# Value Chain Security

Łukasz Bromirski
CTO
Cisco Systems Poland

# Value Chain Security

## Exposures

**Taint**

Alteration allowing unauthorized control or content visibility

**Counterfeit**

Raw materials, finished goods or services which are not authentic

**IP Misuse**

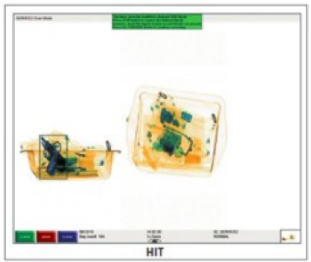
Unauthorized disclosure of intellectual property

**Information Security Breach**

Unauthorized access to confidential information

# How to attack machine learning/AI systems?

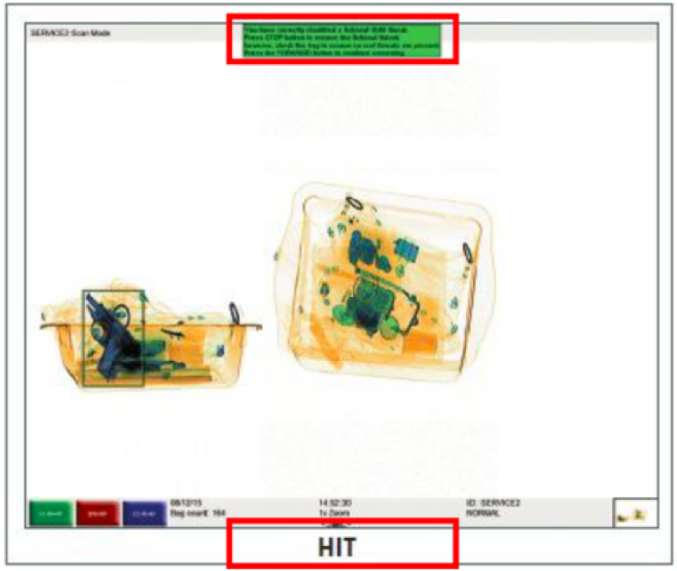

—RAPISCAN THREAT IMAGE PROJECTION—






# ...it's easy because of...

## —RAPISCAN THREAT IMAGE PROJECTION—




# ...embedded, hardcoded backdoors:

# RSA keys…

- „The flaw resides in the Infineon-developed RSA Library version v1.02.013,"
- Impacts a lot of different devices, including:
  - Lenovo laptops
  - Microsoft Surface tablets
  - ID cards used by millions

*COMPLETELY BROKEN —*

## Millions of high-security crypto keys crippled by newly discovered flaw

**Factorization weakness lets attackers impersonate key holders and decrypt their data.**

DAN GOODIN - 10/16/2017, 1:00 PM


Steve Jurvetson

Enlarge / 750,000 Estonian cards that look like this use a 2048-bit RSA key that can be factored in a matter of days.


That plane...
WON'T FLY!

# Value Chain Security

## Trusted Providers of Genuine Solutions

Uncompromised integrity throughout solutions lifecycle – cradle to grave


A Layered Approach

Logical Security

Security Technologies

Physical Security Practices

# „Be the change you want to see in the world”

- SHARE
  - Hackers learn just by observing our actions, while our learning is limited
  - Information, incident information sharing is either non-existent, or limited (and we all focus on building „platforms”...)
- DO
  - You will be hacked.. You will fail... Plan it today!
  - Security by obscurity doesn’t work... Leads to bigger problems that it aims to avoid in the first place
  - Workshops and wargames bring enormous results – do it! Learn from them!
  - Follow trustworthy systems standarization - and organizations deploying them


CISCO