Latest hacking trends

Jean-Philippe Aumasson

- **Phd** EPFL 2009, **cryptography**
- **Kudelski** Group since 2010 (crypto, cybersecurity)
- **Research** and outreach
  - Designer of widely used crypto (BLAKE2, SipHash)
  - Talks at Black Hat, DEFCON, CCC, RSA, etc.
  - A book published, another one next year
- https://aumasson.jp – https://twitter.com/veorq

New attacks appear, old ones don’t disappear.

Google field study (Elie Bursztein):

- 300 USB keys dropped on parking lots, hallways, etc.
- Malicious payload for **45%** of the keys

http://ly.tl/malusb

Old attacks can be come more powerful.

152k cameras in 990Gbps record-breaking dual DDoS

Hacked low-powered cameras and internet-of-things things

http://www.theregister.co.uk/2016/09/27/152463_hacked_cameras_deliver_990gbps_recordbreaking_dual_ddos/

New toys to break:

- **Cars**: connected, self-driving
- **"Things"**: smart home, connected devices

The Washington Post

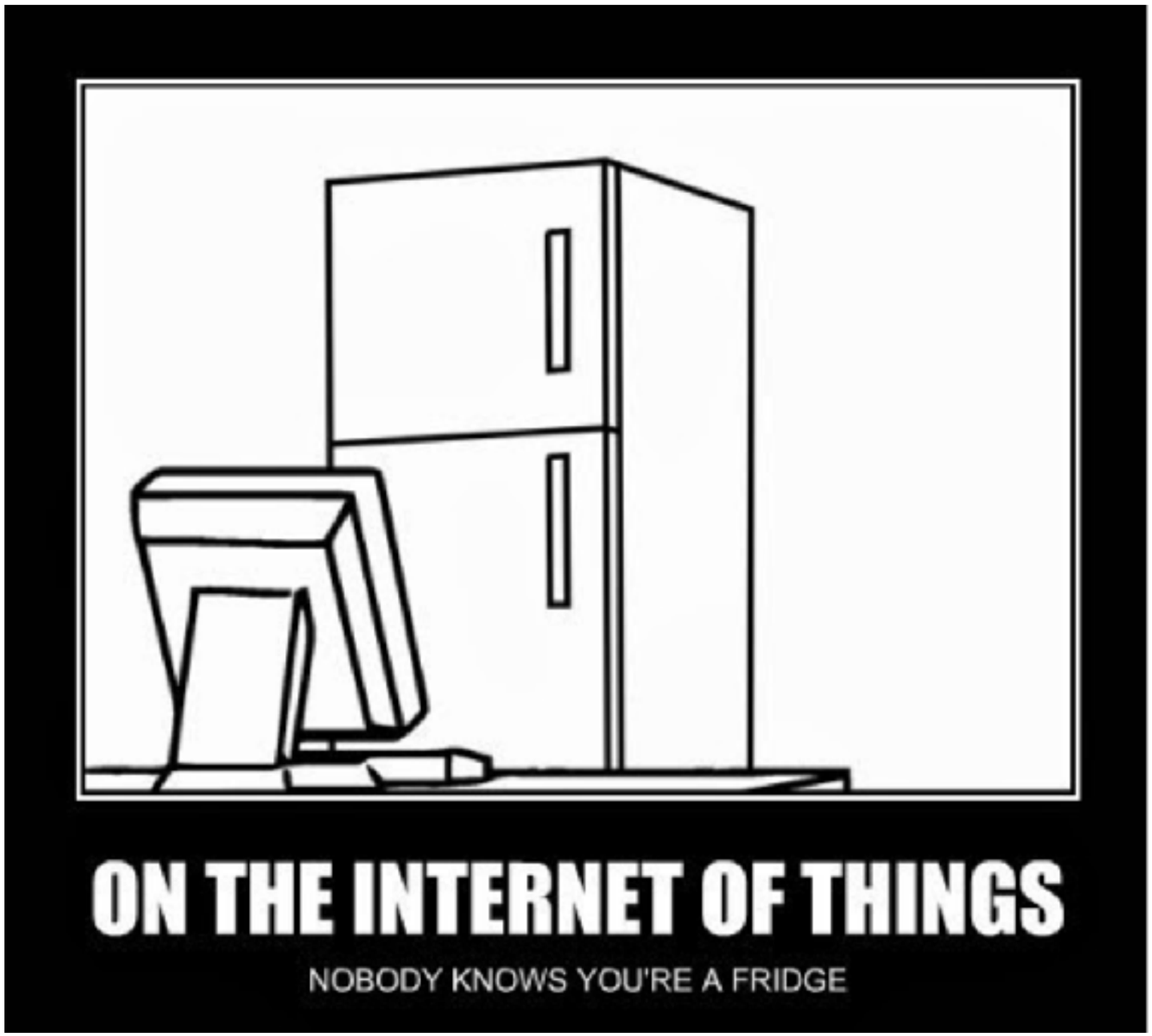
The Switch

Researchers remotely hack Tesla Model S

By Andrea Peterson September 20

Recent research by Tencent labs (China)

https://www.washingtonpost.com/news/the-switch/wp/2016/09/20/researchers-remotely-hack-tesla-model-s/



Often low-cost, low-value devices, hence low-security

Adopt the new innovation and be less secure?

Risk means more things can happen than will happen.

But don’t be paranoid.

Security solutions will be developed...

... and compromised (IBM talk at Black Hat)

Even security products get hacked (by Google Project Zero)

These vulnerabilities are as bad as it gets. They don't require any user interaction, they affect the default configuration, and the software runs at the highest privilege levels possible. In certain cases on Windows, vulnerable code is even loaded into the kernel, resulting in remote kernel memory corruption.

As Symantec use the same core engine across their entire product line, all Symantec and Norton branded antivirus products are affected by these vulnerabilities, including:

- Norton Security, Norton 360, and other legacy Norton products (All Platforms)
- Symantec Endpoint Protection (All Versions, All Platforms)
- Symantec Email Security (All Platforms)
- Symantec Protection Engine (All Platforms)
- Symantec Protection for SharePoint Servers
- And so on.

https://googleprojectzero.blogspot.ch/2016/06/how-to-compromise-enterprise-endpoint.html

New defense for servers and endpoints:

- Secure computation on third-party computers
- Can make reverse engineering impossible

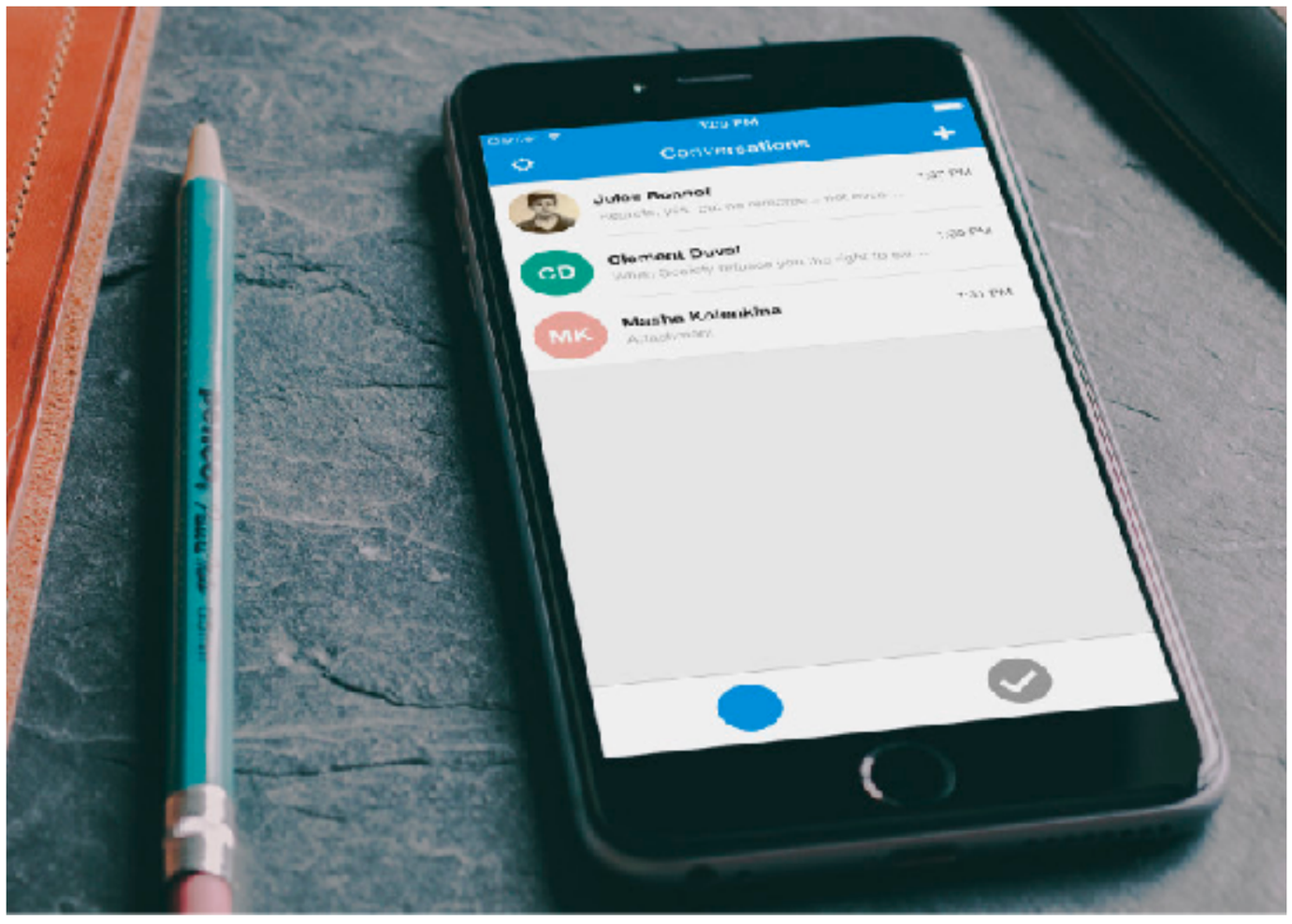
Kudelski Security research presented at Black Hat

Trust no one.

> “ Use anything by Open Whisper Systems.
>
> — **Edward Snowden**, Whistleblower and privacy advocate

Signal: the most trusted secure message & calls application

End-to-end encryption, solid software and architecture



https://whispersystems.org/

Signal, l'application utilisée par l'équipe d'Hillary Clinton pour contrer l'espionnage

LE MONDE I 29.08.2016 à 13h21 • Mis à jour le 29.08.2016 à 14h03

http://www.lemonde.fr/pixels/article/2016/08/29/signal-l-application-utilisee-par-l-equipe-d-hillary-clinton-pour-contrer-l-espionnage_4989345_4408996.html

But **perfection** does not exist: bugs found at last in Signal

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

RISK ASSESSMENT —

Signal fixes bug that lets attackers corrupt encrypted attachments [Updated]

Signal may be the most trusted messaging app, but it's not perfect.

DAN GOODIN - 9/15/2016, 9:45 PM

The researchers privately reported the vulnerabilities to Signal developer Open Whisper Systems on September 13 and the company has already issued an update. Aumasson and Vervier—who are the principal research engineer at Kudelski Security and CEO and head of security research at X41 respectively—said they're still working to determine if the same bugs affect WhatsApp, the Facebook messaging app that also relies on Signal code.

Confidence is good. Facts on your side, better.

Encryption products should not be lemons, ask suppliers:

- Who can access the keys? (only receiver and sender)
- How are keys updated? (they should be)
- Have the architecture and implementation been audited?
- Has the surrounding software been audited?

Flawed encryption can be **worse** than no encryption:
belief in security leads to greater exposure and risk,

Conclusion: maybe there is a solution...


OUR DEVICES ARE NOW 100% SECURE.
I TURNED THEM ALL OFF.
HOW DID YOU DO THAT?
© D.Fletcher for CloudTweaks.com

Thank you.