HADMÉRNÖK

IX. Évfolyam 1. szám - 2014. március

Török Szilárd
torok.szilard@gmail.com

SZEMÜVEGGEL A BIZTONSÁGÉRT

Absztrakt

A gyors technológiai fejlődéssel együtt biztonsági kérdésekkel is szembesülnek az állampolgárok, cégek és kormányok. A magunknál tartott információk és adatok (dokumentumok, fényképek, levelezés, stb.) jelentős mennyisége önmagában hordozza a biztonsági kockázatokat, a visszaélés lehetőségét. Google kifejlesztett egy speciális szemüveget, amelynek célja a mobilitás, a kommunikáció és vizuális kijelzés új felhasználási területének megalkotása - önálló piac és hozzá tartózó igények megteremtésével. Jelen tanulmány a Google szemüveg biztonsági felhasználási lehetőségeit és kockázatait kutatja.

Together with the rapid technological advances citizens, corporations and governments faced with IT security. The usually carried information and data (documents, pictures, emails, etc.) itself has a lot of risks and possibility of abuse. Google has developed a special glasses based aims mobility, communication and augmented reality to create a new market with its own demands. In this publication security domains and risks of Google Glass will be explored.

Kulcsszavak: *Google szemüveg, Adatszivárgást megelőző rendszer vagy Adatszivárgás elleni védelem, kiterjesztett valóság (Augmented Reality), ellenőrzés, biztonsági ellenőrzés ~ Google Glass, Data Leak Prevention or Data Leak Protection (DLP), Augmented Reality, monitoring, security audit*

BEVEZETÉS

A technológiai fejlődéssel együtt mindannyian szembesülünk biztonsági kérdésekkel, legyen állampolgárokról, piaci működésről vagy éppen a közigazgatás területeiről szó. Sokféle adatot és információt tartunk magunknál, amelyek már mennyiségükből adódóan is jelentős biztonsági kockázatot hordoznak - növelve a visszaélés lehetőségét, a lehetséges veszteség nagyságát. Senki nem állíthatja meg a fejlődést biztonsági okokra hivatkozva, de a kontrollt, az adatvédelmet és az adatbiztonságot feladatkörök, jogosultsági szintek és folyamatok alapján szükséges kontrollálni.

2012 nagy újdonsága a Google által bejelentett Google Glass (továbbiakban rövidítve GG) [1]: kijelzőre vetített kép megvalósítása mellett GPS vevő, mikrofonnal és kamerával lett kiegészítve, kommunikációs oldalról pedig Wi-Fi és Bluetooth kapcsolattal rendelkezik a szemüveg. A felhasználási területeinek köre már most elképzelhetetlen sok lehetőséget és ötletet hozott ki a fejlesztők és a felhasználók táborából.

Magyarországon az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (továbbiakban: Ibtv.) [2], valamint a Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat [3] rendelkezik az ország kibervédelmi szervezeti struktúrájáról, a felhasználandó ellenőrzési eljárásrend ugyanakkor tervezés alatt van.

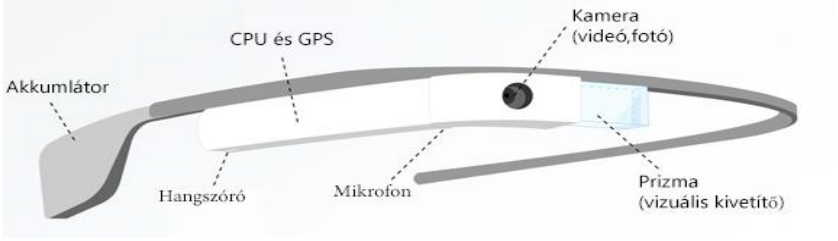
A tanulmány bemutatja magát a Google szemüveget, a biztonsági felhasználási lehetőségeit és kockázatait, amelyek összefüggésben lehetnek az új hazai szabályozási környezettel, akár technológiailag támogatva a bennük szereplő ellenőrzési és IT biztonsági folyamatokat.

GOOGLE GLASS BEMUTATÁSA

A lehetőségek felkutatásához először érdemes részletesen megismerni a már világ szinten bemutatott szemüveg paramétereit.

Google Glass műszaki paraméterei

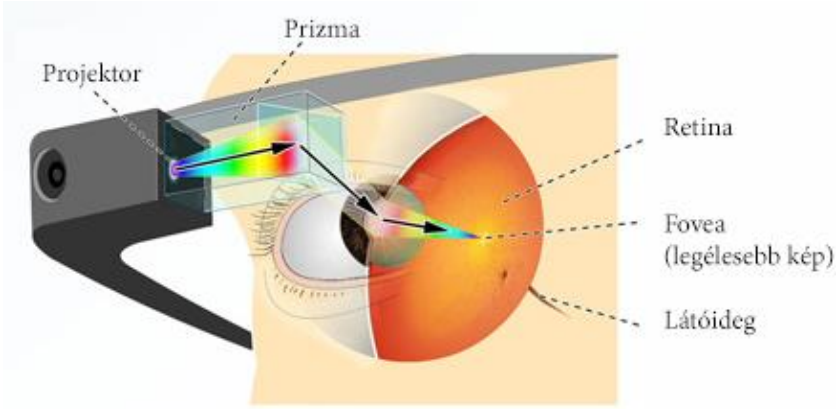
- A szemüveg kerete igen rugalmas, bármilyen arcformához jól illeszthető
- Kivetítőn látható képernyő megfelel egy 25”-os nagyfelbontású képernyő kb. 2,5 méter távolságból történő nézésével
- 5 Megapixeles kamera, 720p felbontású videó-felvétel készítése
- Vezeték nélküli kommunikációk: Wifi - 802.11b/g és Bluetooth
- 12 GB felhasználói memória, Google Felhő szinkronizálással (összesen 16GB)
- Akku kapacitása gyártó szerint egy teljes nap üzemidő, tipikus használat mellett (természetesen vannak olyan funkciói, amelyek jelentősebb akku terheléssel járnak – pl.GPS, videófelvétel, stb.)
- Micro USB csatlakozó és töltő
- Android 4.03 (Ice Cream Sandwich) OS vagy újabb verzió [4]



1. ábra. Google szemüveg fontosabb
Forrás: www.google.com/glass

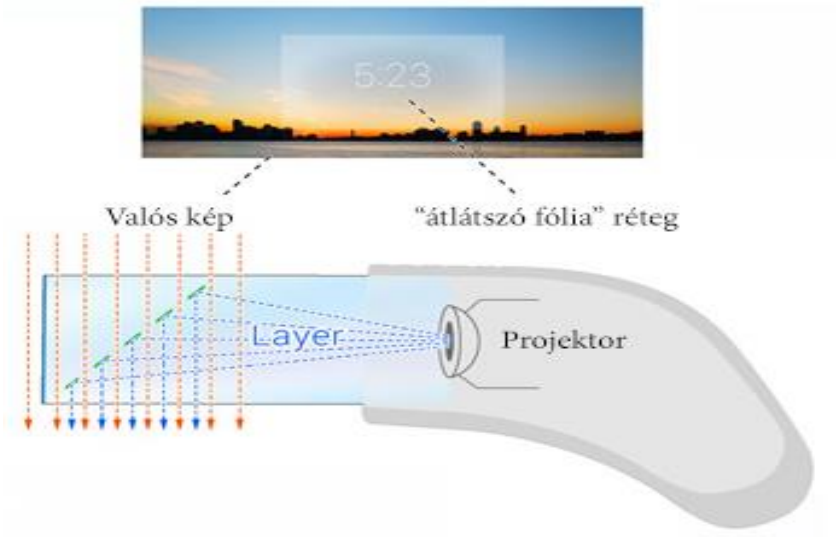
Google Glass kutatási-fejlesztési háttere

„Project Glass” néven ismert kutatás és fejlesztés programban készült el, amelyet azzal a céllal hoztak létre, hogy egy kibővített valóságot megjelenítő, fejre illeszthető kijelzőt alkossanak. Ezt akképpen valósították meg, hogy a szemüveg a rajta elhelyezett prizma segítségével közvetlenül a retinára vetíti a saját maga által alkotott vizuális képet – így az egy átlátszó fóliaréteghez hasonlóan kerül rá a valós képre.



2. ábra. Kivetített köztes vizuális réteg látóidegen történő megjelenítése
Forrás: www.google.com/glass

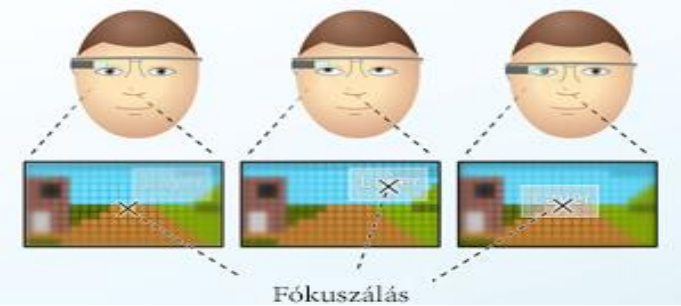
A szemüveg kijelzőjén megjelenő (okostelefon) adatokhoz és ikonokhoz hasonlóan képes megjeleníti a különböző információkat. Irányításának fő tulajdonsága hangvezérlés, azaz egyáltalán nincs szükség kézi irányításra. Android operációs rendszerre mellett a könnyű vezeték-nélküli csatlakozások támogatásával alkották meg a szemüveget a Google X Lab-ben (ugyanitt vezető nélküli autókat is fejlesztenek).



3. ábra. Valós és a szemüveg által készített virtuális réteg működése
Forrás: www.google.com/glass

A fejre illeszthető „kiterjesztett valóságot” mutató kijelzők ötlete bár egyáltalán nem újdonság, a Google szemüvegének kisebb méreteiből adódó jóval kényelmesebb viselés miatt is felkapottabb lett a sajtóban.

A termék mellé egyedi beviteli megoldások is felsorakoznak. Az AR (Augmented Reality – kiterjesztett valóság) rendszerű napszemüveg szemmozgással történő vezérlése túlságosan is megterhelő lehet, míg a puszta kéz felismerése és követése felesleges terhet róna a központi vezérlőegységre.



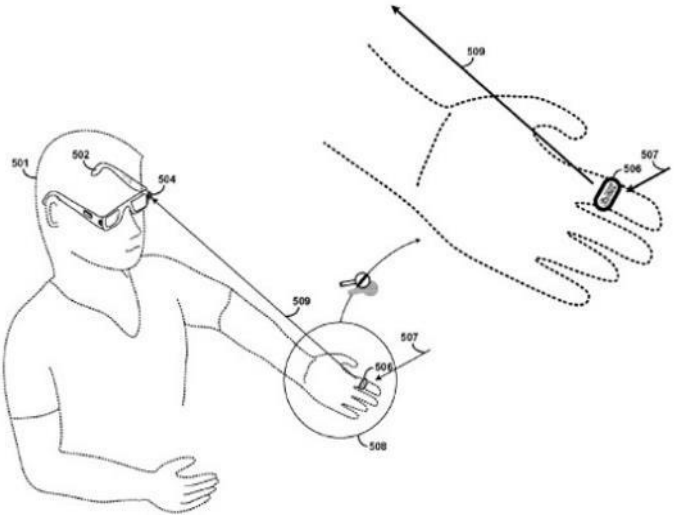
4. ábra. A fókuszálást követi a szemüveg vizuális rétegének kivetítése Forrás: www.google.com/glass

Összefoglalva: tulajdonképpen nincs másról szó, mint egy Google napszemüvegbe oltott telefonról, vagy ha úgy tetszik HUD (Head-up Display – fejmagasságú kijelzőről).

Az eredeti tervekben még a hagyományos szemüvegekre jellemzően a lencséket helyettesítették volna kijelzővel, azonban az újabb formatervezésnek is a technológia fejlődésének köszönhetően lehetővé vált a hétköznapi szemüvegekbe történő integrálása.

Az ipar pozitív visszajelzésekkel fogadta a termék megjelenését, ugyanakkor kritikák és a paródiák keresztttüzébe is került a termék - a lehetséges felhasználási területek és azokkal történő visszaélések miatt. Erre is reagálva a Google kijelentette, hogy nem fogja reklámozásra használni a készüléket. [5]

Google éppen ezért egy infravörös gyűrű bevetésében gondolkodik, amellyel térbeli elmozdulásokat lehet követni és erre alapozott kézmozgás alapú parancsokat definiálni és használni a szemüveggel. [6]



5. ábra. A szemüveg utasítása kéz és az infravörös gyűrű mozgatásával
Forrás: www.theverge.com/2012/5/17/3026571/google-project-glass-infrared-ring-patent

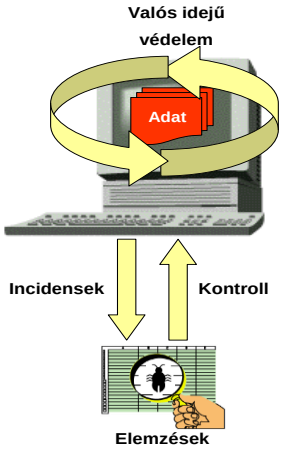
BIZTONSÁGI CÉLÚ FELHASZNÁLÁSI TERÜLETEK

Ebben a fejezetben kerül ismertetésre a Google Glass technológiára alapozott biztonsági vonatkozású lehetőségek és ötletek bemutatása – például az ismert adatbiztonsági és IT biztonsági területeken felhasznált rendszerek és megoldásokkal való összekapcsolásával.

Jelen tanulmányban szereplő kutatás célja, hogy az ismertetett GG alapú megoldás milyen módon tudja hasznosan kiegészíteni az ismert biztonsági és informatikai biztonsági feladatok elvégzését, szabályzások betartatását, továbbá milyen új lehetőségeket biztosíthat ezen a területeken dolgozó, például ellenőrzést végző szakembereknek. (Az ismertetésre került ötletek, megoldások bizonyos esetekben egymásra is épülnek)

Adatszivárgás elleni megoldások (DLP)

Az adatszivárgás elleni megoldások végponti és hálózati oldalon próbálják követni, elemezni vagy akár blokkolni az informatika által kezelt adatokat, azaz az IT biztonsági és adatbiztonsági szabályok betartását kontrollálni.



6. ábra. DLP megoldások magas szintű működése

DLP megoldások fontosabb jellemzői:

- Az információ keletkezésének forrásánál és mozgásánál szükséges jelen lenni. jelen: Kliens oldali és hálózati aktivitások monitorozásával (fájl mozgatása, másolása például hálózati meghajtóról lokálisan használt adattárolóra) egy-egy káreseményhez vezető tevékenységlánc kiinduló fázisában dönt – szabályrendszer alapján – a kockázat szintjéről, és a beavatkozás szükségességéről, ezáltal megelőzheti az adatbiztonságot sértő események bekövetkezését.
- IT biztonságpolitika betartatásának hatékony eszköze. A rendszer a felhasználó igényeinek megfelelően kell paraméterezhető legyen – a paraméterezés feladata a szervezet biztonságpolitikájának leképezése szabályokká, kontrolokká, melyek automatizmusok segítségével, minimális humán interakcióval gondoskodnak a szabályok betartatásáról.
- Nagy felhasználószámú hálózatok központi kontrollja: teljes értékű működési automatizmusok, prevenciók készíthetők, gyakorlatilag az adatvédelmi szabályzatot komplex mondatokba, „ha ez és ez történik, akkor tedd ezt és ezt” típusú elemi relációkba legyenek szervezhetőek. A riasztási, a távoli beavatkozási, és a megelőzési automatizmusok révén minimális személyi felügyelet szükséges akár nagy felhasználószámú rendszerek állandó kontrolljához.

A szervezet igényeinek megfelelően a felhasználói aktivitások mélyreható, illetve teljes naplózására kerül sor. A file- és alkalmazás műveletek, a billentyűzet használat, a ki és belépés idejének rögzítése lehetőséget biztosít számos hasznos elemzésre, lekérdezésekkel, üzleti intelligencia eszközökkel, illetve adatbányászati eljárásokkal magas szinten szintetizált információ nyerhető ki.

Google szemüveg - mint a DLP része

Hatékony segítsége lehet egy IT biztonsági vezetőnek vagy a területen dolgozó ellenőrzést végrehajtó IT biztonsági munkatárs számára egy Google szemüveg típusú megoldás.

Automatikus QR olvasó szoftvert szükséges telepíteni a szemüvegre, majd a felhasználási területen, például a szobák feliratozása mellet érdemes QR kódokkal ellátni. Ennek segítségével nem szükséges az akkut jelentősen terhelő GPS vevő használta, a szemüveg a folyósón, szobák táblái mellett elhelyezett kódokkal azonosítja az ellenőr épületben történő mozgását.

Hang vagy kézmozgás alapú utasításokkal lehetősége van az ellenőrzést végrehajtónak lekérdezni egy adott szobában elhelyezett felhasználók fotóit, a használt számítógépek és ismert, legálisan használható adathordózók típusát vagy akár fotóit egyaránt.

Gyakorlatilag egy igen gyors személyi és adatszivárgással kapcsolatos ellenőrzést lehet végrehajtani a szemüveget viselőnek: azonnal detektálhatja azon személyeket, akik nem a saját számítógépükkel dolgoznak, vagy az engedély nélküli adathordozó használatát.

Belső ellenőrzés IT támogatása

A megoldás informatikai alapú támogatást képes biztosítani egy szervezet belső ellenőrzését végző munkatársainak: az ellenőrzés folyamatát, státuszát, konkrét ellenőrzési listák elvégzését, vagy akár gyors videó konferencián történő egyeztetéseket képes az eszköz megjeleníteni, lebonyolítani.

A háttér informatikai rendszerekkel történő támogatás kiterjedhet a nyilvántartások online szintű ellenőrzésére, gyors-felmérések és azok visszaellenőrzésére is alkalmassá tehető.

Munkahatékonyság elemzés

Személyi ellenőrzéseken belül a hatékonyság ellenőrzése is lehetségessé válik a szemüveg használatával: azonosítható adott munkaterületen a személyek mozgása, számítógépes aktivitása, háttérben akár létszámellenőrzést is végezve.

A hatékonyság ellenőrzés kiterjedhet a munkafolyamatok (QR kódokkal azonosítva), munka időszakok (túlóra, késés, szünetek, stb.) területére is.

Vezeték nélküli hálózati ellenőrzések

A szemüvegbe beépített WiFi vevő segítségével könnyen, akár más folyamat végzése mellett automatikusan elvégezhető a vezeték nélküli hálózatok jelenléte, illegális használata (pl. munkahelyen: saját gépen, telefonon futtatva, zárt intézmény területére benyúló külső/kockázatos Wifi hálózatok kimutatása, stb.) A felmérés folyamatát, hatékonyságának növelését szintén pl. QR kódok elhelyezésével lehet támogatni.

Vezeték nélküli hálózati gyorsellenőrzés

Etikus hackerek munkája során – tipikusan az IT biztonsági sérülékenység vizsgálatoknál - jellemző igény nagyobb intézmények, szervezetek üzemeltetésének vonatkozásában a vezeték nélküli hálózatok feltérképezése: hozzáféréseik ellenőrzése, kvázi WiFi térkép összeállítása irodák, helységek, stb. vonatkozásában, lefedettség és felderíthetőség tulajdonságai, stb.

GG megoldás ilyen irányú felhasználásával a szemüveg beépített WiFi rendszere szkennerként történő alkalmazásával, az etikus hacker vagy az auditor gyorsan és kényelmesen elvégezheti a felmérést, eredményét rögtön képes kielemezni, akár módosítani a felmérés folyamatát, stratégiáját.

Alkalmazás audit

Szervezeteknél használt szoftveres megoldásokra jellemző az egyedi kialakítás, de webes és más keretrendszerek esetén egyedi design elemek (akár logók is) alkalmasak a vizuális beazonosításukra.

Ellenőrzés végzése során ismeretlen alkalmazás futtatását is lehetséges lehet a szemüveggel detektálni (kézjelzést követően központi képfeldolgozó rendszer összeveti a nyilvántartásban levő megoldások fontosabb képi elemeivel), vagy akár az ismeretlen szoftver futtatásának tényét rögzíteni. A megoldást a pontosság és hatékonyság elérése érdekében érdemes lehet QR kód alapú szoba és/vagy személy azonosítással összekapcsolni.

Igazságügyi szakértők támogatása

Informatikai igazságügyi szakértők mindennapos munkája során jellemzően hardvereket azonosítanak, a rajtuk tárolt adatokat és a futtatott környezetet vizsgálják meg, és az ügyfél vagy bírósági folyamatok alapján vizsgálati jelentést készítenek róla.

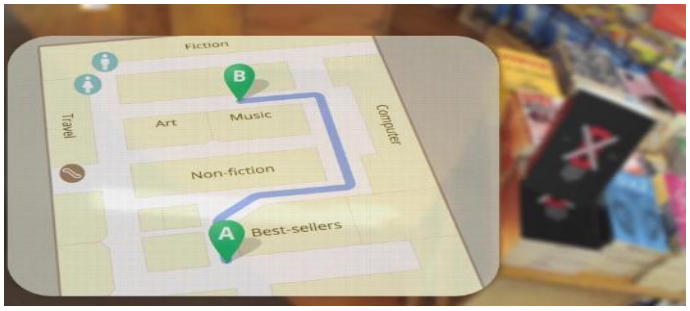
Informatikai vagy általános biztonsági események kapcsán a szemüvegbe épített kamera és videó alkalmas lehet (pl. megfelelő időbélyeg használata mellett) az ilyen típusú vizsgálati feladatok támogatására: adott megállapításokat képekkel, audio és videó felvétellel kiegészítve lehet rögzíteni, dokumentálni. A megoldás kiterjeszthető a rendvédelmi szervek nyomozásainak alátámasztására, támogatására, de akár annak utólagos ellenőrzésére is.

Leltározás

Vonalkódok vagy QR kódok használata mellett egy az általános leltározási folyamatnál jóval gyorsabb és hatékonyabb leltározás alakítható ki, ahol mind a leltározást végző és az abban közreműködő, vagy ellenőrző személy (pl. átadás-átvétel esetén az átvevői oldal képviselője) a HUD képernyőn a belső nyilvántartások adatait láthatja a kódok alapján, lekérdezéseket és saját kimutatásokat, összesítéseket is felvehet a leltározás közben a HUD képernyőjére. Megfelelő informatikai háttértámogatással a leltározás tulajdonképpen valós időben elvégezhetővé válhat.

Nyomozati szerep

Nyomozási folyamatok a GG rendszer használatával nagyobb támogatás biztosítható, hiszen adott helyszínen, a felismert eszköz (vonalkód, QR kód) alapján gyorsított keresések, kimutatások és navigáció jeleníthetőek meg a HUD kijelzőn. [7]



7. ábra. Tájékozódás épületen belül (Forrás: www.pcmag.com)

Lehetőség nyílik az online egyeztetésekre, akár operatív folyamatok irányítási és döntési támogatásainak kivitelezésére is.

Nyomozás során speciális kéz vagy hang alapú utasításokkal további utasítások adhatók ki a virtuális jegyzőkönyv számára, vagy későbbi feldolgozást végzők részére, illetve prompt hang és videó rögzítési funkciók is elérhetővé válhatnak.

Általános azonosítási eljárások támogatása vizuális és hang alapon

GG technológia felhasználásával és online kapcsolattal - például felhőbe feltöltött kép vagy hang alapján - lehetőség van személyek azonosítására, akár hang és arc mozgás kielemzésének felhőbe történő felküldésével és ott történő elemzésével hazugságvizsgálat és egyéb vizsgálatot támogató elemzés lefuttatására is.

Több lépcsős azonosítása és jogosultság kezelés támogatása

A szemüveg által látott például online grafikus jel, kód (pl. QR kód) és hangbevitel használatával (pl. a HUD kijelzőre tett felolvasandó szavak) együttesével igen összetett azonosítások alakíthatóak ki.

Az online informatikai rendszerkapcsolat meglétéből eredően többféle típusú kódok (szobák QR kódja, illetve egy fali kijelzőn online megjelenő QR kód) összevetése mellett további

relációk is megállapíthatóak. Például adott személy azonosítása a biztonsági kamera arc azonosításával, a HUD-on megjelenő kód vagy PIN begépelésével vagy bemondásával, szoba QR kódjának és a munkavégzést elkezdő engedélyének összevetése, vagy akár adott alkalmazás futtatása közben történő összetett jogosultság ellenőrzés végrehajtására is alkalmassá tehető egy GG-vel kiegészített informatikai rendszer.

Rejtett és bizalmas kommunikációk

Saját kézalapú kommunikációk felvételével, egyedi jelek definiálásával mások előtt rejtett jelek, üzenetek adhatók át más személy részére. Ez lehet például egy tárgyalás vagy felmérés során adott jelzés, ami a bizalmas kommunikációban résztvevő számára jelzést vagy információ lekérdezést is adhat a többiek részére.

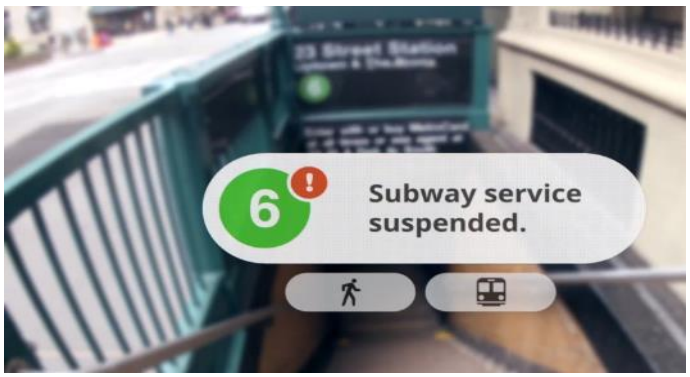
8. ábra: Videó konferencia lehetőségei a szemüveggel
Forrás: The Verge, www.theverge.com

Videó konferenciában levő személyek a szemüveg használatával meg tudják őrizni a másik fél inkognitóját, illetve a kéz és szemmozgás alapú utasításokkal bizalmas jelzéseket is tehet a részt vevők számára.

Riasztások kezelése

GG viselése esetén olyan alkalommal is megkaphatja felelős beosztásban levő személy egy rendszer riasztásait, amikor sem telefon, sem más kommunikációs csatornán nem érhető éppen el (életszerűen azonban WiFi elérés adott), valamint a felhasználó jelzéseivel akár részletesebb információkat is le tud kérni az eseménnyel kapcsolatosan, speciális folyamatok és kommunikációk elindítására is lehetőség biztosít az eszköz.

Lehetőség van távfelügyeleti rendszerbe ügyfélként, vagy felügyelet irányító biztonsági személyként belépni, konkrét vizuális információkat lekérdezni, azokra visszajelzéseket megfogalmazni, akár utasításokat kiadni a rendszer számára (pl. rendőrség értesítése, stb.)



9. ábra: Közlekedési irányítás és információ biztosítás
Forrás: www.pcmag.com

Nagy értékű szállítmányok biztosítása során a vagyonőr által viselt rendszer folyamatosan rögzítheti vagy akár továbbíthatja a képi felvételeket a bevetési irányítási központba.

Állampolgári bejelentések (intelligens 112)

GG hétköznapi használata lehetőséget biztosíthat rendvédelmi szervek, önkormányzatok felé történő jelzések, felvételek, bejelentések küldésére. Felvétel készíthető utcai balesetről vagy bűncselekményről – a telefon elővételének és kezünk lefoglaltságából eredő értékes másodperceket nyerve.

Önkormányzatoknál a helyi ügyek intézése, események bejelentése is lehetséges lenne. Budapesten jelenleg is vannak olyan kerületek, ahol kátyú, de akár hajléktalan és illegális hulladék bejelentés web-es formában létezik. GG-vel a bejelentés, de akár az arról kapott hivatali válasz megjelenítése is hatékony kommunikációt és ügyvitelt eredményezhet, a szemüveg folyamatos használata maga nagyobb bejelentési mennyiséget és hatékonyságot biztosíthat.

Élelmiszerbiztonság

Google Glass használata mindennapok biztonságát is növelheti élelmiszerekre vonatkozó és bolti hálózatbeli információk közvetítésével és elemzésével.

Adott élelmiszert felismerve (embléma, vonalkód, stb.) alapján tájékoztatást adhat étel allergiával kapcsolatban (pl. felhasználó által előre megadott listával történő összevetéssel), akár az adott vagy más bolthálózat által interneten közzétett árlisták alapján alternatívákat, sőt, kedvezőbb árakra is felhívhatja a figyelmet.

Fogyatékkal élők biztonsága

Lévén a szemüveg szárába a speciális hangkeltő a koponyacsontra támaszkodik, így a hangrezgéseket a középfül (légvezetés) megkerülésével tudja közvetíteni a belső fülbe. Ez azon túl, hogy nem korlátozza a környezeti hangok beáramlását, alkalmas lehet halláskárosodott emberek számára is további információs és biztonsági szolgáltatások nyújtására.

10. ábra. Valós idejű szövegfordítás az eredeti szöveg helyére illesztve
Forrás:Word Lens – www.wikipedia.org

Kiemelendő a képelemzéssel történő információk felhasználók részére történő közvetítésének lehetősége:

- pl. látáskárosult részére közlekedési és útviszony információk bemondása (akár lefordítása), amely közlekedési táblára vagy épp lépcsőre, kátyúra, hívhatja fel a figyelmet,
- élelmiszer felismerése és hangalapú ismertetése (látás és halláskárosult szempontjából is hasznos lehet az információ és a jelzés)
- személyek felismerése, vagy egyéb adatok (RFID, WiFi) alapján történő szociális információk továbbítása (kiterjedve a közelben levő ismerősről történő jelzésre, például segítségkérés okán)

FELHASZNÁLÁSI TERÜLETEK KOCKÁZATAI, VISSZAÉLÉSI LEHETŐSÉGEK

A kéretlen reklámokon túl, a Google magánszféra megsértésének, kvázi elleni induló hadviselésének tartják a Google szemüveg használatát, valamint a szemüveg információinak (kéretlenül végzett) begyűjtését együttesen.

Ezen félelmek jogosan kerültek felszínre, hiszen nem ismert, hogy maga a Google (mint marketing irányultságú szolgáltató), mire fogja felhasználni a szemüveg felhasználóinak adatait. [8] Ilyen például a földrajzi helyzet, a felvételek információ mellett további keresési és egyéb felhasználási területek információival történő összevetéséből adódó marketing adatokat is jelenthet, akár a különleges személyes adatokat is érinthet (tényleges politikai és világnézeti meggyőződés). [9]

A GG-re vonatkozó tilalmak, helyi szabályok is megjelentek, ami inkább a felhasználás formájára és területére is vonatkozik. Erre legjobb példa, hogy Kaliforniában megbüntetek egy hölgyet 2013 októberében, mert vezetés közben Google Glass-t viselt – egész pontosan mivel a vezető számára látható monitort viselt, amit az ottani közlekedési szabályok tiltanak. [10]

Valószínű az újabb és újabb biztonsági és egyéb kockázatok sora mind az új felhasználási területekből fognak adódni.

Ilyen például:

- bionikus retinaként jelent meg egy cég terméke, amely egy mesterséges retina funkcióit ellátva képi információkat képes továbbítani a látóidegeken keresztül az agy emberi számára. [11]
- Lehetséges kockázat: agyba bejutó képek megváltoztatása.
- Fordító program jelent meg a GG szemüvegre, amely grafikusan be is helyettesíti az idegen nyelvű szöveg helyére a lehetséges fordítást. [12]
- Azonnal adódik a hibás vagy félreérhető fordításokból eredő problémák sora, ami akár a szándékosan megváltoztatott információival történő visszaéléséig is elvezethet.
- Orvosi konzultációkra történő kísérletezések folynak külföldi egészségügyi intézményekben, amely során egy specialista orvos távolról tanácsot adhat, akár irányíthat műtétet (szóbeli utasításokkal) – interaktívan részt is vesz benne, pl. audio/vizuális közvetítés mellett. [13]
- Kockázat lehet a kommunikáció lehallgatása, egészségügyi információk szivárgása, extrém esetben szándékosan negatívan befolyásolt orvosi beavatkozással végzetes károsodás okozása a betegnek.

Elveszett GG (akár Android telefon) esetére a Google a „remote location”, azaz távolról történő helymeghatározás funkció használatát említi meg a Google Glass saját weboldalán. Lehetséges kockázatai a funkcióból rögtön eredő illegális helymeghatározás, üzenet küldés, akár a telefonon tárolt adatok teljes törlése lehet. [14]

Ugyancsak a GG Android operációs (4.04-es verzióra épülő) rendszeréből ered az a kockázat, hogy a letölthető applikációk ellenőrzésének hiányában a szemüveg tulajdonképpen bármilyen, a szemüveg képességeivel való visszaélésre használható lehet. Lehetséges kockázatok: legmagasabb szintű (root) hozzáférést követően bármilyen, a szemüveg által kezelt, lekért és elemzett adat kiszivárogtatható, akár az adatok feldolgozása alatt megváltoztathatóak, visszaélések kivitelezése a felhasználó tudta nélkül.

Symantech már beszámolt egy komoly IT biztonsági problémáról is: GG által beolvasott QR kód segítségével átkonfigurálható a WiFi beállítás, és így észrevétlenül átirányítódhat az internetes forgalma egy a támadó által lehallgatott, befolyásolt hálózat felé. [15]

A termékben rejlő végtelennek tűnő lehetőségek közül kiemelendő egy amerikai termék (Mutualink), amely segítségével valós időbeli multimédia kapcsolat segítségével hatékonyabbá tehető a közszféra biztonsági szakterületeinek munkája. Fontosabb példák a felhasználás területeire:

- tűzoltók az oltás megkezdése előtt láthatják az érintett terület, épület tervrajzát, leírásait, akár a tűzvédelmi leírásokat,
- Mentők a helyszínre érkezésig bezárólag információt kaphatnak az ellátásra szoruló személyek egészségügyi nyilvántartásaiból (vércsoport, gyógyszerallergia, nyilvántartott betegségek, stb.),
- Katasztrófavédelmi egységek a tájékozódásra, a helyismeret beszerzésére, de akár a műveletek irányításával kapcsolatos információk és utasítások továbbítására is használhatják. [16]

Természetesen a felsorolt felhasználási területek során kezelt információk kiszivárgása és befolyásolása (módosítása) igen jelentős kockázatot hordoz magában.

Egyesült Államokban adatvédelmi és adatkezelési kérdések merültek fel a szemüveg közterületen történő használata (pl. kávézóban videó felvétel készítése) kapcsán. Google Street View (3 dimenziós, térképhez kapcsolt multimédiás adatbázis) több problémát felvetett már, de azokat mindennapi szintű kiterjesztéseként vélik megjelenni a GG közterületi használata esetén – feltehetően a legtöbben nem kérnének engedélyt a szemüveg audio és videó felvételkészítése esetén az érintettektől, és nem is látszik a felvétel készítése (míg telefon és kamera esetén relatív egyértelmű milyen irányban készül a felvétel). [17]

A szemüveggel történő illetlen, modortalan felhasználásra vonatkozóan már külön angol elnevezés is elterjedt: „Glasshole”. Legismertebb, általánosan már elterjedt illetlen GG felhasználási területek:

- mosdó,
- kaszinó,
- udvarlási helyzetek,
- társasági beszélgetésben az online letölthető információkkal felvágni,
- pénzügyek intézése (pl. ATM)

GG típusú technológiák egyre szélesebb körű elterjedése átírhatja az eddigi munkahelyi előírásokat, és újabb személyiségi jogi kérdéseket vet fel. Az új eszközök a viselhető eszközök elterjedése a munkavállalói szerződések és a titoktartási szabályok felülvizsgálatára késztetheti a cégeket.

A Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) megalakulása óta az internet és az új információs technológiák jelentette adatvédelmi kihívásokat is figyelemmel kísérik. Google prezentációt követően a NAIH elnökhelyettese a szemüveg valamennyi funkcióját kipróbálta. NAIH munkatársainak elsődleges érdeklődése az adatvédelmi aggályokra irányult, hiszen a szemüveg titkos megfigyelésekre is alkalmas lehet. [18]

Terjedőben van azon elvárás, hogy a szemüveg kifelé is adjon jelzést arról, hogy pl. videó felvételt rögzít a környezetéről – bár az interneten terjedő hackerek munkája alapján várhatóan ez is könnyen kikapcsolható utólagosan.

Ugyancsak megfogalmazódhat az összegyűjtött személyes adatok tárolása és felhasználása miatti aggály, azaz nem ismeret a sorsuk.

ÖSSZEGZÉS

A tanulmányon keresztül ismertetésre került a Google Glass megoldása, amelyet az újabb és újabb Google fejlesztési bejelentések érdemben nem befolyásolnak, legfeljebb a lehetőségeket listáját bővíthetik.

Az ismertetés kiterjedt a biztonsági és informatikai biztonsági irányú támogatások lehetséges köreire, a benne rejlő aktuális biztonsági célú felhasználású lehetőségek rövid tárházára. Áttekintésre kerültek az ismert adatvédelmi és IT biztonsági kockázatok, a felhasználási területekből adódó további problémák is.

Könnyedén belátható, hogy egy ilyen típusú eszköz (azaz beleértve a Google minden konkurenciáját is), az online számítógép rendszerek és teljesítményeinek összekötésével végtelen biztonságot támogató lehetőséget rejt magában, és pont ebből adódóan az informatikai kockázatok teljesen új dimenziói is megnyíltak.

A röviden ismertetésre került 16 biztonsági és ellenőrzési vonatkozású felhasználási és fejlesztési lehetőség messze nem fedi le az ilyen típusú technológiában rejlő perspektívákat.

Ugyanakkor a bemutatott példák alkalmasak arra, hogy miként jelenhet meg egy új technológia például az IT biztonság modern eszközeként a szervezetek szabályozásainak betartatásaként, ellenőrzési folyamatok, kommunikációk és irányítások támogatásaként, de akár a magánszféra néhány felhasználási területe is izgalmas kihívásokat biztosít a következő évekre.

Felhasznált irodalom

[1] Wikipedia, (2013. november 11.) *Google Glass*. letöltés dátuma: 2013. november 13., forrás: Wikipedia – The Free Encyclopedia: http://en.wikipedia.org/w/index.php?title=Google_Glass&oldid=581136709

[2] Magyar Kormány: A Kormány 1139/2013. (III.21.) határozata Magyarország Nemzeti Kiberbiztonsági Stratégiájáról. Magyar Közlöny, 47. (2013) 6338.

[3] Magyar Kormány: „Az állami és önkormányzati szervek elektronikus információbiztonságáról” szóló törvény, 2013. április 25., 2013/69. 50241.

[4] Google, (2013. november 13.) *Google Glass Tech Spec.* letöltés dátuma: 2013. november 13., forrás: Google Support – Glass: https://support.google.com/glass/answer/3064128?hl=en&ref_topic=3063354

[5] Wikipedia, (2013. december 12.) *Google Glass*. letöltés dátuma: 2013. november 13., forrás: Wikipédia – A szabad enciklopédia: http://hu.wikipedia.org/w/index.php?title=Google_Glass&oldid=13784682

[6] Adi Robertson, (2012. május 17.) *Google Project Glass patent shows control system using infrared rings and fingernails*. letöltés dátuma: 2013. november 13., forrás: The Verge: http://www.theverge.com/2012/5/17/3026571/google-project-glass-infrared-ring-patent

[7] YouTube - Google, (2012. április 4.) *Project Glass: One Day*. letöltés dátuma: 2013. november 12., forrás: YouTube: http://www.youtube.com/watch?v=9c6W4CCU9M4

[8] David Streitfeld, (2012. március 12.) *Google Concedes That Drive-By Prying Violated Privacy,* letöltés dátuma: 2013. december 12., forrás: The New York Times: http://www.nytimes.com/2013/03/13/technology/google-pays-fine-over-street-view-privacy-breach.html?pagewanted=all&_r=3&

[9] Milo Ziannopoulos, (2012. április 2.) *Google Glass and Surveillance Culture,* letöltés dátuma: 2013. december 12., forrás: Slashdot: http://slashdot.org/topic/cloud/google-glass-and-surveillance-culture/

[10] Sky News, (2013. október 30.) *Google Glass Driver Gets Ticket From Police,* letöltés dátuma: 2013. december 12., forrás: Sky News: http://news.sky.com/story/1161741/google-glass-driver-gets-ticket-from-police

[11] Second Sight:*The Argus II Retinal Prosthesis System,* letöltés dátuma: 2013. december 12., forrás: http://2-sight.eu/en/argus-ii-rps-pr-en

[12] Kevin Kelleher, (2010. december 19.) *World Lens + Google Goggles = A useful augmented reality app,* letöltés dátuma: 2013. december 12., forrás: Reuters: http://blogs.reuters.com/mediafile/2010/12/19/word-lens-google-goggles-a-useful-augmented-reality-app/

[13] John Nosta, (2013. június 27.) *How Google Glass Is Changing Medical Education,* letöltés dátuma: 2013. december 12., forrás: Forbes: http://www.forbes.com/sites/johnnosta/2013/06/27/google-glass-teach-me-medicine-how-glass-is-helping-change-medical-education/

[14] Google, (2013. december 12.) *Google Glass Tech Spec*. letöltés dátuma: 2013. december 13., forrás: Google Glass FAQ: https://sites.google.com/site/glasscomms/faqs

[15] Candid Wueest, (2013. július 18.) *Google Glass Still Vulnerable to WIFI Hijacking Despite QR Photobombing Patch*. letöltés dátuma: 2013. december 13., forrás: Symantec: http://www.symantec.com/connect/blogs/google-glass-still-vulnerable-wifi-hijacking-despite-qr-photobombing-patch

[16] Mutualing, (2013. augusztus 19.) *Mutualing Unveils Google Glass for Public Safety,* letöltés dátuma: 2013. december 13., forrás: BusinessWire: http://www.businesswire.com/news/home/20130819005155/en/Mutualink-Unveils-Google-Glass-Public-Safety

[17] Claire Cain Miller, (2013. június 19.) *Privacy Officials Worldwide Press Google About Glass,* letöltés dátuma: 2013. december 13., forrás: The New York Times Technology Blog: http://bits.blogs.nytimes.com/2013/06/19/privacy-officials-worldwide-press-google-about-glass/

[18] Nemzeti Adatvédelmi és Információszabadság Hatóság, (2013. szeptember 11.) *NAIH munkatársai elsők között próbálták ki a Google Glass-t,* letöltés dátuma: 2013. december 13., forrás: NAIH weboldal: http://www.naih.hu/files/GoogleGlass_koezlemeny_2013_09_11.pdf