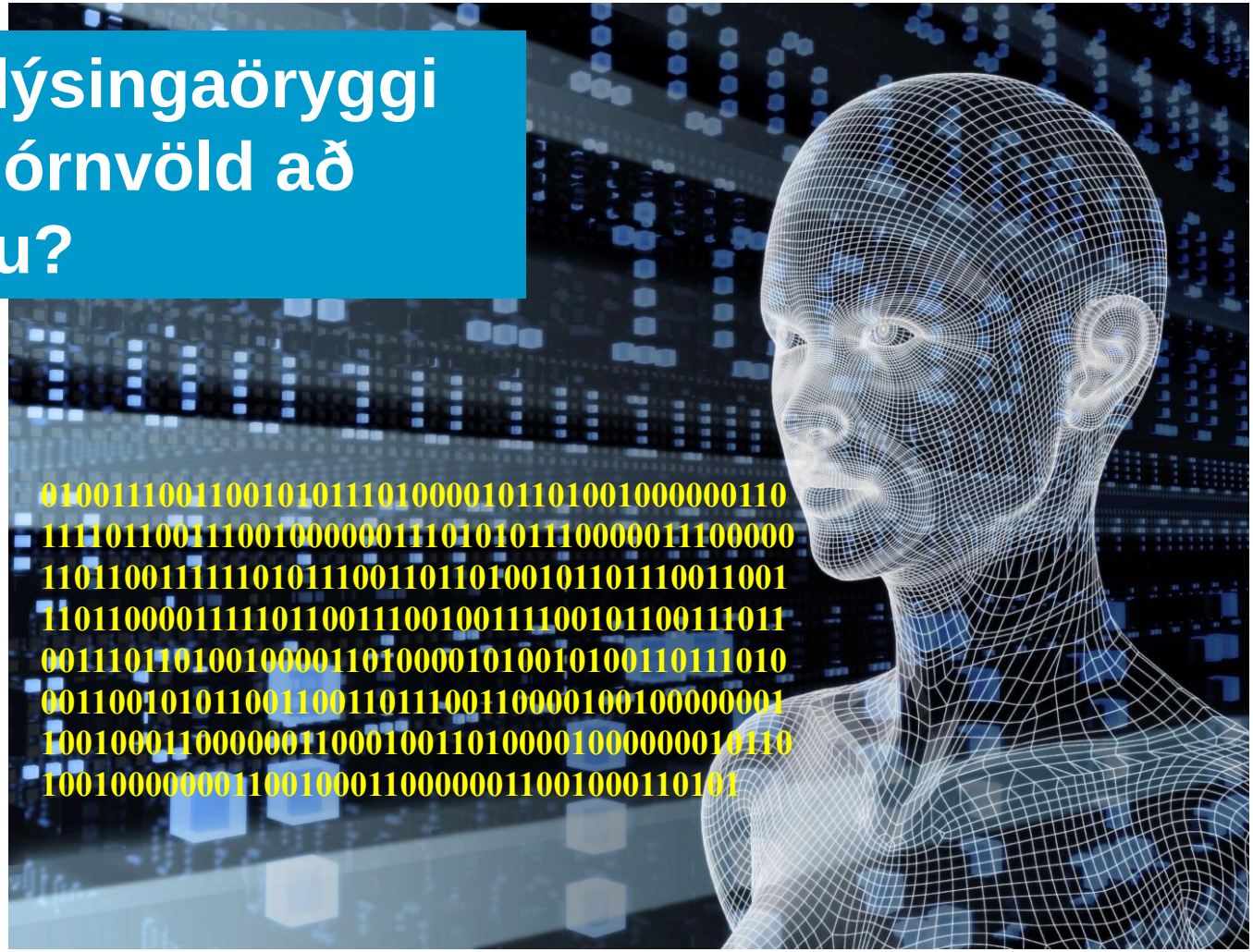
Net- og upplýsingaöryggi Hvað eru stjórnvöld að gera í málinu?



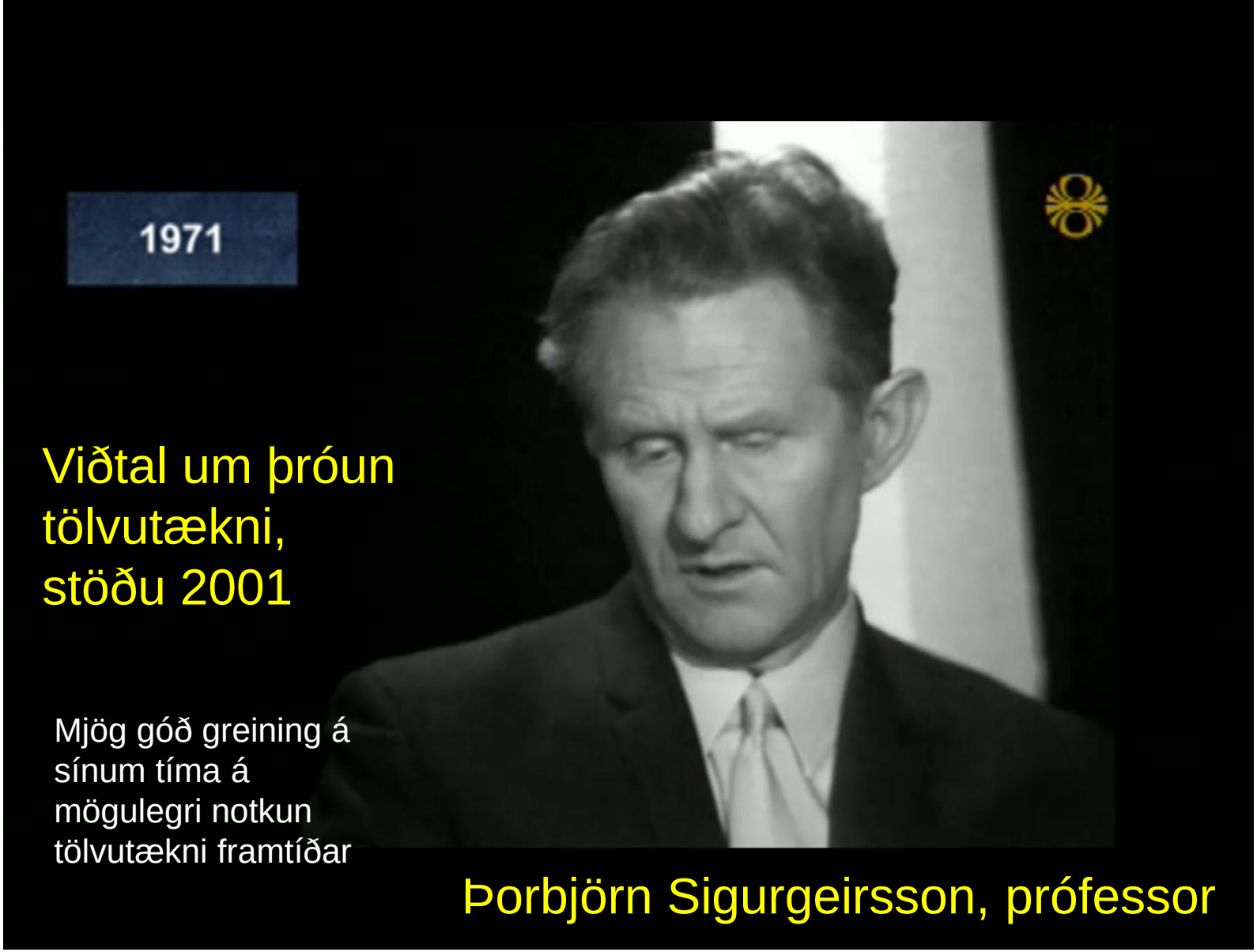
(Net- og upplýsingaöryggi - Stefna 2014 – 2025)

Athugasemd varðandi þessar glærur

- Þessar glærur voru teknar saman vegna kynningar á vinnu stjórnvalda að stefnumótun varðandi net- og upplýsingaöryggi á UT deginum, 27. nóvember 2014. Glærurnar einar sér eru ófullkomin heimild kynningarinnar, þeim var einungis ætlað að vera einskonar leikmynd fyrirlestrarins. Skýringartexta hefur verið bætt inn á einstaka glærur hér til að gera skiljanlegra í hvaða samhengi þær voru notaðar.
- Fyllri upplýsingar um þá vinnu sem var kynnt má fá í frétt á vef innanríkisráðuneytisins, sem birt var daginn eftir. Þar má nálgast drög stefnunnar sem kynnt var og samantekt niðurstöðu samráðsfundar með hagsmunaaðilum, sem haldinn var 2. júní 2014.

Tölvubylting síðustu áratuga: Öld tækifæranna

- fyrir grúskara og notendur

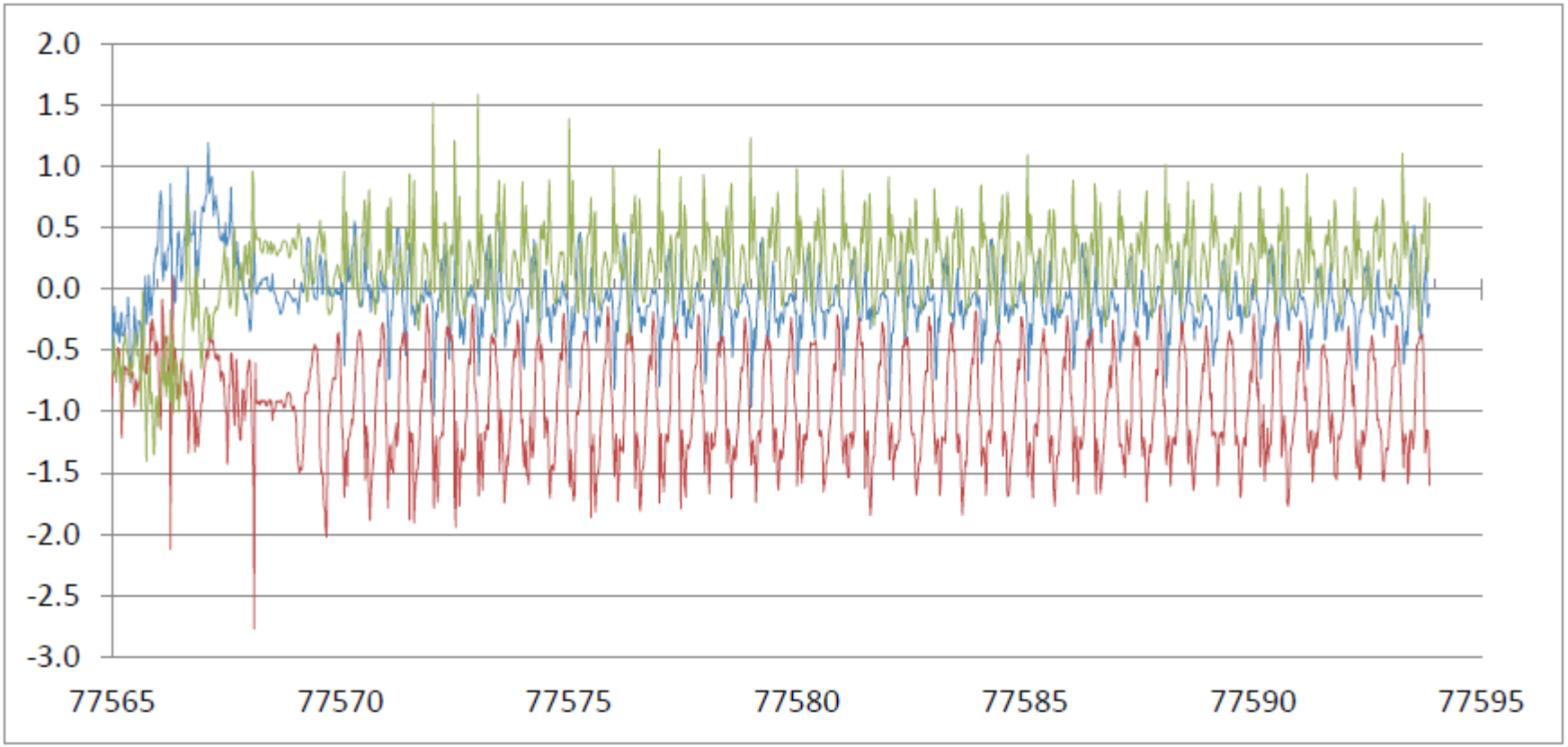


Sjá "Hæpið" 19.11.2014, aðgengilegt á vef RÚV til 17.02.2015

Enn ein listasmíð
Tómasar Ponzi:

Smátæki til að rekja ferðir,
Nýtir GPS
og sólarrafhlöðu,
innan við 10 g.

(meðal fyrri verka er skákforrit,
< 1kB)

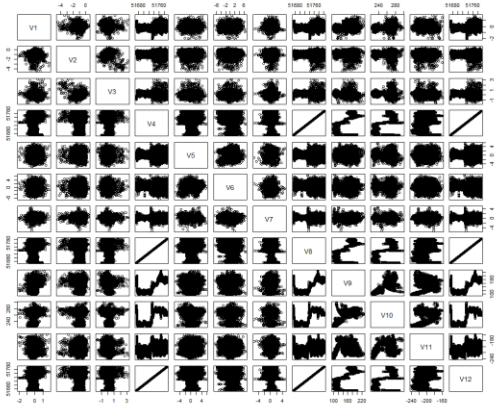


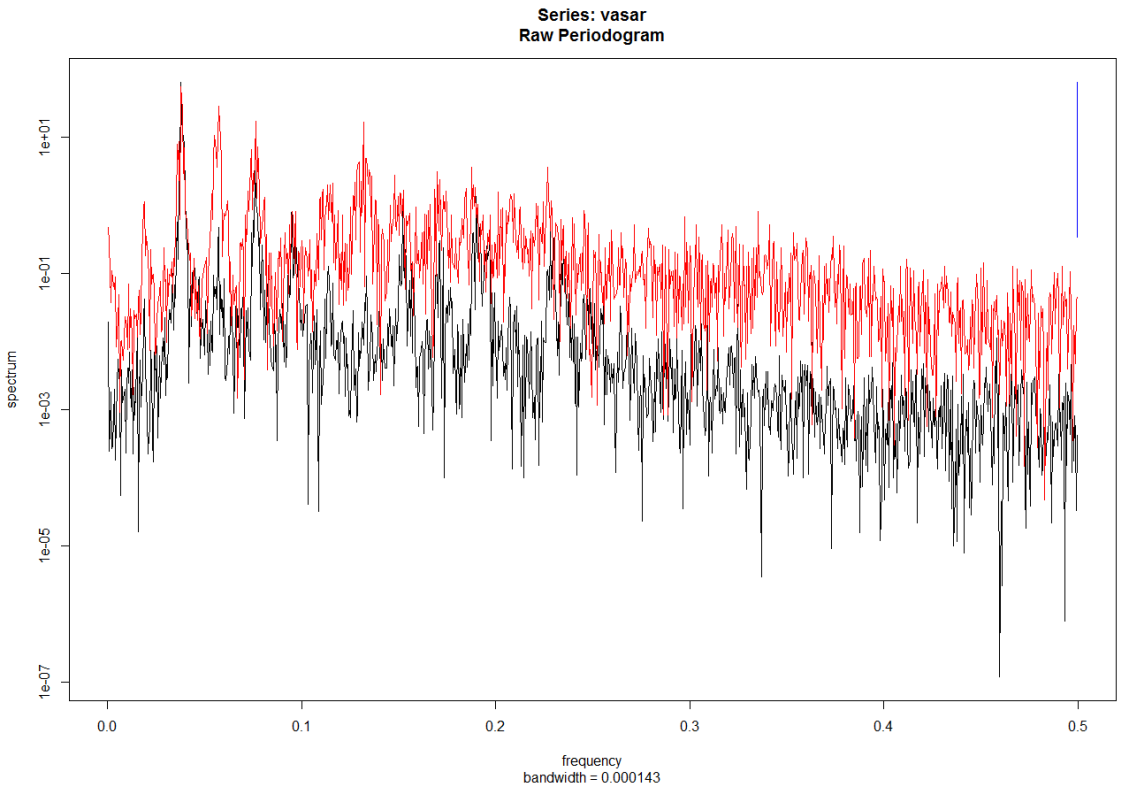
Gengið meðfram Tjörninni. Sveiflur í 3-þátta hröðun á símunum vegna göngu. Kvarði á lóðréttum ás miðast við þyngdarhröðun (g). Þar sem rauði ferillinn er nálægt því að sveiflast um -1 sýnir það að síminn hefur verið næstum lóðréttur, enda var hann í skyrtuvasa. Með því að bera saman gögn frá öðrum skynjurum má fá upplýsingar um hreyfistefnu og jafnvel meta hvar á líkama síminn var og hver gekk með hann.

Tíðnigreining göngu

Rautt: Buxnavasi

Svart: Brjóstvasi





Notaður var iPhone 5s snjallsími (sem er með LIS331DLH MEMS hröðunarskynjara) og lítið forrit sem ég útbjó til að lesa upplýsingar frá þrenns konar hreyfiskynjurum 50 sinnum á sekúndu (svo virðist sem unnt sé að auka söfnunartíðni upp í 120 sinnum á sekúndu, hef ekki prófað það):

a) ***Hröðun*** (þar er þyngdarhröðun innifalin, g = -1 á kvarða símans)
b) ***Snúningur*** (mældur með snúðsjá (gyroscope))
c) Segulstefna

Allir þættir voru mældir með þrívíðum skynjurum og mæling frá hverjum þeirra var tímastimpluð. Á hverri sekúndu voru því skráð 1200 gildi. Í hvorri mælingu hér að neðan var mælt í 30 s (og því safnað 36000 gildum alls). Forritið sendi frumgögn sjálfkrafa í tölvupósti að mælingu lokinni.

Greining gerð með **tölfræðikerfinu R**. Með því má auðveldlega vinna ýmsar upplýsingar úr gögnum, greina hreyfingar og þekkja einstaklinga í sundur

Tölvuþróun **nú**:
Öld tækifæranna

- fyrir skipulagða glæpastarfsemi

Iðnbyltingin er gengin í garð!

(Vel menntaðir og hæfir einstaklingar sem bjóða hugbúnað, vélbúnað og þjónustu til sölu „Crime as a Service – CaaS“)

Sé breskt mat á tjóni af völdum tölvutengdra glæpa yfirfært á Ísland og gert ráð fyrir að tjón á íbúa sé það sama,
þá ætti tjón hérlendis að nema **milljörðum króna á hverju ári**.

Vísindagreinar sem sýna hvernig megi misnota upplýsingar frá skynjurum snjallsíma (sbr. að framan) til njósna.

Mobile Device Identification via Sensor Fingerprinting

Hristo Bojinov
Stanford University

Dan Boneh
Stanford University

Yan Michalevsky
Stanford University

Gabi Nakibly
National Research
& Simulation Center, Rafael Ltd.

Abstract

We demonstrate how the multitude of sensors on a smartphone can be used to construct a reliable hardware fingerprint of the phone. Such a fingerprint can be used to de-anonymize mobile devices as they connect to web sites, and as a second factor in identifying legitimate users to a remote server. We present two implementations: one based on analyzing the frequency response of the speakerphone-microphone system, and another based on analyzing device-specific accelerometer calibration errors. Our accelerometer-based fingerprint is especially interesting because the accelerometer is accessible via JavaScript running in a mobile web browser without requesting any permissions or notifying the user. We present the results of the most extensive sensor fingerprinting experiment done to date, which measured sensor properties from over 10,000 mobile devices. We show that the entropy from sensor fingerprinting is sufficient to uniquely identify a device among thousands of devices, with low probability of collision.

on the device. L
tory settings ther
tifier. The user
the cloud servic
whether it has al
ple trick may al
was blocked to r
identity.

More generall
of much interes
tions providing
remote peers is a
tifying informat
mobile technolo
user privacy and
plore these chal
mobile device pl

To obtain a ro
app developers
vives a device r
shows that 8%

Gyrophone: Recognizing Speech From Gyroscope Signals

Yan Michalevsky Dan Boneh
Computer Science Department
Stanford University

Gabi Nakibly
National Research & Simulation Center
Rafael Ltd.

Abstract

We show that the MEMS gyroscopes found on modern smart phones are sufficiently sensitive to measure acoustic signals in the vicinity of the phone. The resulting signals contain only very low-frequency information (<200Hz). Nevertheless we show, using signal processing and machine learning, that this information is sufficient to identify speaker information and even parse speech. Since iOS and Android require no special permissions to access the gyro, our results show that apps and active web content that cannot access the microphone can nevertheless eavesdrop on speech in the vicinity of the phone.

1 Introduction

Modern smartphones and mobile devices have many sen-

gyroscopes are sufficiently sensitive to measure acoustic vibrations. This leads to the possibility of recovering speech from gyroscope readings, namely using the gyroscope as a crude microphone. We show that the sampling rate of the gyroscope is up to 200 Hz which covers some of the audible range. This raises the possibility of eavesdropping on speech in the vicinity of a phone without access to the real microphone.

As the sampling rate of the gyroscope is limited, one cannot fully reconstruct a comprehensible speech from measurements of a single gyroscope. Therefore, we resort to automatic speech recognition. We extract features from the gyroscope measurements using various signal processing methods and train machine learning algorithms for recognition. We achieve about 50% success rate for speaker identification from a set of 10 speakers. We also show that while limiting ourselves to a small vocabulary consisting solely of digit pronunciations ("one",

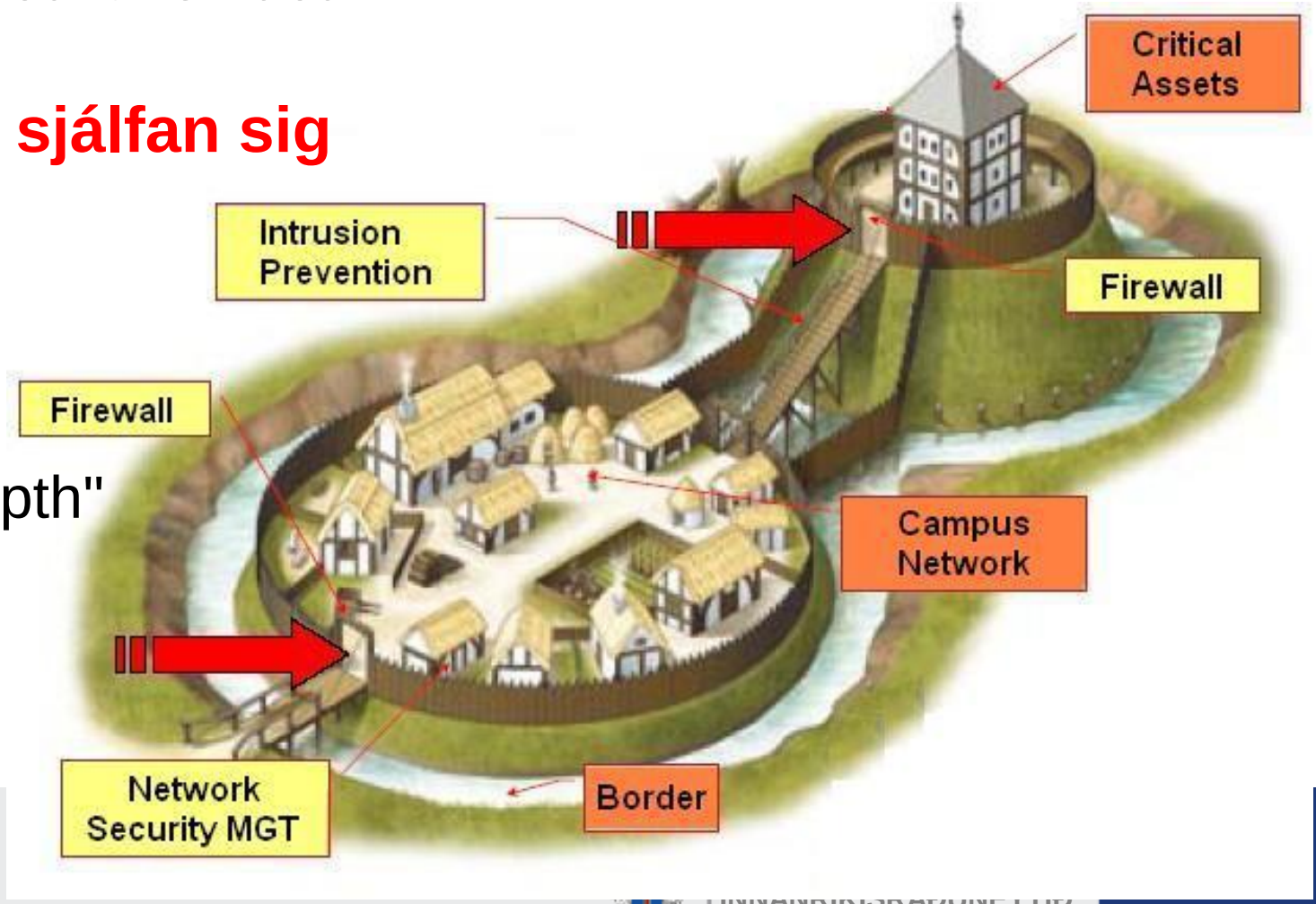

Girnilegar upplýsingar og kerfi á Netinu
Skipulögð (alþjóðleg) glæpastarfsemi
Það borgar sig ekki að vera girnilegasta bráðin!
(sú *matarmesta* eða sú *veikburðasta*)

Varnir tölvukerfis - áhættugreining

Skrif Sun Tzu um herkænskuna,
enn undirstöðurit hernaðar

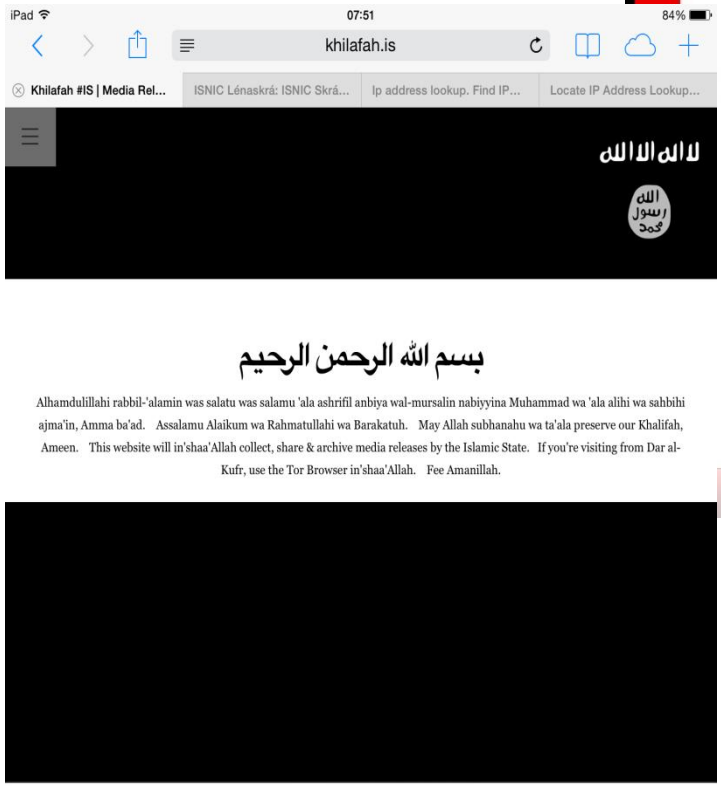
Að þekkja sjálfan sig

„Defence-in-depth"
(stigskipt vörn)



Staða hérlendis?

- Blómleg nýting – margar góðar afurðir
- Öryggissérfræðingar lengi bent á hættumerki:
  - Lítil öryggistengd menntun
  - Menning: Öryggið aftast í stað þess að vera með frá byrjun
  - Skortur á öryggisvitund, áhættugreiningu og skipulagi
  - Skortur á þekkingu, hjá almennum notendum og stjórnendum
- Þurfum að:
  - Bæta vitund
  - Bæta menntun og þekkingu
  - Bæta löggjöf
  - Geta unnið saman (geta sungið í kór, ekki bara hópur einsöngvara)
  - Hafa samstarfsvettvang
  - Hafa varnir (þ.á.m. löggæslu), viðbúnað og prófanir



Heimsfræg dæmi um efni vistað hérlendis!

(þótt efni hafi ekki verið íslenskt)

(*Silkroad* eftir yfirtöku bandríska yfirvalda að ofan og vefur íslamska ríkisins til vinstri)

Samráðsfundur í Safnahúsi, 2. júní 2014

- Um 80 fulltrúar frá um 60 stofnunum, fyrirtækjum og ráðuneytum tóku þátt.
- Þátttakendum skipt í vinnuhópa og hver hópur tók saman smá greinargerð.
- Kærar þakkir til þátttakenda og ekki síst hópstjóra!
- Samantekt þessara greinargerða verður birt með drögum að stefnu á morgun.
- Með stefnudrögunum er leitast við að skapa umgjörð um samvinnu á sviði net- og upplýsingaöryggis, þær aðgerðir sem vinnuhópar minntust á ættu að vera framkvæmanlegar innan þessa ramma.

Net- og upplýsingaöryggi
Stefna 2014 - 2025

0100111001100101011101000010110100100000011011110110011100100000011101010111000001110000011011001111111010111001
1011010010110111001100111011000011111011001110010011110010110011101100111011010010000110100001010010100110111 01
0001100101011001100110111001100001001000000011001000110000001100010011010000100000001011010010000000110010001 10
0000011001000110101

Drög til kynningar - 26. nóvember 2014

Enginn maður er *eyland*, einhlítur sjálfum sér; sérhver maður er brot *meginlandsins*, hluti *veraldar*; ef sjávarbylgjur skola *moldarhnefa* til *hafs*, minnkar *Evrópa*, engu síður en eitt *annes* væri, engu síður en *óðal vina* þinna eða *sjálfs þín* væri; *dauði* sérhvers manns smækkar *mig*, af því ég er íslunginn *mannkyninu*; spyr þú því aldrei hverjum *klukkan* glymur; hún glymur *þér*.

John Donne, 1579-1631,
í þýðingu Stefáns Bjarman á upphafi bókar Hemingways, *Hverjum klukkan glymur*.

Forsíða draga að stefnu um net- og upplýsingaöryggi sem er til kynningar á vef innanríkisráðuneytisins

INNANRÍKISRÁÐUNEYTIÐ

Efnisyfirlit

Ávarp ráðherra 2

Framtíðarsýn og stefna um net- og upplýsingaöryggi 3

Framtíðarsýn 2025 3

Meginmarkmið stefnu 3

Inngangur 4

Netið: Tækifærin, traustið og ógnirnar 5

- Traust – undirstaða notkunar Netsins 5
- Vaxandi ógn vegna glæpa og óheimillar söfnunar og nýtingar upplýsinga 5
- Áherslur grannþjóða 6
- Ábati af samvinnu mismunandi aðila á grunni stefnu 7

Staða á Íslandi varðandi net- og upplýsingaöryggi 8

Stefna og aðgerðir hérlendis: Með öryggi til sóknar 9

Lýsing meginmarkmiða 10

- Endurskoðun stefnu og aðgerðaáætlunar 12

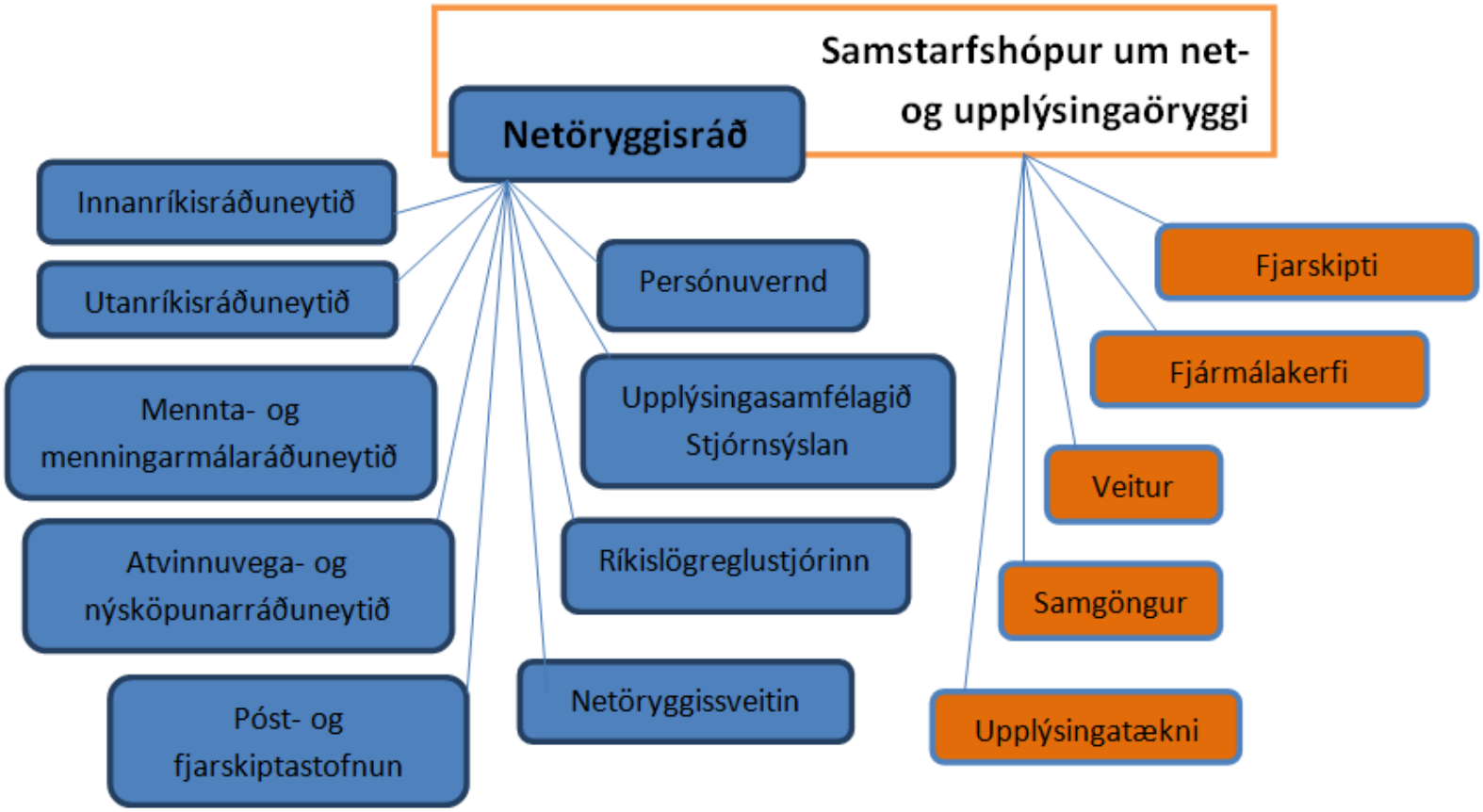
Drög framtíðarsýnar 2025

- Íslendingar búi við Net sem þeir geti treyst og þar séu í heiðri höfð mannréttindi, persónuvernd ásamt frelsi til athafna, efnahagslegs ávinnings og framþróunar.
- Örugg upplýsingatækni sé ein meginstoð hagsældar á Íslandi,
  studd af öflugri öryggismenningu og traustri löggjöf.
- Jafnframt sé samfélagið vel búið til að taka á netglæpum, árásum,
  njósnum og misnotkun persónu- og viðskiptaupplýsinga.

Meginmarkmið stefnu

1. **Bætt þekking**. Almenningur, fyrirtæki og stjórnvöld búi yfir þeirri þekkingu, hæfni og tækjum sem þarf til að verjast netógnum.
2. **Aukið áfallaþol**. Áfallaþol upplýsingakerfa samfélagsins og viðbúnaður verði aukinn þannig að hann standist samanburð við áfallaþol upplýsingakerfa á Norðurlöndum. Þetta sé t.d. gert með samvinnu og með því að öryggi verði órjúfanlegur þáttur í þróun og viðhaldi net- og upplýsingakerfa.
3. **Bætt löggjöf**. Íslensk löggjöf sé í samræmi við alþjóðlegar kröfur og skuldbindingar á sviði netöryggis og persónuverndar. Jafnframt styðji löggjöfin við nýsköpun og uppbyggingu þjónustu sem byggir á öryggi, t.d. hýsingu.
4. **Traust löggæsla**. Lögregla búi yfir eða hafi aðgang að faglegri þekkingu og búnaði til að leysa úr málum er varða net- og upplýsingaöryggi.

Hugmynd vinnuhóps um hugsanlegt skipulag



Meginmarkmið 1: Bætt þekking

Almenningur, fyrirtæki og stjórnvöld búi yfir nægjanlegri þekkingu og hæfni (verkfærum) til að verjast netógnum.

1. **Vitundarvakning**
   Almenn vitund um net- og upplýsingaöryggi verði efld.
2. **Hugtök**
   Viðeigandi alþjóðlegum skilgreiningum hugtaka, sem eru mikilvæg varðandi net- og upplýsingaöryggi, verði safnað og þess gætt að þau hafi verið þýdd þar sem þörf er á.
3. **Grunnnám**
   Net- og upplýsingaöryggi verði hluti tölvutengds námsefnis á öllum skólastigum.
4. **Framhaldsnám**
   Nemendur með grunnpróf frá íslenskum háskólum eigi kost á framhaldsnámi í net- og upplýsingaöryggi sem uppfylli sambærilegar kröfur og grannþjóðir gera til náms á því sviði.
5. **Hönnunargildi**
   Örugg hönnun og persónuvernd verði meðal grunngilda í eflingu íslensks hugbúnaðarstarfs.
6. **Persónuvernd**
   Hugað verði að alþjóðlegum kröfum og skuldbindingum um persónuvernd við uppbyggingu net- og upplýsingaöryggis á Íslandi.

Meginmarkmið 2: Aukið áfallaþol

Áfallaþol upplýsingakerfa samfélagsins verði aukið.

7. **Samstarfsvettvangur**
   Samstarfsvettvangur verði þróaður, þar sem fulltrúar frá opinberum aðilum og einkafyrirtækjum geti unnið saman að málum sem varða net- og upplýsingaöryggi.
8. **Öryggisviðmið**
   Val á viðeigandi viðmiðum (stöðlum jafnt sem öðrum) varðandi net- og upplýsingaöryggi.
9. **Alþjóðlegt samstarf**
   Efla og samhæfa þátttöku Íslands í netöryggisstarfi á erlendum vettvangi.
10. **Traust grunnkerfi**
    Fjarskiptakerfi og grunnkerfi flutningsneta styðji með skilgreindum áreiðanleika net- og upplýsingakerfi mikilvægra innviða samfélagsins, bæði tengingar innan lands og til útlanda.
11. **Stjórnsýslan**
    Net- og upplýsingaöryggi í stjórnsýslunni verði eflt með aukinni fræðslu, samhæfingu og samvinnu.
12. **Greining**
    Helstu ógnir á sviði net- og upplýsingaöryggis verði greindar og mikilvægir innviðir samfélagsins skilgreindir.
13. **Vernd innviða**
    Geta netöryggissveitar til verndar og aðstoðar mikilvægra innviða samfélagsins verði efld og virk allan sólarhringinn alla daga ársins. Sérstök áhersla verði lögð á fjarskipta-, veitu- og fjármálafyrirtæki og þau kerfi sem eru mikilvæg vegna flugsamgangna við umheiminn.
14. **Viðbragð**
    Viðbragðsáætlanir vegna netógna verði þróaðar og prófaðar með æfingum, með sérstakri áherslu á mikilvæga innviði samfélagsins.

Meginmarkmið 3: Bætt löggjöf

Íslensk löggjöf sé í samræmi við alþjóðlegar kröfur og skuldbindingar á sviði netöryggis og persónuverndar. Jafnframt styðji löggjöfin við nýsköpun og uppbyggingu þjónustu (t.d. hýsingu) á þessu sviði.

- Íslensk löggjöf verði endurskoðuð þannig að tryggt sé að hún sé í samræmi við alþjóðlegar skuldbindingar og geri mögulegt að glíma við netógnir með sambærilegum hætti og tíðkast í grannlöndum okkar.
- Jafnframt geri löggjöfin mögulegt að glíma við netógnir með sambærilegum hætti og aðrar ógnir í samfélaginu, eftir því sem við á.

Meginmarkmið 4: Traust löggæsla

Lögregla búi yfir eða hafi aðgang að faglegri þekkingu og búnaði til að leysa úr málum er varða net- og upplýsingaöryggi

- Hæfni lögreglu til að fást við glæpi tengda net- og upplýsingaöryggi verði bætt með aukinni þekkingu byggðri á kennslu, fræðslu, efldri innlendri og alþjóðlegri samvinnu og þeim búnaði sem til þarf.

Með öryggi til sóknar!

- Reisum skýjakjúfa, ekki bara skýjaborgir!
- Gerum öryggi að forgangskröfu í hönnun og notkun hugbúnaðar
- „Security by design“ og „Privacy by design“
- **Tækniþekking** og **rekjanlegt öryggi** eru stoðir sem ýmsar grannþjóðir okkar ætla að byggja efnahagslega sókn á (þetta eru þættir sem ráðgjafafyrirtæki líta til, t.d. við val á staðsetningu gagnavera)
- **Samvinna er auðlind, samvera svo stórs hluta opinbers UT geira eins og á þessum fundi getur skapað okkur sóknarfæri!**
- **Lítið samfélag hefur einnig kosti, nýtum þá!**

Starfshópurinn – þakka gott samstarf!

- Sigurður Emil Pálsson, sérfræðingur innanríkisráðuneytinu
- Guðbjörg Sigurðardóttir, skrifstofustjóri upplýsingasamfélagsins, innanríkisráðuneytinu
- Páll Heiðar Halldórsson, sérfræðingur, innanríkisráðuneytinu
- Jón F. Bjartmarz, yfirlögregluþjónn, embætti ríkislögreglustjóra
- Ágúst Finnsson, sérfræðingur, embætti ríkislögreglustjóra
- Hrafnkell V. Gíslason, forstjóri Póst- og fjarskiptastofnunar
- Stefán Snorri Stefánsson, hópstjóri CERT-ÍS, Póst- og fjarskiptastofnun
- Jónas Haraldsson, sérfræðingur, utanríkisráðuneytinu.
- Þorsteinn Arnalds, sérfræðingur, Persónuvernd