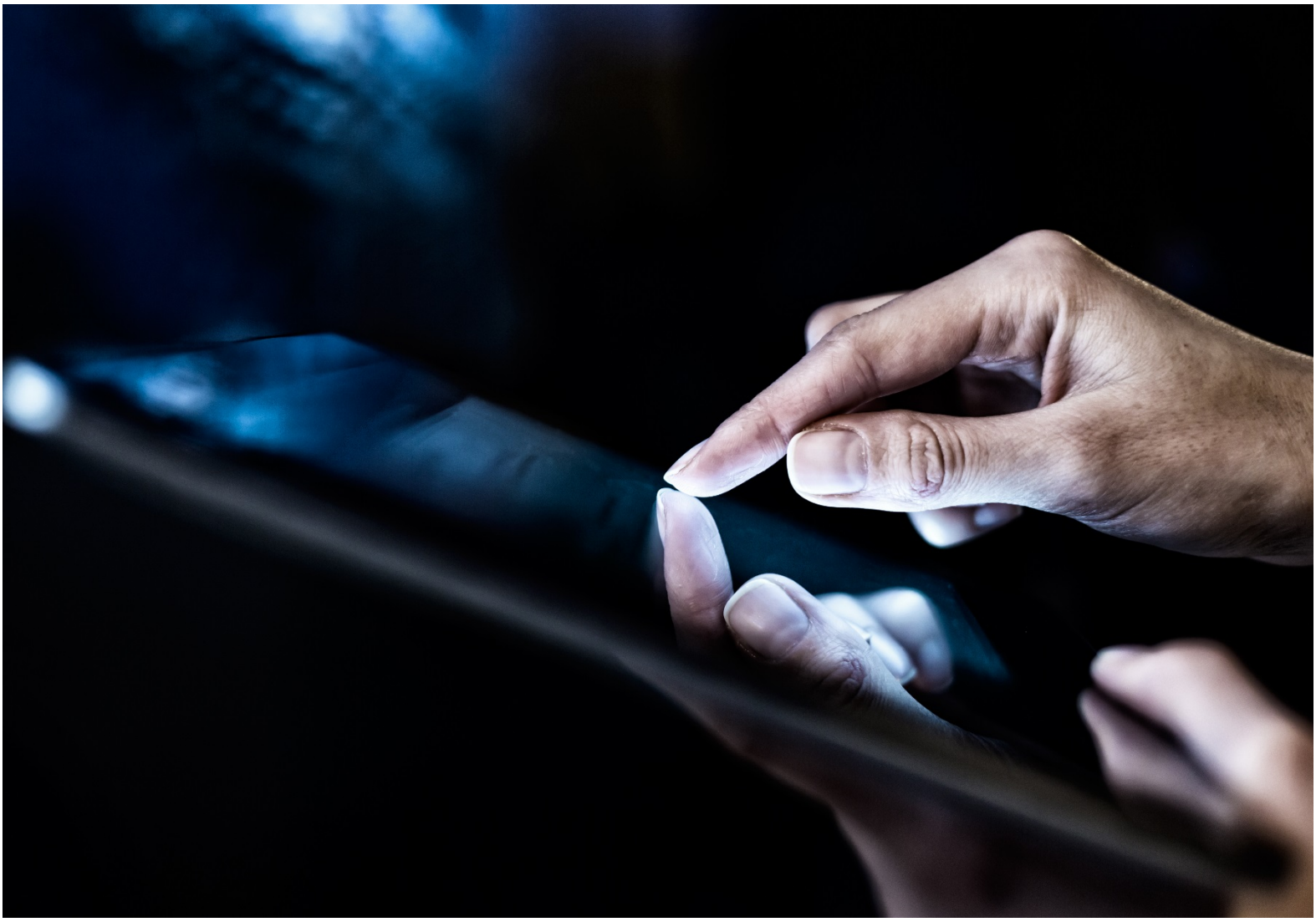
MINIMIZING THE IDENTITY ATTACK VECTOR WITH CONTINUOUS AUTHENTICATION

ABSTRACT

Advances in identity and access management have not been able to keep up with the attackers. Continuous Authentication could thwart attacks that exploit compromised credentials and create a frictionless user experience to better protect enterprise information systems and the data they contain



RSA

KEY POINTS

- Identity is the most consequential attack vector. Ubiquitous, convenient, strong authentication is imperative to mitigating the threat.
- Expanded attack surfaces presented by mobile devices, cloud computing and Shadow IT require that authentication be portable and persistent.
- Adoption of multi-factor authentication and emerging identity and access management solutions have been stunted by inconvenient form factors that create friction between users and getting access to the information they need. Usability improvements are necessary and imminent.
- Analytics that take context from a variety of information sources to determine risk levels, when combined with strong authentication, deliver a more convenient and stronger solution.
- Use of big data, behavioral analytics, and agile security policies will advance the authentication process.

Today, more than ever, organizations need to be aware that compromised identities represent the single biggest attack vector for advanced attackers. The ease with which static passwords can be harvested - from individuals or from bulk password repositories – and packaged together with techniques to exploit them, can lead to devastating consequences. According to the Verizon Data Breach Investigations Report 2015, threat actors used stolen passwords 95% of the time in the most common type of attacks. The lack of sophistication and effort required to carry out an attack using compromised credentials, combined with the potential for rapid and sizeable payoff, gives adversaries clear motivation to continue to pursue this attack vector.

A number of trends make this attack vector even more dangerous:

- The attack surface against which these attacks can be applied is only getting larger and more complicated. With cloud, mobile, and social expanding, the number of applications in both work and personal settings, users create and re-use the same passwords, making attackers' work easier.

- Users access applications in both work and personal contexts, and the boundaries between these two domains are increasingly blurred. An adversary that compromises a user's password through personal channels has likely gathered something that can be used in an attack against their work organization and vice-versa.

- The traditional definition of the user is being challenged. At one time, the word "user" was synonymous with "employee." "Users" are now anybody that accesses the network or applications. They can be partners, vendors, suppliers, audit teams, consultants, customers, and even things. The ability to set and enforce effective access control policies for these "users" is much more challenging now that the landscape has changed. Enterprises deal with different types of users – employees: some within known facilities, some not, partners, customers, etc. Each of these types of users presents unique challenges, which has led enterprises to create different silos for dealing with how best to authenticate them. To address this, while some companies having established sufficient controls over local employee access, they have sub-par levels of control over partner/affiliate users. Meanwhile, many times, such non-local users access the same information or applications as local employees.

- Users knowingly or unknowingly bypass security controls that do not meet their expectations. Today's users, above all, crave flexibility and convenience. They want their work experience to mirror their personal one, complete with one touch access to mobile applications and the ability to access their applications from anywhere and from any device. Security is presumed, and is considered an inhibitor if it prevents them from working in the ways in which they are accustomed. Because many of the tools they use are outside of the purview of the enterprise identity controls, many times, users unknowingly create new risks to the enterprise.

To address this attack vector today, we rely on user authentication. But today's authentication implementations are increasingly unable to address the myriad challenges that have been presented. We authenticate users once, typically at the start of a session, with flawed methods like username and password.

Despite the importance of ensuring that a person accessing a system has permission to do so and is who they say they are, advances in common forms of authentication and access management have been incremental at best. Many current commercially available authentication technologies are intrusive, difficult to manage, and dependent on individual compliance.

But what if we could authenticate in such a way that does not force a trade-off between security and convenience? Could we come up with a model for authentication that is both convenient and more secure for end users? This is the promise of continuous authentication.

Continuous Authentication

Common authentication methods based on passwords, tokens, or fingerprints perform one-time authentication. Once the user logs in, it's assumed it's the right user who's accessing the services on the device. Typically, to determine if it is time to authenticate the user again, such methods rely on users to either log out from applications or devices, or for a session timeout to occur. While the user is logged in, the assumption is that they remain authorized and they are indeed who they say they are.

These point in time methods are not enough, as the applications and services are exposed while it's assumed the right user continues using the service beyond the initial log in. The most common solution to address this concern has been using inactivity or absolute timeouts, which inevitably either fail security goals (too long a timeout) or usability objectives (too short a timeout).

One solution is to authenticate users continuously while they are using a device and automatically log them out when they leave. Existing solutions based on user proximity, while they establish a base point for the user's known or familiar environments, are not sufficient: they only confirm whether the user is nearby but not whether the right user is actually using the device. Additionally, proposed solutions based on behavioral biometric authentication (e.g., keystroke dynamics) may not be reliable.

Continuous authentication, as the name suggests, is ongoing validation of an individual's identity and access privileges by monitoring passive behavioral, temporal and biometric factors. Persistence and portability are inherent. A key principle for successful implementation and adoption of continuous authentication is avoiding or limiting direct engagement with the user. This contrasts with authentication conventions such as session time out and periodic requests to re-enter credentials.

One demonstrated approach to continuous authentication required users to wear a bracelet containing an accelerometer, gyroscope and RFID chip. In a paper presented at 2014 IEEE Symposium on Security and Privacy, researchers from the Institute for Security, Technology, and Society (ISTS) at Dartmouth College and Intel Labs made a case for improving the usability and security of IAM (ZEBRA[1]). With this approach, when the user interacts with a computer terminal, the bracelet records and processes the user's wrist movement and sends it to the terminal. The terminal compares the wrist movement with the inputs it receives from the user, via keyboard and mouse, and confirms the continued presence of the user only if they correlate. Because the bracelet is on the same hand that provides inputs to the terminal, the accelerometer and gyroscope data and input events received by the terminal should correlate because their source is the same – the user's hand movement. In RSA Labs experiments, ZEBRA performed continuous authentication with 85 percent accuracy in verifying the correct user, and identified all adversaries within 11 seconds. For a different threshold that trades security for usability, ZEBRA correctly verified 90 percent of users and identified all adversaries within 50 seconds."

RSA is considering multiple deployment options and performance improvements. These include exploring new form factors, other ways for collecting user data while keeping privacy intact, partnering with wearable technology manufacturers and device makers to integrate continuous authentication into products everyone carries (think Android and iPhone apps), and external sensors.

In addition, as a member of the FIDO alliance, RSA has been actively working on establishing a standard for a common approach to multi-device external authentication. The existence of such a standard would permit authentication solutions to incorporate multiple sources of contextual information, such as "what you have", "what you are", or "where you are" to drive effective authentication decisions. For example, using the FIDO U2F specification, an external authenticator (token, key fob, bracelet, or even the user's mobile phone) can be used to perform initial user authentication for an app running on another device (such as an app running on the users laptop). It would be possible for the same bracelet to locally authenticate the user (using EKG biometrics, as an example) in a seamless and non-intrusive fashion, and on an ongoing basis. The bracelet could transmit messages to the app running on the laptop (e.g., over BLE), letting the application know of any changes to its continuous authentication. In this case, the bracelet could prove that the right user is using the app, without the need to collect or analyze any gesture/movement information from the user. And if/when the bracelet is idle, or is not in the hands of the right user, biometric authentication would fail, preventing unauthorized use of the app within seconds of its detection. This example of a device with the ability to continuously collect and combine multiple sources of contextual information shows the potential of continuous authentication solutions to deliver enhanced security and convenience.

Barriers to Technology Adoption

Despite a recognized need for improved authentication, the commercialization of continuous authentication technology faces challenges. Wearable technology with embedded sensors are an efficient way to collect the required data, but form factor is a barrier. Users may be reluctant to wear another accessory in addition to jewelry they may already wear. Leaving the device at home or losing it is a problem, as are potential allergic reactions to the materials from which devices are fabricated.

[1] "ZEBRA: Zero-Effort Bilateral Recurring Authentication," Shrirang Mare*, Andres Molina-Markham*, Cory Cornelius†, Ronald Peterson*, *Institute for Security, Technology, and Society, Dartmouth College, †Intel Labs, March 2014

Implementation Considerations

Operationalizing continuous authentication will require effort. Successful continuous authentication depends on three core capabilities:

1. Capturing, integrating and storing **data** generated continuously by systems, applications and users is the foundation for some of the implementations of continuous authentication. Large data sets – Big Data – can yield precise, granular insight about users unlocked through a second discipline: analytics.

2. Behavioral **analytics** order and interpret data, transforming facts and statistics into information about users and systems. Baseline normal usage and behaviors – how, when, and where systems, devices and applications are accessed – enable detection of anomalies. In cases of continuous authentication where such analysis is necessary, that may include a range of factors from subtle changes in gestures to changes in location.

3. **Policies** must define the use of continuous authentication. They must dictate where it applies, and how much risk is acceptable for different types of users, applications, and data. It is important to establish authentication policies that are neither so onerous they disrupt or create friction within the business, or so vague and unenforceable as to be useless, on the other. For example, if the coupled-bracelet is battery operated, the user authentication policy should take into account that the rightful user may be using the solution, but with a dead bracelet. In this scenario, the policy could (for example) revert to using traditional forms of user authentication as a backup, and inform the user that they need to recharge their bracelet to go back to hassle-free mode.

Conclusion

Continuous authentication has the potential to modernize an often neglected process: determining if a person attempting to access or use a device, application, server or system, is who they claim to be, throughout their entire interaction with the system. With careful planning and oversight, continuous authentication would thwart attacks that exploit compromised credentials in a way that creates a frictionless user experience to better protect enterprise information systems and the data they contain.

The technology building blocks exist. Operationalizing and implementing is the next step.

Authentication Solutions from RSA

RSA SecurID® Access RSA SecurID Access provides world-leading authentication and access assurance solutions protecting 25,000 organizations and 55 million users. With RSA SecurID Access, organizations can have secure access to cloud and mobile applications without creating roadblocks for users.

About RSA

RSA helps more than 30,000 customers around the world take command of their security posture by partnering to build and implement business-driven security strategies. With RSA's award-winning cybersecurity solutions, organizations can effectively detect and respond to advanced attacks; manage user identities and access; and reduce business risk, fraud and cybercrime. For more information, go to www.rsa.com.

RSA
www.RSA.com