Access control is just the start

_AI-generated image. Prompts: giant eye growing out of a tree in front of an office building, urban environment, digital art.

Expert article

_Marc Bütikofer, Head of Innovation Security Solutions, Airlock
_Michael Doujak, Product Manager, Airlock
Ergon Informatik

Published in SMART insights 2023 magazine

When it comes to online business, classic access controls are no longer up to the job. Only continuous adaptive trust creates the flexibility that companies need today, either to increase IT security, or to improve the user experience.

Anyone wanting access to a digital offer must authenticate themselves. Passwords are an important element of every IT security infrastructure, but a password alone is no longer secure enough. That is why multi-factor authentication (MFA) and passkeys have become standard. Smartphones make this approach easier, as they are always to hand and offer user-friendly MFA. The problem is that hackers are increasingly using methods that do not take effect until the user has successfully cleared the MFA hurdle.

One-time access authorisation no longer enough

Risk-based authentication is one way of dealing with this, as it keeps login processes secure and offers maximum user-friendliness. A variety of signals are used to judge whether or not an authentication attempt is plausible. Those signals might be the IP address or the access location. Risk-based authentication only works during the login, however. It doesn't protect against attacks while an online session is in progress. It doesn't offer adequate protection against man-in-the-middle attacks either, in which a hacker sneaks unnoticed into the communication between two or more parties. The answer here is continuous adaptive trust (CAT), as Gartner calls the principle. Rather than just during login, risk analysis is happening all the time. Artificial intelligence can help here. Machine learning is a good way of picking up anomalies in behaviour while a session is running.

“Continuous adaptive trust is a paradigm shift in IT security.”
_Marc Bütikofer, Head of Innovation Security Solutions, Airlock

“Multi-factor authentication alone is no longer enough.”
_Michael Doujak, Product Manager, Airlock

Security precautions and legitimations for online access can be compared with the traffic system. To drive a car, you need a licence. For online access, you need to authenticate yourself with a password. If you want to drive a truck, you'll need to take an additional test. MFA works in a similar way. From age 75 you need a medical check-up every two years if you want to continue driving in Switzerland. The parallel here is risk-based authentication. Despite all of these measures, the police monitor traffic safety constantly. Speed cameras, for example. CAT performs this role where online access is concerned.

Trust level checked constantly

In addition to checking user authorisations as part of identity and access management, CAT is always assessing signals from risk sensors. Has the browser or IP address changed? What about typical mouse movements or keyboard entries? Existing components such as security gateways make particularly good risk sensors because they monitor all of the interaction between user and application.

CAT constantly checks that the trust it once gave is still justified. The upside here is that security and user experience are in step. The perennial problem for IT security is that more security often means less user-friendliness. The lack of acceptance of the SuisseID, scrapped in 2019, is a prominent example of this balancing act. It should not be confused with its successor, today's SwissID. One of the problems with the SuisseID was the complex registration process, with passport copies, personal appointments, extracts from the commercial register, signatures, and the need for good technical IT skills from readers and drivers. It is far easier to use the SwissID, and all you need is a smartphone.

CAT ensures better security without compromising on user-friendliness. If the risk level is high, the user will have to authenticate themselves again. If it is low, a company can omit this step and thus offer a better user experience. The key is to find the right balance.

An avoidable incident

One case in particular highlights how a lack of balance can result in a security problem. At one Swiss company, a hacker was able to take over a user's running online session. This allowed the attacker to enter a new mobile phone for two-factor authentication. There was no further validation, and from that point it was automatically regarded as fully authenticated. The person was then able to reset the password of the highjacked account and take full control. Although there was other security in place, such as an automatic fraud prevention system, having taken over the account, the hacker could easily fool the controls that triggered the system. CAT could, in all probability, have prevented this attack because the hacker would have had to trick all of the risk sensors at the same time.

Single sign-on increases the need for CAT

CAT becomes particularly relevant in combination with the common 'single sign-on' principle. SSO is convenient for users because they only have to authenticate themselves once for a number of supported online processes to access different accounts. Their identity is confirmed and rights granted for the whole of the session. CAT, meanwhile, keeps checking whether it is appropriate to keep trusting the user.

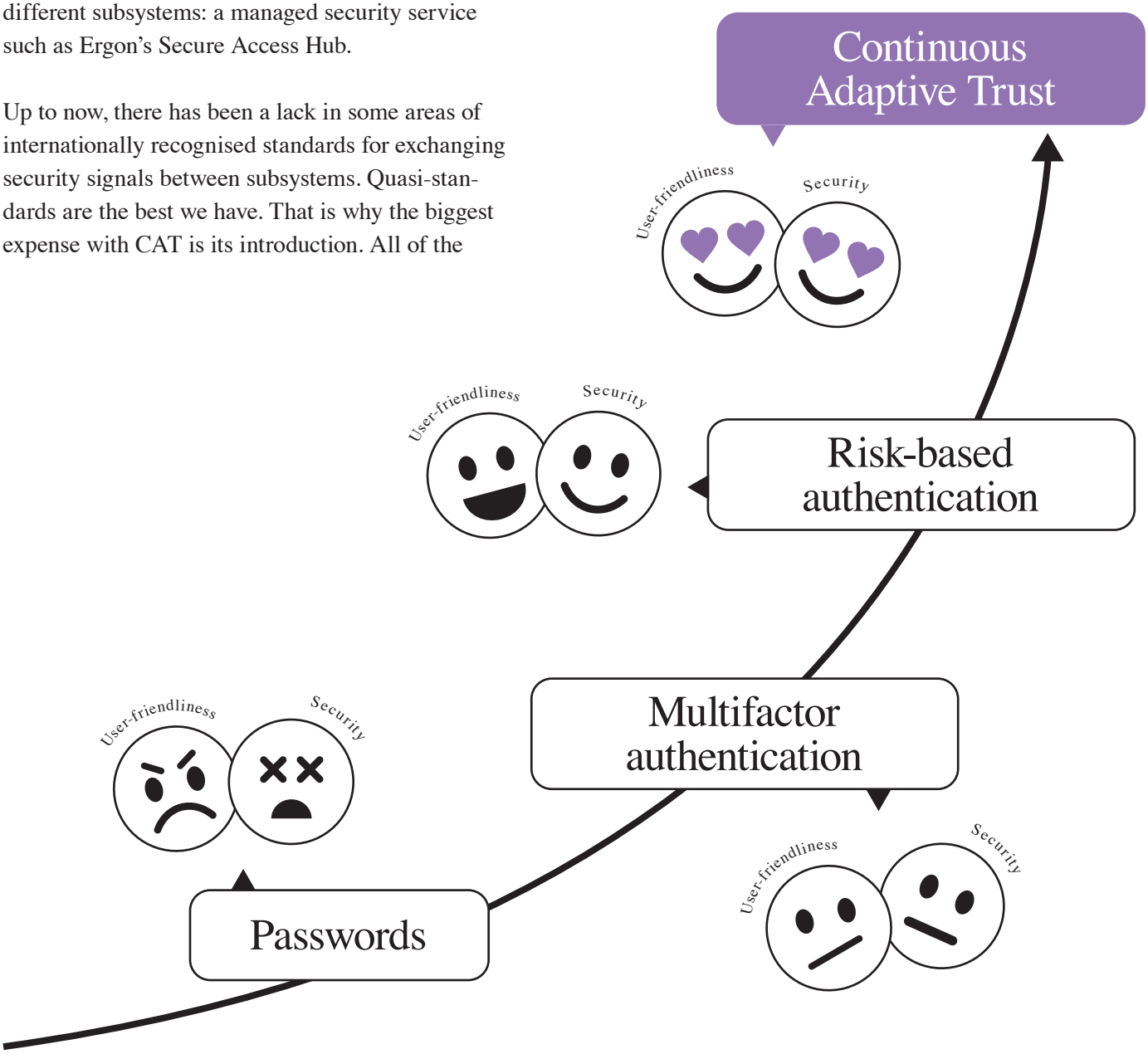
CAT is the perfect complement to the zero-trust model, which assumes that nothing is secure, and takes the default position that no user can be trusted. There is a fairly rigid framework in which each service checks directly at its interfaces whether access is allowed. Zero trust creates a series of little forts, forming a sort of defensive wall both outwardly and inwardly. With CAT, checks are happening all the time until a session ends for good.

Greater security or a better user experience?

Before a company opts for CAT, it should decide what it wants to achieve with it: greater security, or a better user experience? Technical implementation requires the integration of a variety of components. Web application and API protection (WAAP) are

needed to monitor risk signals. Changing the trust level creates identity and access management. Since these components rarely come from the same provider, things can become more complex. That's why it's important to choose a provider that can collate and evaluate the signals from all the different subsystems: a managed security service such as Ergon's Secure Access Hub.

Up to now, there has been a lack in some areas of internationally recognised standards for exchanging security signals between subsystems. Quasi-standards are the best we have. That is why the biggest expense with CAT is its introduction. All of the systems have to be set up, configured, and policies redefined. The results speak for themselves, however. CAT is becoming a competitive edge. />



_Evolution of Authentication