

**Taylan KAPAN**

Yönetici, Ses Teknolojileri / Manager, Speech Technologies
taylan.kapan@speechhouse.com

Ses imzası, şu ana kadar başka hiçbir yöntemin sağlayamadığı oranda güvenlik sağlar.
A voice signature ensures a security level unprecedented in any other previous systems.

Şirketlerin Güvenlik Sorunu ve Ses Biyometrisinin Önemi Yoksa Siz Hala “Anne Kızlık Soyadı” mı Soruyorsunuz?

Security Challenge Facing Companies and Important Role of Voice Biometrics Do You Still Use “Mother’s Maiden Name” as a Security Question?

Çeşitli yöntemlerle gerçekleştirilen kimlik, şifre ve parola hırsızlığı, şirketlerin yıllardır mücadele ettiği bir güvenlik sorunu. Uluslararası Basel kriterleri, güvenlik uygulamalarında 3 faktör olduğunu belirtir. Birinci faktör “anne kızlık soyadı”, “doğum tarihi” gibi kişisel bilgilerinizden oluşur. Kısacası, ne bildiğinizdir. İkinci faktör ise neye sahip olduğunuzdur. Sahip olduğunuz şey, sizi tanımlayan bir akıllı telefon veya bir kod üreticisi olabilir. Üçüncü ve en önemli faktör ise kim olduğunuzdur. Bunun için biyometrik özelliklerinize ihtiyaç vardır. Ses biyometrisi, parmak izi ve yüz taraması teknolojileri bu faktörün içerisinde yer alır.

Birkaç yıl öncesine kadar “Ne bildiğimiz” işlem yapmak için yeterliydi. Herhangi bir şirketin bize verdiği müşteri numarası ve bizim belirlediğimiz bir şifre kapıların açılmasını sağlıyordu. Ancak sonradan bunların kötü niyetli kişiler tarafından çok kolay bir şekilde ele geçirilebilen bilgiler olduğu fark edildi. Yakın zamana kadar “Ne bildiğimiz”in yanına, “Neye sahip olduğumuz”u da ekledik ve şifre/parola gibi bilgilerimizi akıllı telefonlarımızdan veya kod üreticilerimizden tek seferlik kullanmak koşuluyla temin etmeye başladık. Ancak artık bunun da yeterli olmadığını gördük. Zira telefonumuz veya şifre üreten cihazımız kolaylıkla çalınabilir. Çalan kişinin bizim hakkımızdaki diğer bilgilere ulaşması hiç de zor olmayacaktır. (Örneğin eğer bir dayınız varsa anne kızlık soyadı sizin için bir güvenlik kriteri olmaktan çıkar). Sadece bilgiye dayalı güvenlik uygulamaları artık “güvenli” olarak kabul edilmemektedir.

Sen Gerçekten O Musun?

Günümüzde üçüncü faktör olan “Kim olduğumuz” kriterini oyunun içine dahil etmenin güvenlik açısından dramatik etkiler

Phishing and identity theft, carried out by various methods, is a security problem which the companies have been tackling for years. The International Basel Criteria state 3 factors as applicable to security. The first factor consists of personal information such as your “mother’s maiden name” and your “date of birth”. In short, it is what you know. The second factor is what you have. This could be a smart phone or a code generator which identifies you. The third and the most crucial factor is who you are which requires your biometric features. Voice biometrics, finger print and facial scan technologies are listed within the scope of this factor.

Up until a few years ago “what we know” was enough to transact. A customer number assigned to us by a company and a password we created would open the doors. Later however it was seen that this kind of information could easily be obtained by fraudsters. Until recently we have also added “what we own” to “what we know” and started obtaining our usernames/ passwords over our smart phones or code generators for one-off use. Yet, we saw that this was not enough either as our smart phone or password generator could also be stolen easily in which case it shall not be hard for the person stealing our devices to gain access to other information about us. (For example if you have an uncle your mother’s maiden name ceases to be a security criteria for you). Security practices based solely on information are no longer considered “secure”.

Are you really the person you claim to be?

Today, we have discovered that making the third factor, namely the criteria of “who we are”, part of the game would have

yaratacağını keşfettik. Aslında güvenlik konusu temelde şu soruyu sorar; “Sen gerçekten O musun?”

Bu soruya verilen cevapta biyometrik bir gerçeğin olmaması tüm güvenlik uygulamalarını doğası gereği eksik kılar.

Ses biyometrisi, sesin dijital formata dönüştürülerek, içerisinde bulunan karakteristik ve kişiye özel olan parametrelerin kaydedilmesi işlemi temel alır. Sesin içerisinde kişiye özel bulunan parametreler, parmak izi gibi sesin özgünlüğünü tesciller. Bu sebeple ses imzası eşsizdir ve kopyalanamaz özelliğindedir.

Ses Biyometrisini Nerede Kullanabiliriz?

Günümüzde ağırlıklı kullanım alanı çağrı merkezleri olmakla birlikte, ses imzası teknolojisi, akıllı mobil cihazlar, web siteleri, akıllı evler ve arabalarda kullanılabilir. Çağrı merkezinde yoğun olarak kullanılmasının sebebi; kullanım kolaylığıyla beraber sağladığı faydadan ileri gelir.

Ses İmzası Teknolojisi Kullanım Çeşitleri

Ses imzası teknolojisi “metne bağımlı” ve “metinden bağımsız” olmak üzere iki farklı yöntemle uygulanabilir.

Birinci yöntem olan metne bağımlı uygulama biçimi son yıllarda Türkiye’de birçok şirket tarafından uygulandı. Özetle; “benim sesim, benim şifrem” gibi bir giriş cümlesi söyleme gerekliliği duyulan yöntem “metne bağımlı yöntem” denir. Bu yöntem genellikle sesli yanıt sistemlerinde uygulanır. Giriş cümlesi, ses imzası oluşturma esnasında 3 defa tekrar edilirken, doğrulama aşamasında 1 defa söylenmesi doğrulama için yeterli olmaktadır. Türkiye bu alanda dünyada örnek gösterilen öncü bir ülkedir. Zira Türkiye’de şu ana kadar kullanıcılar tarafından 20 milyonun üzerinde ses imzası oluşturulmuştur. Dünyada

dramatic effects in terms of security. Essentially security asks this question: “Are you really the person you claim to be?”

Lack of a biometric component in the response given to this question renders all security practices inherently deficient.

Voice biometrics is based on converting voice into digital format and recording its characteristic and personally identifiable parameters. Parameters of the voice which are specific to the person register the authenticity of the voice just like a fingerprint does. For this reason, voice signature is unique and unduplicatable.

Where can we use voice Biometrics?

Although predominantly used in call centers today the voice signature technology can be used in smart mobile devices, websites, smart homes and cars. The reason it is intensively used in call centers stems from the ease of use and benefits it affords.

Modes of Use of Voice Signature Technology

Voice signature technology can be “text dependent” or “text independent”.

The text dependent system has been used by many companies in Turkey during recent years. Briefly the “text dependent method” requires the user to utter a specific passphrase such as “my voice is my password “. This system is generally used in IVR systems. The passphrase is repeated 3 times to create the voice signature whereas, for verification, uttering it only once is sufficient. Turkey is a pioneer in this area and is cited as a model throughout the world which is supported by the fact that more than 20 million voice signatures have been created by users so far. It is estimated that this number is around 75 million in the world. Seen from



ise bu sayının 75 milyon civarı olduğu tahmin edilmektedir. Bu açıdan bakıldığında Türkiye, ses biyometrisi teknolojileri konusunda belli bir olgunluğa ulaşmış ender ülkelerden biridir.

İkinci yöntem ise “metinden bağımsız” doğrulama biçimidir. Buna “sessiz doğrulama” da denir. Bu yöntemde önceden belirlenmiş bir giriş cümlesine ihtiyaç duyulmaz. Müşteri ile müşteri temsilcisi arasındaki doğal konuşmadan toplanan sesler ile kişinin ses imzası oluşturulur veya kişi doğrulanır. Doğrulamanın başarılı olup olmadığı müşteri temsilcisi ekranında bir uyarı ile belirtilir. Müşteri temsilcisi doğrulama sonucuna göre ilgili aksiyonu alır.

İkinci yöntem özellikle finansal kuruluşlar gibi güvenlik odaklı yapılar tarafından daha çok tercih edilmektedir. Güvenlik öncelikli kuruluşlar çoğunlukla her iki yöntemi hibrid olarak uygulama yolunu seçmektedirler. Nitekim her iki yöntemin uygulanması, eskiden uygulanan şifre ve parola tabanlı güvenlik uygulamalarına göre çok ama çok daha güvenlidir. Hibrid yapı, yapılacak işlem türüne göre istenen yöntemin uygulanabilmesine olanak tanır. Örneğin sesli yanıt sisteminde doğrulanan bir kişi birçok işlemi yapabilirken, yüksek tutarlı bir para transferi için müşteri temsilcisi tarafında da sessiz doğrulamaya tabi tutulabilir. Bunun gibi iş süreçlerinin belirlenmesi, müşteri deneyimini negatif yönde etkilemeden güvenlik seviyesinin artırılabilmesini sağlar. Hibrid çözüm, gücünü bu esneklikten alır.

Ses Biyometrisi Bana Ne Kazandırır?

Ses imzası, şu ana kadar başka hiçbir yöntemin sağlayamadığı oranda güvenlik sağlar. Bu, en başta kimlik ve hesap hırsızlığı yüzünden uğranan zararları büyük oranda ortadan kaldırır. Şirketlerin bu bilgileri gizli tutmalarından ötürü bunu ölçmek bir hayli zor olsa da, miktarın çok büyük olduğu uzmanlar tarafından bilinmektedir. Tabii işin sadece güvenlik boyutu bir şirketin bu çözümü uygulaması için yeterli olmayabilir. Yatırımın geri dönüşü de bu noktada önemlidir. Çağrı merkezlerinde güvenlik doğrulamaları için harcanan süre sektöre ve yapılan işleme göre ortalama 20 ile 90 saniye arasında değişmektedir. Ses biyometrisi çözümü güvenliğin yanı sıra harcanan bu süreden tasarruf ettirerek yatırımın dönüşünü sağlar.

Tüm bunlara ilave olarak müşteri memnuniyetindeki artış da bir kazanç olarak değerlendirilmelidir. Nitekim yapılan araştırmalarda ses imzası kullanan kullanıcıların %74’ü kendilerini yalnızca şifre/parola ile işlem yaptıkları dönemden daha güvende hissettiklerini belirtmişlerdir. Ayrıca kullanıcıların %90’ı ses imzası teknolojisini diğer yöntemlere tercih edeceklerini söylemişlerdir. Bunun yanı sıra hatalı şifre girişlerinden dolayı tekrar eden aramalar da ciddi oranda düşmektedir. Bu oran sektöre ve yapılan işe göre değişken olmakla beraber, %20 ile %70 arasındadır. Yine şifre resetleme için yapılan aramaların oranı, bazı organizasyonlarda %30’lara ulaşmaktadır. Şifreleri unuttuğumuz veya şifre üreten cihazları kaybettiğimiz gibi sesimizi unutmayız veya kaybetmeyiz. Ses biyometrisinin sadece bu özelliği bile klasik yöntemlere göre ne kadar güçlü olduğunun bir göstergesidir.

Hangi Ses Biyometrisi Ürünü?

Ses biyometrisi teknolojilerinde kullanılacak ürünün önemi elbette ki çok büyüktür. Piyasada bu hizmeti veren birçok ürün

this perspective Turkey is among those rare countries which have achieved maturity in voice biometrics technologies.

The second system is the “text independent” speaker verification system. This is also called “silent verification”. Here no pre-determined passphrase is required. The voice signature of a person is created or the identity of the person is verified using phonemes extracted from natural speech between the client and the agent. An alert appears on the screen of the agent as to whether verification is successful or not. The agent takes relevant action based on the result of this verification.

The second system is particularly preferred by security-oriented structures such as financial institutions. Security oriented organizations mostly opt for a hybrid system where both verification methods are used. The implementation of these two methods is much more secure relative to previous user name-and-password-based security systems. The hybrid structure allows the use of the desired method based on the type of transaction to be carried out. For instance, while a person whose identity is verified across an IVR system may carry out several transactions, he may also be subject to a silent verification on the agent side for a money transfer involving a high amount. Determining these types of work processes helps improve security levels without any negative impact on customer experience. It is this flexibility that gives the hybrid solution its strength.

What can I Gain from a Voice Biometrics Solution?

A voice signature ensures a security level unprecedented in any other previous systems. To begin with it substantially eliminates losses sustained due to identity theft and phishing. It is considerably difficult to estimate the magnitude of these losses as companies keep this information confidential. Yet experts know that it is high. Of course security-related considerations, on their own, may not be enough for a company to opt for the voice biometrics technology. At this point the return on investment is also important. The time spent at call centers for identity verification varies between 20 seconds to 90 seconds depending on the relevant sector and transaction. Along with security the voice biometrics solution helps save on time and ensures return on investment.

In addition to all these, increased customer satisfaction levels should also be considered a benefit. Research shows that 74% of users who use a voice signature feel more secure than when they transacted only with a username/password. Furthermore, 90% stated that they would prefer the voice signature technology to other methods. Besides there is a significant decrease in the number of repeated calls due to incorrect password entry which varies according to sector and the transaction and is between 20% to 70%. The percentage of calls made for password resetting is up to 30% in certain organizations. We do not forget or lose our voice as we do our passwords or password generating devices. Even this feature of voice biometrics in an indication of its robustness compared with traditional methods.

Which Voice Biometrics Product?

It goes without saying that the product to be used for voice biometrics technologies plays a very important role. There are several products providing this service in the market yet there is significant difference

bulunmaktadır. Ancak bu ürünlerin performansları arasında ciddi farklar bulunur. Dünya standartları biraz incelenerek bunların da üzerine çıkabilen ürünler araştırmalıdır. Bağımsız kuruluşların değerlendirme raporları ürünler arasındaki farklılıkları objektif bir şekilde ortaya koymaktadır.

Uygulayıcı Firmanın Önemi

Öte yandan ürünle beraber uygulayıcı firmanın deneyimi ve uzmanlığı da hayati önem taşımaktadır. Burada da referanslar önemli bir ölçüt olarak kabul edilebilisahip firmalar diğerlerinden öndedir.

Ses biyometrisi de dahil olmak üzere tüm güvenlik uygulamalarında değişmez bir prensip vardır. Müşteri deneyimi (ya da memnuniyeti) ile güvenlik arasında ters oranda bir ilişki bulunur. Güvenlik ne kadar katı olursa müşteri memnuniyeti o kadar düşer. Şirketler kendi önceliklerine ve hedeflerine göre bu denklemdaki pozisyonlarını belirlerler. Bunun belirlenmesi ciddi analiz, kalibrasyon ve ince ayar süreçleri gerektirir. Uygulayıcı firmanın en büyük rolü ve farkı bu noktada ortaya çıkar. Zira pozisyonunu dengeli bir şekilde belirleyebilmiş şirketler başarılıdır; çünkü hem müşterilerini memnun etmeyi başarmış, hem de arzu edilen ölçüde onların güvenliğini sağlamışlardır.

in their performance. An examination on international standards will help determine those products exceeding those standards. Assessment reports by independent bodies objectively reveal the differences between the products.

Importance of the Executing Firm

On the other hand, along with the product, the experience and expertise of the executing firm plays a crucial role as well. Here too, references can be accepted as important criteria. Firms with good and happy references are ahead of others.

The inversely proportional relationship between customer experience (or customer satisfaction) and security is an invariable principle in all security systems including voice biometrics which means: the stricter the security system the lower the customer satisfaction levels. Companies determine their position in this equation based on their own priorities and objectives which require serious analysis, calibration and tuning processes. The difference and principal role of the executing firm is revealed at this juncture. This is because companies which have determined their position in a well-balanced manner are successful since they manage to keep their customers satisfied and ensure their security at the desired levels.

