CHALMERS
UNIVERSITY OF TECHNOLOGY

UNIVERSITY OF GOTHENBURG

Automotive Software Security Vulnerability Analysis with a Hackathon: A Design Science Study

Bachelor of Science Thesis in Software Engineering and Management

Ashley Key
Joshua Akhigbemen

Department of Computer Science and Engineering
UNIVERSITY OF GOTHENBURG
CHALMERS UNIVERSITY OF TECHNOLOGY
Gothenburg, Sweden 2017

CHALMERS
UNIVERSITY OF TECHNOLOGY

UNIVERSITY OF GOTHENBURG

Automotive Software Security Vulnerability Analysis with a Hackathon: A Design Science Study

Ashley Key
Joshua Akhigbemen

Supervisor: Eric Knauss
Examiner: Regina Hebig

University of Gothenburg
Chalmers University of Technology
Department of Computer Science and Engineering
SE-412 96 Göteborg
Sweden
Telephone + 46 (0)31-772 1000

Department of Computer Science and Engineering
UNIVERSITY OF GOTHENBURG
CHALMERS UNIVERSITY OF TECHNOLOGY
Gothenburg, Sweden 2017

Automotive Software Security Vulnerability Analysis with a Hackathon: A Design Science Study

Ashley Key
Software Engineering and Management
University of Gothenburg
Gothenburg, Sweden
guskeyas@student.gu.se

Joshua Akhigbemen
Software Engineering and Management
University of Gothenburg
Gothenburg, Sweden
gusakhjo@student.gu.se

***Abstract*—Today's vehicles are more innovative and connected than ever and will continue to be so as innovation in the automotive industry keeps moving forward. With this connectivity, remote vehicle hacking becomes a greater threat as it has been proven as a capable approach of altering the functions of a vehicle in motion. This threat creates a heightened concern in the software security development of vehicles. This study will attempt to introduce an additional platform, to the already used in-house penetration testing, for detecting software security vulnerabilities through a hackathon in collaboration with the HoliSec project conducted by the Viktoria Institute. Through a qualitative design science approach and completion of two regulative cycle iterations, artifacts and templates for setting up a hackathon for software security vulnerability detection in the automotive domain were designed, constructed and evaluated.**

Keywords—software security, vulnerabilities, automotive industry, hackathons

I. INTRODUCTION

As today's vehicles are more connected to the internet via vehicle-to-vehicle and vehicle-to-infrastructure through wi-fi, Bluetooth and applications [7], the threat to the security of these vehicles has become an ever more prevalent problem in the automotive industry. With vehicles being connected, it has presented a heightened security concern in the industry with vulnerabilities having been exploited and the threat of future hacks [24]. These security vulnerabilities have become of great importance and the work to fix these issues ever more in focus. In handling these vulnerabilities many companies rely on penetration testing performed within their respective companies or by software security consultancy firms. This is a solid way of approaching the problem, but could there be an additional way of detecting these vulnerabilities? This thesis proposes that there could be an addition in how the automotive industry could approach this issue. A combination of the domains of software security testing and hackathons, in creating an additional method of testing for the detection of vulnerabilities within today's vehicles.

Detection of software security vulnerabilities in the automotive industry has become an important part in the development cycle of vehicle security. Today's vehicles are more and more connected which creates a larger surface for attacks. Hacking into vehicle's remotely is a real threat and has been proven as a capable method of altering the functions of a vehicle in motion. While this problem today is handled through in-house penetration testing and through the service of software security consultancy firms, by only testing in this way creates a possibility of vulnerabilities being missed because of the familiarity with the vehicles being tested. If today's market is any indication, vehicles will continue to become more connected and the weakness of existing software security testing frameworks and practices in detecting these vulnerabilities becomes a major concern.

To design a solution for this problem we will need to gain an understanding of the background and intricacies of a hackathon along with an understanding of the automotive industry's needs. Developing the idea of designing a hackathon that will meet the needs of the industry we intend to answer the following questions.

RQ1: What, if any are the challenges in having a hackathon in the automotive industry?

RQ2: How would the setup of such a hackathon be configured?

RQ3: What artifacts and information would be considered useful in a hackathon for the automotive industry?

In approaching this problem through a qualitative design science approach, we will be creating artifacts and templates that will later be given the perfect opportunity to be tested through the HoliSec project conceived by the Viktoria Institute to be started later in 2018. The design of our solution is to adapt the idea and concept of a hackathon and alter it to meet the needs of the automotive industry. The hackathons intentions will be altered from the normal idea of creating new concepts and applications within a theme for the hackathon, to being a hackathon with an intent of "breaking" pre-existing software. This "breaking" will be conducted by causing as much damage through the vehicle software as possible. Causing this damage through the vehicles software

vulnerabilities makes this purposeful for the automotive industry as vehicles are at risk remotely to such attacks. By creating an environment in which these vehicles can be "broken" without any harm to drivers gives the automotive industry an opportunity to gain a full and complete understanding of the risks posed by security vulnerabilities and acquire a heightened awareness into their handlings of vulnerabilities.

The key results of the study are the collection of artifacts and templates designed and created for the "hackathon package," to be used in three different stages; pre-hackathon, hackathon, and post-hackathon. The artifacts and templates were evaluated in the completion of two iterations for their completeness, clarity and usability for setting up of the event.

In the following sections, we will separate the problem into its smaller parts; hackathons, security vulnerabilities and hackathons in the automotive domain with relevant literature. The research method of choice and the results of our design will follow.

II. RELATED WORK AND BACKGROUND

The following domains were chosen as they are considered the key domains of focus in our thesis. These domains are important in the development of our solution as gaining an understanding of their definition, purpose, and background is important.

A. Hackathons

In understanding a hackathon, there must be a conceptual understanding of the word and what it means. A hackathon, the combination of "hack" and "marathon," is an event usually lasting from a day to a week where those involved in software development collaborate on software projects [1][4]. While those who participate in these events are referred to as "hackers," meaning a clever programmer [12].

Hackathons can be centred around a common theme, domain or simply have the purpose of gathering people to innovate and learn in an exciting environment. This sort of engineering solution is an event where the gathering of a crowd with possible differences in areas of expertise come together to create a solution for the proposed problem decided by the event. There are different types of hackathons for example; hackathons for creation of an application, hackathons using a specific software framework or internal company hackathons [1]. Along with different types of hackathons, there are also different domains in which this event has garnered interest.

Many companies today focus on a common theme or technology to solve problems, for example in an Internet related domain, Google organizes a hackathon where anyone can participate, industry or students, to solve a real-world engineering problem [13]. In the medical domain, John Hopkins University organized MedHacks, an event aimed at trying to solve some the world's healthcare problems around the world [14]. And in the Consumerism domain, Unilever organized a hackathon for innovation within sustainable living [15]. These hackathons have a connection in that there was a problem to be solved and these events held a platform for innovation and ideas for problem solving to take place.

B. Security Vulnerabilities in Vehicles

Security vulnerabilities are a well-documented issue within many domains. With the Internet being a major source of communication and information due to its connectivity to the world, security is a daily concern. Within the domain of security, research has previously been completed in the automotive industry with a focus on security within vehicles. This research started in 2010 from a group of researchers from the University of Washington and the University of California San Diego. Their research focused on a specific part within the vehicle, Controller Area Network bus (CAN bus), which is a component designed to allow microcontrollers and devices to communicate with each other without a host computer [23]. In focusing on this part, the researchers could hack into and manipulate the test vehicle by sending different messages through this CAN bus that could affect the display on the speedometer, kill the engine, as well as affect its braking [5]. Their research has continued through the years as the automotive industry has added new features of connectivity into cars as listed in their following paper [6].

From the year 2010, the automotive industry has developed the "connected vehicle," where vehicles can communicate with other vehicles, the drivers telephone, infrastructure and industry [7]. This type of connectivity creates security problems because with each connection, lies a possible vulnerability. In 2015, Dr. Charlie Miller and Chris Valasek took the work completed by the previously mentioned researchers with the assumption that there was a way to exploit these security vulnerabilities remotely. They focused on Chrysler's Jeep Cherokee to attempt a remote attack to show that a connected vehicle could in fact be exploited without having physical contact with the vehicle [8]. With their success, this hack led to Chrysler recalling 1.4 million of their vehicles.

In remotely attacking the vehicle, Dr. Charlie Miller and Chris Valasek showed the automotive industry that "connected vehicles," had security vulnerabilities that could be exploited without having to be in physical contact with the vehicle. With the evidence of such an attack, the problem is clear that in todays' automotive industry, security vulnerabilities in vehicles are an issue that must be continually handled.

In another study, conducted by Carnegie Mellon University and funded by the US Department of Homeland Security on the vulnerabilities in vehicles, states that since the 1990 Clean Air Act all vehicles built after 1994 were to include on-board computer systems [16]. One of the effects of this law was the mandate for the on-board diagnostic (OBD-II) port and a related standard which allows anyone connecting to it, access to the vehicle to monitor its performance and function [16]. With the developments in mobile devices and the evolution of aftermarket component manufacturers, these ports which were to only be physically accessed, are now open to the Internet. In becoming connected to the Internet, these ports now provide a gateway into the vehicle that can be accessed remotely

providing a threat that they were not originally made to include.

The research that has been completed in this area continues just as the development of connected vehicles and aftermarket components. With these connected vehicles and their vulnerabilities, remote attacks are becoming ever more plausible and the damage that could reap havoc on the industry and every more possible threat.

Developing solutions for such problems as security vulnerabilities have been handled in other domains as well as in the automotive industry. An example from the Internet security domain, Google has dealt with its security vulnerabilities by inviting anyone from the Internet to attempt to hack into its system [9]. Another example from a logistics company Deutsche Post, operating under Deutsche Post DHL Group, also used the Internet to invite researchers to find software security vulnerabilities in 2010 as they were developing a service comparative to Sweden's' BankID [10]. They tested their product by using in-house penetration testers but invited teams of hackers to try to find security vulnerabilities that their team may have not discovered. The result being that teams found vulnerabilities that the in-house testers had not found, and Deutsche Post decided to replicate the hacking method the next year.

C. *Hackathons in Automotive Domain*

Within the automotive domain most hackathons have been for generating new ideas and concepts such as BMWs' "Co-Creation Lab," a virtual meeting place for individuals to share their ideas for the future of the automotive world [2]. BMW also has another hackathon which allows the participants access to data within its cars for the teams to develop new ideas, tools and services for the connected vehicle [22]. Mercedes-Benz hosted a hackathon to find new in-car concepts for innovative ideas in how vehicles could communicate with wearable devices [17]. There have also been hackathons focusing on certain aspects within vehicles, such as the Connected Car Hackathon [3], which organizes an event to design applications for use inside of the car.

When mentioning hackers and security vulnerabilities, in 2016 General Motors (GM), launched in partnership with HackerOne, a submission program for security vulnerabilities within their vehicles. The program allowed for researchers and hackers to submit any security flaws they found in any GM vehicle if they have followed the given rules and did not publicly disclose their findings [18].

The Car Hacking Village, a community developed around finding weaknesses and exploiting them, is a regular participant in DEFCON hackathons [19] and regularly gives "Car Hacking: Hands on Course," at Black Hat events [20]. The global association of engineers of SAE International, who have had a CyberAuto Challenge the previous six years as a practicum-based workshop working on real cars to find solutions to the problem chosen for the event [21].

By sectioning off these three domains we could break down the problem into its more specific parts to gain a better understanding. With an understanding in the background of each section we could now focus on how to best approach the problem to develop a solution.

III. RESEARCH METHODOLOGY

A. *Research Strategy*

The methodology used to complete this thesis is a design science approach based on a qualitative method of data collection. This methodology was chosen because it is centred towards practical problem solving and solution-oriented knowledge where the results have an impact on the automotive industry. The objective being to determine and understand the problem to achieve a solution, developing and providing applicable knowledge that can be used by professionals in the field in question [11].

Based on the problem this thesis intends to answer, our artifacts and templates will first come from understanding the needs of those who could be involved, why those needs exist and their importance. The artifacts and templates to be designed, "hacker package," to answer the research questions will be developed through gaining an insight into hackathons, and the industry needs along with what sorts of information is and could be of importance in our cooperation with Viktoria Institutes HoliSec project.

B. *Regulative Cycle*

The artifacts and templates have been designed from conducted interviews, Table 1, with the main automotive stakeholder involved Volvo Group, security specialists (penetration testing team), project manager of the HoliSec project, as well as interviews from those with experience in the setup of a hackathon. The artifact collection is designed as a regulative iterative cycle borrowed from vanStrien [27], as seen in Figure 1, where every iteration process is fulfilled. This iteration process consists of the following phases; design problem, solution candidate, artifact validation, artifact implementation and artifact evaluation.

The use of the regulative cycle is to understand and solve the identified problem in this study through the completion of the different phases in the cycle. In this case, the problem is to solve the organization of a hackathon for the analysis of software security vulnerabilities in the automotive domain.

The regulative cycle provides the logical framework on how this problem should be solved in the completion of each stage over a period. Each phase of the regulative cycle provides a practical structure on bringing us closer to the solution of the identified problem. The cycle will be used to complete two iterations, with the evaluation phase completed in the first iteration being the information used for the beginning of the second iteration design problem phase. The evaluation in the second iteration will serve as the strongest assessment for analysing, improving and creating artifacts and templates that will be implemented in the HoliSec project.

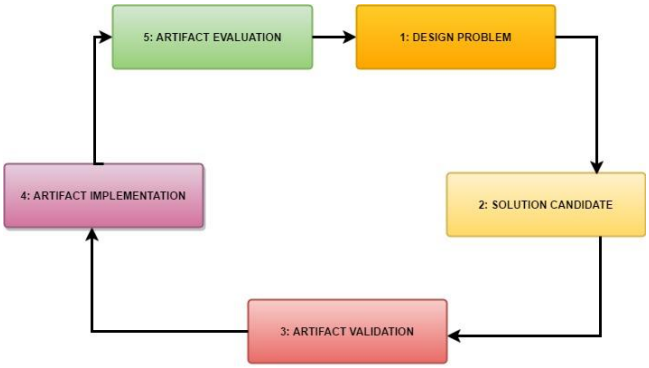

Figure 1: Regulative iterative cycle

1) Design Problem (DP)

Every research starts out by the exploration of a practical problem to establish an in-depth understanding in the landscape of the research topic. The design problem for this paper revolves around existing studies on vehicle security vulnerabilities and why it has become a heightened concern for automotive industries. Knowledge gaps in its base of securing connected components have been identified as an issue and priority should be given to address these knowledge gaps to minimize future security vulnerabilities in the connected vehicles [25]. We intend to address this gap within this issue by using a qualitative method of data collection through existing literature review and conducted interviews within the automotive domain and hackathons. In attempting to have an in depth understanding of the problem in todays' vehicle software security, we must first understand the current methods used in detecting software security vulnerabilities within automotive industries, how they are detected, are the tests completed in-house and could an additional platform help them better test their vehicles to eliminate software security vulnerabilities. Vehicle safety has been a priority but as we have understood from our interviews,

"In the automotive domain safety has always been a major priority, but safety and security are connected. You can't have safety without security – DE-1."

2) Solution Candidate (SC)

In this phase, active discussion and investigation took place contributing to the development and understanding of software security vulnerabilities and what could help in organizing the hackathon event. A solution candidate is a creative step wherein new processes are envisioned to create artifacts and templates that are helpful to solving the design problem. In this case, the idea was to design a package of artifacts and templates that would help in organizing such an event, with its contents being helpful to the stakeholders and invited participants.

We use this phase to construct practical design solutions for the problem under investigation as the proposed solutions bring stakeholders closer to their goals and meet their requirements. Therefore, the design solutions for the difficulties identified are communicated to the stakeholders and presented in the validation and implementation phases. From data collection in the problem investigation phase, we divided the event into three stages to help us simplify the process of organizing the hackathon event; (input) pre-hackathon, (setting) the event and (outcome) post-hackathon.

3) Artifact Validation (AV)

In this design phase, we consider the validity of designed artifacts and templates in solving the design problem along with satisfying the stakeholders. The artifacts and templates are sent to stakeholders to check the validity and context. Once the artifacts and templates are evaluated we repeat the validation phase if there needed redesigning or continue to the implementation phase. When they are validated by the stakeholders the implementation of the artifacts and templates follows.

4) Artifact Implementation (AI)

In the implementation phase, the artifacts and templates that have been validated from the solution candidates phase are now created. The creations are made to have a continuous design and developed to be re-usable.

5) Artifact Evaluation (AE)

In the evaluation phase, the last phase of the regulative cycle, the artifacts and templates are complete when they have satisfied the constraints of the problem they were meant to solve. This is a very important phase in the regulative cycle as it must be carried out carefully to ensure the quality of the artifacts and templates implemented can be evaluated in many terms with functionality, completeness, and usability to name a few [26]. In designing the artifacts and templates we used an iterable way of working to refine them by completing two full iterations of the cycle. All the cycle phases performed in this study gave a clear and comprehensive result at each evaluation phase on what could be improved in the next iteration.

C. Data Collection

Our data collection relied heavily on conducting open-ended question interviews, mainly used in the design problem and artifact evaluation stages, and with our industry supervisor in the artifact validation stage. Interviews were conducted with people directly involved or with knowledge of the HoliSec project. Their knowledge in software security, hackathons and the innerworkings of Volvo were the reasoning as to their being chosen as interviewees.

Table 1: Interview code list and contribution

ID	ROLE	REGULATIVE CYCLE PHASE
SE-1	Systems Engineer at Volvo Bus Corporation	DP, SC
R-1	Senior Researcher at Viktoria Institute. Industry Supervisor	DP, SC, AV
DE-1	Development Engineer with focus on security at Volvo Trucks	DP

AP-1	Associate Professor at Gothenburg University. Hackathon setup experience	DP, SC
PM-1	HoliSec project manager. Electrical and Embedded Systems at Volvo Group	DP, SC
IM-1	Innovation Manager at Volvo Group Trucks Technology. Hackathon setup experience	DP, SC
PT-1	Assurance Security Consulting. Security specialist. Penetration testing	DP, AE1
PT-2	Cure 53. Penetration testing	AE2

IV. RESULTS

A. *Iteration 1: Exploring Hackathons as a Tool for Automotive Software Vulnerability Analysis*

There is an array of processes that are a part of setting up a hackathon and in and among those processes lie certain challenges that must be handled. There is a core of main challenges that occur in developing hackathons with one example, in how members of teams communicate when they have different primary disciplines or area of expertise [4]. Intellectual-property rights [4], pertaining to the person or group that developed a prototype and their publishing of their findings are another challenge. Event personnel serving as domain experts are part of hackathons because of the challenge facing the participants with having to learn a new framework or technology in which to build their prototype.

In developing our design, these challenges have been considered as they could pertain to our setup and development of the event. In our interviews within the automotive industry we have tried to understand their needs and perspective on challenges as well as interviewing those who have been involved in setting up hackathons to develop our design. The interviews conducted also focused on understanding the knowledge base of the interviewee regarding hackathons they have setup along with their experience of the challenges involved.

In our interviews with Volvo Group, we asked from their perspective what their main challenges would be in such an event. Their response was that they saw a few things that would be their main challenges in being part of such an event for example; having the right people, contractual obligations and the vulnerabilities. The challenge of creating interest as to attract the correct people with the skills and expertise so the industry partner gets the most out of their investment. Volvo Group wants an event in which software security vulnerabilities of every degree are to be found and having the right skills and expertise are important. Contractual obligations are also a challenge with the non-disclosure agreement being the most prominent obligation. The expectation that those who will partake in the event must sign this agreement, and Volvo having the rights to the participants' findings until the contract time has expired. This is a challenge as it could mean that experienced professionals may not be interested as they would not be allowed to immediately post their findings. The last challenge being the vulnerabilities discovered concerns Volvo Group as they will need to take the information and determine how they will proceed once the event ends. Analysing the qualitative and quantitative data from the event and how to turn those results into use and,

"An increased awareness about vehicular security across various stakeholders; increased knowledge about security vulnerabilities in the automotive industry; greater interests in the subject in academia and research institutes; new possibilities of collaboration across stakeholders; and new methodologies of handling security challenges – PM-1."

In our interviews with those who have had experience with hackathons, participation and setup, we wanted to gain information from their experiences. To hear how their hackathons were setup and the challenges they faced. Also, wanting to gain an understanding into what sorts of artifacts and templates were designed and what parts of a hackathon they felt were important. In their responses, the challenges they faced were budget, location and technical platforms. The challenge of budget was a common theme in being able to secure a location to fit the size and expectations of the event, cater food and snacks for all participants and to pay for the technical experts that were to be on site throughout the entire event. The other challenge that they faced were the technical platforms that were to be used and how to create an atmosphere for the participants to learn these platforms to produce a prototype for the event.

"One problem is the technology and technical stuff to learn to develop something. The need to have the experts. There should be experts in the technologies present, domain experts because there could be a lot of questions – AP-1."

"… the space, you need to have a physical space. Hackathons should not be in a space that is familiar, but it's a cost. – AP-1."

The challenges mentioned by each group were taken to account, as shown in Figure 2, in designing artifacts and templates that would strengthen our basis on the idea of how we wanted to solve the problem. We would need to create artifacts and templates of a high level of detail and responsibility for the industry perspective as well as to generate interest and comfort level for the basic details in an overall development of a hackathon.

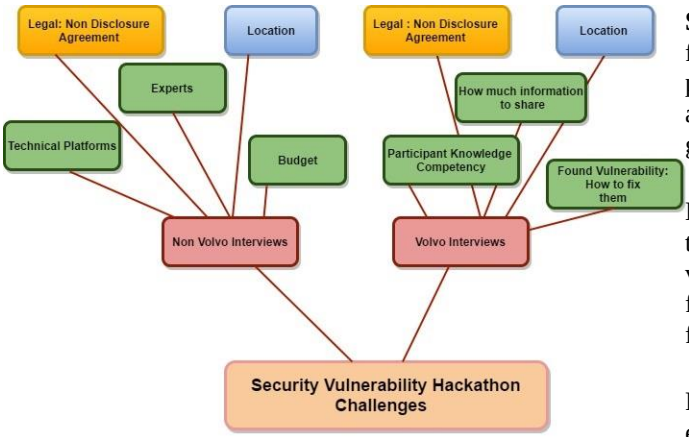

Figure 2: Hackathon Challenges

1) Iteration Development

In the first iteration of our regulative cycle, we focused on understanding the design problem and brainstorming the sort of solution candidates that could help solve the design problem. As shown in Table 2, the breakdown of work completed in the first iteration. The artifact evaluation was completed by a company who has experience in penetration testing within the automotive industry.

Table 2: Summary of Iteration 1

REGULATIVE CYCLE PHASE	KEY RESULTS
Design Problem	*Setting up a hackathon for software security vulnerability analysis*
Solution Candidates	***Pre-hackathon**: Advertisement plan, invitation, application form, NDA, guidelines, code of conduct, technical specifications* ***Hackathon**: schedule, security vulnerability report* ***Post-hackathon**: exit survey*
Artifact Design Validation	*Senior Researcher at Viktoria Institute, HoliSec project*
Artifact Implementation	*Advertisement plan, invitation, application form, NDA, guidelines, schedule, technical specifications, security vulnerability report, exit survey*
Artifact Evaluation	*Evaluated by Assured Security Consultants*

Design Problem: The HoliSec project is creating an event, an additional approach and platform, to hack into connected vehicles and expose its software security vulnerabilities. This will be a challenge based on the existence of such an event hasn't been organized previously between these domains. The study will develop the artifacts for how such an event can be organized and setup.

Solution Candidate: In the pre-hackathon stage, the following are thought to be designed and to be sent out to the participants and stakeholders; advertisement plan, invitation, application form, non-disclosure agreement (NDA), guidelines, code of conduct, technical specifications.

During the hackathon stage, the event is ongoing and therefore the artifacts needed for this stage are the schedule and security vulnerability report. The schedule contains times in which food is available along with times where experts are available for questions and for validation of discovered vulnerabilities.

For the post-hackathon stage, the participants will receive an exit survey and the found vulnerabilities are evaluated both quantitatively and qualitatively for the company champion to decide if the event was a success and what its future decisions entail. In this stage, in the advertisement plan, there is a suggested seminar or conference for the participants to talk about their discoveries and experience with the event.

Artifact Validation: Our artifacts and templates were validated by our industry supervisor, R-1, within the HoliSec project. The candidates were reviewed and validated to implement with an exception for the code of conduct as its purpose was seen redundant with its similarity to guidelines.

Artifact Implementation: The following were created; *Advertisement plan, invitation, application form, NDA, guidelines, schedule, technical specifications, security vulnerability report, exit survey*

Artifact Evaluation: Our artifacts and templates were sent to software security experts with experience in the automotive domain and hackathons, Assured Security Consultants. These experts evaluated each artifact and template and were given the opportunity to openly add comments of the overall impression and completeness of the artifacts. The feedback received was based on its completeness, clarity and usability.

"Overall the artifacts are valid and useful but need more work and focus on the content – PT-1."

B. Iteration 2: Modification of implemented artifacts and templates from evaluation phase of Iteration 1

In starting the second iteration of the regulative cycle we first considered the feedback we received from the development of our artifacts and templates from Iteration 1. Some of the artifacts and templates had more feedback than others and our focus began on those with the most feedback and need of revision. Some of the feedback we received on our artifacts and templates can be found below:

Invitation template*: "There is a lot of information missing; Who can join the contest? How to apply? How many participants in a team? Only companies? Only universities? How are teams selected? What to test? How many teams? If I am interested – what is the next step? What happens then? Is there a timeline? -PT-1."*

Advertisement plan artifact: *"Divide advertisement plan in sections, depending on purpose – what is PR and what is aimed towards finding teams and participants – PT-1."*

Security vulnerability report template: *Should we add impact? In what way does this bug create an impact on the target system? – PT-1."*

1) Iteration Development

For the second iteration, we focused more on the evaluation received from the first iteration in developing the artifacts and templates. The feedback received was used to revise and update to meet a higher standard. As shown in Table 3, the summary of work completed in Iteration 2, the solution candidates are the same from the artifact implementation phase from Iteration 1, as these are to be revised. The evaluation phase of Iteration 2 is completed by a different company that has no experience within the automotive industry.

Table 3: Summary of Iteration 2

REGULATIVE CYCLE PHASE	***KEY RESULTS***
Design Problem	*Reiterating over the artifacts based on their evaluation feedback and planning based on the additional feedback.*
Solution Candidates	***Pre-hackathon****: Advertisement plan, invitation, application form, NDA, guidelines, technical specifications* ***Hackathon****: schedule, security vulnerability report,* ***Post-hackathon****: exit survey*
Artifact Design Validation	*Senior Researcher at Viktoria Institute, HoliSec project*
Artifact Implementation	*Advertisement plan, invitation, application form, NDA, guidelines, schedule, technical specifications, security vulnerability report, exit survey*
Artifact Evaluation	*Evaluated by Cure 53*

Design Problem: With the completion of Iteration 1 our goal for this phase was to focus on the feedback received. We read through each artifact and templates evaluation feedback and will build on its development in continuing to develop solutions to the problem described in the previous iteration.

Solution Candidate: The candidates for this phase are the artifacts and templates that were created, implemented and evaluated from Iteration 1; *Advertisement plan, invitation, application form, NDA, guidelines, technical specifications schedule, security vulnerability report, exit survey.*

Artifact Validation: The feedback received from the evaluation phase in Iteration 1 was reviewed by our industry supervisor, R-1, within the HoliSec project. They then validated the artifacts and templates and decided that all feedback should be taken into consideration and were to be updated accordingly.

Artifact Implementation: The following were revised based on the evaluation from iteration one while those not listed from iteration one did not need to be revised; *Advertisement plan, invitation, application form, NDA, guidelines, security vulnerability report.*

Artifact Evaluation: Our artifacts were sent to software security experts with no experience in the automotive domain but with experience in hackathons, Cure 53. The feedback received focused mainly on the guidelines artifact and some of its content while the other artifacts and templates were evaluated as being complete, clear and usable,

"*The docs look solid! Only the guidelines seem a big vague - PT-2."*

The feedback also revealed an issue of document format for which format, i.e. Word, LibreOffice or other, the participants may find easier to open and use.

C. Completed works from Iteration cycles

In Table 4, each artifact and template created and implemented through the completion of two regulative cycles can be found with its description and purpose.

Table 4: Artifact and template summary

IMPLEMENTED	***DESCRIPTION AND PURPOSE***
Advertisement plan	*Detailed artifact on how to market and advertise the event. Also contains a marketing strategy timeline. Created to have a visual plan on how to reach target audiences.*
Invitation	*Detailed template for inviting potential participants with information pertaining to the event. Created to appeal to potential participants so that they will want to partake in the event.*
Application form	*Detailed artifact for participants to fill in to be considered for the event based on their credentials. Created for the stakeholders and jury to know and decide if those who have applied have the right competencies for being involved in the event.*

NDA	*Detailed template describing the rules of confidentiality for those chosen by the jury to participate to sign. Created for the stakeholders to control the flow of sensitive information.*
Guidelines	*Detailed artifact describing the rules that apply for those participating in the event. Created so that all participants know from the beginning the rules they must adhere.*
Schedule	*Detailed template describing a possible schedule for participating teams, including times for participating experts. Created as a schedule for teams to know when to expect food and technical experts.*
Technical Specifications	*Detailed artifact describing the technical information, concerning the test objects, for the chosen participants that they will only have received after signing the NDA. Created so the participants have the necessary technical information before the event begins to gain familiarity with the test objects and their design.*
Security Vulnerability report	*Detailed template providing a layout for the participants to report the vulnerabilities found on the test objects to be judged by the jury based on a CVSS scale for severity. Created so the vulnerabilities that are found can be judged and categorized for future handlings from the stakeholders.*
Exit survey	*Detailed artifact for the participants to give feedback on their overall experience concerning the event. Created to gain feedback from the participants to use for possible future events.*

The artifacts and templates developed and revised based on the evaluation feedback through the two iterations can be found here: https://github.com/akey15/bachelorThesis_artifacts.

V. THREATS TO VALIDITY

In creating, implementing and evaluating the artifacts and templates for this project we needed to keep an open approach into our design. The possibility of the replication of this event in another setting or with another company is a major factor in the design of our artifacts and templates. One threat to our study is if the same results hold if another automotive company replicated the design of our artifacts and templates. We mitigated this risk by choosing knowledgeable people within the automotive and software security industry to conduct our interviews to gain a foundation and understanding of the problem within their domain. We asked open-ended questions pertaining to the challenges from their perspective in the industry without having a pre-conceived idea of expected answers and designed our artifacts and templates from their responses. We could also mitigate the threat of difficulty of replication by creating artifacts as well as templates to make the replication process easier to be altered to fit the needs for any future event.

Another threat to validity is within the conducted interviews and the questions that were asked as seen in Appendix A and B. Content and construct validity was mitigated by asking questions pertaining to the domains included within the problem of our study. We mitigated the construct validity by disclosing our interview guide to be transparent and by asking questions that could be traced back to our study with the answers from the interviewees tracing back to helping develop the artifacts and templates.

A risk to our study would be in our interviews with industry, because their responses could be determined as biased as only focusing on Volvo Group. This was a trade-off by deciding to go in-depth with Volvo Group instead of a shallow investigation with several companies, also making it clear that Volvo Group was our industry champion.

VI. DISCUSSION

The research completed in this study was aimed at designing a hackathon for the detection and analysis of software security vulnerabilities in the automotive industry. A design which will later be used for the HoliSec project being completed by the Viktoria Institute with Volvo Group as the industry subject.

The data was collected through interviews with participants mainly involved in the HoliSec project, from Volvo Group to penetration testers and software security experts. The information of the collected data provided us with insight into the innerworkings of Volvo in their handling of software security vulnerabilities and the challenges involved, as well as how security experts view the challenges the automotive industry faces with connected vehicles. The data collected also gave us an understanding of the challenges in developing an event from the industry perspective as well as possible participants. As shown in our results, the data led to the development of our artifacts and templates from a high-level design of a non-disclosure agreement to a lower level design of a schedule of the event.

We addressed the main research question *(What if any are the challenges in having a hackathon in the automotive industry?)* in section IV.A and created a mind map, Figure 2,

to show that from our industry and non-industry interviews there were common challenges that could be faced in having a hackathon event in the automotive industry.

We also addressed our second research question *(How would the setup of such a hackathon be configured?)* by developing the advertisement plan artifact and the schedule template, in which we show how the event should have its beginnings with advertising and marketing and how the event should function during the days in which the groups have access to the test objects.

In answering the third research question *(What artifacts and information would be considered useful in a hackathon for the automotive industry?)* we used the regulative cycle described in section III and developed artifacts and templates in an iterative development manner as shown in section IV. These artifacts and templates are broken down into certain categories as to their use; pre-hackathon, hackathon, post-hackathon. We designed artifacts as well as templates to create a simple way of replication for future events. The evaluation of our artifacts and templates were completed by penetration testers and software security experts, first evaluated with experience in the automotive industry and secondly with no experience in the automotive domain. This was done to ensure the artifacts and templates created could be understood and replicated without needing an in-depth technical understanding of the automotive domain.

Our scientific contribution to this problem is the creation of a "hacker package" artifacts and templates for the set-up of a hackathon for software security vulnerability analysis. This study is filling a gap for research and artifacts developed for connecting two domains, hackathons and the automotive industry. The advantage that this hackathon could bear would be the implications of detecting vulnerabilities not previously known and having the opportunity to fix those problems, and in return creating a safer vehicle. As vehicle safety is of utmost importance, there can be no disadvantages in attempting an event of this nature to find vulnerabilities. The evaluation of such an event would contribute greatly to the existing body of literature as a study exactly like this has not been done. The expected result of this type of hackathon would be the detection of more software security vulnerabilities than previously found, and that would strengthen the notion of adding such an event to the automotive industry. As this study is the setup of such an event, the ground stages for the HoliSec project, it intends to contribute technically by creating a "hackathon package," a collection of artifacts and templates deemed to be useful and important for intent of hacking into the test objects.

VII. CONCLUSION

This study designed artifacts and templates for the setup of a hackathon for the analysis of software security vulnerabilities vehicles in the automotive domain to later be used in the HoliSec project to be completed by the Viktoria Institute. The data was gathered by interviews from Volvo Group, penetration testers and software security experts and were qualitatively analysed by focusing on the challenges of handling software security vulnerabilities and the challenges of setting up a hackathon adapted to the automotive industry.

The results of the study are a "hackathon package," a collection of artifacts and templates to be used in three different stages; pre-hackathon, hackathon, and post-hackathon. A collection we feel has answered our research questions and has also met an industry quality standard for completeness, clarity and usability that we set out to accomplish. Our study has contributed by the joining of two domains, hackathons and the automotive industry.

For future work, we suggest more iterations and evaluations over the artifacts and templates completed in this study. We feel having them evaluated by two companies, with and without automotive industry experience, was very helpful in finding the correct way to design our artifacts and templates. We would suggest that this way of evaluation be continued so the artifacts and templates created can be understood and appreciated by any participants in future events.

ACKNOWLEDGEMENTS

We want to thank our supervisor Eric Knauss for his help and insight in leading us through this process. And we would also like to thank our industry supervisor, Ana Magazinius, for her engagement and helpfulness and for her help in gaining valuable interviews with the correct people and helping focus our direction.

REFERENCES

[1] (2017, March 20). Hackathon - Wikipedia. Available: https://en.wikipedia.org/wiki/Hackathon

[2] M. Bartl, G. Jawecki, and P. Wiegandt, "Co-creation in new product development: conceptual framework and application in the automotive industry," in Conference Proceedings R&D Management Conference–Information, Imagination and Intelligence, Manchester, 2010, vol. 9, pp. 1-9.

[3] (2016, March 23). Connected Car Hackathon Presented by MTC. Available: https://connected-car.devpost.com/

[4] M. Komssi, D. Pichlis, M. Raatikainen, K. Kindström, and J. Järvinen, "What are Hackathons for?," (in English), IEEE Software, vol. 32, no. 5, pp. 60-67, 2015.

[5] K. Koscher et al., "Experimental Security Analysis of a Modern Automobile," in 2010 IEEE Symposium on Security and Privacy, 2010, pp. 447-462.

[6] S. Checkoway et al., "Comprehensive Experimental Analyses of Automotive Attack Surfaces," in USENIX Security Symposium, 2011, pp. 1-16: San Francisco.

[7] T. Bécsi, S. Aradi, and P. Gáspár, "Security issues and vulnerabilities in connected car systems," in 2015 International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS), 2015, pp. 477-482.

[8] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," Black Hat USA, vol. 2015, 2015.

[9] J. Condliffe. (2012, March 20). Chrome Finally Breached in Google's $1 Million Hackathon. Available: http://gizmodo.com/5891508/chrome-finally-breached-in-googles-1-million-hackathon

[10] H. Broberg and L.-O. Berntsson, “HoliSec: Automotive Security and Privacy”.

[11] J. W. Creswell, Research design: Qualitative, quantitative, and mixed methods approaches, 4 ed. California: Sage publications, 2013.

[12] M. Rouse. (2014, April 5). What is hackathon? - Definition from WhatIs.com. Available: http://searchcio.techtarget.com/definition/hackathon

[13] (2017, April 2). Hash Code 2017 by Google. Available: https://hashcode.withgoogle.com/

[14] (2016, April 2). MedHacks 2.0 - The Premier Biotech and Healthcare hackathon at Johns Hopkins University. Available: http://medhacks.org/

[15] (2016, April 5). Re.Hack 2016: Unilever's Annual eCommerce. Available: http://www.hackathon.com/event/rehack-2016--unilevers-annual-ecommerce-hackathon-25351899213

[16] D. Klinedinst and C. King, "On Board Diagnostics: Risks and Vulnerabilities of the Connected Vehicle," Carnegie Mellon University Software Engineering Institute-CERT Coordination Center, Urbana-Champaign, ILMarch 2016 2016.

[17] T. News. (2015, April 8). Mercedes-Benz Research hosting automotive Hackathon: Hack with the best | Telematics Wire. Available: http://telematicswire.net/mercedes-benz-research-hosting-automotive-hackathon-hack-with-the-best/

[18] A. Greenberg. (2016, March 22). GM Asks Friendly Hackers to Report Its Cars’ Security Flaws. Available: https://www.wired.com/2016/01/gm-asks-friendly-hackers-to-report-its-cars-security-flaws/

[19] (2016, March 23). Car Hacking Village. Available: http://www.carhackingvillage.com/

[20] (2016, March 23). Black Hat USA 2016. Available: https://www.blackhat.com/us-16/training/car-hacking-hands-on.html

[21] (2017, March 25). 2017 SAE Battelle CyberAuto Challenge - Events - SAE International. Available: http://www.sae.org/events/cyberauto/

[22] (2015, April 8). Hack The Drive. Available: http://hackthedrive.com

[23] (2017, April 8). CAN bus - Wikipedia. Available: https://en.wikipedia.org/wiki/CAN_bus

[24] H. Yu and C. W. Lin, "Security concerns for automotive communication and software architecture," in 2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2016, pp. 600-603.

[25] S. Parkinson, P. Ward, K. Wilson, and J. Miller, "Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges," (in English), IEEE Transactions on Intelligent Transportation Systems, vol. PP, no. 99, pp. 1-18, 2017.

[26] R. H. Von Alan, S. T. March, J. Park, and S. Ram, "Design science in information systems research," (in English), MIS quarterly, vol. 28, no. 1, pp. 75-105, 2004.

[27] P. J. vanStrien, "Towards a methodology of psychological practice - The regulative cycle," (in English), *Theory & Psychology*, vol. 7, no. 5, pp. 683-700, 1997.

Appendix A
Industry Interview Guide – Volvo Group

- Can you explain the concerns within the industry concerning security vulnerabilities with connected vehicles and the difficulties of handling these vulnerabilities?
- The HoliSec project will attempt to do something that has not been completed before, what about the idea of a hacking event resonated with your company?
- Why did you decide to take part?
- What, if any, do you see as the challenges for the setup of such an event?
- The participants of this event, is it thought that they will be in teams or as individuals or a mix? Will those invited to this event have different domains of knowledge?
- Will everything be open to hacking or will there be restricted areas?
- What results are you expecting once this project concludes? If successful, could there be a plan to take the results and create a new way of working in-house in detecting these vulnerabilities?
- Do you think it would become a re-occurring event within Volvo Group if it does prove to be successful?

Appendix B
Non-industry Interview Guide

- What is your experience with hackathons?
- What has been your involvement in hackathons; participation, setup?
- In creating and setting up a hackathon event, what pieces would you say were important? The most significant?
- What are difficulties that come with setting up and executing a hackathon?
- For an automotive hackathon, hacking into a vehicle, what would you expect to be difficulties in the setting up and executing this type of hackathon?
- What sort of artifacts would you deem necessary in setting up and execution of a hackathon?

Appendix C
Artifact and Template Evaluation Questions

Invitation:

Is this invitation clear to the subject matter and purpose of the event?

Advertisement plan:

Are the channels of advertisement and marketing correct and sufficient?

Does the timeline cover the complete event, from beginning to end?

Application form:

Is the form clear and concise?

Is there any information that should be added?

Non-disclosure agreement:

Do the contents of the agreement cover a general perspective for hackathons?

Technical specifications:

Are these specifications sufficient for gaining a base understanding of the test object?

Guidelines:

Are the guidelines appropriate for the event?

Schedule:

Is the schedule sufficient?

Are the experts' times sufficient?

Security vulnerabilities report:

Is this a proper way to report vulnerabilities?

Exit survey:

Are these questions valid in evaluating the experience of the participants?

Overall impression:

Do these artifacts create a good foundation to run an automotive hackathon?

Other feedback: