

# VEÐUR OG VINDAR Í ÖRYGGISHEIMUM

Skýrslutæknifélagið

18. október 2017

Svavar Ingi  
Hermannsson  
CISSP, CISA, CISM

# YFIRLIT

- Íslenski hlekkurinn
- Núverandi áhættur
- Framtíðaráhættur
- Hvað getum við gert?

# ÍSLENSKI HLEKKURINN

Veður og  
vindar

# ÍSLENSKI HLEKKURINN - ÖRYGGISVITUNDARVAKNING



# ÍSLENSKI HLEKKURINN



- June 2012 - LinkedIn compromised, estimated 6.5 million users e-mails + password hashes compromised
- May 2016 - Turns out 117 million users email addresses + password hashes were stolen in 2012 (the Russians - [https://en.wikipedia.org/wiki/2012\\_LinkedIn\\_hack](https://en.wikipedia.org/wiki/2012_LinkedIn_hack))

# ÍSLENSKI HLEKKURINN

- Until may of 2016 – only a small group of Russian hackers had access to the password hashes
- “dadada” - Mark Zuckerberg used his LinkedIn password on twitter and pinterest -  
<https://www.theguardian.com/technology/2016/jun/06/mark-zuckerberg-hacked-on-twitter-and-pinterest>
- If Zuckerberg used his password elsewhere, who else might have?

# ÍSLENSKI HLEKKURINN - SPURNINGAR

- “Thank you for the information. I have an anti-virus product which protects my password, isn't that enough?”
- “I don't understand this.. My brother invited me to join this, but I never did anything with this and I don't understand what it is?”
- “I'm not using this link, so I would like to ask you to terminate it for me”
- “You are of course financially responsible in case of damages from this, after not talking about this break in for 4 years!”
- “How do I know if I can trust this e-mail?”

# NÚVERANDI ÁHÆTTUR

Meira af því  
sama.



# NÝLEGAR FYRIRSAGNIR



## Microsoft Kept Secret That Its Bug-Tracking Database Was Hacked In 2013

Tuesday, October 17, 2017 Mohit Kumar

[Tweet](#) [G+ Share](#) [Share](#) 14 [in Share](#) 156 [f Share](#) 934 [Share](#)



# NÝLEGAR FYRIRSAGNIR



INTRO

## INTRODUC

We discovered serious weakne range of a victim can exploit th novel attack technique to read sensitive information such as c **against all modern protected** manipulate data. For example,



PÓST- OG  
FJARSKIPTASTOFNUN



Fjarskipti < Póstþjónusta < Neytendur < Lög og reglur < Úrlausnir < **Um PFS** <

Fréttir

Um PFS > Fréttir > Frétt

Skrifstofa

Starfsfólk

Laus störf

Skipulag

Stefnur PFS

Útgefið efni

Saga

Gjaldskrá PFS

Alþjóðasamstarf

Tenglar

Eyðublöð

Merki PFS

## Öryggisbrestur í þráðlausum tengingum – Notendum bent á að forðast WiFi tengingar á næstunni

16. október 2017

Almennum notendum þráðlauss búnaðar s.s. tölvu og farsíma er nú ráðlagt að forðast notkun þráðlauss nets tímabundið vegna alvarlegs veikleika sem hefur uppgötvast í WiFi öryggisstaðlinum, WPA2, sem á að tryggja öfluga dulkóðun í þráðlausum netkerfum.

Algengasti auðkenningar- og dulkóðunar staðallinn fyrir þráðlausar nettengingar (WiFi) í dag er WPA2. Í dag var gefin út skýrsla um nokkra veikleika í samskiptareglum WPA2 sem gerir hann veikan fyrir árásum á þau tæki sem nota nettengingarinnar. Veikleikinn er nefndur „Krack“ eða „Key Reinstallation Attacks“.

Árásaraðili sem er innan dreifisvæðis þráðlausu nettengingarinnar getur nýtt sér veikleikana og þannig lesið upplýsingar sem ættu að vera dulkóðaðar. Í einhverjum tilvikum getur einnig verið mögulegt að breyta gögnum eða koma inn gögnum, t.d. vírusum í gegnum tenginguna á



# NÝLEGAR FYRIRSAGNIR

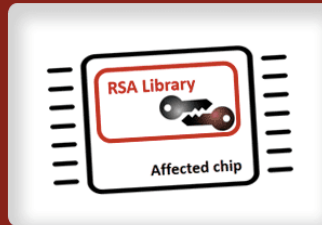


## Serious Crypto-Flaw Lets Hackers Recover Private RSA Keys Used in Billions of Devices

Monday, October 16, 2017 Swati Khandelwal

[Tweet](#) [G+ Share](#) [Share](#) 21 [in Share](#) 674 [f Share](#) 2.16k [Share](#)

### ROCA Attack



# NÝLEGAR FYRIRSAGNIR



The Register  
Biting the hand that feeds IT

ENTRE SOFTWARE SECURITY TRANSFORMATION DEVOPS BUSINESS PERSONAL TECH

**Security**

## Drive-by Wi-Fi i-Thing attack, oh my!

### Don't skip this update

By Richard Chirgwin 3 Apr 2017 at 22:46 23  SHARE ▼

Apple hasn't provided much detail, but you don't want to ignore the latest iOS release – 10.3.1 – because it plugs a very nasty Wi-Fi vulnerability.

Cupertino has rushed out the [emergency patch](#) because: "An attacker within range may be able to execute arbitrary code on the Wi-Fi chip" – meaning, presumably, that malicious packets gave attackers a vector.


The fix for the bug, which Apple attributes to Gal Beniamini of Google's Project Zero, was a buffer overflow fixed by better input validation.

The bug affected iPhone 5 and later, iPad 4th generation and later, and iPod touch 6th generation and later.

The release of 10.3.1 comes just a week after Apple released 10.3.

# NÝLEGAR FYRIRSAGNIR




 DATA CENTRE SOFTWARE SECURITY TRANSFORMATION DEVOPS BUSINESS PERSONAL TECH

## Security

### Missed patch caused Equifax data breach

Apache Struts was popped, but company had at least TWO MONTHS to fix it

By [Simon Sharwood](#), APAC Editor 14 Sep 2017 at 02:09 65  SHARE ▼

Equifax has revealed that the cause of its massive data breach was a flaw it should have patched weeks before it was attacked.

The company has updated its [www.equifaxsecurity2017.com/](http://www.equifaxsecurity2017.com/) site with a new "A Progress Update for Consumers" that opens as follows:

# NÝLEGAR FYRIRSAGNIR



ENTRE SOFTWARE SECURITY TRANSFORMATION DEVOPS BUSINESS PERSONAL TECH

## Security

### **Deloitte is a sitting duck: Key systems with RDP open, VPN and proxy 'login details leaked'**

Yes, that's Gartner's security consultancy of the year

By [Iain Thomson](#) in [San Francisco](#) 26 Sep 2017 at 20:33

78

SHARE ▼

# NÝLEGAR FYRIRSAGNIR

ZDNet



REUTERS



Exclusive: U.S. Homeland Security found SEC had 'critical' cyber weaknesses in...



Mexico tech industry benefits from U.S. anti-immigration stance

## SEC addressing trading

The commission said



By [Charlie Osborne](#) for

#TECHNOLOGY NEWS SEPTEMBER 21, 2017 / 3:38 PM / 25 DAYS AGO

## Exclusive: U.S. Homeland Security found SEC had 'critical' cyber weaknesses in January

Sarah N. Lynch

4 MIN READ



WASHINGTON (Reuters) - The U.S. Department of Homeland Security detected five “critical” cyber security weaknesses on the Securities and Exchange Commission’s computers as of January 23, 2017, according to a confidential weekly report reviewed by Reuters.

# NÝLEGAR FYRIRSAGNIR



The Washington Post  
*Democracy Dies in Darkness*



BOOKING.COM  
**I AM SERVICED APARTMENTS**  
Book now | £169

Learn more

National Security

## Israel hacked Kaspersky, then tipped the NSA that its tools had been breached



# NÝLEGAR FYRIRSAGNIR

- Crypto-busters reverse nearly 320 MEELLION hashed passwords (*Troy Hunt's passwords (from various data breaches)*).
- HACKERS GAIN 'SWITCH-FLIPPING' ACCESS TO US POWER GRID CONTROL SYSTEMS
- “745,000 pacemakers have been confirmed as having cyber-security issues that could let them be hacked. “
- “Watch a hacked robot stab a tomato”
- Russian agents hacked US voting system manufacturer before US election – report
- Hackers breached defenses of US voting machines in less than 90 minutes
- “THE FBI WARNS THAT CAR HACKING IS A REAL RISK”

# VERIZON DATA BREACH INVESTIGATION REPORT (DBIR) - 2017

**“People are also still failing to set strong passwords.**

**80% of hacking-related breaches leveraged either stolen passwords and/or weak or guessable passwords.”**

# FRAMTÍÐARÁHÆTTUR

Hverju  
þurfum við  
að hafa  
áhyggjur af?

# FRAMTÍÐARÁHÆTTUR

- Meira af þessu sama
  - IoT
  - Gagnaöflun
  - Áhrif á kosningar?
  - Áhrif á markaði?
  - Annað?

**HVAÐ GETUM VIÐ GERT?**

Hvaða  
lausnir eru í  
boði?

# HVAÐ GETUM VIÐ GERT?

- Almenn öryggisvitunardvakning
- Ókeypis Phishing þjónusta fyrir litla aðila:  
<https://phishinsight.trendmicro.com/en/>
- Þjálfun kerfisstjóra (t.d. Securing Microsoft Windows Server 2016)
- Þjálfun netmanna (CCNA/CCNP Security)
- Aðrar öryggisgráður: CISSP / CISA / CISM o.fl.

# HVAÐ GETUM VIÐ GERT?

Umræðuskjal - Samningsviðauki vegna  
upplýsingaöryggis

<https://www.stjornarradid.is/efst-a-baugi/frettir/stok-frett/2017/01/06/Upplýsingaoryggi-samningsvidauki-leidbeiningar-og-eydublod-fyrir-gerd-ahaettumats/>

# TAKK FYRIR!

■ Spurningar?

[svavar@security.is](mailto:svavar@security.is)

<http://www.security.is/>