Universidad de Buenos Aires
Facultad de Ciencias Exactas y Naturales

Planilla a completar para presentación de Cursos de Posgrado

1.- DEPARTAMENTO de COMPUTACIÓN

2.- NOMBRE DEL CURSO: **Protegiendo la privacidad de datos mediante el uso de lenguajes de programación**

.

3.- DOCENTES:

RESPONSABLE/S: ...Dr. Alejandro Russo..
COLABORADORES: .....
AUXILIARES: .....

4.- CARRERA de DOCTORADO

5.- AÑO: 2018..... CUATRIMESTRE/S: ..primero..

6.- PUNTAJE PROPUESTO PARA CARRERA DE DOCTORADO: .....

7.- DURACIÓN (anual, cuatrimestral, bimestral u otra): 4 semanas

8.- CARGA HORARIA SEMANAL:

Teóricas: ..3.....
Problemas: .2.....
Laboratorio: .....
Seminarios: ..1.....
Teórico – Práctico: .....
Salida a Campo: .....

9.- CARGA HORARIA TOTAL: 24 HS

10.- FORMA DE EVALUACIÓN: Presentación de la profundización de algún tema en un seminario y la entrega de ejercicios de programación avanzados para la librería MAC y el navegador COWL

11.- PROGRAMA ANALÍTICO:

Unidad 1: introducción a seguridad mediante lenguajes de programación. Reticulados para seguridad. Flujos explícitos e implícitos. Diferentes definiciones de no interferencia. Sistemas de tipos y monitores para garantizar no interferencia. Sistemas estáticos vs. dinámicos. Prueba de seguridad. Análisis de manchas. Implementación de análisis de manchas en Python.

Unidad 2: Seguridad en lenguajes funcionales. Monadas y el control de efectos laterales. Monadas para estado. Modelado de reticulados en Haskell. Introducción a Safe Haskell. Conceptos e ideas detrás de la librería MAC para el control del flujo de la información. Conceptos e ideas detrás de la librería LIO en Haskell. DCC en Haskell.

Unidad 3: Seguridad web. Politica del mismo origin (SOP). Politica del control de contenido (CSP). Reticulados descentralizados. Reticulados para aplicaciones web. Protegiendo la privacidad de datos en la web con COWL. Protegiendo la privacidad de datos en JavaScript con JSFlow. El peligro de las extensiones.

Unidad 4: Canales encubiertos. Concurrencia en sistemas de control de flujo de información. Ataques de cache. Planificador (scheduler) basado en instrucciones. Evaluación perezosa y fuga de información.

12.- BIBLIOGRAFÍA:

Flexible Dynamic Information Flow Control in Presence of Exceptions
Deian Stefan, Alejandro Russo, John Mitchell, and David Mazières
JFP 2016
In Journal of Functional Programming, Cambridge University Press

Encoding DCC in Haskell
Maximilian Algehed and Alejandro Russo
PLAS 2017
In Proc. of ACM Workshop on Programming Languages and Analysis for Security

Securing Concurrent Lazy Programs Against Information Leakage
Marco Vassena, Joachim Breitner and Alejandro Russo
CSF 2017
In Proc. of IEEE Computer Security Foundations Symposium

Functional Pearl: Two can keep a secret, if one of them uses Haskell (video)
Alejandro Russo
ICFP 2015
In Proc. of ACM SIGPLAN International Conference on Functional Programming

The Most Dangerous Code in your Browser
Stefan Heule, Devon Rifkin, Alejandro Russo, and Deian Stefan
HotOS 2015
In Proc. of USENIX Workshop on Hot Topics in Operating Systems

A Library For Removing Cache-based Attacks in Concurrent Information Flow Systems
Pablo Buiras, Deian Stefan, Amit Levy, Alejandro Russo, and David Mazières

TGC 2013
In Proc. of International Symposium on Trustworthy Global Computing

Eliminating Cache-Based Timing Attacks with Instruction-Based Scheduling
Deian Stefan, Pablo Buiras, Edward Z. Yang, Amit Levy, David Terei, Alejandro Russo, and David Mazières
ESORICS 2013
In Proc. of European Symposium on Research in Computer Security

Disjunction Category Labels (code)
Deian Stefan, Alejandro Russo, David Mazières, and John C. Mitchell
NORDSEC 2011
In Proc. of Nordic Conference in Secure IT Systems

A Taint Mode for Python via a Library
Juan José Conti and Alejandro Russo
NORDSEC 2010
In Proc. of Nordic Conference in Secure IT Systems

Dynamic vs. Static Flow-Sensitive Security Analysis
Alejandro Russo and Andrei Sabelfeld
CSF 2010
In Proc. of IEEE Computer Security Foundations Symposium

From dynamic to static and back: Riding the roller coaster of information-flow control research
Alejandro Russo and Andrei Sabelfeld
PSI 2009
In Proc. of Andrei Ershov International Conference on Perspectives of System Informatics

Securing Timeout Instructions in Web Applications
Alejandro Russo and Andrei Sabelfeld
CSF 2009
In Proc. of IEEE Computer Security Foundations Symposium