WPI

CS 4404 - Network Security

Mission 2 (25 points)
Launched: Thursday, Nov. 10, 2022
Due: Monday, Nov. 28, 2022 at 11:59:00pm

Mission 2: Is Multi-factor a Non-Factor?

Security researchers have long expressed concern about the authentication process associated with the ubiquitous username and password method. These researchers have expressed concern about easily guessed passwords, reused passwords, and even password sharing. Some have speculated that the only good thing about the approach is that it's easy to prompt users to enter the information.

There has recently been a movement to implement multi-factor authentication in which end-users must present multiple pieces of evidence in order to authenticate successfully. Importantly, these "factors" must be different: simply providing two different passwords to login does not suffice. Typically, factors boil down into the following categories:

- What you know (e.g., passwords, passcodes, secret answers)
- What you have (e.g., piece of hardware, particular computing device)
- What you are (e.g., biometrics, voice/face recognition)
- Where you are (e.g., using GPS or wireless beaconing)
- When you are (e.g., time constraints for access patterns)

While multi-factor authentication can be useful, the details really matter in security. We have examples where biometrics have been easily forged (e.g., using photographs) and hardware has been compromised (e.g., poorly seeded random-number generators on hardware tokens). In this mission, we will explore what multi-factor has to offer and what makes an approach robust or weak.

Reconnaissance Phase

In the reconnaissance phase, our mission is to demonstrate mastery of the following concepts:

- **Three different factors:** The team must explore three different factors of authentication, excluding the "what you know" factor since password limitations are pretty intuitive and obvious. One of these factors must include secret codes sent to a phone via short message service (SMS). The team must identify the security goal associated with these factors. The team must describe what assumptions each factor makes and what happens if that assumption does not hold.
- **Three different failures:** For each of the three factors chosen, the team must cite and describe examples of how the a high-profile implementation of the factor failed. Media articles can be a great start while CVE entries[1] are great for understanding the vulnerability background. As an example, for the SMS codes, teams might want to look at how attackers might be able to gain access to the codes via SIM swapping/cloning/hijacking or number porting.
- **Three different successes:** For each of the three factors, provide an example of the factor's use that seems to be pretty robust and effective today. Describe what controls and countermeasures allow the implementation to be effective. If the approach is only a partially success, describe the setting where the factor works well and where it is weak.

In performing reconnaissance, the team should show that they have multiple credible sources that support their conclusions. After all, the team itself must be resilient against misinformation attacks.

[1] Consult further: `https://cve.mitre.org/`

Infrastructure Building Phase

Having studied multi-factor authentication, the team should study one of the more interesting factors in detail. To do so, the team will implement a playground to explore how an attack on the factor would work and how to implement controls that would prevent the attacks from succeeding. Ideally, students would choose one of the failure scenarios from the reconnaissance review and implement it as faithfully as possible. Then, the students would attack the factor (described in the attack phase, which is the next section) and then try to prevent future such attacks (in the defense phase), possibly using insight gained from a successful scenario in the reconnaissance section.

The teaching staff is providing virtual machines on the isolated computer network in the Zoo lab. There are a few purposes for this: 1) it provides a safe space to experiment with attacks without worry of affecting others, 2) having multiple "machines" sometimes makes it easier to debug things (e.g., running `tcpdump` on each), and 3) it provides a standard platform for grading. Remember, any infrastructure building must be easily replicated with step-by-step instructions and copies of any configuration files or details (e.g., "change the IP address in line 17 of file X to A.B.C.D"). Students can easily reformat one of the provided VMs and run through the instructions step-by-step to confirm they are complete.

Naturally, the infrastructure building phase provides the foundation for the remainder of the project. Before assembling the infrastructure, the team will need to plan what will happen in the attack and defense phases. The team should build a minimal implementation of the system that includes all the key components needed for implementing and demonstrating the attack and the defense. This is a "tools and techniques" class, so the team should feel free to make use of freely available existing tools in building the infrastructure.

> **Helpful Hint:** Before continuing, the team should read the rubric that is common to all the missions. The missions in this class provide students with significant latitude to choose what they want to learn, what tools they want to use, and how to structure their projects. As a result, the rubric focuses on the extent to which the student teams can demonstrate independent learning and topic mastery through the mission, rather than the coverage of particular technical topics. This freedom is meant to encourage students to explore a topic they care about, but the lack of detail can also seem daunting. The final section of this document provides some guidance on how to scope a mission.

Attack Phase

Students should select at least one network-based attack from the reconnaissance phase and consider how to implement it. The attack must have a significant impact on the authentication system. For logistical reasons surrounding shared infrastructure, the chosen attack must not be a resource exhaustion attack (e.g., anything that saturates the network, memory, or computational resources of the involved systems).

Students should avoid trivial attacks that exploit application vulnerabilities that the students themselves introduce. For example, an SQL injection attack in which the students create an application vulnerable to SQL injection is considered trivial. Part of the scoring for the attack phase is realism, ambition, and degree of learning.

Students must provide the necessary details of the configuration setup, the attack itself, and results needed for a reviewer to know the attack is real, to replicate the experiment, and to validate the results in the Mission Debriefing Report. The attack should have measurable, quantifiable outcomes and an indication of the resources needed to launch the attack. Consider the Mission Debriefing Report the team's only opportunity to provide evidence to convince the a deployer of the authentication factor that there is a legitimate concern.

Defense Phase

After completing the attack phase, the students must create a proposed defense against the attack. The defense should be effective and realistic for deployment. For example, while DNA testing may be useful

for ensuring a user's identity, it is probably unrealistic; it would likely yield significant backlash from the employees and would be too expensive (and slow) for an organization to implement. The description of any defense should include a discussion on feasibility and costs: what will the organization have to do, what resources are required, and why is it reasonable to assume those resources are available?

Students should demonstrate that the defense successfully mitigates the attack. They must provide all details of the defense, including any tools and configuration changes, along with log evidence demonstrating the attack was blocked. The defense should allow the team to demonstrate significant learning of new knowledge and/or ingenuity. A correct but trivial defense may not earn many points according to the grading rubric.

Mission Debriefing Report

The Mission Debriefing Report is the team's opportunity to explain the identified security goals and attack vectors in the authentication infrastructure, including all the results from the reconnaissance phase. The report should then focus on a single network-based attack and demonstrate the negative consequences of not addressing the vulnerability the attack exploits. The report should then provide a feasible solution to defend the infrastructure.

The Mission Debriefing Report should be comprehensive and provide conclusive supporting evidence. It is likely that such a report will be at least five pages of write-up and any figures, followed by an appendix of supporting evidence (e.g., screenshots, output of terminal windows, log file output). In addition to the write-up, the debriefing report should include additional supporting files, such as source code or configuration files. For the report to be scientifically valid, enough detail must be provided that would enable the grader or another member of the class to create and run the experiment without the need to ask questions.

Mission Rubric

The mission score can be broken down into five components, each of which are scored independently. The total score is out of 25 points. The following are the components:

1. Reconnaissance: 4 points
2. Infrastructure Building: 5 points
3. Attack: 5 points
4. Defense: 5 points
5. Mission Debriefing: 6 points

When working together, teams are required to evaluate their partners. While no additional credit is awarded for completion of these evaluations, a **3 point penalty** will be assessed to the project grade for any student working in a team who fails to complete a project partner evaluation.

We now describe each of the project components and how they are graded.

Reconnaissance: 4 points

Rubric:

- 4 points: The team has identified a comprehensive set of security goals for the targeted system. Each security goal is described in detail and the impact of not achieving the security goal is clearly stated. The description includes at least one realistic attack vector for each security goal. The countermeasures for each attack vector are likely to be effective and realistic to deploy.
- 3 points: The reconnaissance phase is generally good, but a key security goal may be missing. Alternatively, one or more security goals is not described in sufficient detail or the attack vectors or countermeasures are not fully developed or are unrealistic. This score reflects solid work with relatively minor deficiencies.
- 2 point: The reconnaissance phase omits two or more key security goals. Alternatively, multiple security goals lack detail or attack vectors or countermeasures are poorly formulated or unrealistic. This score reflects work with moderate deficiencies.
- 0 points or 1 point: The reconnaissance phase has significant limitations. The work does not demonstrate a comprehensive review of the problem or the analysis is severely flawed.

Infrastructure Building: 5 points

Rubric:

- 5 points: The infrastructure is realistic and appropriate for the scenario evaluated. The details of the design are obvious with clear configuration files and step-by-step instruction on how the team built the infrastructure. An independent party would clearly be able to follow these instructions to quickly replicate the experimental setup. There is clear evidence that the team learned how to use the provided infrastructure and gave serious consideration into the best configuration that would enable a clear demonstration of the attack and its defense.
- 4 points: The infrastructure setup is generally good, but some details may be missing or some steps in the instructions may have minor errors. With some problem-solving efforts and additional time, an independent party would likely be able to replicate a close approximation of the experimental setup. The team used the provided infrastructure and designed a configuration that adequately enables a demonstration of an attack and defense.

- 3 points: The infrastructure setup has flaws or significant omissions in its instructions or design documentation. An independent party would have trouble recreating the experimental setup. The team used the provided infrastructure, but the configuration limits the effectiveness of an attack or defense demonstration.
- 2 points: The infrastructure setup is flawed and/or is inadequately described to allow replication. The team deviated from the provided infrastructure or the application of the infrastructure has the potential to undermine the validity of the attack or defense experiments.
- 0 points or 1 point: The infrastructure setup has severe flaws that greatly undermine its utility.

Attack: 5 points

Rubric:

- 5 points: The team identifies a realistic, high-impact attack vector. The attack is implemented flawlessly and the description of the attack and its supporting documentation allows an independent party to replicate the attack. The documentation provides evidence that conclusively shows that the team mounted the attack and that the attack was successful. To earn this score, the attack and/or the implementation of the attack must demonstrate significant independent learning or creative thinking by the team. The attack must be sufficiently complex that the students needed to invent or configure existing tools to effectively launch it.
- 4 points: The team identifies a realistic attack vector. The attack is implemented well and the supporting documentation is solid, but may be missing minor details that are needed to replicate the attack. The supporting documentation generally shows the attack was implemented and was likely successful. The attack showed that the students learned about a new way to launch an attack, but the team may have used an obvious or straightforward methodology to launch the attack.
- 3 points: The team identifies an attack vector, but it may be low impact or may be less realistic. The attack implementation or its supporting documentation may have small flaws. The supporting evidence suggests the attack was implemented and may have been effective, but the support is not conclusive. The attack itself may not have been sophisticated or provided significant learning opportunities for students.
- 2 points: The students identified an attack vector, but it may be low impact or unrealistic. The supporting documentation or evidence of the attack is lacking. The attack itself is trivial and there is little evidence the students learned much from the exercise.
- 0 points or 1 point: The attack has severe flaws that greatly undermine its utility.

Defense: 5 points

Rubric:

- 5 points: The team identifies a realistic, high-impact defense. The defense is implemented flawlessly and the description of the defense and its supporting documentation allows an independent party to replicate the defense. The documentation provides evidence that conclusively shows that the team mounted an effective attack and that the defense prevented the attack from being successful. To earn this score, the defensive approach and/or the implementation of the defense must demonstrate significant independent learning or creative thinking by the team. The defense must be sufficiently complex that the students needed to invent or configure existing tools to effectively deploy it.
- 4 points: The team identifies a realistic defensive strategy. The defense is implemented well and the supporting documentation is solid, but may be missing minor details that are needed to replicate the defense. The supporting documentation generally shows the defense was implemented and was likely

successful. The defense showed that the students learned about a new way to protect a system, but the team may have used an obvious or straightforward methodology to deploy the defense.

- 3 points: The team identifies a defensive strategy, but it may be low impact or may be less realistic. The defense implementation or its supporting documentation may have small flaws. The supporting evidence suggests the defense was implemented and may have been effective, but the support is not conclusive. The defense itself may not have been sophisticated or provided significant learning opportunities for students.
- 2 points: The students identified a defensive strategy, but it may be low impact or unrealistic. The supporting documentation or evidence of the defense is lacking. The defense itself is trivial and there is little evidence the students learned much from the exercise.
- 0 points or 1 point: The defense has severe flaws that greatly undermine its utility.

Mission Debriefing Document: 6 points

The mission debriefing document includes the write-up associated with the reconnaissance, attack, and defense. The primary grading of those sections are described above. The mission debriefing document includes overall communication strategy, organization of the information, and interpretation of the data. It also includes supporting appendices and related files.

Rubric:

- 6 points: The report has an introduction and a conclusion section that clearly explain the scenario being evaluated, its importance, the key components that require evaluation, and the results of the specific attack and defense the team evaluated. The report makes use of figures or tables where appropriate to succinctly inform the reader of results. Key supporting information is placed in an easy to read appendix to the report. Additional files are clearly labeled and easy to understand. A README file is provided describing each of the supporting files. All tools are described and the mechanism to obtain the tools (e.g., URLs, relevant repository names) are provided. Where necessary, appropriate academic or technical sources are referenced and cited. The document is compelling, accurate, and leaves little doubt about the attack, defense, and recommendations.
- 5 points: The report has an adequate introduction and conclusion that describe the scenario, its importance, key components, and results. The report is understandable and makes the appropriate points, but the presentation may be suboptimal. The appendix contains supporting information but may have only basic explanation or description of the information. All the supporting files and evidence are included, but it may take extra time to locate. The tools are described, but information on how to obtain them may be missing in some cases. Some academic and technical sources are cited, but there may be instances in which additional citations would be useful. The document is accurate and descriptive, but the document may not be as convincing due to writing limitations or insufficient evidence.
- 4 point: The report has some flaws or omits some of the important points described above. The report may be unclear or unconvincing in places and supporting evidence may be missing, hard to find, or inconclusive. The report is generally accurate, but with apparent flaws or omissions.
- 0-3 points: The report has deficiencies that hinder understanding, omits important data, or provides inadequate support. One of the report sections may be missing or incomplete.