile, come mostrato nella figura seguente.



  L'obiettivo principale dell'attività progettuale è lo studio e l'analisi dei principali ransonware recentemente diffusi nel panorama mobile.
- **Numero partecipanti:** Max. 2.

Progetto 9

- **Titolo:** Sistemi Biometrici: Studio ed Analisi delle nuove proposte e delle nuove integrazioni nei dispositivi portabili.

- **Tipologia:** Progetto Teorico/Pratico.
- **Prerequisiti richiesti:** Nessuno.
- **Descrizione ed obiettivi del progetto:** Oggigiorno, i contesti di utilizzo dei dispositivi portabili non si limitano al solo instant messaging, social networking, etc., ma vi sono nuovi ed importanti contesti. Ad esempio, gli smartphone vengono sempre più utilizzati per pagamenti di beni e servizi. Ad esempio, vi sono diversi servizi che permettono di pagare tramite smartphone (Apple Pay, Samsung Pay, Android Pay, etc.) e/o di effettuare micro-pagamenti (acquisti in-app, etc.). Pertanto, l'autenticazione in questi dispositivi diventa un problema sempre più delicato. Infatti, si è passati dall'autenticazione mediante la scansione biometrica dell'impronta digitale (Touch ID, etc.), alla più precisa autenticazione mediante scansione tri-dimensionale del volto (Apple Face ID, Windows Hello, etc.), fino ad arrivare all'autenticazione mediante la scansione dell'iride. L'obiettivo dell'attività progettuale sarà caratterizzato dall'analisi dei nuovi sistemi biometrici, integrati nel panorama mobile (come ad esempio, il sistema di riconoscimento Apple Face ID), e dallo studio delle loro peculiarità.
- **Numero partecipanti:** 1.

- **Titolo:** Nuovi Rischi e Minacce derivanti dalla Realtà Aumentata (Augmented Reality - AR).

- **Tipologia:** Progetto Teorico/Pratico.
- **Prerequisiti richiesti:** Nessuno.
- **Descrizione ed obiettivi del progetto:** La Realtà Aumentata (Augmented Reality o AR) è una nuova tecnologia che potrebbe diffondersi presso il grande pubblico nel futuro prossimo. Tramite l'AR, la percezione sensoriale umana viene "arricchita". Ad esempio, ad una scena reale, possono essere aggiunti oggetti bi-dimensionali e/o tri-dimensionali. Tali oggetti saranno visibili esclusivamente mediante appositi visori (per favorire una fruizione più completa) oppure, i contenuti "aggiunti" potranno essere fruiti mediante lo schermo di uno smartphone/tablet.

  L'obiettivo dell'attività progettuale sarà innanzitutto lo studio dei concetti chiave relativi all'AR, per poi proseguire con l'analisi delle possibili rischi, minacce e contromisure per questa nuova tecnologia, tenendo soprattutto in considerazione che spesso esse fanno ampio uso della rete.

- **Numero partecipanti:** 1.

Progetto 11

- **Titolo:** Analisi Comparativa dei Meccanismi di Sicurezza utilizzati da weChat e Signal.

- **Tipologia:** Progetto Pratico.
- **Prerequisiti richiesti:** Conoscenze di base nell'ambito dei sistemi operativi per dispositivi mobili. Familiarità con strumenti per l'analisi dell'attività del sistema operativo e del relativo traffico di rete.
- **Descrizione ed obiettivi del progetto:** L'obiettivo dell'attività progettuale è quello di analizzare la sicurezza di weChat e Signal sotto molteplici aspetti. In particolare, lo studente dovrà analizzare quali sono le proprietà di sicurezza garantite all'utente, quali sono le eventuali problematiche di sicurezza che tali applicativi potrebbero causare al sistema operativo (backdoor, etc.), quali sono le eventuali attività sospette sia a livello di sistema operativo che di rete (information leakage, processi sospetti, etc.). Lo studente dovrà infine definire l'ambiente di testing e la metodologia di analisi che ha utilizzato, spiegando e documentando ciascuna fase dell'analisi in maniera opportuna.
- **Numero partecipanti:** Max. 2.

Progetto 12

- **Titolo:** Portable Windows 10 PE per Digital Forensics.
- **Tipologia:** Progetto Pratico.
- **Prerequisiti richiesti:** Nessuno.
- **Descrizione ed obiettivi del progetto:** L'obiettivo dell'attività progettuale è quello di creare una versione "portable" di Microsoft Windows 10, da poter essere direttamente eseguita tramite CD/DVD, penna, o altro supporto rimovibile. Tale versione dovrà contenere i più comuni strumenti per la digital forensics supportati da Windows, oltre che i più comuni strumenti diagnostici in dotazione alle distribuzioni portable/live dei sistemi operativi (System repair, etc.). Lo studente dovrà infine documentare in maniera opportuna l'utilizzo e le principali funzionalità offerte dalla versione "portable" da loro creata.
- **Numero partecipanti:** 1.

Progetto 13

- **Titolo:** Tecniche e Strumenti di Data Carving per Dispositivi Mobili.

- **Tipologia:** Progetto Pratico.
- **Prerequisiti richiesti:** Nessuno.
- **Descrizione ed obiettivi del progetto:** L'obiettivo dell'attività progettuale è quello di analizzare le principali metodologie e strumenti per il data carving (o file carving) su dispositivi mobili. Lo studente dovrà innanzitutto analizzare quali sono le principali tecniche e strumenti di data carving per i sistemi operativi Android e iOS. Lo studente dovrà inoltre mostrare reali esempi di recupero dati, in entrambi i sistemi operativi, documentando opportunamente l'utilizzo di ciascuna tecnica/strumento in ciascuna fase del recupero. In aggiunta, lo studente dovrà argomentare e motivare quali sono le tipologie di dato che le tecniche di data carving permettono di recuperare in maniera più accurata e su quale sistema operativo hanno più successo tali tecniche. Lo studente dovrà infine definire l'ambiente di testing e la metodologia di analisi che ha utilizzato, spiegando e documentando ciascuna fase dell'analisi in maniera opportuna.
- **Numero partecipanti:** Max. 2.

Progetto 14

- **Titolo:** Nuove Misure di Sicurezza in iOS 11 e loro Implicazioni dal punto di vista Forense.
- **Tipologia:** Progetto Teorico/Pratico.
- **Prerequisiti richiesti:** Nessuno.
- **Descrizione ed obiettivi del progetto:** L'obiettivo dell'attività progettuale è quello di analizzare le principali misure di sicurezza adottate in iOS 11, analizzando ed argomentando in che modo esse vanno ad impattare su una eventuale analisi forense. Lo studente dovrà inoltre argomentare quali sono le differenze o similitudini riscontrate applicando tecniche di data carving in iOS 10 ed iOS 11, per il recupero della medesima tipologia di dato. Lo studente dovrà inoltre definire l'ambiente di testing e la metodologia di analisi che ha utilizzato, spiegando e documentando ciascuna fase dell'analisi in maniera opportuna.
- **Numero partecipanti:** Max. 2.

Progetto 15

- **Titolo:** Sicurezza in ambito Personal Area Network (PAN) e nelle Body Area Network (BAN).

- **Tipologia:** Progetto Teorico/Pratico.
- **Prerequisiti richiesti:** Conoscenze di base nell'ambito delle reti di calcolatori.
- **Descrizione ed obiettivi del progetto:** Le Personal Area Network (PAN) e nelle Body Area Network (BAN) stanno ricevendo un sempre maggiore interesse, sia dal punto di vista tecnologico che scientifico, soprattutto perché esse vanno a costituire alcune tra le componenti più importanti nel settore dell'Internet of Things (IoT) e delle Smart Cities. In queste tipologie di rete, dati i loro contesti applicativi (monitoraggio della salute e del benessere, medicina personalizzata, etc.), vengono sempre più spesso scambiate informazioni sensibili. Per questo motivo, gli aspetti relativi alla loro sicurezza sono di primaria importanza. L'obiettivo dell'attività progettuale è innanzitutto quello analizzare le principali problematiche di sicurezza in ambito PAN e BAN, oltre alle relative soluzioni proposte. Lo studente dovrà inoltre enfatizzare il perché tali contesti richiedono strumenti di sicurezza "ad hoc". Infine, lo studente dovrà analizzare e documentare opportunamente Blueborne, una recente vulnerabilità che colpisce Bluetooth.
- **Numero partecipanti:** 1.

Progetto 16

- **Titolo:** Malware Challenge – Gruppo 1: Creazione.
- **Tipologia:** Progetto Pratico.
- **Prerequisiti richiesti:** Nessuno.
- **Descrizione ed obiettivi del progetto:** L'obiettivo dell'attività progettuale, denominata "Malware Challenge", è quello di simulare tutte le fasi del ciclo di vita di un malware, comprese la sua diffusione e la sua rilevazione. In particolare, l'obiettivo dell'attività progettuale relativa al Gruppo 1 sarà quello di creare un **semplice** Malware, il cui comportamento malevolo (ed il sistema operativo da infettare) sarà a discrezione dei componenti del gruppo. Il Malware suddetto dovrà essere creato in maniera tale da implementare tutte le fasi del ciclo di vita che tipicamente lo caratterizza (Infezione, Quiescenza, Replicazione e Propagazione, Azioni Malevole).
- **Numero partecipanti:** Max. 2.

Progetto 17

- **Titolo:** Malware Challenge – Gruppo 2: Rilevazione.
- **Tipologia:** Progetto Pratico.
- **Prerequisiti richiesti:** Nessuno.
- **Descrizione ed obiettivi del progetto:** L'obiettivo dell'attività progettuale, denominata "Malware Challenge", è quello di simulare tutte le fasi del ciclo di vita di un malware, comprese la sua diffusione e la sua rilevazione. In particolare, l'obiettivo dell'attività progettuale relativa al Gruppo 2 sarà quello di analizzare il Malware creato dal Gruppo 1, mediante le opportune tecniche definite allo stato dell'arte (Analisi Statica, Analisi Dinamica White Box e Black Box).
- **Numero partecipanti:** Max. 2.

Progetto 18

- **Titolo:** Deanonimizzazione di utenti whatsapp.
- **Tipologia:** Progetto Pratico.
- **Prerequisiti richiesti:** Nessuno.
- **Descrizione ed obiettivi del progetto:** Supponendo di disporre di un db contenente le foto profilo, la descrizione e lo status di un insieme di profili whatsapp, si adopereranno tecniche di reverse image search e record linkage per associarli con i corrispondenti profili facebook (o di altri social network). Il progetto è il follow-up di un precedente progetto di estrapolazione dati di utenti sconosciuti via whatsapp.
- **Numero partecipanti:** 1.

Progetto 19

- **Titolo:** Analisi di sicurezza di applicazioni di messaggistica istantanea.

- **Tipologia:** Progetto Pratico.
- **Prerequisiti richiesti:** Nessuno.
- **Descrizione ed obiettivi del progetto:** Scopo del progetto è studiare le possibilità vulnerabilità di sicurezza delle principali applicazioni di messaggistica istantanea, analizzando come queste trasmettono i dati sulla rete (cifrati o in chiaro, utilizzando un protocollo noto o sconosciuto), come conservano i dati sulla memoria locale del dispositivo e come conservano i dati in memoria, valutando le eventualità vulnerabilità delle soluzioni adottate. Nota: whatsapp è stato già analizzato nel progetto precedente e, pertanto, potrebbe essere escludo dallo studio.
- **Numero partecipanti:** 1**.**

Domande?