DIMITRIS GLYNOS (@dfunc) / dimitris @ census-labs.com
eHealth FORUM 2016

MEDICAL DEVICE SECURITY

CENSUS
IT Security Works

ABOUT CENSUS S.A.

- We deliver security assessment services to customers worldwide

- Recent medical projects include:

  - Assessments of smart medical devices

  - Assessments of DICOM software components

  - Penetration tests to clinics

  - Assessment of platform for the exchange of medical data

"SMART" MEDICAL DEVICE CHARACTERISTICS

- Communication-enabled devices (Internet of Medical Things) capable of interacting with medical information systems

- Remote management

- Firmware updates

- Communication with vendor / clinic via special gateway

Examples of smart devices

CENSUS
IT Security Works

TYPICAL ISSUES

- Security defects in the device software

  - may allow an unauthorised entity to **control** the device and **collect** / **tamper** device data

- Insecure setup (flat network, default passwords etc.)

  - may allow an unauthorised entity to gain **remote access** to the device (sometimes from any point in the hospital network)
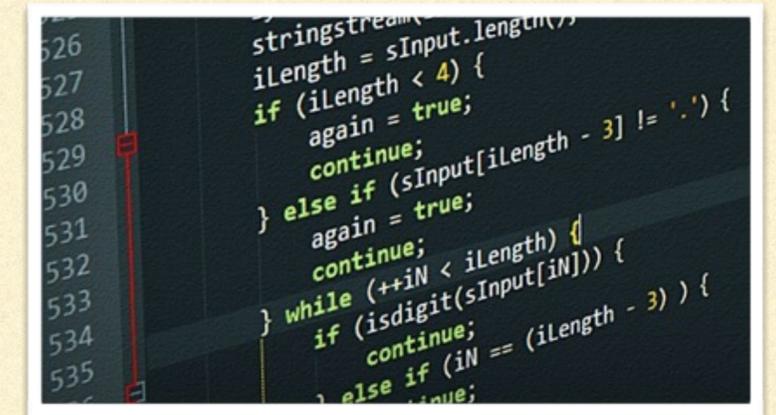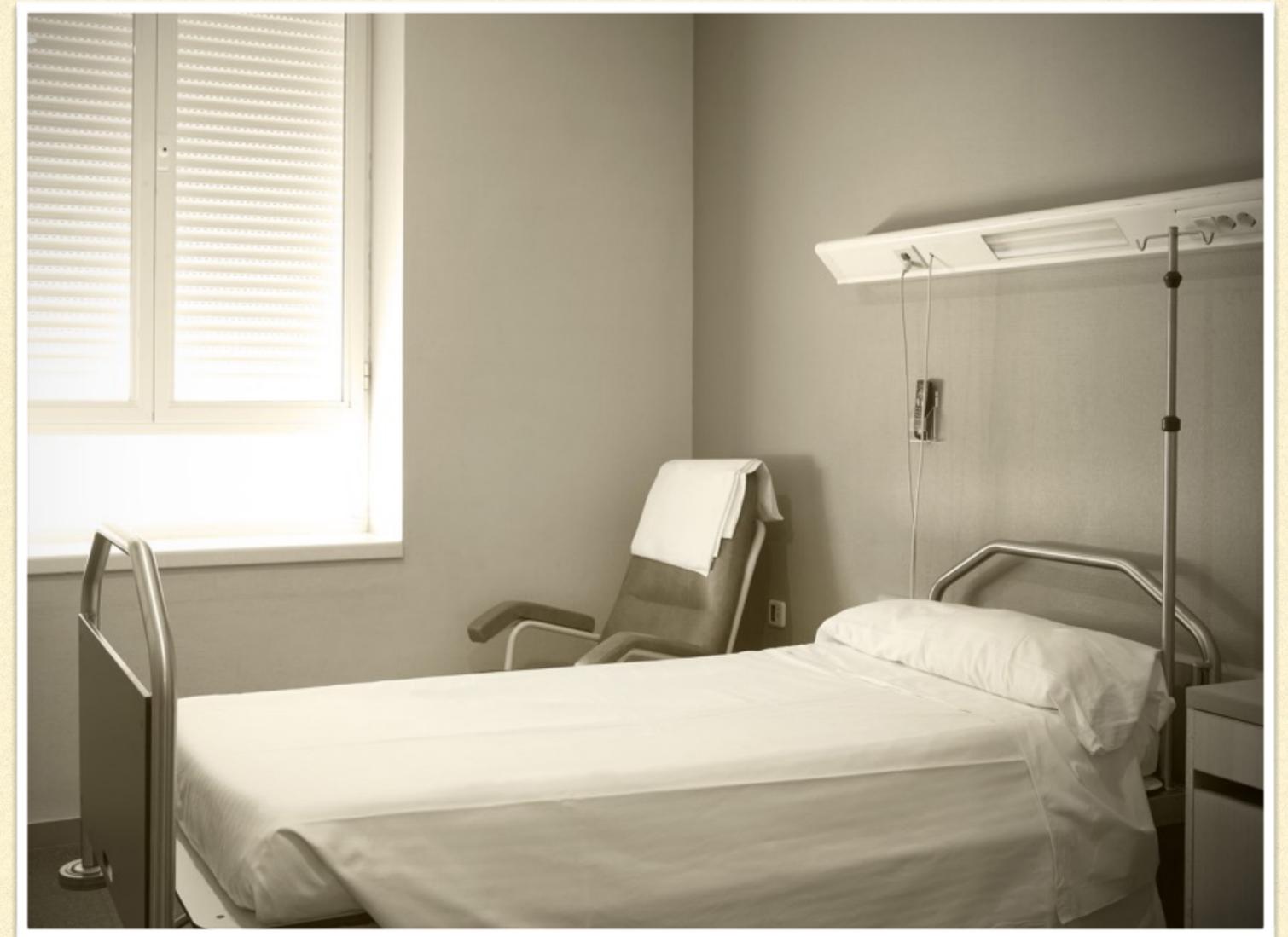
CENSUS
IT Security Works

THE RISKS

- Casualties

- Severe degradation of services

  - e.g. destruction of blood stock

- Clinical data theft and disclosure

- Financial and reputation impact

BUT WHO WOULD EXPLOIT THESE?

- A terrorist ?

- A nation-state actor ?

- A thief ?

- Someone working for a competitor (or an insurance company or …) ?

- An insider ?

- Does it matter ?

MAJOR CHALLENGES

- Vendors tend to make minimum security efforts during development

- A security patch may take a VERY LONG time to be prepared and rolled out

- Doctors prefer to work with certain equipment based on non-technical factors

- Medical devices are not treated as critical infrastructure

  - Insecure setup and use

  - Vulnerability exploitation may go unnoticed

THE WAY FORWARD

- Governance

  - We need **information security officers** (not just IT officers) in medical institutions

- Awareness

  - Regular **security awareness training** for staff

CENSUS
IT Security Works

THE WAY FORWARD

- Enhanced Device Certification Process

  - Make **security assessments** part of the **Device Certification** process

    1. Require a Secure SDLC-type lifecycle from the vendor

    2. The certification body must carry out security assessments to the device independently

- Setup Evaluation

  - Include **security assessments** in the **Device Installation** process

Development
Phase

Design
Phase

Product
Security
Checks

Release
Phase

Post-Release
Issue Handling

CENSUS
IT Security Works

THE WAY FORWARD

- Security Architecture

  - **Control** physical, network and service access

  - **Audit** interactions (tie to per-user accounts, no common / default credentials)

  - **Protect** data storage and transmission

THE WAY FORWARD

- Openness

  - Information about critical security defects **must be disseminated** to all stakeholders

  - Third parties must be **allowed** to conduct security research on medical devices

QUESTIONS?

Follow us on Twitter!
@census_labs

Thank You!

CENSUS
IT Security Works