Context-aware Anomaly Detection for Electronic Medical Record Systems

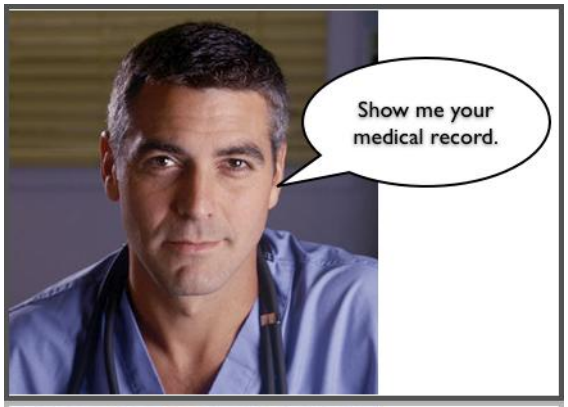
Xiaowei Li
Prof. Yuan Xue, Dept. of EECS, Vanderbilt University
You Chen
Prof. Bradley Malin, Dept. of Bio-informatics, Vanderbilt University

USENIX HealthSec '11
San Francisco, CA
August, 9, 2011

VANDERBILT

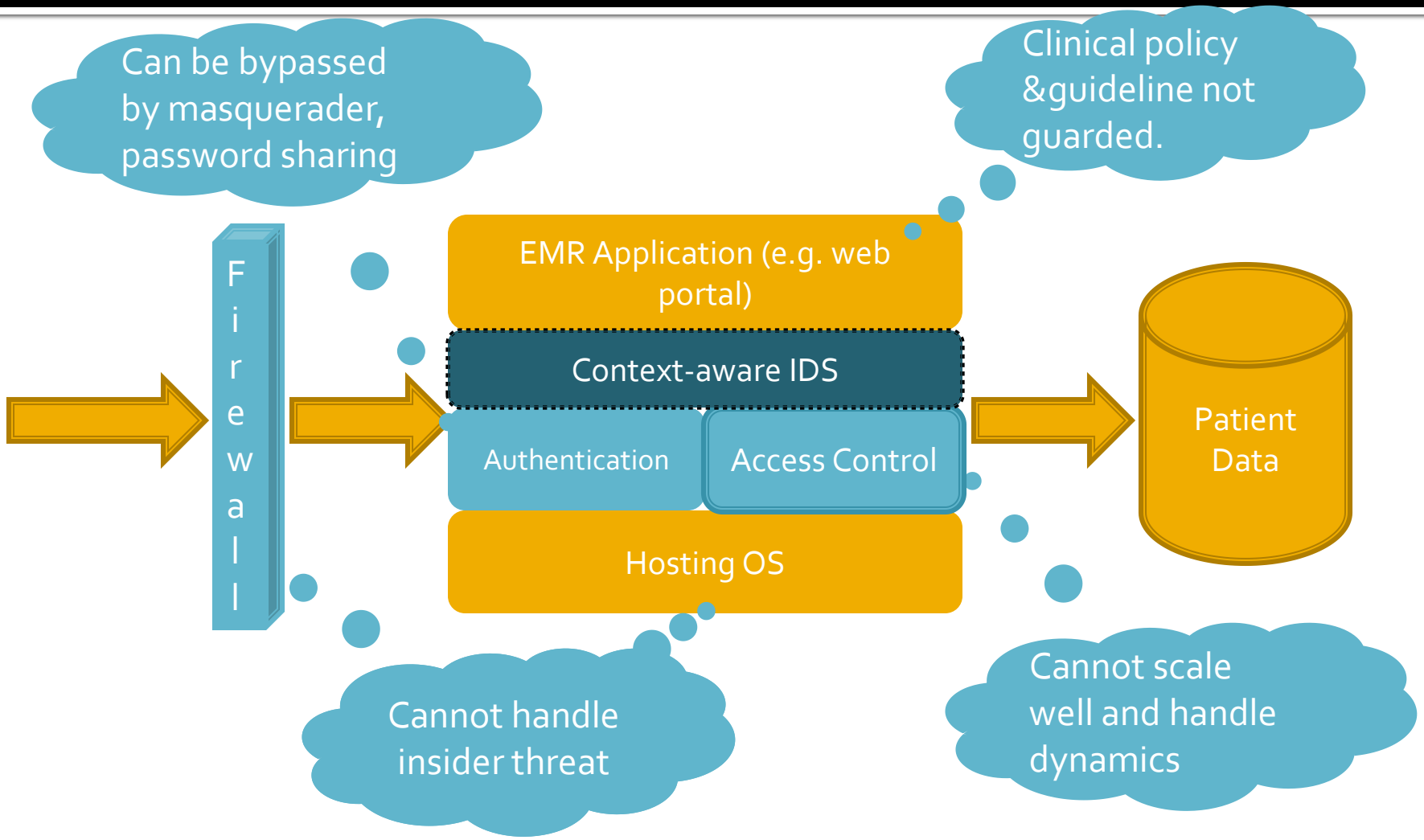
Background

- EMR system is a critical component in today's Health Information Architecture, integrated with a variety of clinical systems, including laboratory, pharmacy, billing, decision support, etc.
- EMR helps streamline clinical workflow, facilitate information sharing and health service delivery.
- However, data security & privacy is challenging:
  - Keep the confidentiality and integrity (tamper-resistant) of patient data.
  - Comply with various regulations & policies, such as HIPPA, etc.
  - …



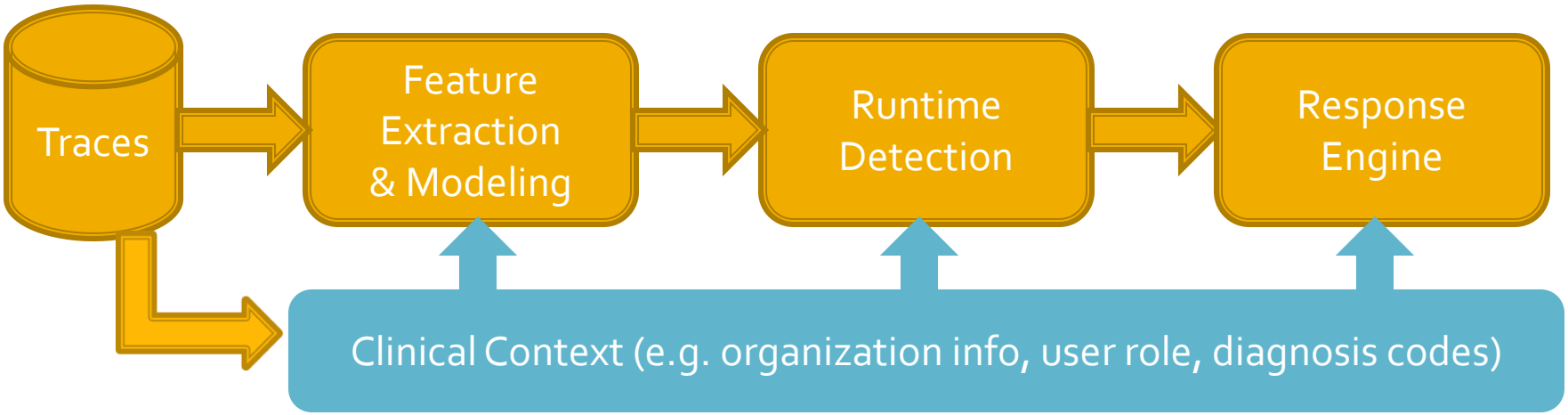
VANDERBILT

EMR Security Landscape



Context-aware Anomaly Detection

- Objective: build an intrusion detection system (IDS), specially tailored to the EMR system, leveraging knowledge & traces from clinical environment.

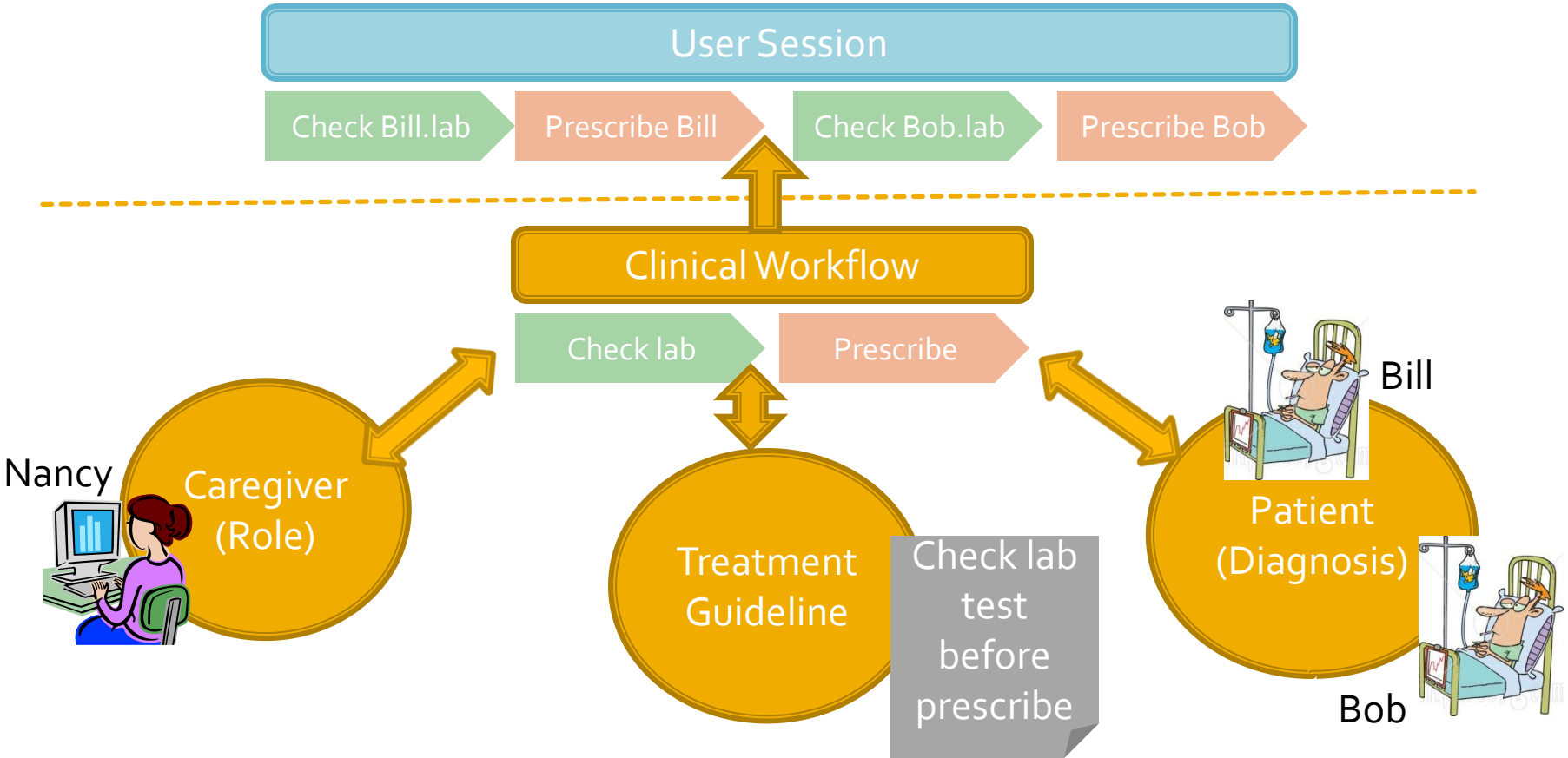


- Key: extract differentiating features that accurately characterize the unique behaviors of EMR users based on historical user sessions.

VANDERBILT

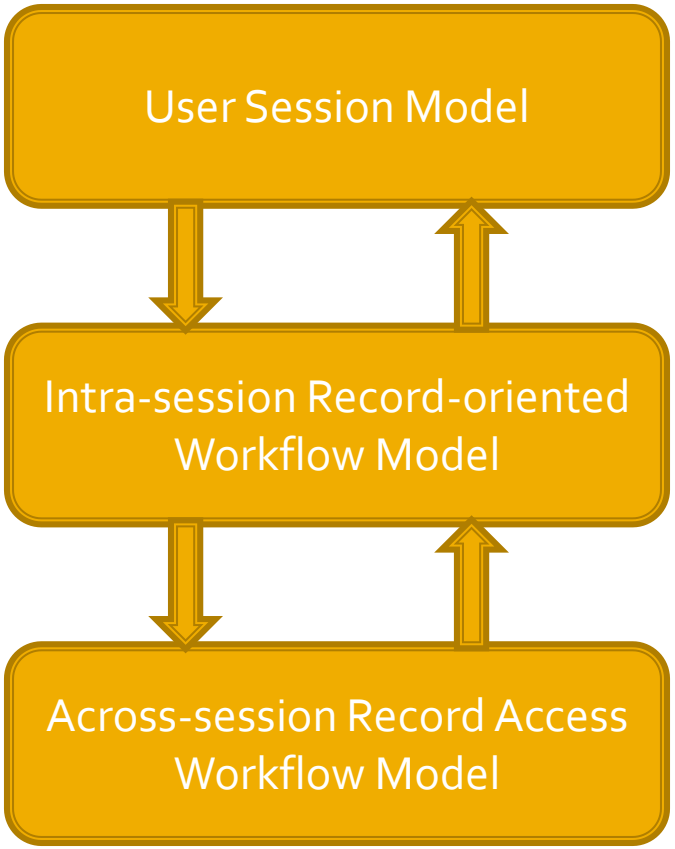
Clinical Workflow

- A clinical workflow is a sequence of operations performed on the patient record by the caregiver during the patient receives healthcare services.



Three-tier Workflow Model

- 1st Tier: profiling user behavior for each user/role;
- 2nd Tier: decompose a session into a set of record-oriented clinical workflows.
- 3rd Tier: indicating the treatment guideline applicable for the patient, involving multiple users/roles.
- Modeling techniques: action set/sequence.
- Other challenges: user behavior may migrate/evolve with time; a patient associated with multiple disorders.



VANDERBILT

Thanks!

Problem & approach → Modeling technique → Implementation → Evaluation

VANDERBILT

Challenges

- Traditional Mechanisms:
  - Authentication
  - Access control: RBAC, EBAC [5], etc.
  - Network firewall, hardening operating systems and software (e.g., web portal)
  - …
- A unique challenging landscape in clinical environment:
  - Authentication can be bypassed (e.g., password sharing, masquerader)
  - Access control may not scale well with the dynamics and coarse-grained implementation allows for privilege abuse/misuse.
  - Traditional IDS cannot handle insider threats.
  - Moreover, clinical treatment guidelines are too complex to be modeled and explicitly enforced, which make space for guideline violation.
  - ….