Poster: The Petri Dish Attack - Guessing Secrets Based on Bacterial Growth

Katharina Krombholz
SBA Research
kkrombholz@sba-research.org

Adrian Dabrowski
SBA Research
adabrowski@sba-research.org

Peter Purgathofer
TU Wien
purg@igw.tuwien.ac.at

Edgar Weippl
SBA Research
eweippl@sba-research.org

***Abstract*—PINs and unlock patterns remain by far the most common knowledge-based authentication methods on mobile devices. Biometric authentication methods such as fingerprints also rely on PINs and unlock patterns as fallback methods. In recent years, several attacks on knowledge-based mobile authentication have been presented, e.g., shoulder-surfing [1], smudge attacks [2] and thermal attacks [3]. In this poster, we present the *Petri dish attack*, a novel attack to guess secrets based on bacterial growth. We conducted a series of lab experiments with 20 Petri dishes to evaluate the feasibility of this new attack and unfortunately were not able to successfully conduct the attack on off-the-shelf smartphones. However, we still believe that our results are valuable to the scientific community and provide a baseline to explore future cross-domain attack vectors and interdisciplinary approaches on smartphone security.**

1. Concept and Threat Model

In recent years, several attack scenarios based on human traces left on smartphone touchscreens have been presented, e.g., smudge attacks [2] and thermal attacks [3]. The common threat model behind these attacks is that the user leaves their smartphone unattended after a successful authentication session. Thermal attacks require a short period of time between the completion of a successful authentication session and the execution of the attack, as thermal traces are highly volatile. Hence, their feasibility in practice is rather limited. In contrast, smudge attacks can be highly successful after a longer period of time assuming that the screen has not been (intentionally or unintentionally) wiped before the attack.

Our Petri dish attack follows a similar threat model: if a smartphone is left unattended the attacker can create a germ imprint on a previously prepared Petri dish with an agar-based growth medium which is often used to foster growth of Escherichia coli (E.coli), one of the most common type of bacteria found on human hands. Then, the attacker immediately closes the lid after creating the germ imprint and stores the dish in an incubator at 37°C to foster bacterial growth. After the colonies have spread, the attacker looks at the dish and uses the visual cues left by the spread bacteria colonies to guess the previously input secret.

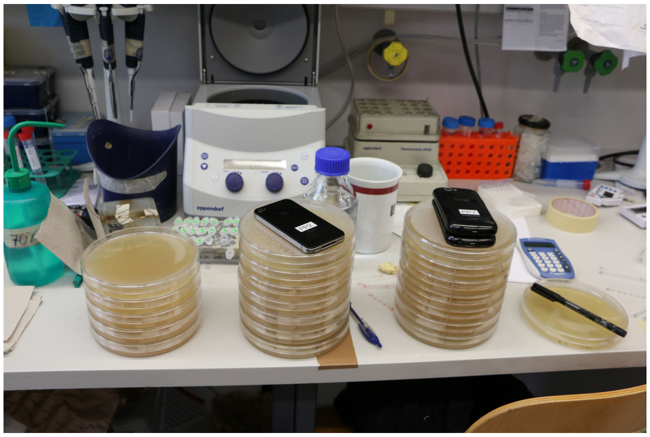


Figure 1. The study setup.

2. Lab Study

To evaluate the feasibility of the Petri dish attack, we conducted a series of experiments at the Max Perutz Laboratories in Vienna. We used 20 Petri dishes with a previously prepared fertile soil optimized for E.coli bacteria which is one of the most commonly found type of bacteria on human hands and hence often left on surfaces that we frequently touch in our everyday lives. We furthermore used an iPhone 4 and a Galaxy S2 and an additional iPhone 4 and Galaxy S2 with a screen protector. Figure 1 shows how we conducted the experiments.

We tested both PINs (4-digit sequences) and unlock patterns and furthermore tested the authentication schemes on a regular screen which was not previously cleaned, a screen that was previously wiped off with clothing tissue before the PIN/pattern was entered, and a screen that was previously disinfected with Ethanol before the PIN/pattern was entered. Each of these combinations of conditions was tested on a screen with and without a protective cover.

After the germ imprint was made, we immediately closed the lid of the respective Petri dish. All Petri dishes were stored in an incubator at 37°C for 25 hours. The dishes were incubated upside-down to reduce the risk of contamination from airborne particles settling on them and to furthermore prevent water condensation that may disturb or compromise bacterial growth. After 25 hours, most Petri

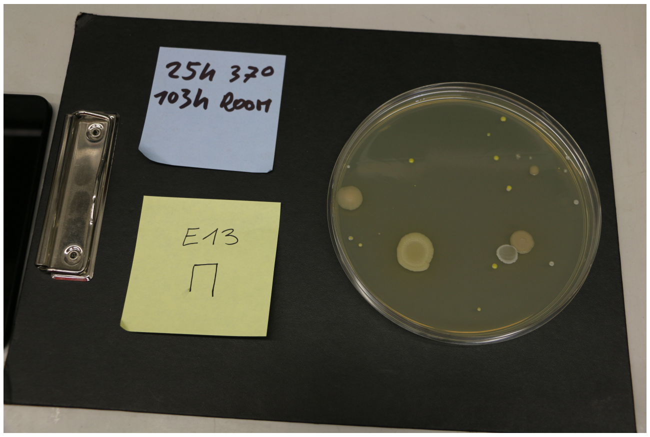


Figure 2. The entered unlock pattern had the shape of a Greek capital letter 'Π'. The screen had no protective cover and was previously wiped.

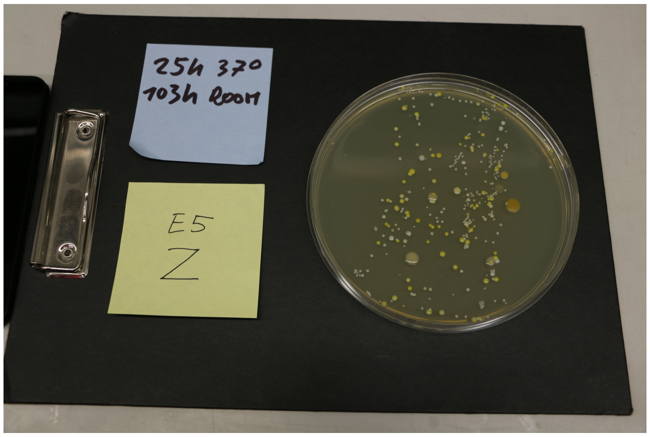


Figure 3. The entered unlock pattern had the shape of a Latin capital letter 'Z'. The screen had no protective cover and was not previously wiped.

dishes had visible colonies of bacteria and yeast on them. All dishes were photographed for subsequent analysis. After another 103 hours at room temperature, the colonies have significantly spread and the dishes were again photographed. Finally, all photographs have been analyzed regarding their potential to guess the secrets. To our surprise, no germ imprint provided sufficient visual cues to guess a secret regardless of the studied condition. Figure 2, Figure 3, and Figure 4 show selected results after 25 hours in the incubator and 103 hours at room temperature.

3. Discussion

To our surprise, not even the germ imprint from a previously disinfected screen had enough visual cues to guess the secret after a successful authentication session. Due to the supervision of lab assistants we made sure that our experiments were conducted in line with the standards of biologists. In order to understand reasons behind these results, we asked the lab personnel to audit our germ imprints and discussed the results with them. We conclude that the E.coli bacteria on our hands do not leave sufficient traces on the surface of a screen to successfully guess a previously input secret. The bacteria and yeast colonies that spread on the fertile soil were arbitrary.

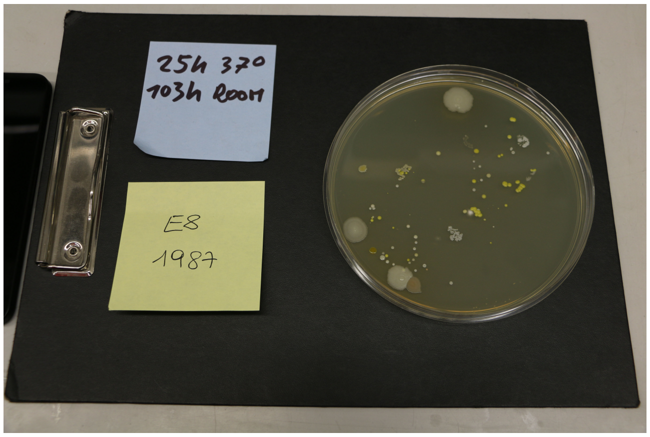


Figure 4. The entered PIN was '1987'. The screen was not previously wiped.

4. Conclusion

In this poster, we presented the *Petri dish attack*, a new type of attack to guess a secret based on visual cues from bacterial growth. We conducted a series of lab experiments. Our results suggest that the Petri dish attack is not feasible under the studied conditions as human hands do not leave sufficient traces of E.coli on smartphone touchscreens. Irrespective of the negative results, we propose to further investigate how human traces left during the authentication process can be used to guess secrets.

Acknowledgments

We would like to thank Verena Jantsch and her team of PhD students and postdoctoral researchers at the Max Perutz Laboratories in Vienna for providing their lab space and materials to us. Without their help in conducting the experiments, this poster would not have been possible. This research was partially funded by COMET K1 and Bildungskarenz (AMS).

References

[1] M. Eiband, M. Khamis, E. von Zezschwitz, H. Hussmann, and F. Alt, "Understanding Shoulder Surfing in the Wild: Stories from Users and Observers," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, 2017, pp. 4254–4265.

[2] A. J. Aviv, K. L. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge attacks on smartphone touch screens." *WOOT*, vol. 10, pp. 1–7, 2010.

[3] Y. Abdelrahman, M. Khamis, S. Schneegass, and F. Alt, "Stay cool! Understanding Thermal Attacks on Mobile-based User Authentication," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, 2017, pp. 3751–3763.

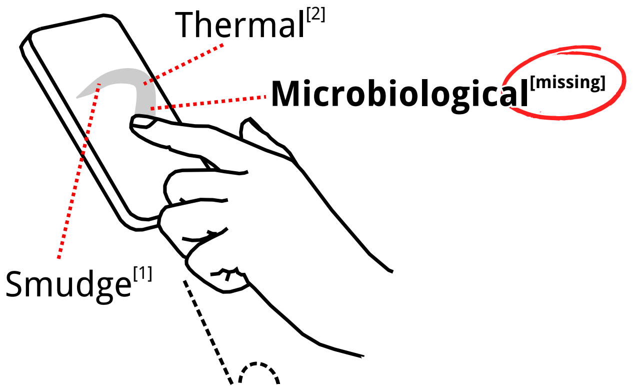
The Petri Dish Attack
Guessing Secrets Based on Bacterial Growth

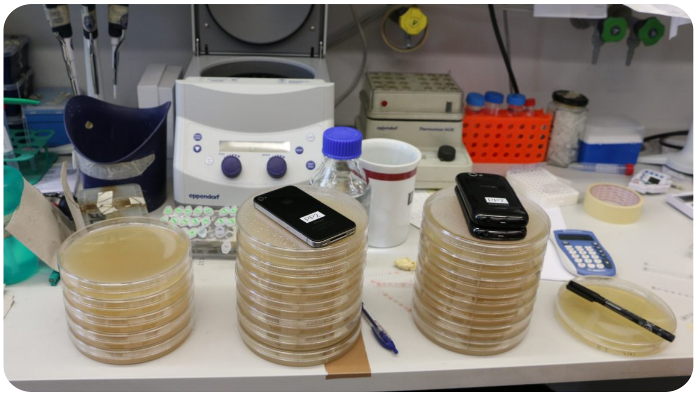
Katharina Krombholz
SBA Research

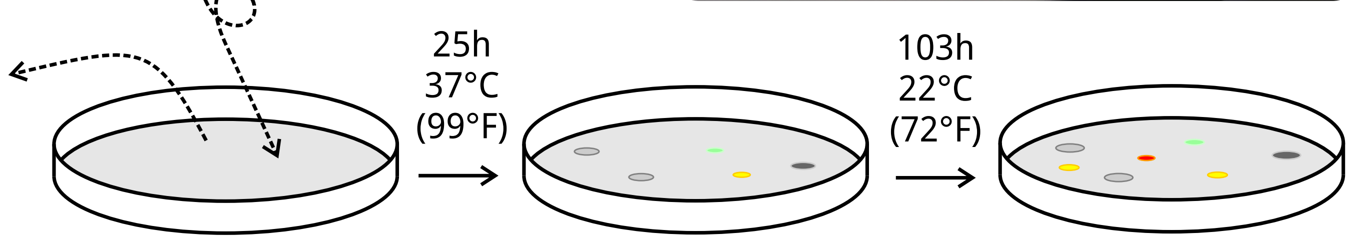
Adrian Dabrowski
SBA Research

Peter Purgathofer
TU Wien

Edgar Weippl
SBA Research







Study Setup

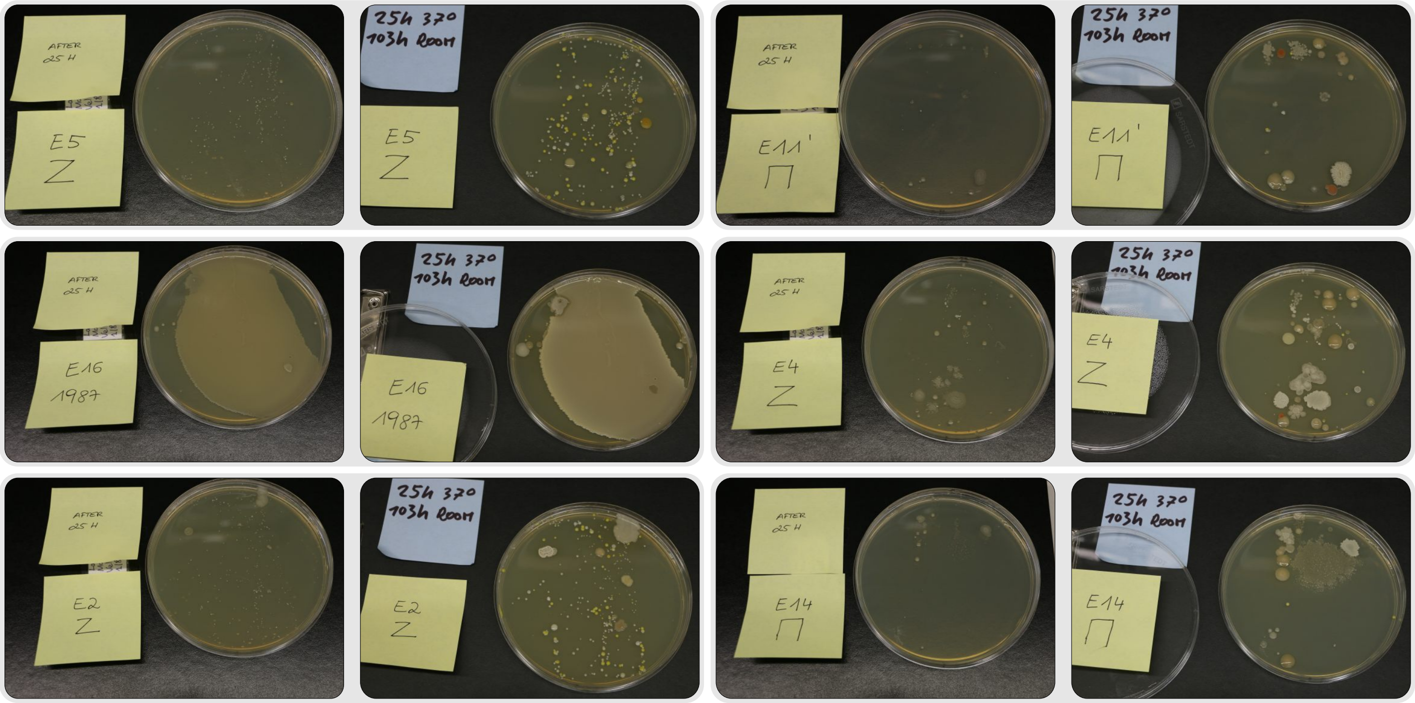
- two iPhone 4 and two Galaxy S2
- 20 Petri dishes
- fertile soil favouring E.coli

Conditions

- w/ and w/o screen protector film
- multiple PINs and unlock patterns
- w/ and w/o prior cleaning
- w/ and w/o desinfection

Conclusion

Not enough E.coli are transferred to provide sufficient visual clues to guess a secret.



Legend for examples above: **E5** Galaxy S2, pattern, not wiped; **E16** iPhone w/ film, pin, not wiped; **E2** Galaxy S2, pattern, not wiped; **E11** iPhone w/ film, desinfected; **E4** iPhone w/ film, desinfected; **E14** iPhone, desinfected

[1] A. J. Aviv, K. L. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge Attacks on Smartphone Touch Screens.", Usenix WOOT 2010.
[2] Y. Abdelrahman, M. Khamis, S. Schneegass, and F. Alt, "Stay Cool! Understanding Thermal Attacks on Mobile-based User Authentication", CHI 2017, ACM