



WORKSHOP
CYBER4HEALTH
Osservatorio sulle vulnerabilità cyber e fisiche
dei dispositivi medici



Exposed and Vulnerable: The Global Challenges of Hidden Threats in Medical Devices



Giuseppe Bianchi

Professor, University of Roma Tor Vergata

Director, National CNIT Network Assurance & Monitoring LAB

Giuseppe Bianchi



consorzio nazionale
interuniversitario
per le telecomunicazioni

The cyber medical apocalypse...

Press release – May 17, 2028 – The world is in the midst of a **catastrophic cyber attack on medical devices**, with hackers unleashing a relentless wave of destruction on patients and healthcare providers. Exploiting a litany of vulnerabilities, these cyber criminals have taken control of devices and are causing them to malfunction with **deadly consequences**.

From **pacemakers** to **insulin pumps**, nothing is safe from the fury of these malicious hackers, who have plunged the world into a dark age of pain and suffering. Countless lives have been lost as **these once life-saving devices now deal out death** and destruction at every turn.

The future looks bleak indeed. **The cost of repairing and replacing affected devices is incalculable**, and the damage to the global economy is devastating. But most of all, the toll on the human soul is immeasurable, as we mourn the loss of our loved ones and struggle to cope with a world where every day is a battle against the unremitting wrath of these cyber attackers.

FAKE

Giuseppe Bianchi



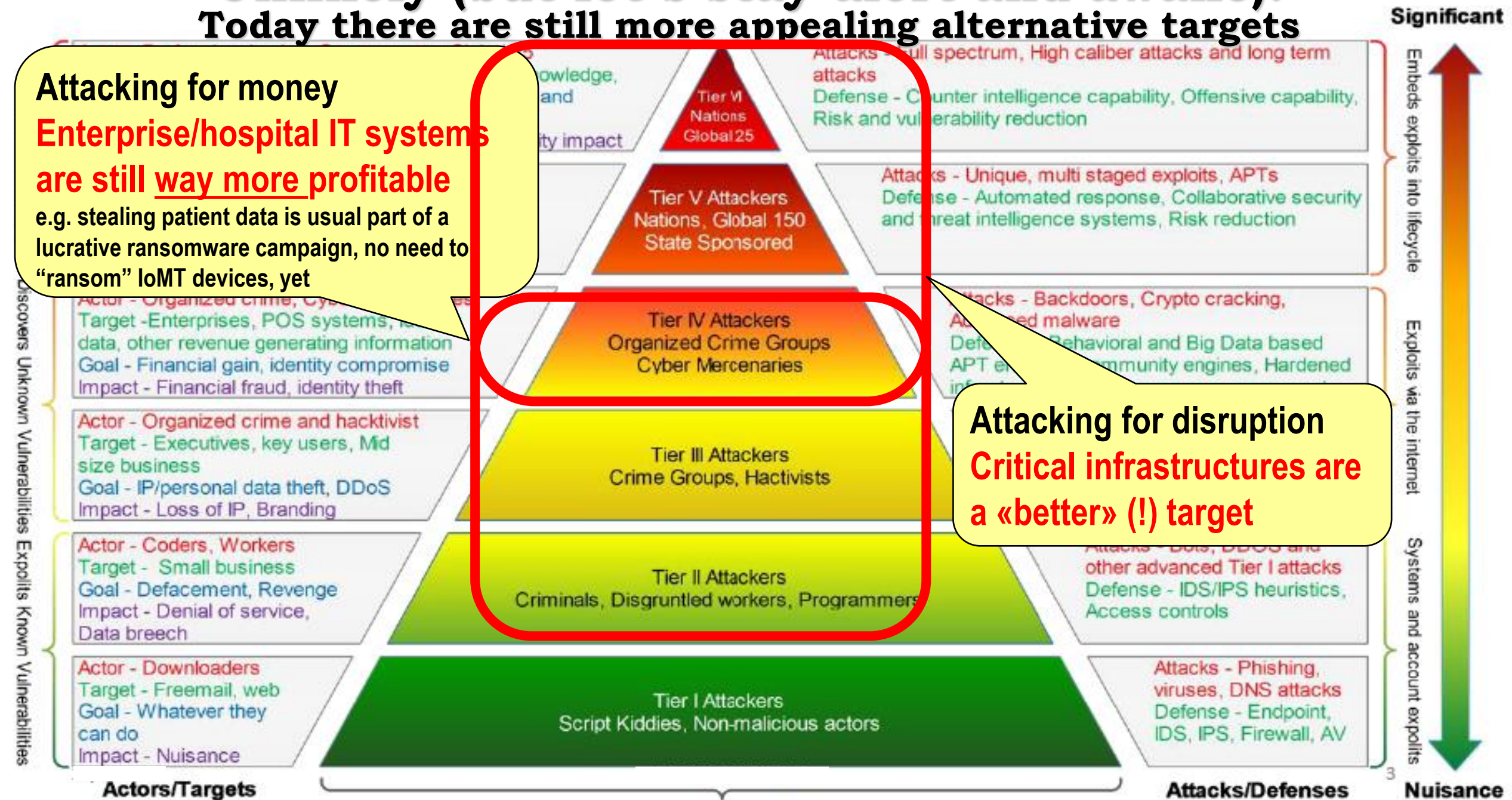
Unlikely (but let's stay alert and awake): Today there are still more appealing alternative targets

Attacking for money

Enterprise/hospital IT systems
are still way more profitable

e.g. stealing patient data is usual part of a
lucrative ransomware campaign, no need to
"ransom" IoT devices, yet

Attacking for disruption
Critical infrastructures are
a «better» (!) target



Discoverers Unknown Vulnerabilities Exploits Known Vulnerabilities

Rather... Cyber- physical IoT Ransomware

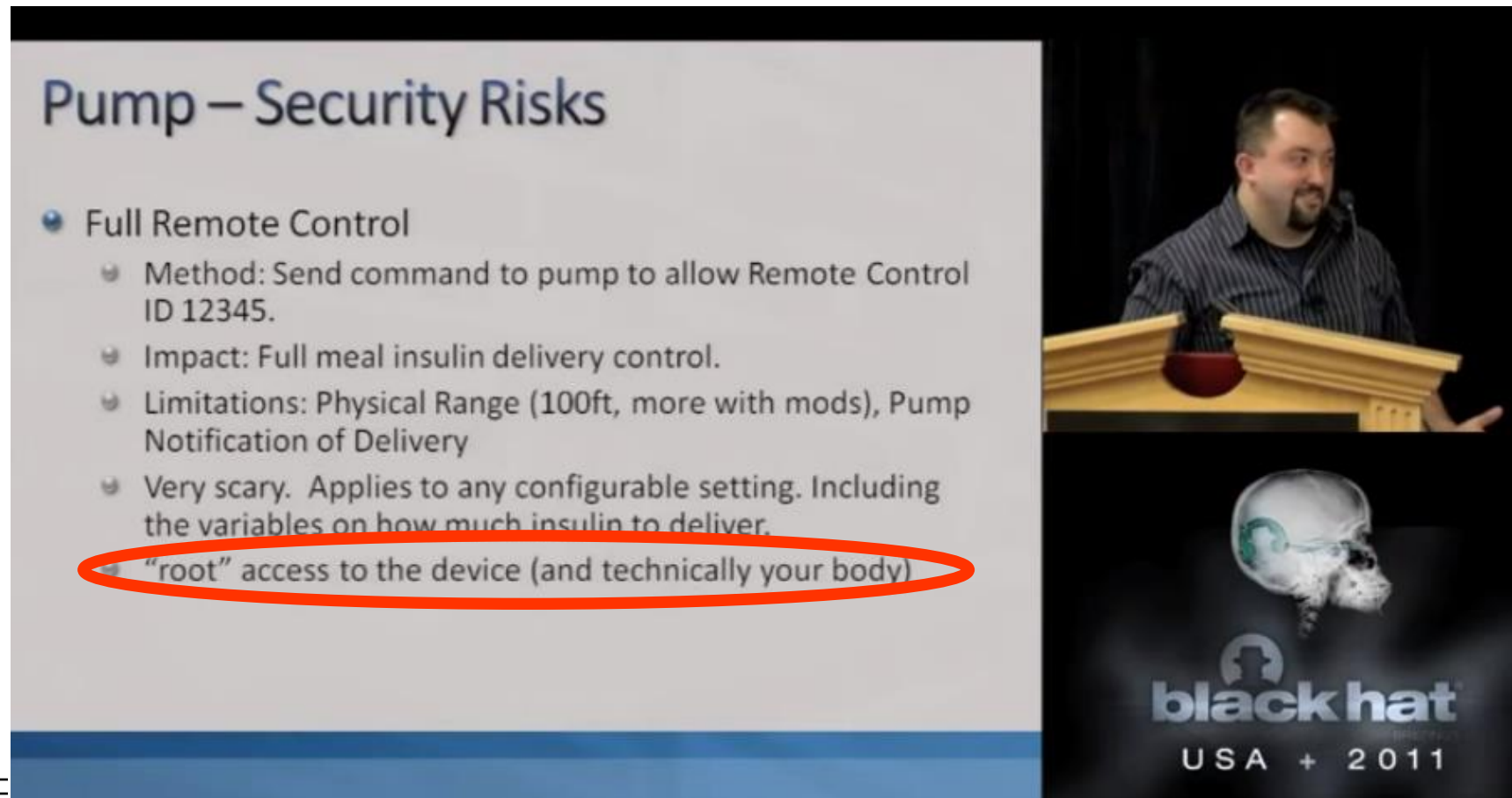
Predicted since
at least a dozen
years ago;
coming soon?



But what makes the Internet of Medical Devices different from a cybersec perspective?

MedDev Security started much later than other fields

Basically zero discussion before the 2011 BlackHat talk on insuline pump attack...



Pump – Security Risks

- Full Remote Control
 - Method: Send command to pump to allow Remote Control ID 12345.
 - Impact: Full meal insulin delivery control.
 - Limitations: Physical Range (100ft, more with mods), Pump Notification of Delivery
 - Very scary. Applies to any configurable setting. Including the variables on how much insulin to deliver.
 - **"root" access to the device (and technically your body)**

black hat
USA + 2011

But what makes the Internet of Medical Devices different from a cybersec perspective?

Medical Devices: long lifecycle, certification constraints

→ Vulnerabilities often unpatched for loooong time!!

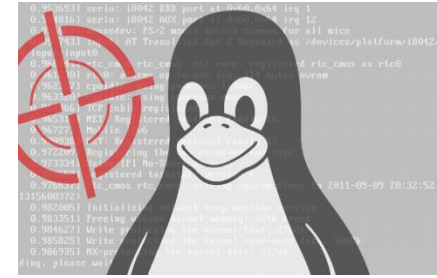


Better late than never: something is now moving

- **March 2022: PATCH Act** (Protecting and Transforming Cyber Health Care Act)
 - Updates to be provided by manufacturers, and for the entire lifecycle
 - SBOM (Software Bill Of Materials): SW dependencies must be made explicit

But what makes the Internet of Medical Devices different from a cybersec perspective?

Do you really need a «full» Windows or Linux in your MedDev?!



→ **General purpose OS in a device:**

⇒ An overkill, and a richer vehicle for vulnerabilities

→ Especially when out of date – more later

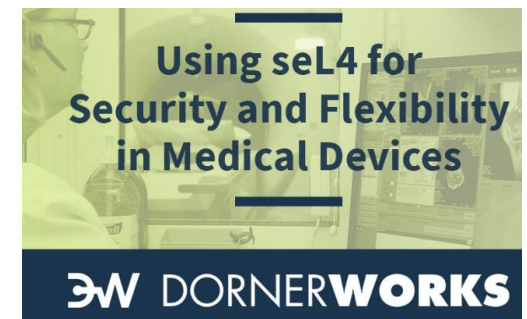
→ **So why? Cheap and easy to develop upon!**

→ **Alternatives? Less is more, in security!!**

⇒ IoT-specific secure OSs (e.g. RIOT)



⇒ Mission-critical micro kernels (e.g. SEL4)



But what makes the Internet of Medical Devices different from a cybersec perspective?

Usable «break-the-glass» security: a must for some MedDev



Some anomalous percentages in MedSec

→ **94% of healthcare delivery organizations give third parties access to their systems.**

⇒ Attackers may target a (weaker) third party

→ 36% of ransomware indeed caused by third party)



→ **Vulnerabilities: o(20%) critical (CVSS \geq 9) – more later**

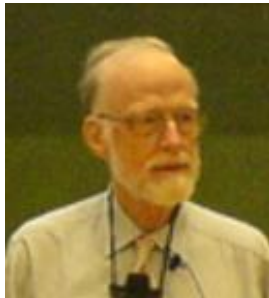
⇒ In layman terms: if security fails, it fails **badly**

→ (so far) limited attention to secure design

Security by obscurity? Forget it, today!

There are two ways of constructing a software design: One way is to make it so simple that there are obviously no deficiencies, and the other way is to make it so complicated that there are no obvious deficiencies.

Tony Hoare
turing award



Giuseppe Bianchi

Let's take a peek at this code
(by reversing it)
(powerful tools today)

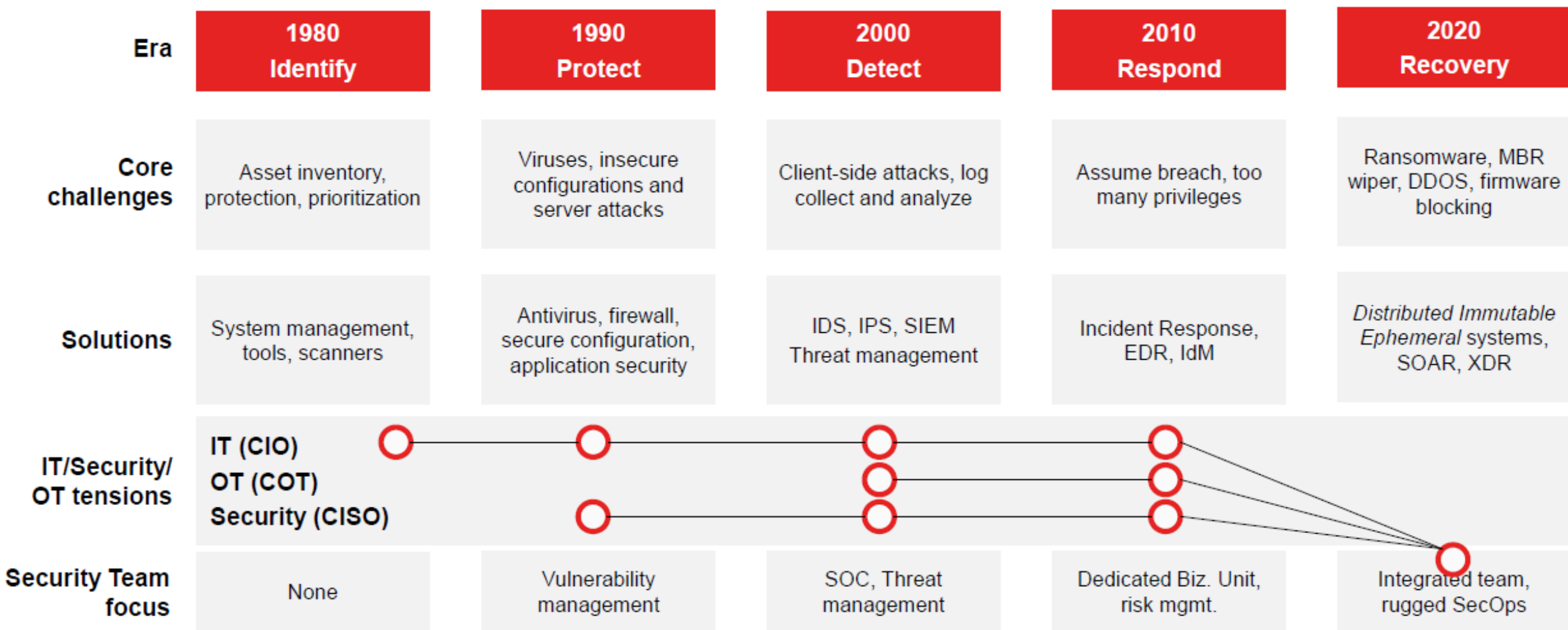
The app was so obfuscated that its obvious vulnerabilities had been hiding in plain sight for years

[from 2023 talk on different context (banking app) - but MedDev SW may even be worse...]



Thai Duong
Chief at Calif Inc. | 3,141,592,653 followers

Protecting MedDev? Not like protecting usual IT systems! (we don't have all such experience & tools)



But at least MDS² can help assessing MD sec

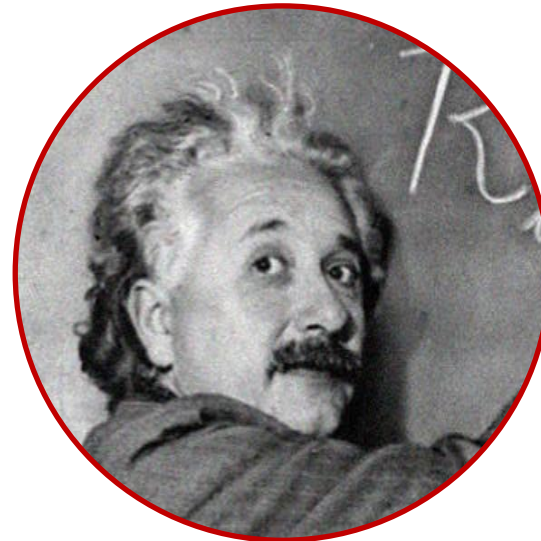
- **MDS2** = Manufacturer Disclosure Statement for Medical Device Security
 - ⇒ developed by Natl. Electrical Manufacturers Assoc. (NEMA)
- Voluntary standard: MD manufacturers use it to share security-related information with healthcare orgs
- Form/questionnaire - clarifies roles and responsibilities; enhances visibility and evaluation of device security
 - ⇒ **2019 version → 216 questions covering 23 security capabilities**

Example questions:

- How can the connected medical device be patched?
- Does it require physical access, or can updates be provided remotely?
- Can the operator install patches on their own, or does it all need to go through the vendor?
- Are there any built-in security safeguards and capabilities such as encryption, auto-logout, malware detection, or physical locks?
- Does the device have anti-malware software? If not, can it be installed by the operator?
- What types of private data are stored on the device, and how are they transmitted?

keep in mind: Y/N responses just a start... Apparently trivial questions are much subtler than what you may expect

MDS2 Q TXCF-2: Is personally identifiable information encrypted prior to transmission via a network or removable media?



Q: Device: uses AES?

A: Yes → perfect, no problem!

Q: Device: uses AES?

Which AES? (ECB very bad, GCM required)

Where/how key is stored?

IV reused? SIV? Critical in GCM

Power/EM side channel?

Timing channels?

...

A: should be acceptable,

but let's stay awake and

systematically check

via DevSecOps

Take home: we need more skilled folks!

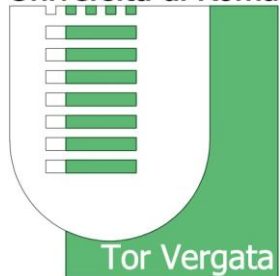


WORKSHOP
CYBER4HEALTH
Osservatorio sulle vulnerabilità cyber e fisiche
dei dispositivi medici



Thank you!

Università di Roma



Giuseppe Bianchi

Professor, University of Rome Tor Vergata

Director, National CNIT Network Assurance & Monitoring LAB

Giuseppe Bianchi



consorzio nazionale
interuniversitario
per le telecomunicazioni