Neustar NIST Authentication Commentary

Submitted by Neustar
August 10, 2020

Primary Contact:

Scott Straub

Table of Contents

Introduction

Neustar is a leading Global Information Services Provider and unique telecommunications partner with the most complete understanding of how to connect people, places, and things through online and offline identity attributes. Founded in 1996, Neustar is a large business and employs over 1,800 people across the globe, and has revenues exceeding $700M.

We help clients grow, guard, and guide their businesses through our authoritative OneID™ system. Neustar's OneID is a unique, accurate, and real-time identity system, continuously corroborated through 50 billion transactions across digital traffic, customer interactions and verifications. In the competitive marketplace, Neustar is regarded as the market leader in authoritative identity resolution and maintains the largest and most accurate identity repository of consumer information available in the U.S.

As the leader in responsible identity resolution, we use our expertise in real-time addressing, authentication, and analytics to provide marketing, risk, digital defense and performance, and communications solutions for over 11,000 clients globally, including numerous Fortune 500 companies and 60 of the Fortune 100 companies. Neustar solutions empower major government agencies and security units, all leading financial institutions and credit card issuers, and all leading communications service providers. Delivering actionable identity is at the core of everything we do, and responsible identity has been at the heart of our business since its inception.

Our vision for identity resolution and authentication is also fully aligned with Neustar's overall mission to be the undisputed global leader in "Connection Science", which consists of data science and algorithm development around calculating the highest quality, most authoritative consumer, device and organizational identity resolution, including all the linkages between these identities, deriving valuable attributes from these identities to fuel numerous risk, security, and marketing use cases. Neustar brings this all together with industry-leading expertise in Analytics, Addressing, and Authentication, underpinned by our unparalleled authoritative Identity system 'OneID'.

Including Call Center Authentication in Authentication and Lifecycle Management Guidelines

The existing scope of 800-63B is limited to online systems as reflected in the first sentence of the introduction to the Authentication and Lifecycle Management Guidelines, "Digital identity is the unique representation of a subject engaged in an online transaction." The content of the guideline describes the authentication levels and requirements for different approaches for authenticating to online systems via a web session or mobile device. The current guidelines do not address authentication to a call center even though subjects engage directly with interactive voice-response systems, which perform many of the same transactions as online systems, and the callers typically interact with a customer service representative (CSR) who will then need to verify the identity of the caller. The omission has created a large gap in the way personal data, financial assets, and much needed benefits, like Social Security, or Medicare are protected in government systems.

Call centers represent a significant source for fraudulent Account Takeovers (ATOs). ATOs occur when a nefarious actor steals someone's identity and then impersonates the victim using sophisticated social engineering techniques to pass a call center's identity verification checks. This fraudulent behavior can

be halted and Neustar is recommending NIST consider expanding the definition of digital identity guidelines to include contact centers and/or interactive voice response systems (IVR).

According to the 2020 State of Call Center Authentication Survey, call centers are the source of ATOs 20% of the time across all industries. Within financial services, call centers are the source of ATOs 35% of the time. Recognizing this risk, financial service organizations have been deploying improved authentication technology.

Percent of Respondents Indicating calls centers are the origin of most account take-overs.

All Markets	20%
Financial Services	35%

Protecting citizen accounts in government systems should not be limited to online access. The IVRs and agents answering calls need identity verification and authentication technologies to prevent impersonation of an account owner without materially degrading the customer experience. The need for strong authenticators in this area, and expansion of the definition of a digital identity, is made more urgent by the widespread practice in government agencies of using knowledge-based authentication to determine caller identity. Multiple data hacks (1,473 data breaches in 2019 exposed over 164 million consumer records according to the ID Theft Center) and the proclivity of Americans to publish personal information on social network sites has undermined the concept that answers to personal questions are predictive of identity.

In summary, everyone's identity has already been stolen and the criminals are targeting call centers as the weakest link in the chain to perpetrate their fraud against the most vulnerable populations. The ongoing practice of using knowledge-based authentication in government call centers represents a major vulnerability. The next revision of the Authentication and Lifecycle Management Guidelines need to fill this gap by addressing call center identity verification and authentication.

Using Phones as Out of Band Authenticator for Phone Calls

A caller's phone is an ideal physical device to use as an authenticator because it is possessed by the claimant for legitimate calls and has been binded by the carrier at issuance of the phone. In addition, the Public Switched Telephone Network (PSTN) provides a secure, highly trusted means to create an out-of-band channel to inspect the calling device to establish that is legitimate and not spoofed, hacked, manipulated or virtualized. Because direct inspection of the calling device can be made within the PSTN, no secret needs to be sent from a verifier to an authenticator to a user to link a primary channel and secondary channel, as is the case with use of phones for online (web) access. The entire inspection process of live phone calls can be completed before a call is answered, while being invisible to a caller.

The sections below describe the requirements for this approach. The requirements are described in the same structure used in the current document for single factor One Time Passcode (OTP) devices in section 5.1.4. While the OTP processes differs from caller authentication, they both share use of the phone as an ownership-factor of authentication.

Out-of-band Devices

Supported phone devices should include all devices that are physical, can be uniquely identified and associated with an individual through the device phone number (or Automatic Number Identification, ANI).

This includes mobile phones, residential land-line phones and residential phones supported by cable modems. Each of these types of phones is physical and can be directly linked to a personal identity. Inspection should be consistently performed across all carriers originating calls from supported devices.

Out-of-band Authenticators

The out-of-band authenticator shall establish a separate channel with the verifier in order to inspect a claimant call

- The authenticator should receive the calling ANI, called ANI and, if available, any call data delivered when a call connects from a verifier.
- The authenticator shall establish a separate channel from the claimant phone call for inspection
- The authenticator shall perform an end-to-end inspection and confirmation of the phone call from the device to the call center
- The authenticator shall confirm that the calling device is unique, authentic and physical and that the call is not virtualized, spoofed, shared, anonymously provisioned, illegitimate, altered or hacked.
- The authenticator should also consider risk indicators such as device swap, SIM swap, number reassignment, call routing, originating carrier reputation and prior activity by the calling device and calling number.
- The authenticator shall use consistent process to inspect calls from all carriers and all line types.
- The authenticator shall return an authentication result (token) to the verifier designating whether the ANI presented by the claimant is registered to the device the claimant is using to contact the call center and that the device is in a live call with the call center.
- The authenticator should complete this process between the time a call connects to the call center and time the call is answered so that results can be used route callers and determine additional authentication strategies.

Out-band-verifiers

An out-of-band verifier plays a limited operational role in device-based inspection of phone calls.

- The verifier shall provide the calling ANI and called ANI to an authenticator over an encrypted communication, and optionally call data provided by a terminating carrier.
- The verifier shall receive the authentication token from the authenticator over an encrypted communication.

Summary

Extending the Authentication & Lifecycle management guidelines to include call center authentication will provide agencies with the best practices they need to close a serious security gap. Using the recommendations, we have provided above, this can be done in a way to better secure accounts while improving the caller experience by reducing or eliminating time spent on using knowledge-based authentication approaches.