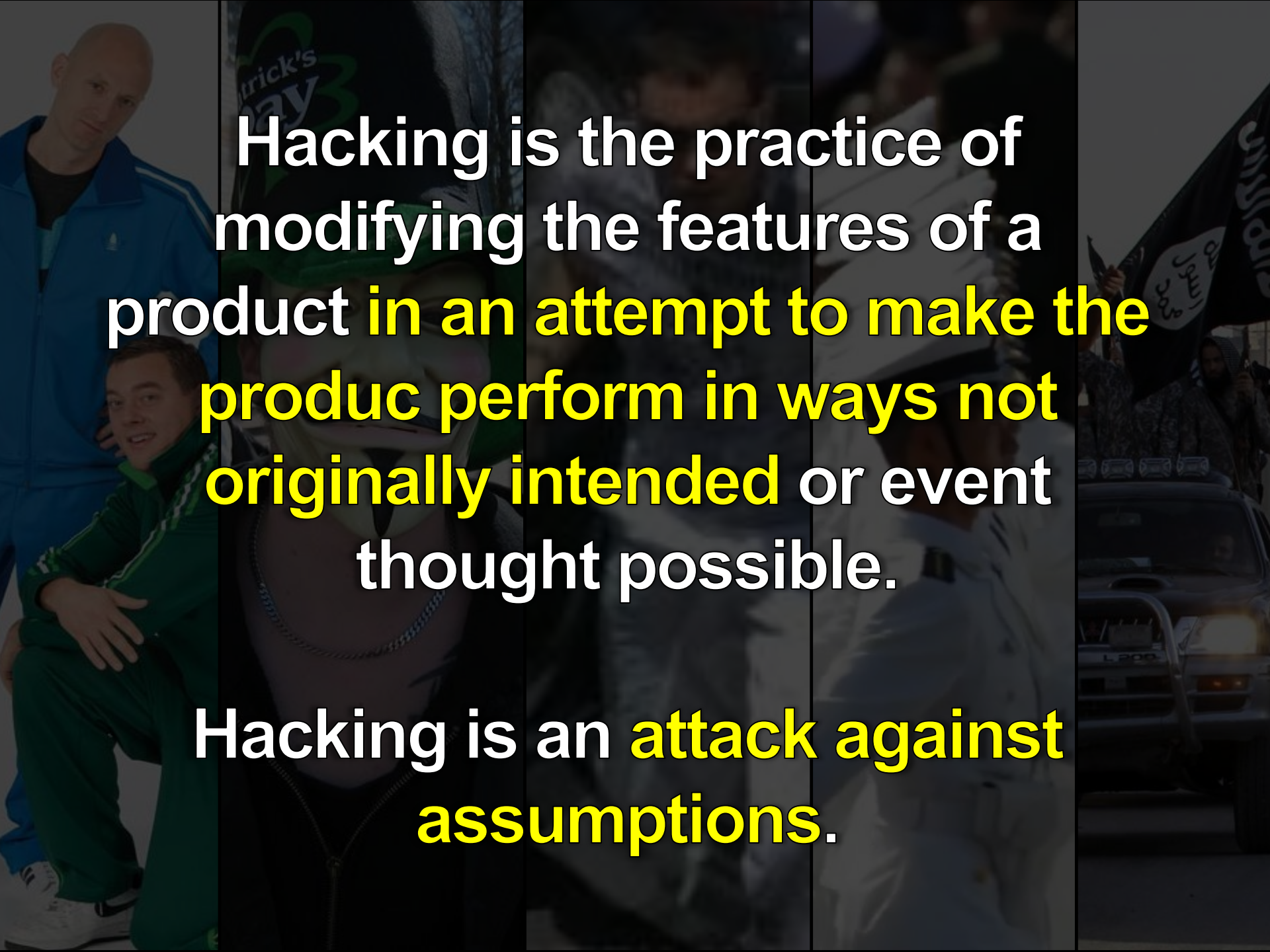
Corporate Hacking

Has Hacking Finally Made it to the Boardroom?

F-Secure / Erka Koivunen
@ekoivune

https://business.f-secure.com/

Software → ???? → Profit!!



Hacking is the practice of modifying the features of a product in an attempt to make the produc perform in ways not originally intended or event thought possible.

Hacking is an attack against assumptions.

WHO ARE
THE
HACKERS?

Photo: Wired

WELCOME
TO A WORLD
RUN BY
SOFTWARE

United States Government Accountability Office

GAO

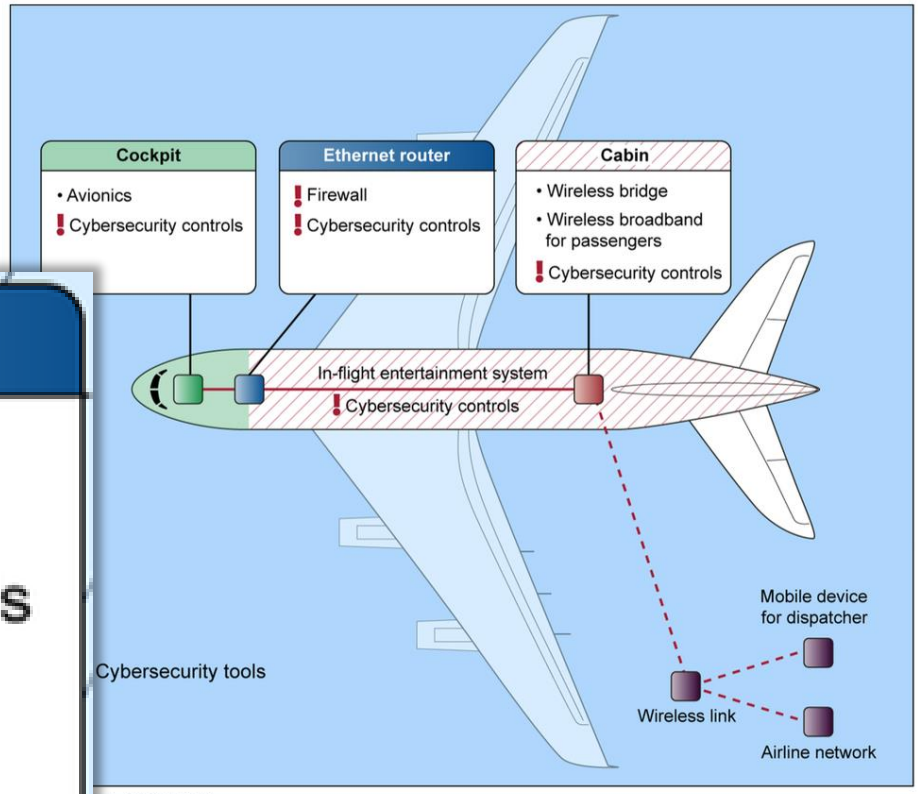
Report to Congressional Requesters

April 2015

AIR TRAFFIC CONTROL

FAA Needs a More

Figure 4: Aircraft Diagram Showing Internet Protocol Connectivity Inside and Outside of Aircraft



GAO-15-370

Ethernet router
! Firewall
! Cybersecurity controls

Photo: The Telegraph

REMEMBER
THE
HACKERS?

TIME TO
INTRODUCE A
NEW
PROTAGONIST?

KSWAGEN

Cases of Ethically-Challenged Corporate Hacking

- Sony BMG rootkit 2005
- Lenovo 2014 – 2015
  - Superfish et al.
- Ashley Madison
  - Female bots
  - $19 deletion fee
- Volkswagen
  - emissions test rigging

Cases of Ethically-Challenged Corporate Hacking

- Sony BMG rootkit 2005
- Lenovo 2014 – 2015
  - Superfish et al.
- Ashley Madison
  - Female bots
  - $19 deletion fee
- Volkswagen
  - emissions test rigging

Turn your Product into Software

↓

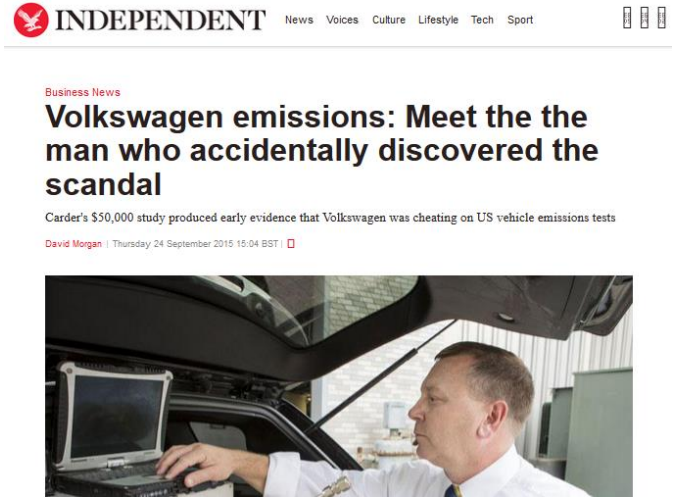
Hack Away

↓

Profit!!

(Just don't get caught)

SHOULD WE
JUST
ACCEPT THIS?


INDEPENDENT News Voices Culture Lifestyle Tech Sport

Business News

Volkswagen emissions: Meet the the man who accidentally discovered the scandal

Carder's $50,000 study produced early evidence that Volkswagen was cheating on US vehicle emissions tests

David Morgan | Thursday 24 September 2015 15:04 BST |

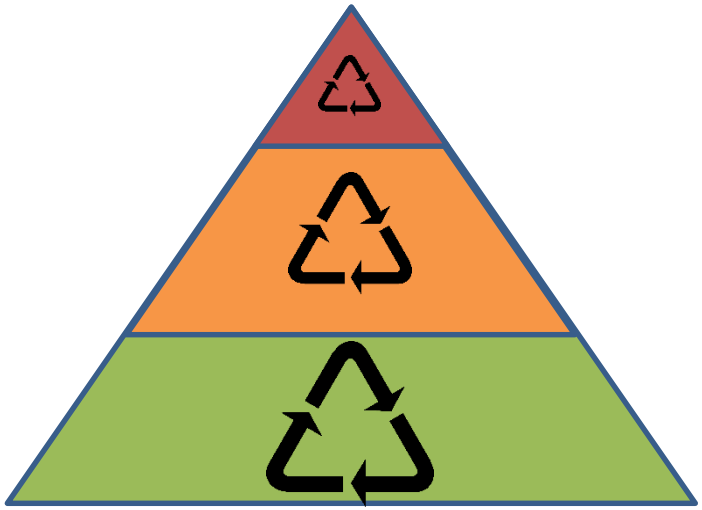
Proposed Solution #1: Encourage Third Parties to Find Deficiencies

PROMOTE VULNERABILITY RESEARCH

4.7.5 The Vendor shall maintain integrity of the software build including upgrades, operating systems and application from factory to desk. The Vendor shall demonstrate that the software build (both proprietary and off-the-shelf) delivered to TSP is the same as the software build agreed with TSP. The software should not have such bugs which could hamper security in future including any unauthorized leakage of TSP Information including Sensitive Information.

Proposed Solution #2: Address the Externality of Risks

SOFTWARE LIABILITY?



Proposed Solution #3: Force Threats and Incidents more Visible

MANDATORY REPORTING?

- Software is everywhere
- Software is capable of everything
- Software will be used for everything

→ Strong incentives to engage in unethical business practices

→ Need to ensure that cheaters will be exposed

IV Foro de la Ciberseguridad

CSC Cyber Security Center

Una iniciativa de isms forum spain

Patrocina:

Akamai

BLUE COAT

Deloitte.

intel Security

IBM

NECSIA

SAMSUNG

Symantec.

TREND MICRO

Colaboran:

Obra Social "la Caixa"

apd Asociación para el Progreso de la Dirección — el saber conecta

Sigue el Foro en Twitter #4ForoCEC #CyberSecurity