Threat Intelligence for SAP Enterprise Threat Detection

Opportunity for a 6 months internship

at SAP Product Security Research - SAP Labs France
Nice-Sophia Antipolis

SAP Product Security Research is part of the global Products and Innovation unit of SAP and is addressing the major security and trust challenges in the context of highly dynamic service-oriented architecture such as automated management of security certification for software service, Business-driven approaches to the specification and enforcement of security and dependability requirements, Trust and data protection infrastructure for managing & assessing the risks associated with identity authentication and the trustworthiness of actors and Technology for the formal specification and automated validation of Trust and Security of service-oriented architectures..

Product Security Research proposes a 6-month internship in its Sophia-Antipolis offices (Nice, France).

INTERNSHIP TOPIC

Information sharing, specially threat information, seems to be an appealing technology to fight against information security breaches in a timely manner. Recent efforts of STIX (Structured Threat Intelligence Expression) [4], CybOX (Cyber Observable eXpression) [7], TAXII [8], MAEC [9], IOC [10] specifications recognize this. SAP's information security threat monitoring tool called SAP Enterprise Threat Detection [6] is an application level intrusion detection system [5] to monitor user activities and application interactions in order to detect hacking attempts, anomalous actions and perform appropriate mitigations thereby. Threat intelligence for SAP ETD also is a valuable approach to investigate. In this spirit the goal of the internship is the following:

1. Analyzing STIX, CybOX, TAXII, MAEC, IOC and related community driven specifications and methodologies. Propose integration approaches of STIX, CybOX etc. into SAP ETD

2. Developing a simplistic proof of concept demonstrating the integration.

The candidate must have good experience of mobile and/or web application development and should have handful experiences in SQL, Java, JavaScript, HTML5 and Eclipse. Knowledge of exploit development [11] and SAP technology [2, 3] is a plus. He/she must be familiar with the basic security concepts like authentication, integrity, confidentiality, authorizations, access control, certificates etc.

We expect that 30% of time will be dedicated to research activities, and 70% to software development.

CANDIDATE PROFILE

- University Level: Last year of MSc in Computer Science or beyond
- Experience in Java, SQL (expert)
- Experience in iOS/android (desired)
- XML and XML Schema (understand and extend the existing schemas)
- Fluency in English (working language)
- Abilities in organizing meeting and contacting people
- Good oral and written communication skills in English, ability to synthesize

REFERENCES

[1] OWASP mobile security project
https://www.owasp.org/index.php/owasp_mobile_security_project#tab=top_10_mobile_risks

[2] SAP HANA http://www.saphana.com/

[3] SAP UI5 http://scn.sap.com/community/developer-center/front-end

[4] STIX, https://stix.mitre.org/

[5] GUIDE TO INTRUSION DETECTION AND PREVENTION SYSTEMS
HTTP://CSRC.NIST.GOV/PUBLICATIONS/NISTPUBS/800-94/SP800-94.PDF

[6] SAP Enterprise Threat Detection http://scn.sap.com/docs/DOC-58501

[7] CybOX, https://cybox.mitre.org/

[8] Taxii, https://taxii.mitre.org/

[9] MAEC, http://maec.mitre.org/

[10] OpenIOC, http://www.openioc.org/

[11] Exploit Development http://www.offensive-security.com/metasploit-unleashed/exploit_development

INTERNSHIP CONTEXT

SAP

As the world's leading provider of business software, SAP delivers products and services that help accelerate business innovation for our customers. We believe that doing so, will unleash growth and create significant new value – for our customers, SAP, and ultimately, entire industries and the economy at large. Today, more than 248500 customers in more than 188 countries run SAP applications – from distinct solutions addressing the needs of small businesses and midsize companies to suite offerings for global organizations.

SAP Product Security Research in Sophia Antipolis

SAP Product Security Research Sophia-Antipolis is located in one of the most important scientific parks in France, and worldwide. A high concentration of IT and telecommunication industries within walking distance, proximity to research centres (INRIA, CNRS, etc.), as well as universities and engineering schools (Polytech Nice, Eurecom, etc.) provide an ideal working environment. Based at SAP Labs France, SAP Product Security Research Sophia-Antipolis addresses the upcoming security needs, focusing on increased automation of the security life cycle and on providing innovative solutions for the security challenges in networked businesses, including cloud, services and mobile.

STANDARD INTERNSHIP PACKAGE

- *Salary*: depending on the length of the internship and your diploma.
- *Lunch*: SAP Labs France has a local cafeteria; interns contribute 2,33 Euro/lunch, like other SAP employees.
- *Holidays*: French Bank Holidays
  - January 1st; March 28th, May 1st, May 5th, May 8th, May 16th, July 14th; August 15th , Nov 1st and 11th; December 25th
- *Travel*: no trip will be paid by SAP.
- *Accommodation*: SAP can propose an accommodation for the duration of your internship. The accommodation is subsidized by SAP: the intern pays a reduced rate of 375 €uro.

CONTACTS AND PROCEDURE

Please send **in English** your CV, a cover letter and any relevant documents to the following persons stating the title of the Internship in the subject: [Internship Application] Internship's title.

Supervisor
Dr. Mohammad Ashiqur Rahaman
mohammad.ashiqur.rahaman@sap.com

Administrative point of contact
Sylvine Eusebi
sylvine.eusebi@sap.com
Tel. +33-(0)4-92286477