Broken Access Control (Summary Post)

As I mentioned in my initial post, Broken Access Control is now number 1 on the OWASP Top 10 for 2021. Broken access control is at the top of the list, as the potential impact on the system can be enormous. For example, attackers can easily take over applications with bank data requests or other sensitive data if the system has no access control.

Many faulty access control systems are not problematic for attackers to detect and exploit. Often, all that is required is to search through requests for functions or content that should not be granted. If a vulnerability is discovered, the consequences can be the disclosure of unauthorised content. In addition, an attacker may be able to modify or delete content, perform unauthorised functions, or even take over the management of the entire website. The following updated UML activity diagram demonstrates that, without access control, an attacker can easily destroy the entire system (Onlinesolutionsgroup, 2022).

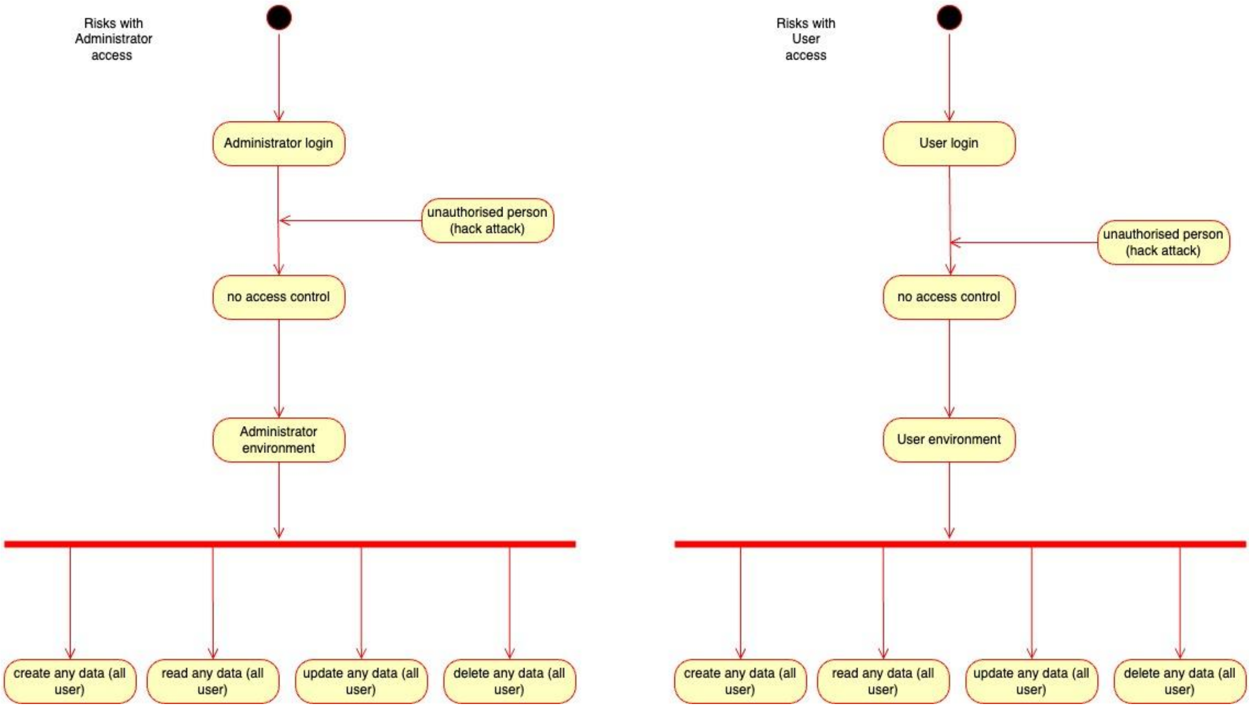
Risks with Administrator access
Administrator login
unauthorised person (hack attack)
no access control
Administrator environment
create any data (all user)
read any data (all user)
update any data (all user)
delete any data (all user)
Risks with User access
User login
unauthorised person (hack attack)
no access control
User environment
create any data (all user)
read any data (all user)
update any data (all user)
delete any data (all user)

Figure 1: Activity Diagram: Activity diagram User vs Administrator Power

There is also a dependency between this category and the "Identification and Authentication Failure" category, which is number 7 of the top 10. As Etkin mentioned, authentication and authorisation go hand in hand, and the vulnerability in one category inevitably affects the other. Thus, the risks of non-authentication should be taken very seriously, and a 100% functioning access control system is required.

To mitigate the risks, proper documentation of authentication from the earliest stages of software development is the key to greater security and, in particular, to greater security in access control. Furthermore, penetration is a valuable method for finding access control risks.

References:

Onlinesolutionsgroup (2022) Broken Access Control. Available from: https://www.onlinesolutionsgroup.de/blog/glossar/b/broken-access-control/ [Accessed 06 October 2022].