17-423/723: Software System Design

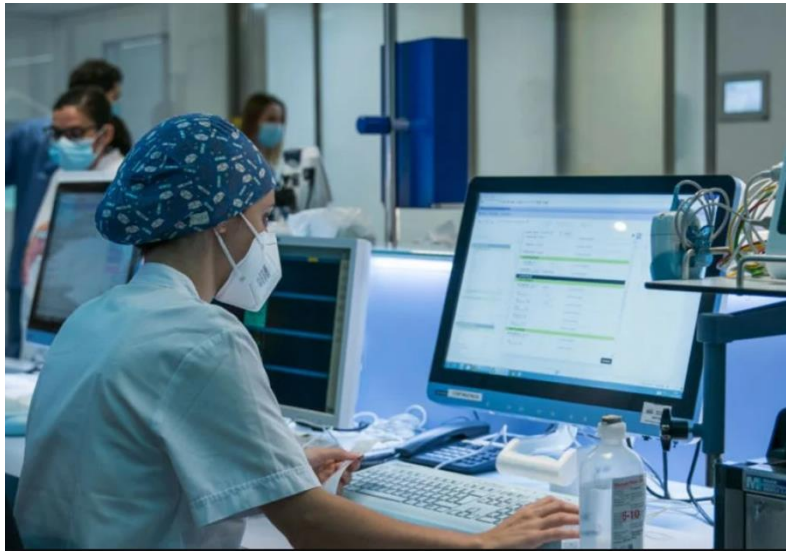
Recitation

Activity: Design for Security

April 2, 2026

Example: Healthcare System

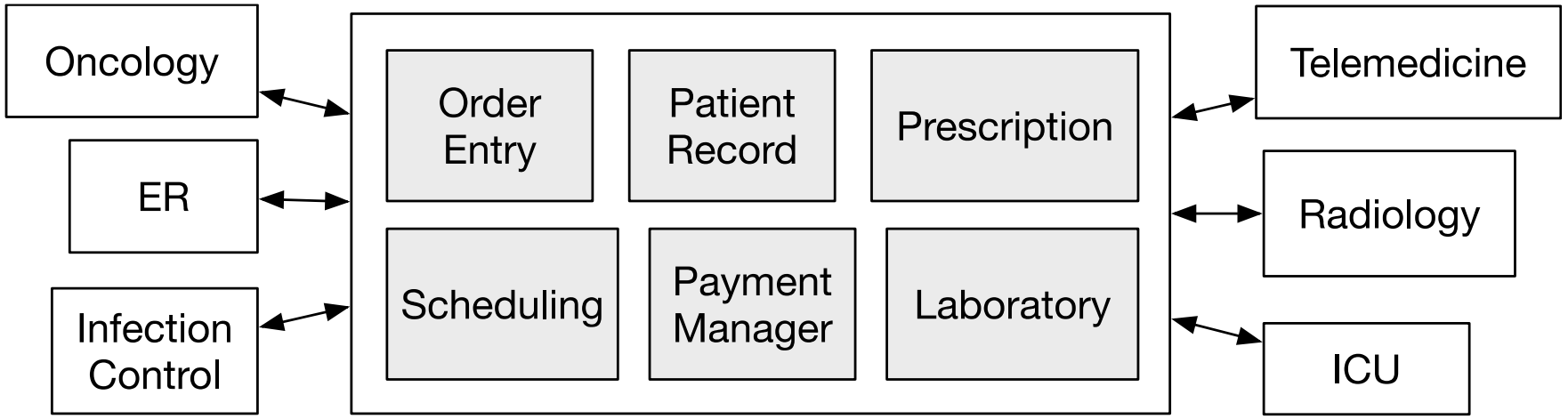
- "Conti" ransomware attack on the Health Service Executive (HSE) of Ireland, May 2021
  - Largest known attack on health IT to date
- Entire system shutdown; numerous hospitals and critical patient care disrupted



"For some oncology patients in the middle of treatment, the incident meant that hospitals didn't have access to the patient's radiotherapy plans and could not safely continue treatment without new medical imaging."

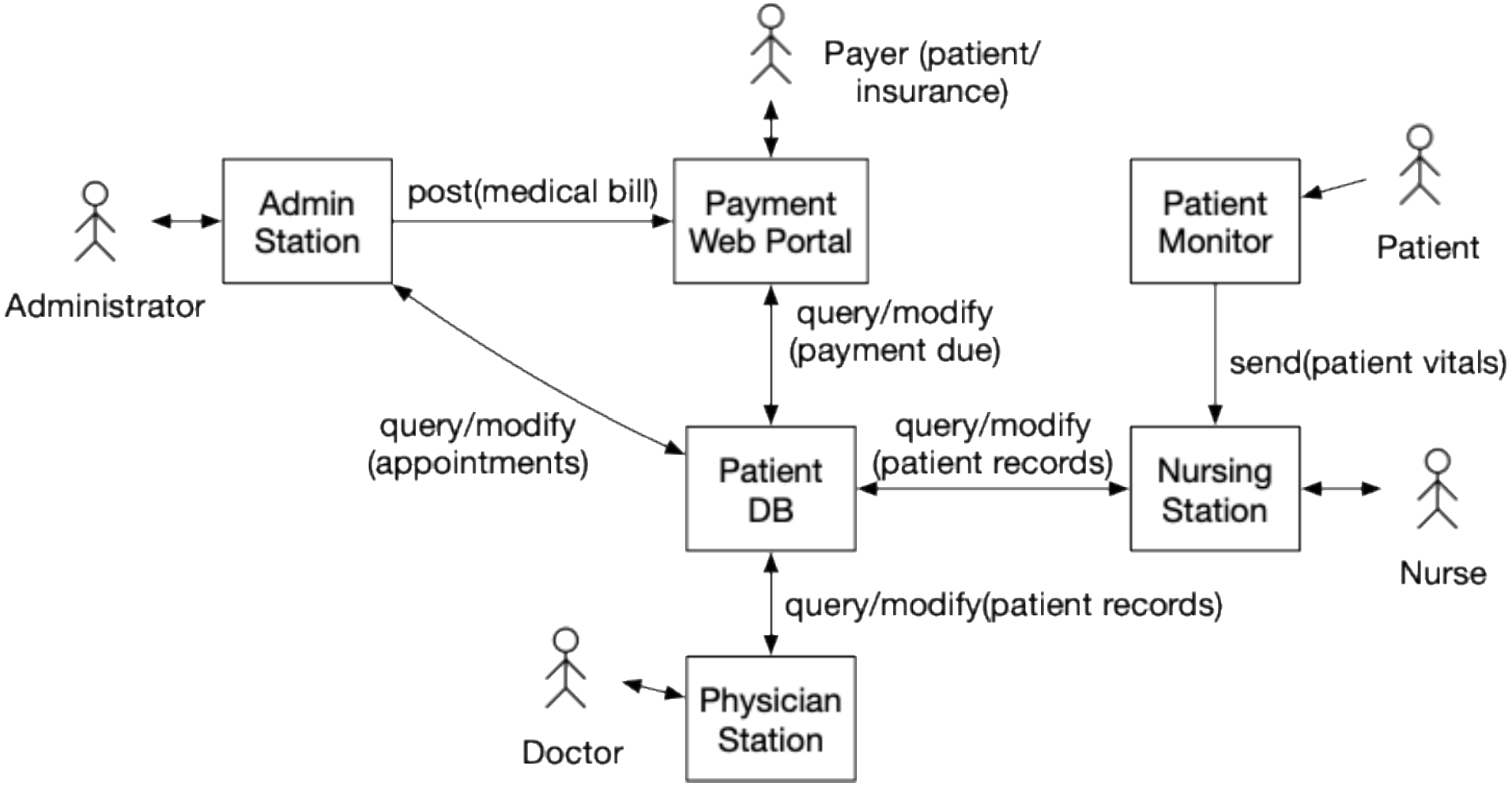
Source: *Conti cyber attack on the HSE: Independent post incident review*, PwC (2021)

Brittleness in System Design



- Typically designed around a set of core components, used by user-facing services (of different criticality levels)
- Complex, undesirable **dependencies** among components & services
  - Q. What's the TCB in this system?
- A failure/compromise in a core component => a failure in multiple services that depend on it

Sample System Architecture



Component Responsibilities

Component	Responsibilities
Admin Station	Used by administrative staff for appointment scheduling and billing
Payment Portal	Processes billing and insurance claims; reads patient financial and demographic data
Patient DB	Central data store; holds medical history, diagnoses, medications, insurance info, billing records
Patient Monitor	Bedside device; continuously reads and transmits vitals (heart rate, BP, O2)
Nursing Station	Used by nurses; views vitals, updates care notes, retrieves physician orders
Physician Station	Used by doctors; reviews records, makes diagnoses, initiates orders

Activity #1: Threat Modeling

- **Security requirements**
  - **Integrity**: The medical records of each patient are modified only by the nurses and the doctor who are treating the patient.
  - **Availability**: Patient vitals are continuously monitored and updated.
- **Activity**: Apply STRIDE to identify potential attacks
  - Indicate trust boundaries (trusted vs. untrusted components)
  - For each untrusted connection or component, identify relevant STRIDE threats
  - For each possible threat, devise a mitigation strategy

Activity #2: Principle of Least Privilege

- Recall: **Principle of Least Privilege**
  - A component should be given the minimal privileges needed to fulfill its functionality
- **Activity**: Identify components with unnecessary privileges

Activity #3: Trusted Computing Base (TCB)

- Recall: **Trusted computing base (TCB)**
  - Components that are responsible for establishing a security requirement(s)
- **Activity**: Identify and minimize TCBs
  - For each of the two security requirements (integrity and availability), identify the TCB that is responsible for it
  - Consider: Is the TCB larger than necessary? Does it include components with high risks of exposure?
  - If so, suggest a way to re-design the system to reduce the size of the TCB