Towards Automated Logging for Forensic-Ready Software Systems

❑ **Presenter:** Fanny Rivera Ortiz

❑ **Supervisor:** Dr. Liliana Pasquale

❑ **Email:** fanny.riveraortiz@ucdconnect.ie

❑ **Twitter:** @friverao

1 Motivation

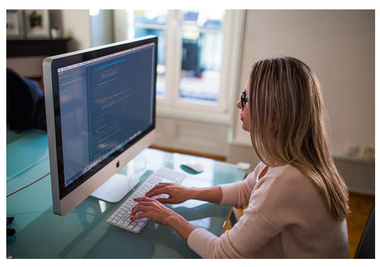
❑ Security incidents could be undetected for long periods of time.

❑ The OWASP identified insufficient logging as one critical vulnerability for web applications.

OWASP Open Web Application Security Project

❑ Insufficient logging might be due to:

- ❖ Insufficient security expertise of software developers [1].
- ❖ Difficulties of the software developers to identify where and what to log [2].



2 Related Work

❑ Logging in Software Systems [4]

Logging mechanisms should:

- ❖ Capture the context information about the incident.
- ❖ Be "human-readable".
- ❖ Represent the user behaviour.
- ❖ Enforce integrity.
- ❖ Be black-box tested.

❑ Limitations:

- ✖ These principles were obtained considering the health care domain.
- ✖ No technical suggestion is provided about how logging should be implemented in a software system.

❑ Engineering forensic-ready software systems:

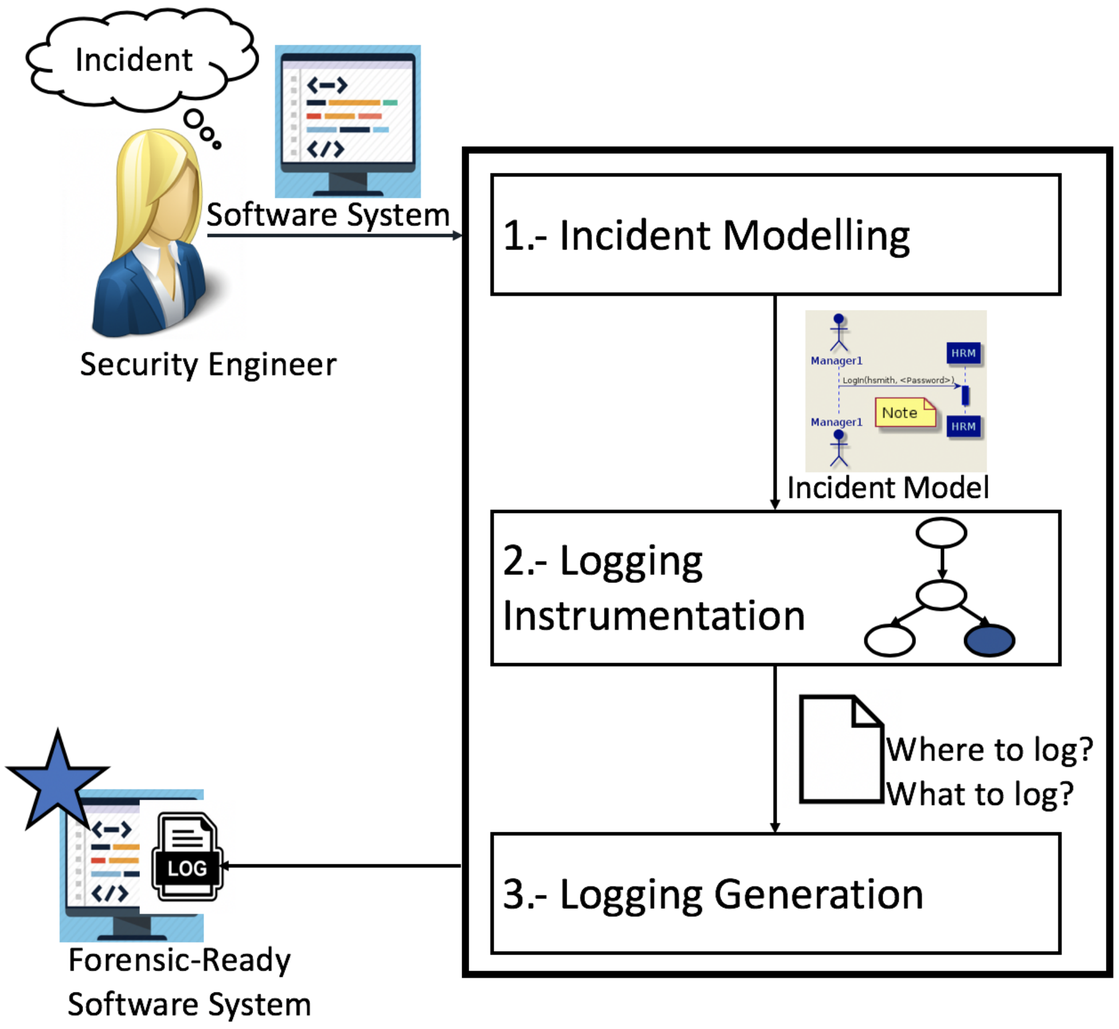
- ❖ Alrajeh et al. [5] defined a framework for evidence preservation requirements for forensic-ready systems.
- ❖ Pasquale et al. [6] determined the requirements that forensic-ready software systems have and the challenges to engineer such systems.

❑ Limitations:

- ✖ This work does not focused on how to save evidence in advance to detect incidents using generated logs.

3 Engineering Forensic-Ready Software Systems

"Forensic-Ready Systems" can log a minimum amount of relevant data to detect and investigate security incidents [3].



4 Evaluation

Assess:

- ❑ **Relevance:** The logs generated by the software system cover the events that occur during an incident.
- ❑ **Minimality:** The logs generated by the software system do not record events that are not part of potential security incidents.
- ❑ **Performance:** Evaluate the overhead of security logging.

Future Work

Develop our automated approach:

- ❑ **Incident Modelling:** Allow the security engineer to annotate the Incident Model with conditions determining whether logging should be performed.
- ❑ **Logging Instrumentation:** Use the incident model with a software control flow graph to determine where and what to log logging statements should be implemented.
- ❑ **Logging Generation:** Instrument the software system using Aspect Oriented Programming to generate logging instructions in designated locations.

[1] H. Assal, Hala and S. Chiasson (2019) "Think secure from the beginning": A survey with Software Developers. In Proceedings of the Conference on Human Factors in Computing Systems Proceedings (CHI'2019). Glasgow, Scotland, UK: ACM, p. 13.
[2] J. Zhu, P. He, Q. Fu, H. Zhang, M. R. Lyu, and D. Zhang (2015). Learning to log: Helping developers make informed logging decisions. In Proceedings of the 37th International Conference on Software Engineering (ICSE'15)., vol. 1. Florence, Italy: IEEE/ACM, pp. 11.
[3] F. Rivera-Ortiz and L. Pasquale (2019). Towards Automated logging for forensic-ready software systems. In Proceedings of the 6th International Workshop on Evolving Security and Privacy Requirements Engineering (ESPRE'19). Jeju Island, South Korea: IEEE, p. 7.
[4] J. King and L. Williams (2014). Log Your CRUD: Design Principles for Software Logging Mechanisms. In Proceedings of the 2014 Symposium and Bootcamp on the Science of Security (HotSoS'14). Raleigh, North Carolina, USA: ACM, 2014, p. 10.
[5] D. Alrajeh, L. Pasquale, and B. Nuseibeh (2017). On Evidence Preservation Requirements for Forensic-Ready Systems. In Proceedings of the ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC/FSE'17). Paderborn, Germany: ACM, p. 10.
[6] L. Pasquale, D. Alrajeh, C. Peersman, T. Tun, B. Nuseibeh, and A. Rashid (2018). Towards Forensic-Ready Software Systems. In Proceedings of the 40th International Conference on Software Engineering (ICSE18). Gothenburg, Sweden: ACM, p. 4.

Ireland's European Structural and Investment Funds Programmes 2014-2020
Co-funded by the Irish Government and the European Union

European Union
European Regional Development Fund

Tionól Réigiúnach an Deiscirt
Southern Regional Assembly