Poster: On the Usability of Secure GUIs

Atanas Filyanov[1], Aysegül Nas[1], Melanie Volkamer[2], Marcel Winandy[1]

[1] Horst Görtz Institute for IT-Security, Ruhr-University Bochum, Germany

[2] Dpmt. of Computer Science, Technische Universität Darmstadt, Germany

{atanas.filyanov, ayseguel.nas, marcel.winandy}@trust.rub.de, melanie.volkamer@cased.de

1. INTRODUCTION

We use commodity computing platforms for many tasks, including entering or editing sensitive data on them. Unfortunately, the graphical user interfaces (GUI) running on these devices are not designed to provide a secure means of ensuring users that they are interacting with the authentic application and not with some fake one. These design weaknesses are often exploited by adversaries. They try to steal security sensitive data by tricking users to enter such data into "authentic"-looking applications.

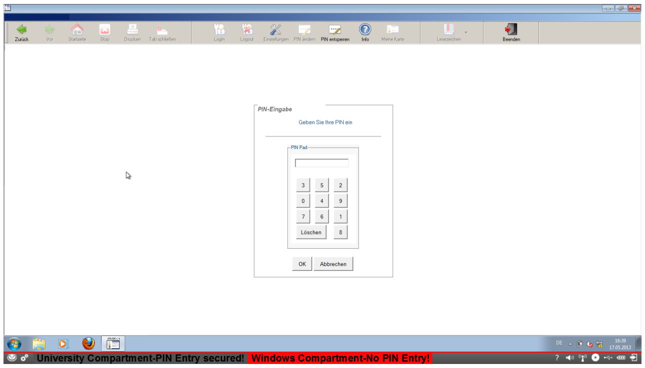
Secure GUIs have been proposed as a solution to this problem, e.g., [2, 6, 4], and few commercial secure operating systems employ these concepts, e.g., [3]. The main idea is that a trusted part of the operating system controls what is displayed on the screen, and the user is always able to invoke a trusted path to this part. Most of the secure GUI proposals include a reserved area on the screen that is used to display information about which application is currently having the input/output focus of the user and what type of security or trustworthiness this application has (e.g., trusted/untrusted or confidential/secret/topsecret). The reserved area in the proposed secure GUI implementations is usually a top- or bottom-screen status bar, e.g., [3].

Obviously, it is very important that users know the meaning of the reserved area of secure GUIs, perceive the information in it, and only edit or enter sensitive data if the authentic application with the corresponding sensitivity level is enabled. A potential drawback of existing secure GUI implementations is that such indicators are passive ones – i.e., the system does not actively prevent (because it is technically not possible to do so) the user from entering sensitive data in any untrusted application – and it is already known from previous research in usable security [1, 5, 7, 8] that passive indicators do not provide effective protection against attacks in the web browser context. However, we want to find out whether passive security indicators can still have a meaning in the context of Secure GUIs.

While existing proposals [2, 6, 4, 3] provide strong security guarantees from a technical point of view, none of them has been evaluated with respect to the effective protection for the average users. Thus, it is not known whether any of them provides an effective protection.

2. OUR USABILITY STUDY

With our research we try to shed light in this situation. We study two different approaches to display the reserved area as trusted status bar: one on the top of the screen and one on the bottom (see Figure 1), as these are the most common places for status bars in the default settings of most of the operating systems (note that the trusted status bar is different and in addition to the normal status bar of, e.g., Windows operating system). The approaches we evaluated support four different virtual machines (here called compartments) while for the user study only two were started – a standard Windows (the Windows compartment) and a secure compartment for privacy sensible university services (the university compartment). Note, the authentic university services are not reachable from the first compartment and no other web services than the ones provided by the university can be accessed from the university compartment. This research is part of a project at our university to improve the functionality and the usability of an existing security-enhanced operating system with secure GUI implementation. As part of this project 130 students from different departments received laptops running this secure GUI implementation when agreeing to help improving both; e.g. by providing feedback and participating in user studies. In the first phase of the project, we improved the design of the status bar with respect to the colors and the labels used for the different compartments throughout pre-tests and an online survey before. These were evaluated in the user study.



Geben Sie Ihre PIN ein

University Compartment-PIN Entry secured! Windows Compartment-No PIN Entry!

Figure 1: Secure GUI status bar (at the bottom) indicating the current active compartment

In the second phase, we evaluated the same status bar once being displayed at the top and once at the bottom of the display by conducting a lab user study in order to answer the following *research question*: How likely do participants select the proper compartment with the two different secure GUI implementations. *The user study consists of the following parts:*

- The students were welcomed and received the instructions including the overall scenario (job application) and the corresponding tasks to be conducted.
- The students solved four tasks on a test laptop (it was not possible to use their laptop as the new interfaces was not yet been deployed). The study conductor took notes about successful and failed tasks.
- After every task, each participant evaluated it, by answering questions on a second laptop. Note, the reason for using a second laptop was to have time to adjust the test laptop unnoticed between two tasks.
- The students filled out a questionnaire about their demographics and they were asked to not reveal any information about the study.

We included two uncritical tasks (one that was possible in both compartments and one that was only possible to execute in the Windows compartment) and two tasks for which it was necessary to enter the student ID and the corresponding PIN (for both tasks the university compartment must be used). The participants used their own student credentials. In more detail, the *tasks* are the following:

- **Task 1** (Search in local net) The participants were asked to check whether any foreign language courses are offered at the university in the next semester. (*Proper Execution:* As the corresponding page is provided by our university any of the two compartments can be used to properly execute this task.)
- **Task 2** (PIN entry w/o attack) Afterwards, the participants were asked to download their recent transcript of records from the university server. (*Proper Execution:* The participant uses the university compartment.)
- **Task 3** (Search in Internet) Next, we ask the participants to search for a photo studio in order to get a professional photos for their CVs. (*Proper Execution:* The participant uses the Windows compartment.)
- **Task 4** (PIN entry w/ attack) We ask the participants to download their matriculation certificate to include it in the application. (*Proper Execution:* The participant uses the university compartment. Note, this task was more difficult than task 2 because we launched unnoticed a fake university application in the Windows compartment while they answered the survey at the second laptop.)

With these tasks we can check whether participants switch from the Windows compartment to the university compartment before entering their PIN (task 2 and 4) and whether they switch from the university compartment to the Windows compartment for a search on the Internet (task 3). We can also check whether they switch from the Windows compartment to the university compartment before entering their PIN although the Windows compartment provides a (fake) university application (task 4).

Ethical requirements for research involving human participants are provided by an ethics commission at the university. The relevant ethical requirements (participant consent and data privacy) were met.

3. RESULTS

26 of these students participated in our lab study, 13 in each of the two groups. The group with the status bar displayed at the top of the screen is in the following called Group-Top and the one with the status bar displayed at the bottom is called Group-Bottom. They were randomly selected while being a representative sample of the 130 students who received a laptop. Four people selected the university compartment from the beginning until the end of the test, hence we excluded them from the following evaluation.

Our results show that the status bar, independent from being displayed at the top or the bottom of the screen, enables participants to select the proper compartment in two of three cases: For task 2 (PIN entry w/o attack) in Group-Top 11 out of 12 and in Group-Bottom 9 out of 10 switched from the Windows compartment to the university compartment. For task 3 (Search in Internet) in Group-Top 11 out of 12 and in Group-Bottom 10 out of 10 switched from the university compartment to the Windows compartment. However, in task 4 (PIN entry w/ attack), only 5 out of 12 (Group-Top) and 6 out of 10 (Group-Bottom) noticed that the university application in the Windows compartment is not authentic and switched to the university compartment before entering the PIN. Obviously, they have understood the meaning of the different compartment however, the authentic-looking (but faked) university application in the Windows compartment was convincing enough for in total 11 out of 22. Thus, the evaluated status bars do not yet effectively protect users, and future research is necessary.

4. ACKNOWLEDGMENTS

First, second, and last author were partially funded by the German state NRW and supported by the EU Regional Development Fund under the project RUBTrust/MediTrust.

5. REFERENCES

[1] R. Dhamija, J. D. Tygar, and M. Hearst. Why phishing works. In *CHI '06: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 581–590. ACM, 2006.

[2] J. Epstein. A prototype for Trusted X labeling policies. In *Proceedings of the Sixth Annual Computer Security Applications Conference (ACSAC)*, pages 221–230. IEEE, 1990.

[3] G. Faden. Solaris Trusted Extensions: Architectural Overview. Sun Microsystems White Paper, Apr. 2006.

[4] N. Feske and C. Helmuth. A Nitpicker's guide to a minimal-complexity secure GUI. In *Proceedings of the 21st Annual Computer Security Applications Conference*, ACSAC '05, pages 85–94, Washington, DC, USA, 2005. IEEE Computer Society.

[5] S. E. Schechter, R. Dhamija, A. Ozment, and I. Fischer. The emperor's new security indicators. In *Proceedings of the 2007 IEEE Symposium on Security and Privacy*, pages 51–65. IEEE, 2007.

[6] J. S. Shapiro, J. Vanderburgh, E. Northup, and D. Chizmadia. Design of the EROS trusted window system. In *Proceedings of the 13th USENIX Security Symposium*, pages 165–178. USENIX, 2004.

[7] T. Whalen and K. M. Inkpen. Gathering evidence: use of visual security cues in web browsers. In *Proceedings of Graphics Interface 2005*, GI '05, pages 137–144. Canadian Human-Computer Communications Society, 2005.

[8] M. Wu, R. C. Miller, and S. L. Garfinkel. Do security toolbars actually prevent phishing attacks? In *Proc. of the SIGCHI conference on Human Factors in computing systems*, pages 601–610. ACM, 2006.

On the Usability of Secure GUIs

Atanas Filyanov[1], Aysegül Nas[1], Melanie Volkamer[2], Marcel Winandy[1]

[1] System Security Lab, Horst Görtz Institute for IT-Security, Ruhr-University Bochum, Germany

[2] SecUSo, Department of Computer Science, Technische Universität Darmstadt, Germany

Problem Statement

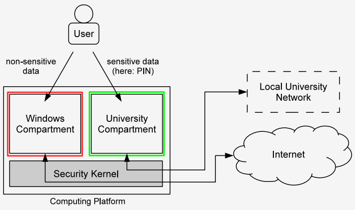
- We input sensitive data on commodity devices daily.
- Device GUI systems do not provide trustworthy assurance about the active application.
- Secure GUIs have been proposed to address this issue.
- Most Secure GUIs use passive indicators on a reserved area of the screen to indicate the trustworthiness of the focused application.
- Passive indicators are proved to be ineffective in the context of web browsers.

Research Questions

- Have passive security indicators a meaning in the context of Secure GUIs?
- Are students in our project more likely to select the proper compartment with the TrustBar (the reserved visual indication area of the screen) at the top of the screen or with the TrustBar at the bottom of the screen?
- Do the participants select the proper compartment when they are presented with a fake (and authentic looking) client in an untrustworthy compartment?

Research Project

- Goal: to develop and evaluate a secure operating system for information flow control and protection of sensitive data.
- 130 students from our university participated in our case study.
- We prepared 130 laptops with our tested system and four compartments (Windows, Linux, University, and Internet), technically virtual machines.
- Each participant received one laptop to work with.



System architecture of our prototype

Compartment overview screen

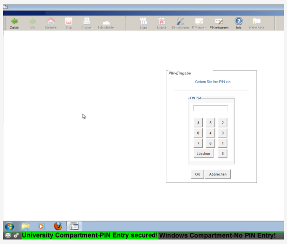
Study Settings

- We conducted a study with a group of 26 out of the 130 participants.
- Each participant used her own student card for PIN entering.
- We provided a test laptop with a modified interface.
- For half of the people the TrustBar was at the top, and for the other, at the bottom of the screen.
- The laptop had Windows and University compartments installed.
- The participants received a scenario and test assignments.
- The participants completed four tasks and filled out a demographics survey.
- The study conductor took notes about successful and failed tasks.

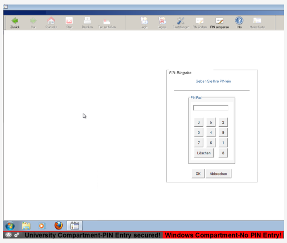
Test setup

Test Assignments

- Task 1: Search for a language course in the local university network. Proper Execution: Each compartment could be used to execute the task.
- Task 2: PIN entry w/o attack . The participant should download a transcript of records. Proper Execution: The university compartment should be used.
- Task 3: Search in Internet: The participant should search for a photo studio. Proper Execution: The participant uses the Windows compartment.
- Task 4: PIN entry w/ attack. The participant should download a matriculation certificate. Note: We started a fake university client in the Windows compartment. Proper Execution: The participant notices the fake client by observing the secure GUI and switches to the university compartment.



University compartment is active
(authentic university client application)



Windows compartment is active
(fake university client application)

Results and Future Work

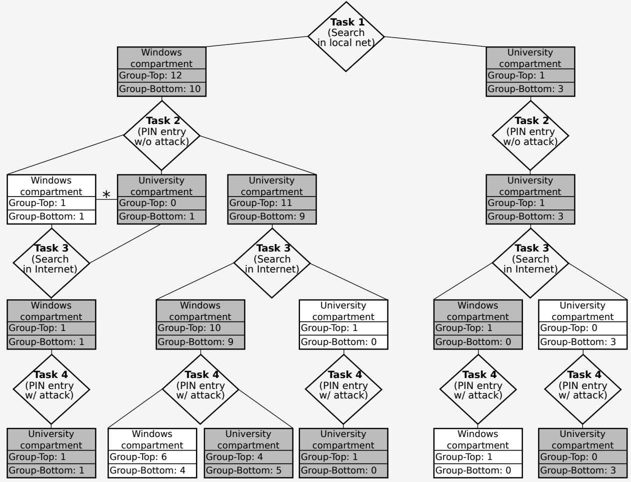
- The table below shows the success rate for the individual tasks.
- When no attack is mounted, success rate is $\geq$ 90%.
- When an attack is present, success rate drops to 50%, which is better than the 10% success rate to detect phishing as known from the literature [1].
- Further target groups are needed for more precise results.

Number of participants who decided to switch to the proper compartment (note that we do not include Task 1 in the results, as it could be done in each compartment):

	Task 2 (PIN entry w/o attack)	Task 3 (Search in Internet)	Task 4 (PIN entry w/ attack)
Group-Top	11 of 12 (91,7%)	11 of 12 (91,7%)	5 of 12 (41,7%)
Group-Bottom	9 of 10 (90%)	10 of 10 (100%)	6 of 10 (60%)
Total	20 of 22 (90,9%)	21 of 22 (95,4%)	11 of 22 (50%)

[1] R. Dhamija, J. D. Tygar, and M. Hearst. Why phishing works. In CHI 06: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pages 581–590. ACM, 2006.

How many participants switched to which compartment after each task:


Task 1 (Search in local net)
Windows compartment Group-Top: 12 Group-Bottom: 10
University compartment Group-Top: 1 Group-Bottom: 3
Task 2 (PIN entry w/o attack)
Task 2 (PIN entry w/o attack)
Windows compartment Group-Top: 1 Group-Bottom: 1
*
University compartment Group-Top: 0 Group-Bottom: 1
University compartment Group-Top: 11 Group-Bottom: 9
University compartment Group-Top: 1 Group-Bottom: 3
Task 3 (Search in Internet)
Task 3 (Search in Internet)
Task 3 (Search in Internet)
Windows compartment Group-Top: 1 Group-Bottom: 1
Windows compartment Group-Top: 10 Group-Bottom: 9
University compartment Group-Top: 1 Group-Bottom: 0
Windows compartment Group-Top: 1 Group-Bottom: 0
University compartment Group-Top: 0 Group-Bottom: 3
Task 4 (PIN entry w/ attack)
Task 4 (PIN entry w/ attack)
Task 4 (PIN entry w/ attack)
Task 4 (PIN entry w/ attack)
Task 4 (PIN entry w/ attack)
University compartment Group-Top: 1 Group-Bottom: 1
Windows compartment Group-Top: 6 Group-Bottom: 4
University compartment Group-Top: 4 Group-Bottom: 5
University compartment Group-Top: 1 Group-Bottom: 0
Windows compartment Group-Top: 1 Group-Bottom: 0
University compartment Group-Top: 0 Group-Bottom: 3

* The participant switched to the university compartment, after she received the error message.

This research was part of the RUBTrust/MediTrust project. http://www.rubtrust-meditrust.de

Project partners: Sirrix AG security technologies RUB

This project was partially funded by: Ziel2.NRW Regionale Wettbewerbsfähigkeit und Beschäftigung; EUROPÄISCHE UNION Investition in unsere Zukunft Europäischer Fonds für regionale Entwicklung; Ministerium für Wirtschaft, Energie, Industrie, Mittelstand und Handwerk des Landes Nordrhein-Westfalen