

Trend Security 2018

Budi Rahardjo (ID-CERT)

6 Desember 2017

Kolla Space, Jakarta

Confidentiality, Integrity, Availability

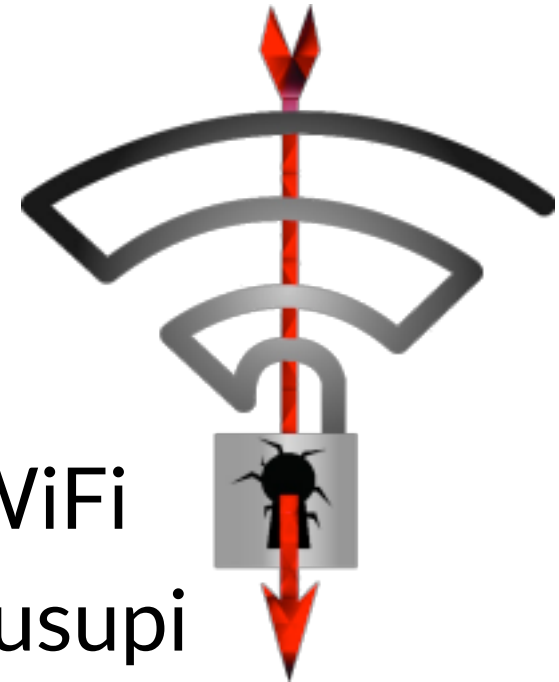
RECENT SECURITY CASES

INDONESIA COMPUTER EMERGENCY RESPONSE TEAM



Masalah WiFi

- Key Reinstallation Attacks (KRACKs)
www.krackattacks.com
- Kelemahan dari WPA2 yang digunakan untuk melindungi WiFi
- Data data disadap, diubah, disusupi (Man-In-The-Middle Attack)





www.telkomsel.com/



Murahin harga KUOTA INTERNET, bangsat..!!!

Dear, kampret.

Lu jadi operator kagak usah mahal-mahal. Taik!

Pegimane bangsa Indonesia mau maju kalo internet aja mahal. Babi!

Makan aja susah, apalagi beli kuota internet. Monyet!

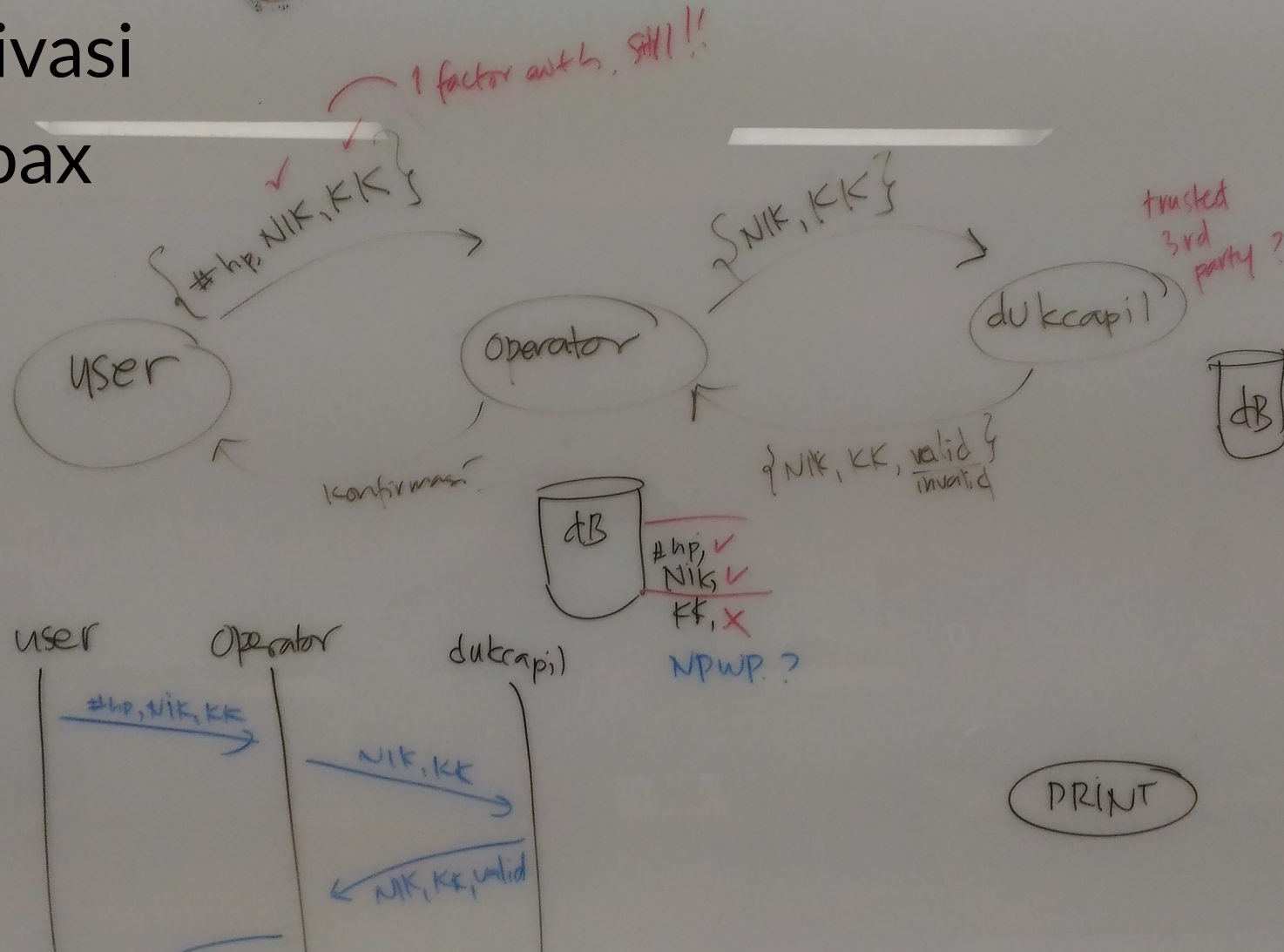
Murahin harga kuota internet, Nyet! Kagak usah pake dibagi-bagi 2G/3G/4G. Gobloggg!

Gue kagak butuh HOOQ, VIU, iming-iming kuota music ame video lu. Anjingg!!!

Gue cuma butuh KUOTA INTERNET. TITIK.

Verifikasi Nomor Handphone

- Privasi
- Hoax



Identity Theft

- Banyak pengguna yang memiliki password yang sama untuk layanan e-Commerce / market place
 - Bobol di satu tempat, bobol di semua tempat
 - Bagaimana juga ada *rogue services*?



Ooops, your files have been encrypted!

English

You became victim of the PETYA RANSOMWARE!

The harddisks of your computer have been encrypted with an m encryption algorithm. There is no way to restore your data w key. You can purchase this key on the darknet page shown in

To purchase your key and restore your data, please follow th steps:

1. Download the Tor Browser at "https://www.torproject.org/" help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

<http://petya37h5tbhyvki.onion/N19fvE>

<http://petya5koahsf7sv.onion/N19fvE>

3. Enter your personal decryption code there:

If you already purchased your key, please enter it below.

Key:

Payment will be raised

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost

5/20/2017 00:47:55

Time Left

06:23:57:37

[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)

Check Payment

Decrypt

Man in the Browser: Zeus Crimeware as a Services

[contoh akun yang kena – dihapus]

<https://mivecblog.com/2015/04/03/hati-hati-dengan-malware-zeus-atau-rekening-anda-terkuras-bahis/>

INDONESIA COMPUTER EMERGENCY RESPONSE TEAM

id.cert

Gagal Fungsi Satelit Telkom-1



Telegram Down



Telegram Messenger  @telegram · 33m

The cause of the connection issues in Asia is a major power outage in our datacenter in SG (supposed to never happen). Hang on!

 85  366  183



Telegram Messenger  @telegram · 1h

The main network switch went down in the Telegram server cluster in Singapore. Asian users are affected. Investigating and fixing!

 288  1.0K  422

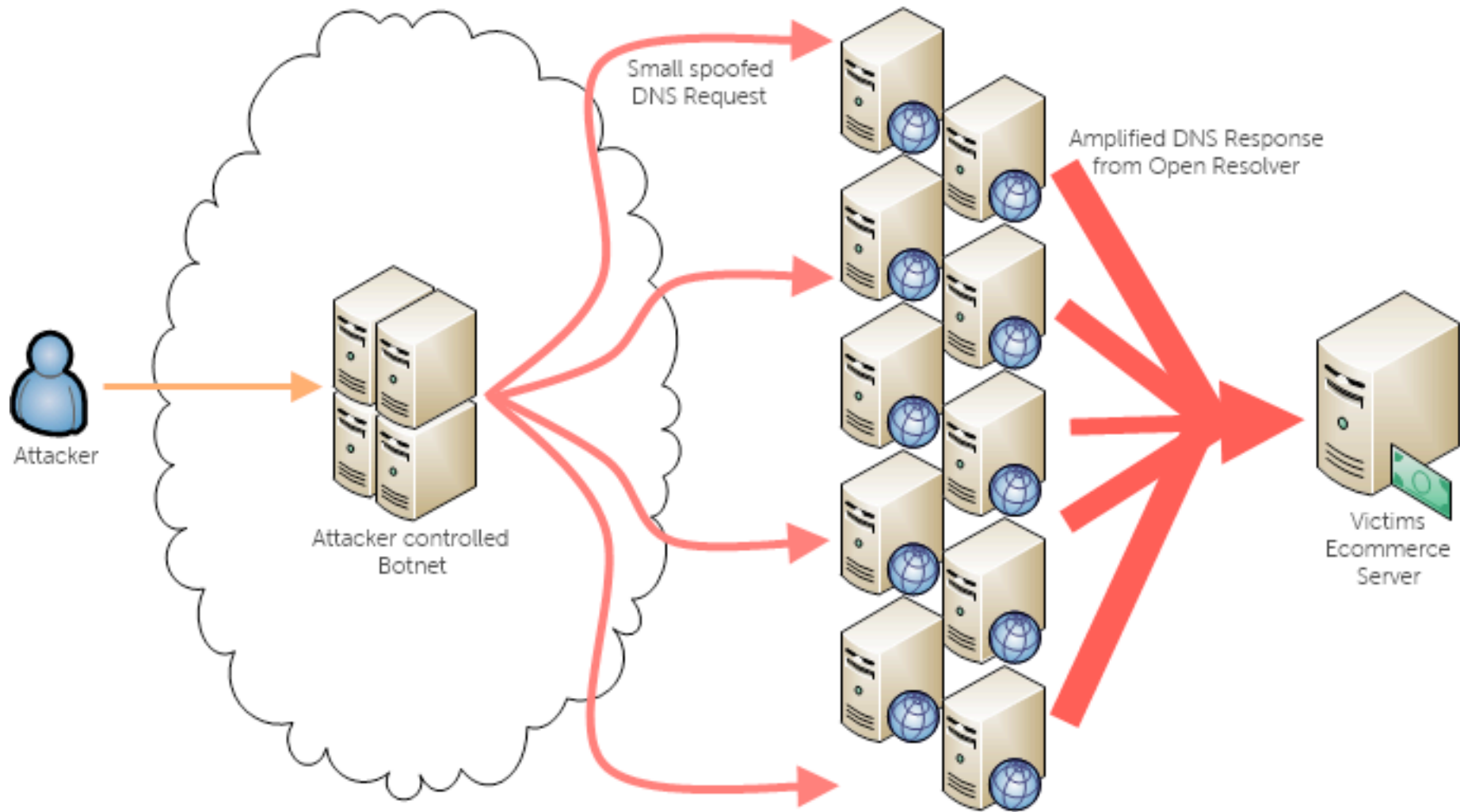


Telegram Messenger  @telegram · Sep 13

And it's up! Sorry, Germany and the CIS, you were affected most. Please give us a few more minutes to sync you with the rest of the world.

 44  51  265

DDoS Attack



<http://www.evilsec.net/2015/04/drdoS-denial-of-service-on-steroids/>

INDONESIA COMPUTER EMERGENCY RESPONSE TEAM



Internet of Things

IOT

INDONESIA COMPUTER EMERGENCY RESPONSE TEAM



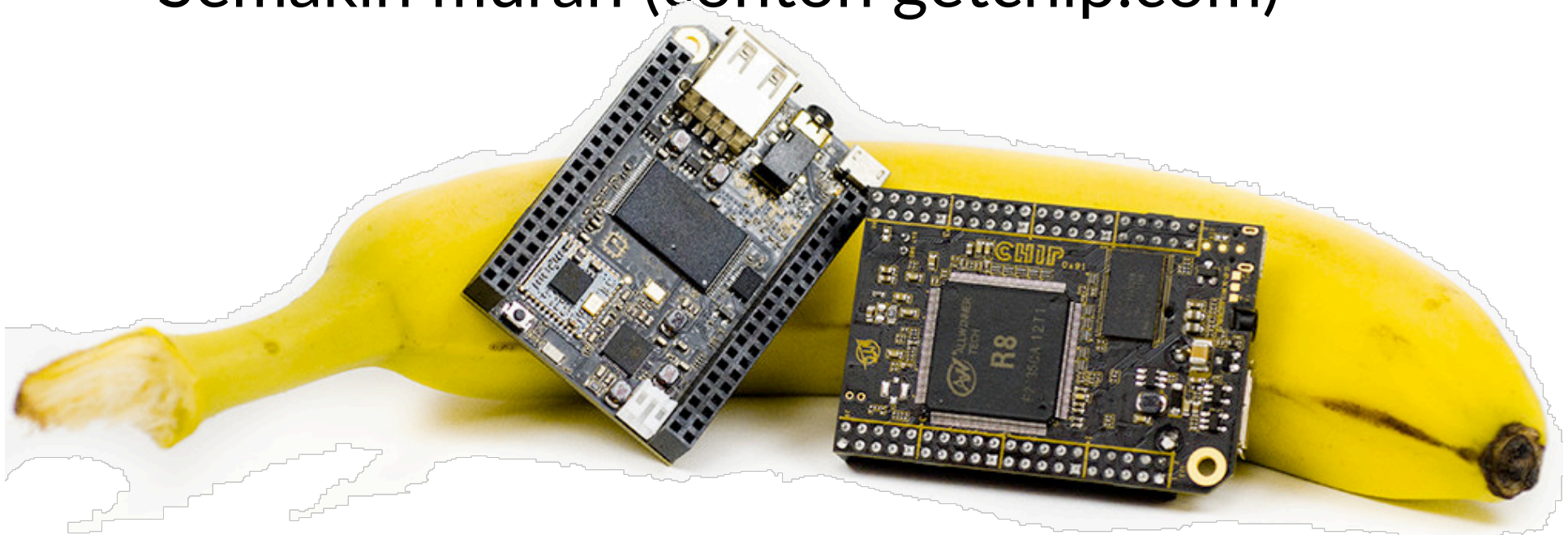
"Things"

Semua! Apa saja!

- Dahulu hanya komputer saja yang dapat diprogram
- Sekarang semua benda dapat diprogram

Gara-gara Hardware

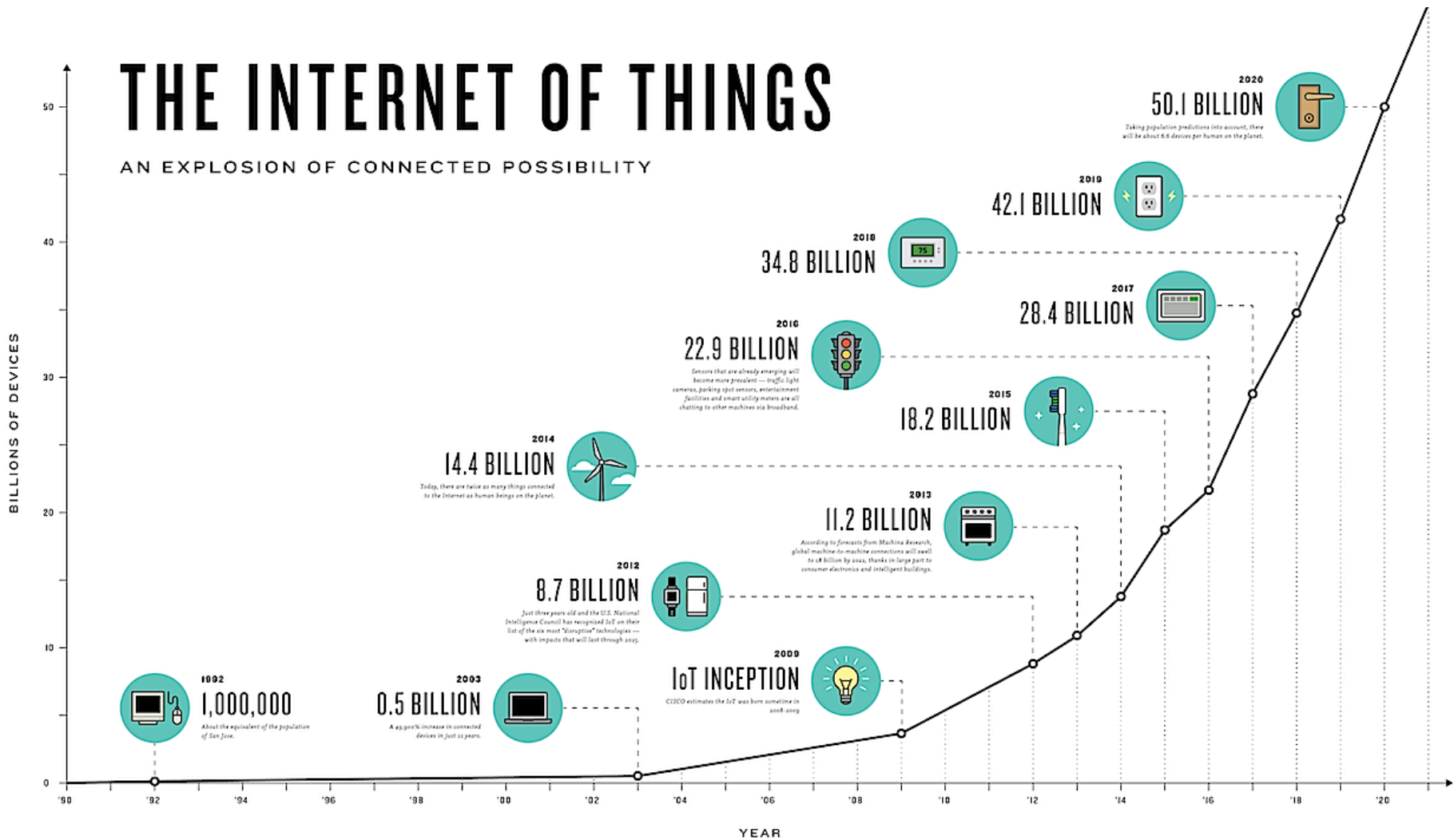
- Semakin kecil (tapi kemampuan komputasi meningkat, hemat batre)
- Semakin murah (contoh getchip.com)



“Internet”

- Maknanya adalah terhubung ke jaringan
 - Jaringan ada dimana-mana
 - WiFi, LoRa, NBloT, 5G
 - Protokol: MQTT
- Biaya penggunaan jaringan semakin murah

Eksponensial!



IoT Security

- *Constrained devices*, keterbatasan kemampuan komputasi dari perangkat IoT
- Jumlah perangkat yang sangat banyak
 - Industry 4.0, agriculture, smart city, lifestyle, ...
- Dijadikan bagian dari botnet untuk melakukan DDoS attack
 - Mirai, CCTV attack ...

CCTV Botnet

Hacking CCTV
Cameras to
Launch DDoS



INDONESIA COMPUTER EMERGENCY RESPONSE TEAM



Fintech Security

- Blockchain merupakan teknologi di belakang banyak inisiatif fintech
- Banyak fraud / penipuan, menurunkan tingkat kepercayaan
- Regulasi diperketat
- Dibutuhkan standar security sendiri
 - Lebih baik self-regulating

Lain-lain

- Regulasi
 - Contoh: pemanfaatan cloud di luar negeri
- Cyberwar?
 - Belum, tetapi bukan berarti lalai
- Application security

Penutup

- Permasalahan security (Confidentiality, Integrity, Availability) akan tetap muncul
- Akan semakin banyak masalah yang muncul dikarenakan meningkatnya jumlah aplikasi dan perangkat