The PKI Fallacy

What is it, and why is debunking it critical for digital security?

According to Verizon's annual 2021 Data Breach Investigations Report, weak user authentication and human interface error represented roughly 85% of all data breaches last year. Emphasizing these statistics, recent, high-profile data breaches and online frauds made headlines that further substantiate the report's analyses.

As the world rolls toward digital credentialing, mobile driver licenses, passports, and other remote credentialing methods, it is naturally important to understand the potential vulnerabilities of various possible systems, architectures, and components so that we can proactively guard against what could enable breaches. We believe modern Identity Management System (IDMS) models, including various Electronic ID (eID) and Mobile Drivers License (mDL) models, are flawed and vulnerable to the attacks discussed in the Verizon report.

For example, the attack vector that launched the notorious SolarWinds breach, which affected numerous companies and government agencies, exploited "strong" *device* authentication insufficiently protected by weak *user authentication*, with the goal of accessing a network and ultimately executing a Remote Access Trojan (RAT) malware supply-chain attack. The weak user verification and authentication provided the attackers the opportunity to enroll a new, yet equally strongly authenticated device in parallel under a legitimate user's account. This allowed the attacker to re-authenticate repeatedly, creating an "advanced persistent threat" (APT), an intrusion that goes undetected for extended periods. In this case, the attacker had unlimited access to the victim's networks for nine months.

Additionally, U.S. federal and state government COVID19 pandemic financial support distributions were and continue to be compromised through the exploitation of weak identity verification, proofing, and user authentication in remote environments. To date, the estimated value of those pandemic-related identity frauds exceeds $70 billion and is growing. Any Identity Management System (IDMS) that relies on this combination of strong device authentication and weak user authentication, is vulnerable to phishing, man-in-the-middle, device spoofing, and RAT attacks, as well as potential resultant APTs.

This vulnerability can be called "The PKI Fallacy" or "The Device Authentication Fallacy", which suggests that if the Public Key Infrastructure (PKI) certificate, token or device is deterministically authenticated, the user of the device is somehow *also* authenticated. This is a false logic progression based on an erroneous industry preference for "deterministic" decisions (a binary yes/no) over a "probabilistic" decision (a statistical probability). PKI is deterministic for the device, while biometric matching is probabilistic for the person. Network and device authentication proponents seem to choose PKI deterministic outcomes over biometric probabilistic outcomes, as 100% seems stronger than 99.9%.

Considering that the PKI in the device can't know, nor even care what user is holding it, how "deterministic" can a device authentication transaction actually be, if the user authentication probability is less than 100% correct? Logically, failing to verify and authenticate the device holder while relying on a 100% deterministic device authentication (PKI) could create a false sense of security. In effect, the 100% PKI deterministic outcome erroneously validates a less-than 100% probabilistic user authentication. In combination, the end result authentication remains probabilistic, and that probability may be far less than 99.9%, depending on the method of user authentication. This is exactly what happened with the Solarwinds breach. Strong biometric liveness and matching solve for this vulnerability.

The reasons industry has tended to gravitate toward deterministic models and away from probabilistic models is two-fold. First, deterministic device authentication is automated, simple and inexpensive to use. Second, most biometrics simply have not achieved a satisfactory level of probabilistic match confidence, or assurance, that the biometric sample was collected in real-time from the correct living human. Consequently, many IDMSs have been designed with non-biometric authenticators, often a second cryptographically validated device, supported with a password. In other words, these systems typically use device authentication, supported by a password, to support device authentication, *also* supported by a password.

Moreover, the biometric matching systems onboard most handheld devices do not associate nor bind the biometric with an actual user's identity profile. Rather, they simply register the biometric data anonymously, in the secure element on the device, and match the nameless stored biometric to the newly collected biometric data, during user authentication transactions. Trust is the key word in this scenario, as that current user is only trusted to be the authentic privilege owner. We could call this "anonymous biometrics". Anonymous biometrics reduce the probability, or match confidence, of the user authentication, and by extension, the device

authentication. Bad data in is bad data out. If you don't know who is biometrically enrolling on the device, you are less likely to know who is actually using the device.

Further, this combination could enable fraud and attacks. If a fraudulent user *enrolls* on the device as the legitimate privilege holder, the in-device biometric sensor would authenticate that user as if they were the legitimate privilege holder. By extension, if the device cannot know whether the device user is the legitimate privilege holder, the relying third party (the app, server or business) also cannot know whether the device user is the legitimate privilege owner. This too, is what happened with the Solarwinds breach.

Importantly, recent and substantial progress in biometric matching confidence, especially with the invention of three-dimensional face liveness and matching, has materially increased the utility of mobile or remote biometric verification and authentication. And a more balanced approach has begun to emerge. Adding a third dimension to the data increases the amount of accessible, unique, and measurable biometric data by orders of magnitude, greatly increasing match confidence and severely limiting the utility of 2D photos and video in imposter attacks. This advancement in biometrics enables institutions to authenticate an actual person - bound to an actual user profile - with high confidence, rather than to a device only *presumed* to be controlled by the appropriate person. This closes the PKI and Device Authentication Fallacy vulnerability.

To suggest that PKI and Device Authentication Fallacy vulnerabilities are less important or “don’t scale”, is naive at best, conflicting wildly with the Solarwinds breach example. Strong, well-developed identity verification and authentication must be included in a properly designed identity management system to mitigate such vulnerabilities and achieve full functionality in remote, mobile ecosystems. Yet, today’s eID and mDL systems not only focus primarily on PKI-based device authentication, but are also typically supported by weak user verification during enrollment, and weak user authentication during active use, if user verification and authentication are proposed at all. The eID/mDL systems, as described in several recent major Requests for Information (RFI) from the American Association of Motor Vehicle Administrators (AAMVA), DHS, and other stakeholders, effectively ignore strong user verification and authentication, but focus on deterministic device authentication. Relevant ISO eID and mDL standards authenticate an mDL credential by authenticating a device or digital object, but do little to actually verify or authenticate the entitled mDL privilege-holder.

To mitigate the results of the inherent weaknesses in the current approach, we strongly recommend requiring liveness-proven biometric identity proofing, enrollment, and user authentication, in *addition* to standardized strong device authentication.

About the author

Jay Meier is an award-winning financial securities analyst and subject matter expert in identity access management, credentialing, and biometrics. Jay is the author of *Secure Credentialing & Identification*, one of the most comprehensive analyses of ID-related markets. He currently serves as FaceTec's SVP of North American Operations.

Definitions

RAT - A remote access Trojan (RAT) is a malware program that gives an intruder administrative control over a target computer.

PKI - A public key infrastructure (PKI) is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption.

mDL - A mobile driver license (mDL) is a digital representation of the information contained in a physical DL or non- driver identification card, securely stored on a smart mobile device such as a smartphone or a tablet, owned and controlled by the mDL holder.

eID - An electronic identification (eID) is a solution for proving the identity of citizens or organizations that can reside on a user's digital device.