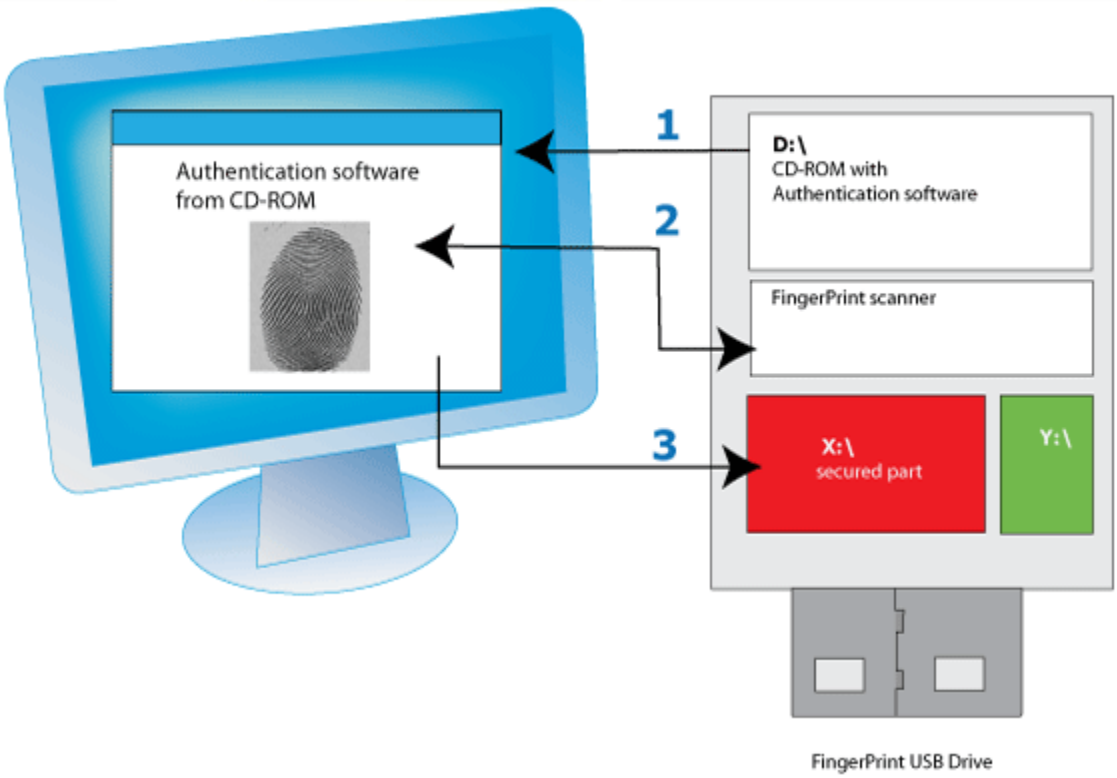
National Datacenter

DCERT

DATACENTER EMERGENCY RESPONSE TEAM

# ХАЛДЛАГАД ХАРИУ ҮЙЛДЭЛ ҮЗҮҮЛЭХ БАГ

## *Нууц үг: 4 Биометрик токен ба түүнийг хэрхэн хуурамчаар даван гарах вэ*




Баталгаажуулалтын механизм нь байнга сайжирч байдаг боловч эдгээр нь бүрэн хэмжээний найдвартай биш байсаар байна. Нууц үг хэрэглэхэд аюулгүй ач холбогдол өндөртэй олон асуудал байдаг. Гэвч хэрэглэгчид богино, тааварлах боломжтой нууц үгийг сонгох эсвэл өөрийнхөө бүх цахим хаягтаа нэг ижил нууц үгийг ашигласаар байна. Үүнтэй зэрэгцэн, бид өөрсдийн хувийн мэдээллийг итгэл хүлээлгэн өгч буй байгууллагууд өөрсдийн цуглуулсан мэдээллийг алдаж, хэдэн мянган хэрэглэгчдийн нууц үгийг алдсаар байгаа юм.

Эдгээр баталгаажуулалтын стандартын үр дүнд бид итгэх боломжгүй байна. Та дижитал сертификат, техник хангамжид суурилсан токен мөн биометрик гэсэн олон факторыг өөрийгөө баталгаажуулахдаа ашиглах боломжтой. Яг өнөөгийн байдлаар биометрик нь хэрэглэхэд хялбархан байдаг учраас түгээмэл хэрэглэгдэх болоод байна. Хэдэн зуун ширхэг маш урт, ялгаатай нууц үгийг цээжилж байснаас өөрийн компьютер эсвэл гар утас руугаа нэвтрэхдээ мэдрэгч дээр өөрийн хурууг

тавих, эсвэл тэдэн рүү зүгээр л нүдээрээ харахад хангалттай гэхээр гайхалтай биш гэж үү?

Майкрософтын Hello, Апплийн FaceID зэрэг энэ төрлийн баталгаажуулалтууд хэрэгжээд эхэлчихсэн тул та ийм төрлийн баталгаажуулалт нь магадгүй ирээдүйн чиг хандлага болж байгааг анзаарсан байх.

Гэвч Биометрик шийдэл бидэнд тулгараад буй баталгаажуулалтын бүх асуудлыг шийдэж чадаж байна уу?

Би энэ асуултанд үгүй гэж хариулна. Биометрикийн баталгаажуулалт нь алдаа бага гаргадаг хэдий ч алдаа гаргадаггүй гэсэн үг биш юм. Биометрик шийдэл хэрэгжсэнээс хойш, хакерууд болон аюулгүй байдлын судлаачид биометрик баталгаажуулалтыг олон удаа давж гарч чадсан байна.

Өнгөрсөн хугацаанд болсон, хамгийн томоохон дөрвөн биометрик баталгаажуулалтын халдлагыг авч үзье.

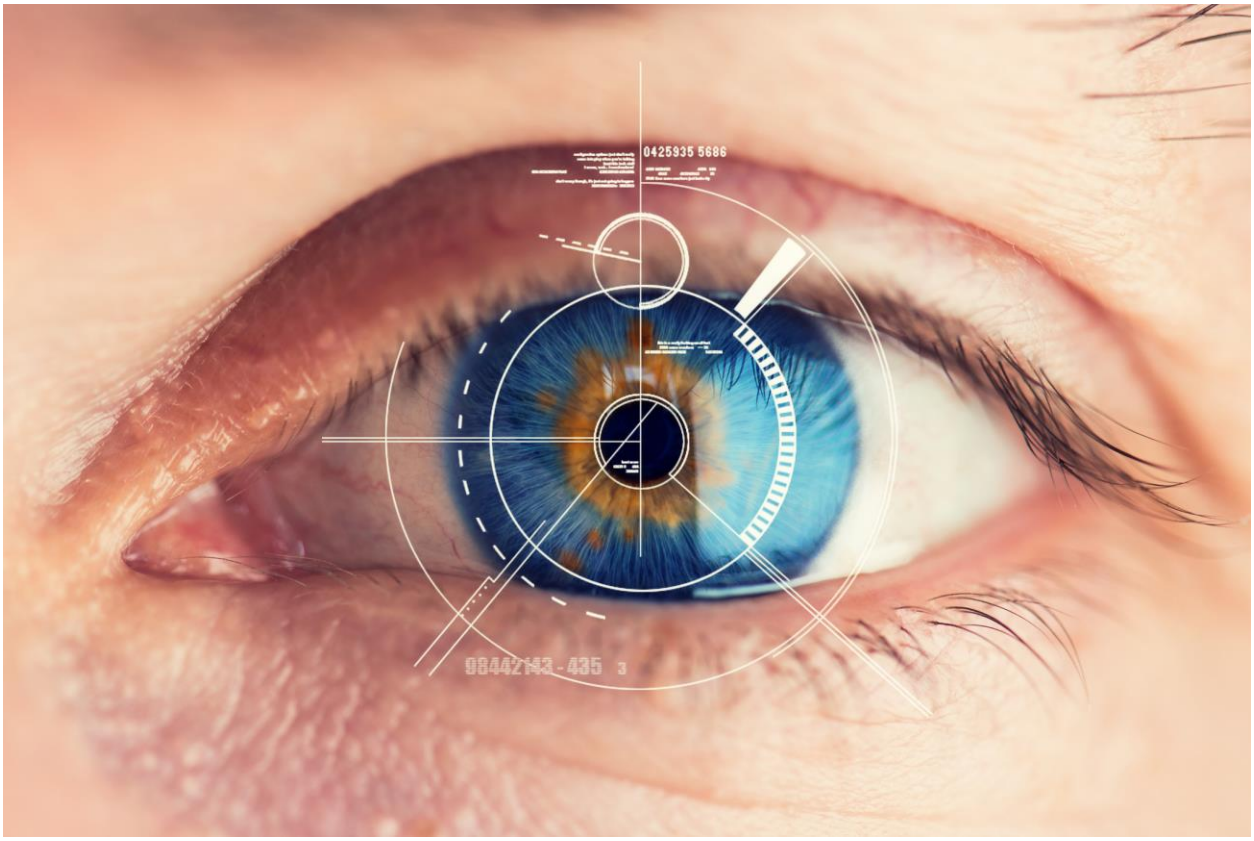
**1. Гюмми Баавгай (резинен чихэр) Хуруу уншигч төхөөрөмжийн баталгаажуулалтыг хуурч чадсан нь:**

Биометрик хэмээх үгийг хэлэх үед танд хамгийн түрүүнд хуруу унших шийдэл санагдаж байгаа байх. Компьютерийн системд хэрэглэгдэж эхэлсэн анхны биометрик шийдлүүдийн нэг бөгөөд өнөөдөр хуруу унших баталгаажуулалт маш түгээмэл хэрэглэгддэг болсон байна. Гэвч, хуруу унших төхөөрөмж нь судлаачдын хамгийн түрүүнд, маш хямд өртөгөөр халдаж болохыг нь илрүүлсэн биометрик шийдлүүдийн нэг юм.

2002 онд Цутому Мацутомо гэх судлаач хуруу унших шийдлийг хэрхэн энгийн хуучны Гюмми Баавгай (резинен чихэр)-ээр хуурах аргыг олсон бөгөөд энэ мэдээллээ нийтэд ил болгосон байна. Мацумото хүний гарын хээг хуулийн байгууллагынхантай ижил аргаар буюу шилэн дээрээс авсан бөгөөд улмаар түүнийгээ Гюмми Баавгай ашиглан хуруу уншигч төхөөрөмжид уншуулсан байна. Багахан хэмжээний хүчин чармайлт гаргаад л эдгээр баавгайнуудын ихэнх нь хуруу уншигч төхөөрөмжийг хуурч дөнгөсөн байна. Мэдээж хугацаа өнгөрөх тусам биометрик нь хөгжиж, илүү боловсронгуй болсоор байна. Сүүлийн үеийн хуруу уншигч төхөөрөмжүүд илүү өндөр нягтралтайгаар унших эсвэл дулаан мэдрэх, зүрхний цохилт мэдрэх зэрэг нэмэлт шалгууртай болсон. Гэсэн хэдий ч үүнийг хуурч дөнгөх судлаачдын арга, техник ч гэсэн хөгжиж байна. 2013 онд Хаос Компьютерийн

Клуб iPhone -ийн TouchID хуруу уншигчийг зах зээлд гарснаас нь хойш маш богино хугацааны дараа хуурч дөнгөсөн юм. Сүүлийн үед судлаачид хуруу уншигчийг хуурахдаа зөвхөн цаас болон цавуу ашиглаж байна. Хэдийгээр хуруу уншигч нь ухаалаг утас руу хандах процессыг маш хялбархан болгож буй хэдий ч бид эдгээр шийдэлд 100 хувь найдаж болохгүй юм.

**2. Iris сканнерийг хуурах нь**




Бид чамин, үнэтэй “iris” сканнер-ийг киноноос олон удаа үзсэн билээ. Гэвч эдгээр нүдэнд суурилсан биометрик төхөөрөмж нь зөвхөн уран зөгнөлт зохиолд л байдаг зүйл биш юм.

Харамсалтай нь эдгээр нь хуруу уншигчаас илүү найдвартай баталгаажуулалтын механизм биш юм. 2012 онд судлаачид iris уншигчийг нүдний торлог бүрхэвчний зурагтай яг ижилхэн зураг ашиглан хэрхэн хуурах аргыг үзүүлсэн. Үүний хамгийн сонирхолтой хэсэг нь судлаачид хуурамч торлог бүрхэвчний зургийг

iris биометрик төхөөрөмжийн өгөгдлийн сан дахь мэдээлэлд тулгуурлан хуулбарласанд байгаа юм. Нууц үг бүхий өгөгөдлийн санг ашиглан нууц үгийг задрах

эрсдэл үүсдэгтэй ижил байдлаар, iris-ийн өгөгдлийн сан нь нүдний торлог бүрхэвч скандах төхөөрөмжийг хуурч дөнгөх эрсдэлтэй мэдээллийг агуулж байдаг байна.

### 3. Цаас ашиглан нүүр таних сканнерыг хуурах нь

Биометрик шийдэл дэх сүүлийн үеийн тренд мэдээ бол нүүр таних механизмтэй холбоотой юм. Майкрософтын Hello зэрэг шийдлийг ашиглан та өөрийн компьютер эсвэл гар утсыг өөрийн төхөөрөмж рүү харснаар л нээх боломжтой юм. Энэ шийдэл нь хэрэглээ талаасаа бол мөрөөдлийн шийдэл шиг сонсогдох хэдий ч мөн л энэ баталгаажуулалтыг хуурч нэвтрэн ороход боломжтой байна.

2011 он руу эргэн харвал, блоггер, судлаач андройд системийн нүүр таних механизмыг энгийн (хөдөлгөөнгүй) зураг ашиглан хуурч болохыг маш хурдан илрүүлсэн байдаг. Та өөрийнхөө хөдөлгөөнт бус зургийг авч, түүнийгээ өөрийн утсандаа харуулан, тэгээд л гүйцээ, та утас руу нэвтэрчихнэ гэсэн үг. Борлуулагчид нь энэ асуудлын хүрээнд нүүр таних нүүр унших механизмд шинээр хөдөлгөөн (амьд хүн эсэхийг нь шалгах) таних шалгуур оруулж өгсөн юм. Ингэснээр тухайн төхөөрөмж нь камер руу харж буй хүнийг амьд хүн мөн эсэхийг нь таних юм. Харамсалтай нь Фотошоф ашиглан хийсэн нүд анивчих эффект нь энэхүү шинэ шалгуурыг хялбархан давж чадсан юм. Зөвхөн өөрийнхөө хөдөлгөөнгүй зургийг нүдээ нээсэн болон нүдээ нээгээгүй байдлаар аваад эдгээр зургаа хооронд сольж харуулснаар нүүр таних механизмын амьд байгаа эсэхийг шалгах шалгуурыг даваад гарчихна гэсэн үг. Эцэст нь сайн мэдээ гэвэл энэхүү нүүр таних механимз нь хөгжсөөр байгаа юм.

### 4. 3D принтерээр 3D нүүр унших механизмыг даван гарах

2017 онд Аппл FaceID гэгдэх шинэ нүүр скандах механизмаа танилцуулсан юм. Гаднаас нь харвал энэ нүүр скандах механизм нь бусад нүүр унших механизмтай ижилхэн мэт сэтгэгдэлийг хэрэглэгчид өгнө. Гэвч, гар утасны камер нь нүүр таних процессыг нарийвчлал өндөртэйгээр хийж, хуурамчаар даван гарах боломжийг хүндрүүлжээ.

Ялангуяа, тухайн утас нь (TrueDepth) хэдэн мянган инфраред гэрлийн туяаг мэдрэгч рүү илгээж, энэ туяа нь таны нүүрийг нарийвчлал өндөртэйгээр таньдаг юм. Энэ механизм нь таны нүүрний 3 -D дижитал загварыг үүсгэж түүнийгээ хадгалдаг ба таны нүүрийг маш олон өнцгөөс таних чадвартай. Apple энэхүү шийдлээ Суралцагч машин (Machine learning)-г ашиглан сайжруулсан бөгөөд өөрөөр хэлбэл энэхүү суралцагч машин нь таныг малгай, шил гэх мэт гоёл чимэглэлийн зүйл өмссөн байх үед ч таних чадвартай юм. Эдгээр нэмэлт шалгуур болон сайжруулалт нь нүүр таних биометрикийг сум нэвтрэхгүй мэт найдвартай болгох ёстой байсан бөгөөд мэдээж эдгээр сайжруулалт нь нүүр таних механизмыг хүчирхэг болгосон. Гэвч Apple өөрийн FaceID -г гаргаснаас 7 хоногийн дараа Вьетнамийн аюулгүй байдлын судалгааны баг үүнийг хакердсан гэдгээ мэдэгдсэн. Үүнийг хийхийн тулд 3D принтер болон нүдний 2D инфраред зураг, мөн нүүрний маск хийх гар ажиллагаа шаардагдах юм. Үнэнийг хэлэхэд өөр ямар ч судалгааны баг бие даан энэхүү халдах арга нь боломжтой гэдгийг баталгаажуулаагүй байна. Миний таамгаар бол бид удахгүй, нүүр таних механизмыг сайжруулж, түүнийг хуурах магадлалыг илүү хүнд болгох шинэчлэл удахгүй гарах байх, гэвч өнөөдрийг хүртэл 2D болон 3D нүүр таних механизм нь төгс биш хэвээр байсаар л байна. Одоо ч гэсэн биометрик баталгаажуулалтын шинэ боломжууд гарч ирсээр байна жишээлбэл, зүрхний цохилт, компьютерын гар дээр үг бичих хурд мөн үүгээр ч зогсохгүй тархины долгионы үелзэл хүртэл шалгах гэх мэт

Түүхээс харахад, халдагч этгээдүүд хуулах, хулгайлах, тойрч гарах гээд тэдэнд хэрэгтэй бүхий л хүчин зүйлсийг хэрхэн хийхээ хайж олж чадаж байгааг хангалттай харуулсан байна. Хэрвээ бид зөвхөн биометрикд найдвал, өмнө нь нууц үг ашигладаг байсантайгаа ижил төрлийн асуудлуудтай тулгарах магадлалтай байна. Одоо л гэхэд, халдагч этгээд таны хурууны хээг эсвэл нүүрийг тань хуулбарлан авсан байхад та эдгээр аргыг баталгаажуулалдаа хэрэглэхэд аюулгүй байдлын асуудалтай тулгарна.

Гэхдээ, ямарч баталгаажуулалтын токен бүрэн найдвартай биш юм. Цоо шинэ төрлийн биометрик шийдэлд найдаж байснаас хамгийн аюулгүй шийдэл нь олон хүчин зүйлийн баталгаажуулалт (нэгээс олон хүчин зүйл ашиглах) ашиглан өөрийн аюулгүй байдлыг хангах нь илүү найдвартай юм.

**Эх сурвалж**: https://www.darkreading.com/operations/passwords-4-biometric-tokens-and-how-they-can-be-beaten/a/d-id/1330939

2017.2.13