Block 5

In conjunction with my PhD research (http://pjmorris.github.io/Security-Practices-Evaluation-Framework/index.html), we are conducting a survey of security practice use in software development teams. We seek to understand security practices from the point of view of the personnel who exercise the effort and appreciate the costs and benefits of using those practices. The survey is anonymous; we do not track or record your identity. If you choose to participate, you will be eligible for a drawing to win one of eight $25 Amazon gift cards.

For each of 13 software development security practices, described in the survey, we ask five questions:

* How often do you use or engage in this practice?
* Have you received any training in the use of this practice?
* Is this practice easy to use?
* Does this practice assist in preventing and/or removing security vulnerabilities on your project?
* How much time, on average, does it take to apply this practice?

Please answer the questions in the context of your work on [project name].

We provide space at the end for you to provide comments on the practices, our survey, and security in general. By collecting and analyzing this data, we intend to aid development teams in security practice selection.

We expect this survey to take no more than 15 minutes of your time. We thank you in advance for your participation.

Block 2

INFORMED CONSENT FORM for RESEARCH
Software Development Security Practices Survey
Patrick Morrison, and Dr. Laurie Williams, North Carolina State University and International Business Machines

What are some general things you should know about research studies?
You are being asked to take part in a research study. Your participation in this study is voluntary. You have the right to be a part of this study, to choose not to participate or to stop participating at any time without penalty. The purpose of research studies is to gain a better understanding of a certain topic or issue. You are not guaranteed any personal benefits from being in a study. Research studies also may pose risks to those that participate. In this consent form you will find specific details about the research in which you are being asked to participate. If you do not understand something in this form it is your right to ask the researcher for clarification or more information. A copy of this consent form will be provided to you. If at any time you have questions about your participation, do not hesitate to contact the researcher(s) named above.

What is the purpose of this study?
We seek to understand security practices from the point of view of the personnel who exercise the effort and appreciate the costs and benefits of using those practices. This study will collect data about developer use of security practices while developing software. We plan to use this data to develop a model supporting security practice selection in software development.

What will happen if you take part in the study?
If you agree to participate in this study, you will be asked to take one online survey. You will be asked to answer a number of questions about your use of software development security practices. We estimate that this survey will take less than 15 minutes. You may take this survey anywhere you have access to it. Your survey responses are not connected to your name or email address, and the researchers cannot link your responses to your name or email address.

Risks
We do not anticipate any risks to participation. However, if you experience any discomfort or choose to stop taking the survey for any reason, you may leave the survey at any time by closing your browser.

Benefits
We do not anticipate any direct benefits to you for participating in this survey. Your responses will help researchers, and software development managers understand and refine the use of security practices in software development. We will also use this data to compare security practice use across different projects and organizations.

Confidentiality
The information in the study records will be kept confidential to the full extent allowed by law. Data will be stored securely on password protected computers and hard drives belonging to the researchers. No reference will be made in oral or written reports which could link you to the study. You will NOT be asked to write your name on any study materials, so no one can match your identity to the answers that you provide.

Compensation
On completion of the survey, you are eligible for a raffle for one of eight $25 Amazon gift cards, to be conducted when the survey closes. If you are one of the eight raffle winners, you will receive a $25 Amazon gift card, via the email address we used to contact you.

What if you have questions about this study?
If you have questions at any time about the study or the procedures, you may contact the Principal Investigator, Patrick Morrison, at pjmorris@ncsu.edu.

What if you have questions about your rights as a research participant?
If you feel you have not been treated according to the descriptions in this form, or your rights as a participant in research have been violated during the course of this project, you may contact Deb Paxton, Regulatory Compliance Administrator, Box 7514, NCSU Campus (919/5154514).

Consent To Participate
I have read and understand the above information. I have received a copy of this form. I agree to participate in this study with the understanding that I may choose not to participate or to stop participating at any time without penalty or loss of benefits to which I am otherwise entitled.

- ◯ Yes
- ◯ No

Demographics

What is your project's name?

(Optional) What is your project's repository url?

How many years have you worked on this project?

How many hours per week do you work on this project?

What is your role on the project? You may select multiple options, if you play multiple roles.

- [ ] Developer
- [ ] Quality Assurance
- [ ] Project Management
- [ ] Requirements Engineer
- [ ] Designer/User Experience
- [ ] Documentation/Technical Writing
- [ ] Database Administrator
- [ ] Build Administrator
- [ ] Security
- [ ] Other

What best describes your primary role on this project?

Are you physically co-located with other members of the team?

Yes	No
☐	☐

Block 4

We have summarized software development practices described in Cigital's BSIMM, Microsoft's SDL, OWASP CLASP, and the SAFECode initiative.

Full documentation for the 13 security practices we ask about is available at the following link: http://pjmorris.github.io/Security-Practices-Evaluation-Framework/guidebook.html

Here, we present summaries of the 13 security practices:

Perform Security Training - Ensure project staff are trained in security concepts, and in role-specific security techniques.

Apply Data Classification Scheme - Maintain and apply a Data Classification Scheme. Identify and document security-sensitive data, personal information, financial information, system credentials.

Apply Security Requirements - Consider and document security concerns prior to implementation of software features.

Apply Threat Modeling - Anticipate, analyze, and document how and why attackers may attempt to misuse the software.

Document Technical Stack - Document the components used to build, test, deploy, and operate the software. Keep components up to date on security patches.

Apply Secure Coding Standards - Apply (and define, if necessary) security-focused coding standards for each language and component used in building the software.

Apply Security Tooling - Use security-focused verification tool support (e.g. static analysis, dynamic analysis, coverage analysis) during development and testing.

Perform Security Review - Perform security-focused review of all deliverables, including, for example, design, source code, software release, and documentation. Include reviewers who did not produce the deliverable being reviewed.

Perform Security Testing - Consider security requirements, threat models, and all other available security-related information and tooling when designing and executing the software's test plan.

Publish Operations Guide - Document security concerns applicable to administrators and users, supporting how they configure and operate the software.

Perform Penetration Testing - Arrange for security-focused stress testing of the project's software in its production environment. Engage testers from outside the software's project team.

Track Vulnerabilities - Track software vulnerabilities detected in the software, and prioritize their resolution.

Improve Development Process - Incorporate ``lessons learned'' from security vulnerabilities and their resolutions into the project's software development process.

Block 5

How Often Do You Engage in the Following Activities?

	Daily	Weekly	Monthly	Quarterly	Annually	Less than Annually	Not Applicable
Perform Security Training	○	○	○	○	○	○	○
Apply Data Classification Scheme	○	○	○	○	○	○	○
Apply Security Requirements	○	○	○	○	○	○	○
Perform Threat Modeling	○	○	○	○	○	○	○

Document Technical Stack	○	○	○	○	○	○	○
Apply Secure Coding Standards	○	○	○	○	○	○	○
Apply Security Tooling	○	○	○	○	○	○	○
Perform Security Review	○	○	○	○	○	○	○
Perform Security Testing	○	○	○	○	○	○	○
Publish Operations Guide	○	○	○	○	○	○	○
Perform Penetration Testing	○	○	○	○	○	○	○
Track Vulnerabilities	○	○	○	○	○	○	○
Improve Development Process	○	○	○	○	○	○	○

How much time, on average, does it take to apply this practice each time you apply it?

	15 minutes or less	15-30 minutes	30 minutes-1 hour	1-4 hours	4-8 hours	1-2 days	3-5 days	More than 5 days	Not Applicable
Perform Security Training	○	○	○	○	○	○	○	○	○
Apply Data Classification Scheme	○	○	○	○	○	○	○	○	○
Apply Security Requirements	○	○	○	○	○	○	○	○	○
Perform Threat Modeling	○	○	○	○	○	○	○	○	○
Document Technical Stack	○	○	○	○	○	○	○	○	○
Apply Secure Coding Standards	○	○	○	○	○	○	○	○	○
Apply Security Tooling	○	○	○	○	○	○	○	○	○
Perform Security Review	○	○	○	○	○	○	○	○	○
Perform Security Testing	○	○	○	○	○	○	○	○	○
Publish Operations Guide	○	○	○	○	○	○	○	○	○
Perform Penetration Testing	○	○	○	○	○	○	○	○	○
Track Vulnerabilities	○	○	○	○	○	○	○	○	○
Improve Development Process	○	○	○	○	○	○	○	○	○

Rate your agreement with "I have been trained in the use of this practice":

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Not Applicable
Perform Security Training	○	○	○	○	○	○
Apply Data Classification Scheme	○	○	○	○	○	○
Apply Security Requirements	○	○	○	○	○	○
Perform Threat Modeling	○	○	○	○	○	○
Document Technical Stack	○	○	○	○	○	○

Apply Secure Coding Standards						
Apply Security Tooling						
Perform Security Review						
Perform Security Testing						
Publish Operations Guide						
Perform Penetration Testing						
Track Vulnerabilities						
Improve Development Process						

Rate your agreement with "This practice assists in preventing and/or removing security vulnerabilities on our project":

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Not Applicable
Perform Security Training						
Apply Data Classification Scheme						
Apply Security Requirements						
Perform Threat Modeling						
Document Technical Stack						
Apply Secure Coding Standards						
Apply Security Tooling						
Perform Security Review						
Perform Security Testing						
Publish Operations Guide						
Perform Penetration Testing						
Track Vulnerabilities						
Improve Development Process						

Rate your agreement with "This practice is easy to use":

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Not Applicable
Perform Security Training						
Apply Data Classification Scheme						
Apply Security Requirements						
Perform Threat Modeling						
Document Technical Stack						

Apply Secure Coding Standards						
Apply Security Tooling						
Perform Security Review						
Perform Security Testing						
Publish Operations Guide						
Perform Penetration Testing						
Track Vulnerabilities						
Improve Development Process						

Block 4

To enter the raffle for one of eight $25 Amazon.com gift cards, please enter the best contact email to reach you.