Attack-Aware Applications

Tolga Ünlü

Introduction

- Tolga Ünlü, PhD Student @AbertayCyber
- From Germany, Bavaria 🇩🇪
- University of Applied Sciences Kempten, Germany:
  - 2009/2014 Computer Science (BSc.)
- Abertay University:
  - 2012/2013 Computing & Networks (BSc. Hons)
  - 2015/2016 Ethical Hacking & Computer Security (MSc.)

@tolgauedev

Introduction

- Web Engineer @OFYZ, Kempten, Germany:
  - Full Stack Development (JavaScript, PHP, MySQL)
  - Student Project/Internship Supervision

aumentoo

- Platform for Startup and Innovation Management
- Decision Support for Startup Cooperation
- Research: AI-based Startup Success Prediction

Attack-Aware Applications

- Applications that are able to detect and respond to **attacks** and **attacker behavior**

- Utilizes **application context** for the detection process

- Enables **real-time insights** into an applications **current security posture**:

  - Is someone currently probing my application?
  - Where are the hotspots of my application?
  - In which state was the application during an attack?

PhD Research

- Concept addresses current and relevant issues in application security (lack of visibility and timely defense)

- Can be automated to a certain degree but not completely
  - Needs to be done by developers on top of other tasks

- Research Question (Current):
  How can the attack-awareness integration be made more usable?

- Research Aspects:
  - Integration Methods & Automation
  - Utilization of existing Roles, Tools and Environments in SW-Dev

Current PhD Research Status

- Short Paper Submitted for IEEE Cyber Security 2020 (Under Review): *A Taxonomy of Approaches for Integrating Attack Awareness in Applications*

Developer-Driven

The detection capability is directly built into the target application by the developers

Agent-Driven

The detection capability is provided by a software agent that makes applications attack-aware at runtime

Future Work

- **In Progress:** Design and Application of an Activity (e.g. Survey) to gather feedback and integration requirements from developers

- Dissemination of the Concept and Research Findings (e.g. Meetups, Security/Developer Events, Societies)

- **Ongoing:** Informal Discussions/Dialogs with Persons working with the same or a related concept (academia and industry)

Thank you!