DIMITRIOS GLYNOS (@dfunc) / dimitris @ census-labs.com
2nd ENISA eHealth Cyber Security workshop, Vienna, Austria 2016

MEDICAL DEVICE SECURITY

CENSUS
IT Security Works

ABOUT CENSUS S.A.

- We provide IT 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

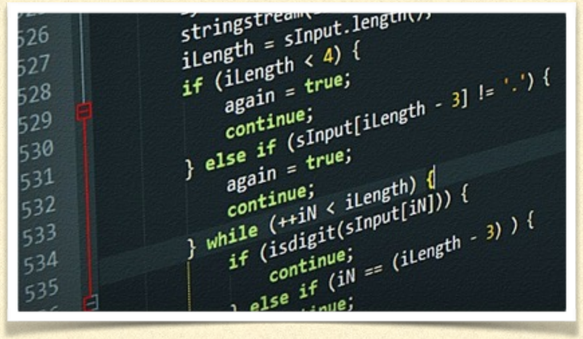
"SMART" MEDICAL DEVICE CHARACTERISTICS

- Communication-enabled medical devices (Internet of Medical Things) capable of interacting with Medical Information Systems
- Remote monitoring and management capabilities
- Firmware update capabilities
- Sometimes require a separate "gateway" device for communication with vendor / clinic

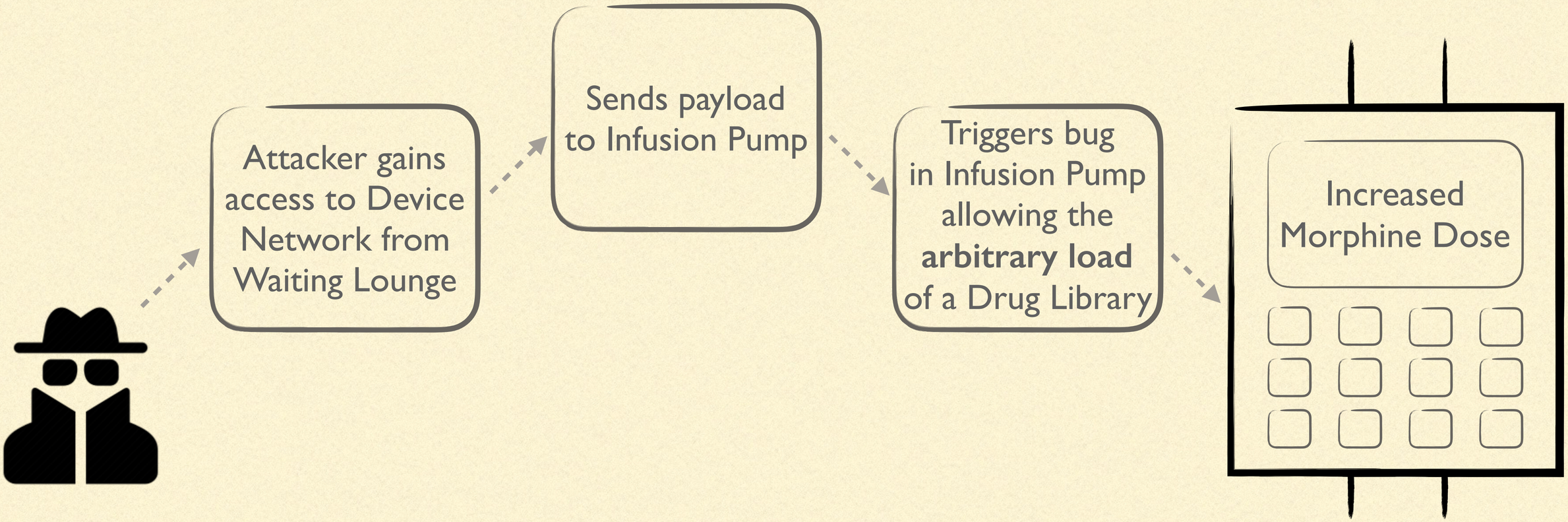
Examples of smart devices

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)

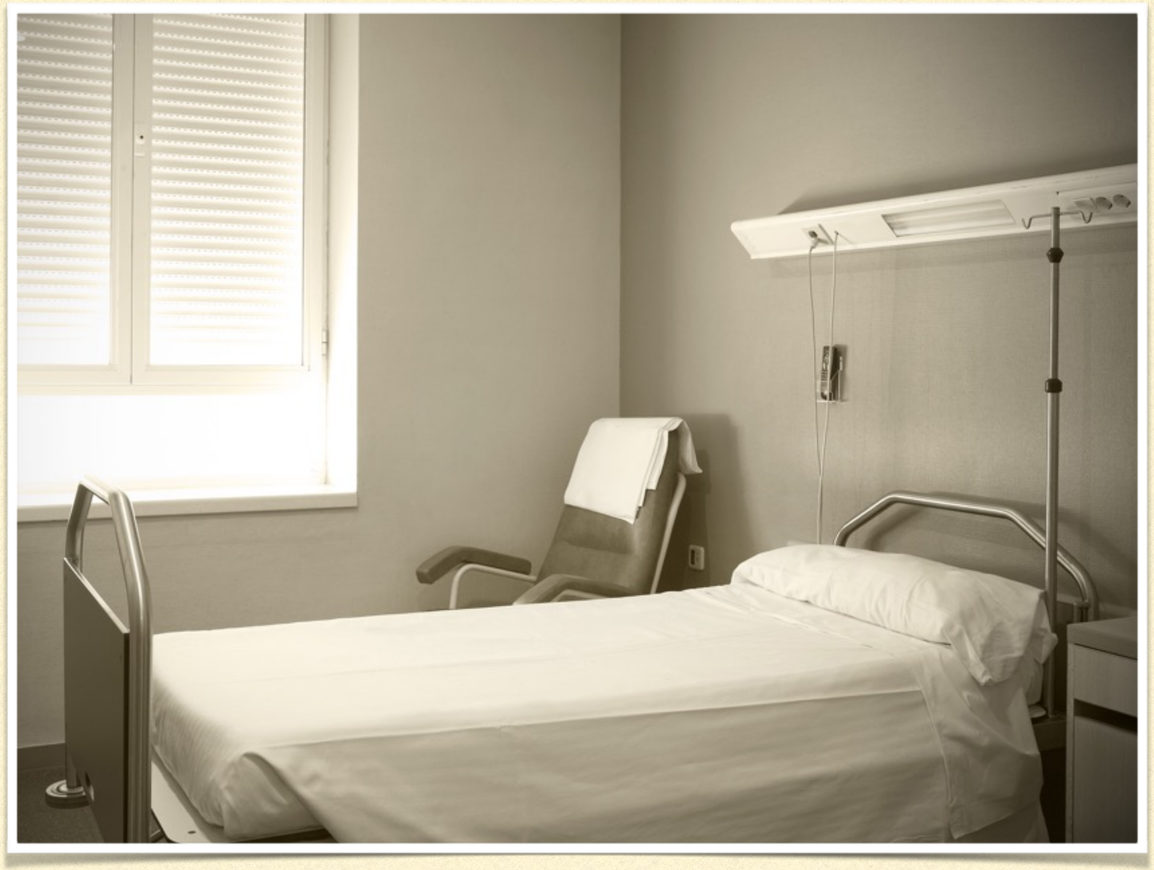


EXAMPLE ATTACK SCENARIO



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

- At minimum, vendors will meet the security requirements set by certification bodies
- Doctors prefer to work with certain equipment based on non-technical factors
- A security patch may take a VERY LONG time to be prepared and rolled out
- 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

THE WAY FORWARD

- Security Architecture for Medical Device setups
  - **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

- Medical Devices need to pass three levels of Security Assessments prior to use

Secure SDLC followed by Vendor

Independent Assessment executed / commissioned by Certification Body

Independent Assessment executed / commissioned by Medical Institution

THE WAY FORWARD

- Product Security Checks
  - make sure that **the Vendor has taken security into consideration** during all phases of product development
- Model Security Assessment
  - makes sure that a **certified product meets security standards** and ships with mitigations for all identified vulnerabilities (or at least the significant ones)
- Setup Security Assessment
  - makes sure that the **setup of a particular device** is in accordance with the **organisation's security policy**

THE WAY FORWARD

- Build upon Audited Components
  - Applies both to Vendors and Medical Institutions

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