Relazione Finale di Dottorato

Enrico Bacis

30/09/2019

Attività di Ricerca

Nel corso del primo anno di dottorato (XXXII ciclo) in *Ingegneria e Scienze Applicate* presso l'*Università degli Studi di Bergamo*, abbiamo affrontato il tema della security nell'ambito dei servizi cloud centralizzati. In questo scenario, il Cloud Service Provider (CSP) è considerato "*honest-but-curious*", ossia esegue sempre le richieste dell'utente ma potrebbe accedere ai dati, se non protetti. Una semplice difesa è quella di applicare uno strato di cifratura, tuttavia le modalità di cifratura classiche richiederebbero di effettuare una ri-cifratura ogni qualvolta si voglia revocare l'accesso ad un utente. Abbiamo quindi proposto una modalità di cifratura con forte inter-dipendenza mutua nella rappresentazione cifrata. In questo modo, per revocare l'accesso è sufficiente ri-cifrare una porzione della risorsa. Lo sviluppo di questa tecnica ha dato luogo ad una pubblicazione alla conferenza *ACM Conference on Computer and Communications Security* [4].

Durante il secondo anno abbiamo studiato come le garanzie di sicurezza nei sistemi centralizzati, analizzate durante il corso del primo anno, potessero essere applicate ad ambienti di cloud storage decentralizzato. In questi ambienti, i dati vengono suddivisi tra vari partecipanti di una rete peer-to-peer in cambio di un pagamento. Tuttavia, questi partecipanti potrebbero agire in maniera disonesta e ignorare le richieste di cancellazione/revocata inviate dal proprietario, al fine di massimizzare il loro guadagno. Abbiamo proposto una soluzione che bilancia disponibilità e sicurezza dei dati e che permette inoltre al proprietario di impostare i valori di soglia richiesti. La tecnica proposta sfrutta la dinamicità delle reti decentralizzate per minimizzare il re-upload. Questo lavoro ha dato luogo a una pubblicazione alla conferenza internazionale *IEEE Global Communications Conference (GLOBECOM)* [8] e ad un articolo sulla *IEEE Transactions on Information Forensics and Security (TIFS)* [9]. Durante il secondo anno, ho anche collaborato alla scrittura del capitolo "*Protecting Resources and Regulating Access in Cloud-based Object Storage*" del libro "*From Database to Cyber Security*" [7], pubblicato da *Springer*.

Quando si tratta con ambienti di storage decentralizzati, un aspetto importante da considerare è l'individuazione di attori malevoli. Una volta individuati, è possibile smettere di remunerarli e spostare i dati verso nuovi attori. Questo processo deve tuttavia poter avvenire anche quando il proprietario è off-line e senza dover imporre vincoli di fiducia su alcuno dei partecipanti della rete. Per risolvere questo problema, durante il terzo anno abbiamo proposto un nuovo modo per il rilascio automatizzato di informazioni segrete ad istanti di tempo futuri. Questa tecnica può essere utilizzata per creare dei protocolli di *delegated challenge-response* che, a loro volta, possono essere utilizzati per garantire le proprietà di confidenzialità e affidabilità ai sistemi di storage completamente distribuiti. Questo lavoro ha dato luogo ad un articolo che si trova attualmente in fase di revisione [11].

Collaborazione in Progetti Europei

Grazie alla supervisione del mio advisor Prof. Stefano Paraboschi, durante il primo ed il secondo anno di dottorato ho avuto la possibilità di collaborare al progetto europeo EscudoCloud (nell'ambito del programma Horizon 2020). Questo mi ha dato l'opportunità di conoscere e lavorare con gli altri partner del progetto, tra i quali vi sono sia partner accademici (Università degli Studi di Milano e TUD Damstadt) che industriali (Dell EMC, IBM, SAP, British Telecom, Wellness Telecom). Il progetto europeo ha coinvolto il nostro gruppo di ricerca nella realizzazione di diversi strumenti open source (disponibili all'indirizzo `https://github.com/escudocloud`), nonché alla scrittura di articoli per conferenze [3, 5, 1, 12] e di deliverable di progetto, tra cui quelli che ci hanno visto maggiormente coinvolti sono stati [15, 10, 14, 13, 6, 16].

Durante il terzo anno, invece, ho collaborato al progetto europeo MOSAICrOWN (nell'ambito del programma Horizon 2020), che coinvolge sia partner accademici (Università degli Studi di Milano) che industriali (Dell EMC, SAP, Mastercard, W3C). Il progetto ha già portato alla realizzazione di una demo presentata durante la conferenza internazionale IEEE International Conference on Pervasive Computing and Communications [2].

Periodi di ricerca all'estero

- Nei mesi da Luglio a Settembre 2017 ho svolto un periodo di ricerca all'estero a Monaco di Baviera (DE) presso l'ente di ricerca Google Germany GmbH, su tematiche relative alla sicurezza del linguaggio WebAssembly, attualmente supportato da tutti i browser più diffusi.
- Nei mesi da Luglio a Ottobre 2018 ho svolto un periodo di ricerca a Londra (UK) presso l'ente di ricerca Google UK, su tematiche relative alla sicurezza delle applicazioni Android, con particolare attenzione
- Nei mesi da Luglio a Novembre 2019 ho svolto un periodo di ricerca a Zurigo (CH) presso l'ente di ricerca Google Switzerland GmbH, su tematiche relative alla privacy dei dati degli utenti del web.

Frequenza di Corsi

Corsi di Laurea Magistrale offerti dall'Università degli Studi di Bergamo:

- *Intelligenza Artificiale*, Prof. Francesco Trovò

Corsi di dottorato:

- *Introduzione alla Programmazione Scientifica*, Prof. Francesco Fassò, presso Università degli Studi di Bergamo
- *Internet Economics*, Prof. Nicola Gatti, presso Politecnico di Milano
- *Biometric Systems*, Prof. Angelo Genovese, presso Università degli Studi di Bergamo
- *Uso di Strumenti Informatici a Supporto del Ricercatore*, Prof. Angelo Gargantini, presso Università degli Studi di Bergamo
- *Data Security and Privacy in the Cloud*, Prof.ssa Sara Foresti, presso Università degli Studi di Bergamo
- *Practical Approaches to Cloud Assurance and Security*, Prof. Claudio Ardagna, presso Università degli Studi di Milano

Scuole per dottorandi:

- Python for Scientific Computing (Florence)
- Google 2nd PhD Summit on Web Application Security (Munich)
- Google PhD Interns Summit Conference 2017 / 2018 / 2019 (San Francisco)
- Google 5th / 6th PhD Summit on Compilers and Programming Languages (Munich)

Presentazioni

Presentazioni a conferenze internazionali:

- ACM Workshop on Information Sharing and Collaborative Security (WISCS), 2016
- IEEE International Conference on Communications and Network Security (CNS), 2017
- Cyber Security Awareness Week (CSAW), 2017
- IEEE International Conference on Pervasive Computing and Communications (PERCOM), 2018

Seminari interni:

- Binary Analysis and Reverse Engineering
- Programming Paradigms
- Competitive Programming

Seminari esterni:

- Improving Android Security (Tech Talk @ Google Munich)
- Bitcoin and Blockchains (Ordine degli Ingegneri di Bergamo)
- Non solo Bitcoin (Ordine degli Ingegneri di Como)

Pubblicazioni

La lista completa delle pubblicazioni scritte durante il dottorato si trova in allegato a questo documento.

Attività di dottorato

Per quanto concerne le attività di dottorato ed i crediti formativi, allego a questo documento la tabella che riporta la mia situazione finale.

Riferimenti bibliografici

[1] Enrico Bacis, Alan Barnett, Andrew Byrne, Sabrina De Capitani di Vimercati, Sara Foresti, Stefano Paraboschi, Marco Rosa, and Pierangela Samarati. Distributed shuffle index: Analysis and implementation in an industrial testbed. In *Proc. of the 5th IEEE Conference on Communications and Network Security (CNS 2017)*, Las Vegas, NV, USA, October 2017. poster.

[2] Enrico Bacis, Sabrina De Capitani di Vimercati, Dario Facchinetti, Sara Foresti, Giovanni Livraga, Stefano Paraboschi, Marco Rosa, and Pierangela Samarati. Multi-provider secure processing of sensors data. In *Proc. of the 17th IEEE International Conference on Pervasive Computing and Communications (PerCom 2019)*, Kyoto, Japan, March 2019.

[3] Enrico Bacis, Sabrina De Capitani di Vimercati, Sara Foresti, Daniele Guttadoro, Stefano Paraboschi, Marco Rosa, Pierangela Samarati, and Alessandro Saullo. Managing data sharing in openstack swift with over-encryption. In *Proc. of the 3rd ACM Workshop on Information Sharing and Collaborative Security (WISCS 2016)*, Vienna, Austria, October 2016.

[4] Enrico Bacis, Sabrina De Capitani di Vimercati, Sara Foresti, Stefano Paraboschi, Marco Rosa, and Pierangela Samarati. Mix&Slice: Efficient access revocation in the cloud. In *Proc. of the 23rd ACM Conference on Computer and Communication Security (CCS 2016)*, Vienna, Austria, October 2016.

[5] Enrico Bacis, Sabrina De Capitani di Vimercati, Sara Foresti, Stefano Paraboschi, Marco Rosa, and Pierangela Samarati. Distributed shuffle index in the cloud: Implementation and evaluation. In *Proc. of the 4th IEEE International Conference on Cyber Security and Cloud Computing (IEEE CSCloud 2017)*, New York, USA, June 2017.

[6] Enrico Bacis, Sabrina De Capitani di Vimercati, Sara Foresti, Stefano Paraboschi, Marco Rosa, and Pierangela Samarati. Final Versions of Tools for Security With Multiple Providers. Deliverable D4.3, ESCUDO-CLOUD, 2017.

[7] Enrico Bacis, Sabrina De Capitani di Vimercati, Sara Foresti, Stefano Paraboschi, Marco Rosa, and Pierangela Samarati. Protecting resources and regulating access in cloud-based object storage. In *From Database to Cyber Security: Essays Dedicated to Sushil Jajodia on the Occasion of his 70th Birthday*. Springer, 2018.

[8] Enrico Bacis, Sabrina De Capitani di Vimercati, Sara Foresti, Stefano Paraboschi, Marco Rosa, and Pierangela Samarati. Dynamic allocation for resource protection in decentralized cloud storage. In *Proc. of the 2019 IEEE Global Communications Conference (GLOBECOM 2019)*, Waikoloa, Hawaii, USA, December 2019.

[9] Enrico Bacis, Sabrina De Capitani di Vimercati, Ssara Foresti, Stefano Paraboschi, Marco Rosa, and Pierangela Samarati. Securing resources in decentralized cloud storage. *IEEE Transactions on Information Forensics and Security (TIFS)*, 15(1):286–298, December 2019.

[10] Enrico Bacis, Sabrina De Capitani di Vimercati, Sara Foresti, Stefano Paraboschi, Marco Rosa, Ali Sajjad, Pierangela Samarati, Mathias Björkqvist, Christian Cachin, Björn Tackmann, Ahmed Taha, Patrick Metzler, Salman Mazoor, and Neeraj Suri. Final Report on Data Protection and Key Management Solutions. Deliverable D2.6, ESCUDO-CLOUD, 2017.

[11] Enrico Bacis, Dario Facchinetti, Marco Rosa, Marco Guarnieri, and Stefano Paraboschi. I *Told* You Tomorrow: Practical Time-Locked Secrets using Smart Contracts.

[12] Enrico Bacis, Marco Rosa, and Ali Sajjad. Encswift and key management: an integrated approach in an industrial setting. In *3rd Workshop on Security and Privacy in the Cloud (SPC 2017)*, pages 483–486, Las Vegas, NV, USA, October 2017. IEEE.

[13] Daniel Bernau, Andreas Fischer, Anselme Kemgne Tueno, Christian Cachin, Björn Tackmann, Enrico Bacis, Sabrina De Capitani di Vimercati, Sara Foresti, Giovanni Livraga, Stefano Paraboschi, Marco Rosa, Pierangela Samarati, Roberto Sassi, Ahmed Taha, Nicolas Coppick, Ruben Trapero, and Neeraj Suri. Report on Secure Information Sharing in the Cloud. Deliverable D3.5, ESCUDO-CLOUD, 2017.

[14] Enrico Bacis and Sara Foresti. Tools for selective and private multi-user queries and interactions. Deliverable D3.4, ESCUDO-CLOUD, 2017.

[15] Stefano Paraboschi, Christian Cachin, Enrico Bacis, and Marco Rosa. Report on data and access protection. Deliverable D2.3, ESCUDO-CLOUD, 2016.

[16] Ahmed Taha, Heng Zhang, Neeraj Suri, Sara Foresti, Giovanni Livraga, Andrew Byrne, Alan Barnett, Enrico Bacis, Marco Rosa, and Ali Sajjad. D4.4 – Report on Multi Cloud and Federated Cloud. Deliverable D4.4, ESCUDO-CLOUD, 2017.