

Modeling Abstractions for Representing Privacy and Security in Patient Portals

Sean Duncavage, Janos L. Mathe, Jan Werner, Gabor Karsai, Akos Ledecz, Bradley Malin, Janos Sztipanovits
Institute for Software Integrated Systems, Vanderbilt University

Goal

Define the necessary abstractions to represent complex interdependencies within health information systems (HIS)

- How can we create high-fidelity, formal models?
- What are the privacy and security implications?
- What information is passed among care providers and patients?
- Where is this information stored?

Methodology: Model Abstractions

Abstractions express features unique to HIS in four modeling aspects

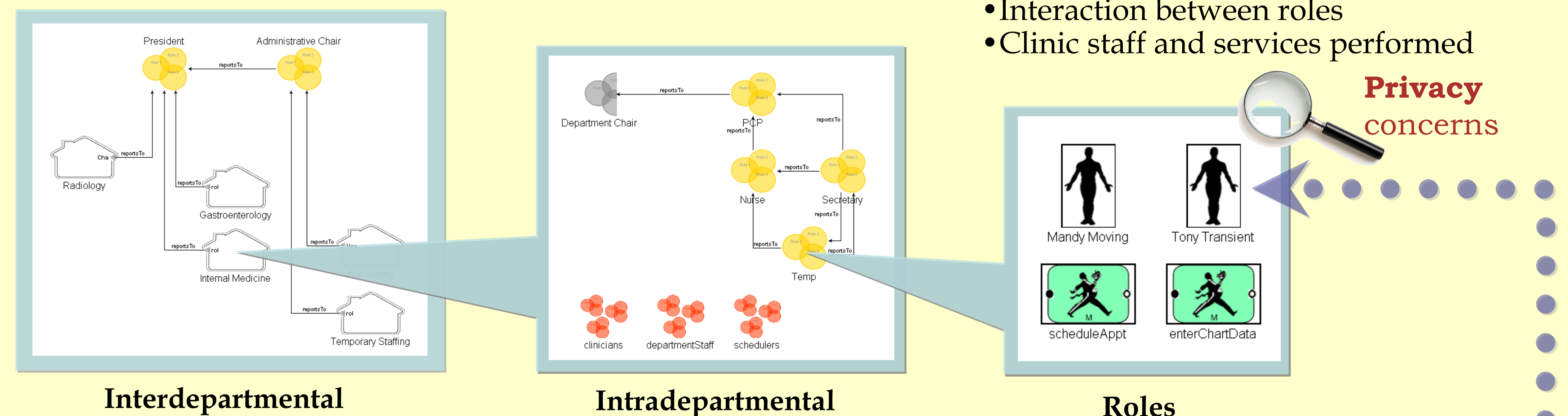
- **Organizational:** define the architecture at the human level and indicate knowledge available to roles
- **Deployment:** define the underlying computer network infrastructure
- **Service:** define the workflows of hospital staff and software
 - Control flows: the sequence of service invocations
 - Data flows: the movement of information
- **Data:** define the structured information in the system

Methodology: Collaborative Approach

- Met with Vanderbilt University Medical Center stakeholders to create a Domain-Specific Modeling Language for patient portals
- Doctors, EMR software developers, and privacy officials provided domain knowledge of the MyHealth@Vanderbilt system
- Diverse viewpoints revealed the necessary abstractions
- Iteratively refined the modeling language

Results

Organizational Models



Organizational models specify human coordination within HIS

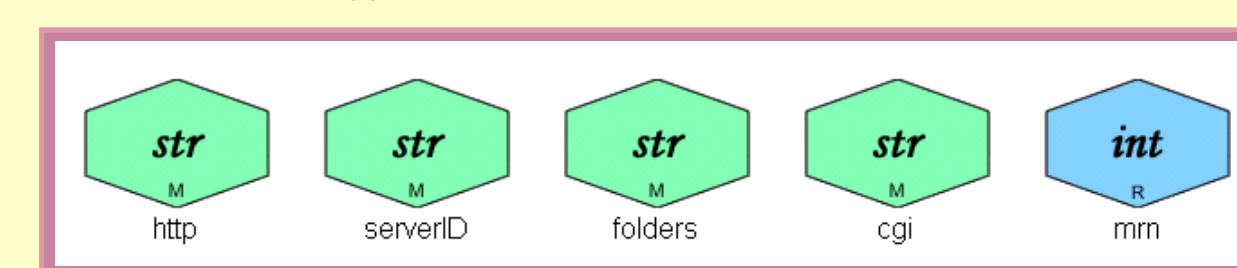
- Interaction between clinics
- Roles and groups of roles within clinics
- Interaction between roles
- Clinic staff and services performed

Data Models

Data models specify the information in the HIS

- Simple and compound data types
- Represent permanent patient information and transient material

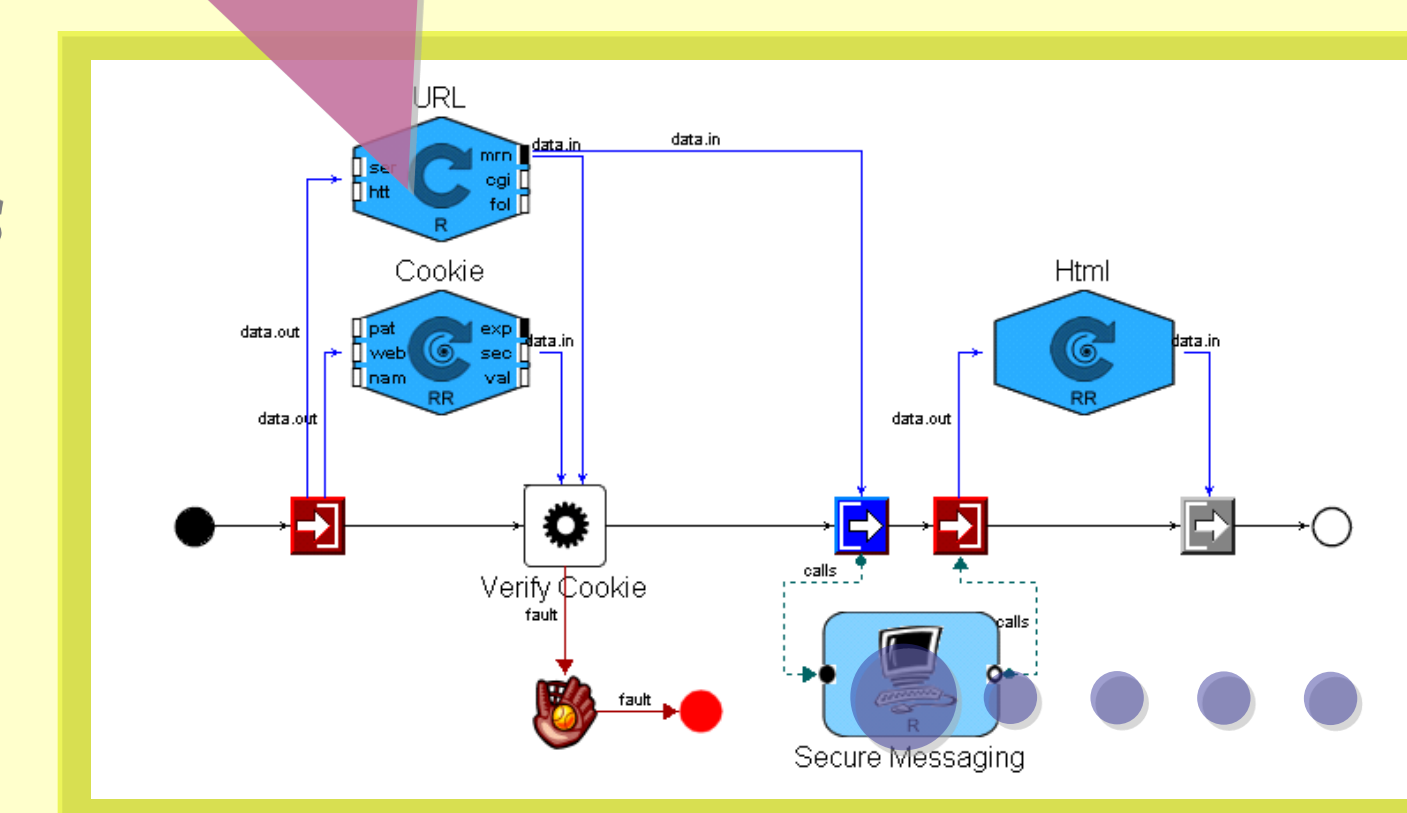
Compound Data Structure



Service Models

Service models specify workflows

- Data transactions
- Actors involved



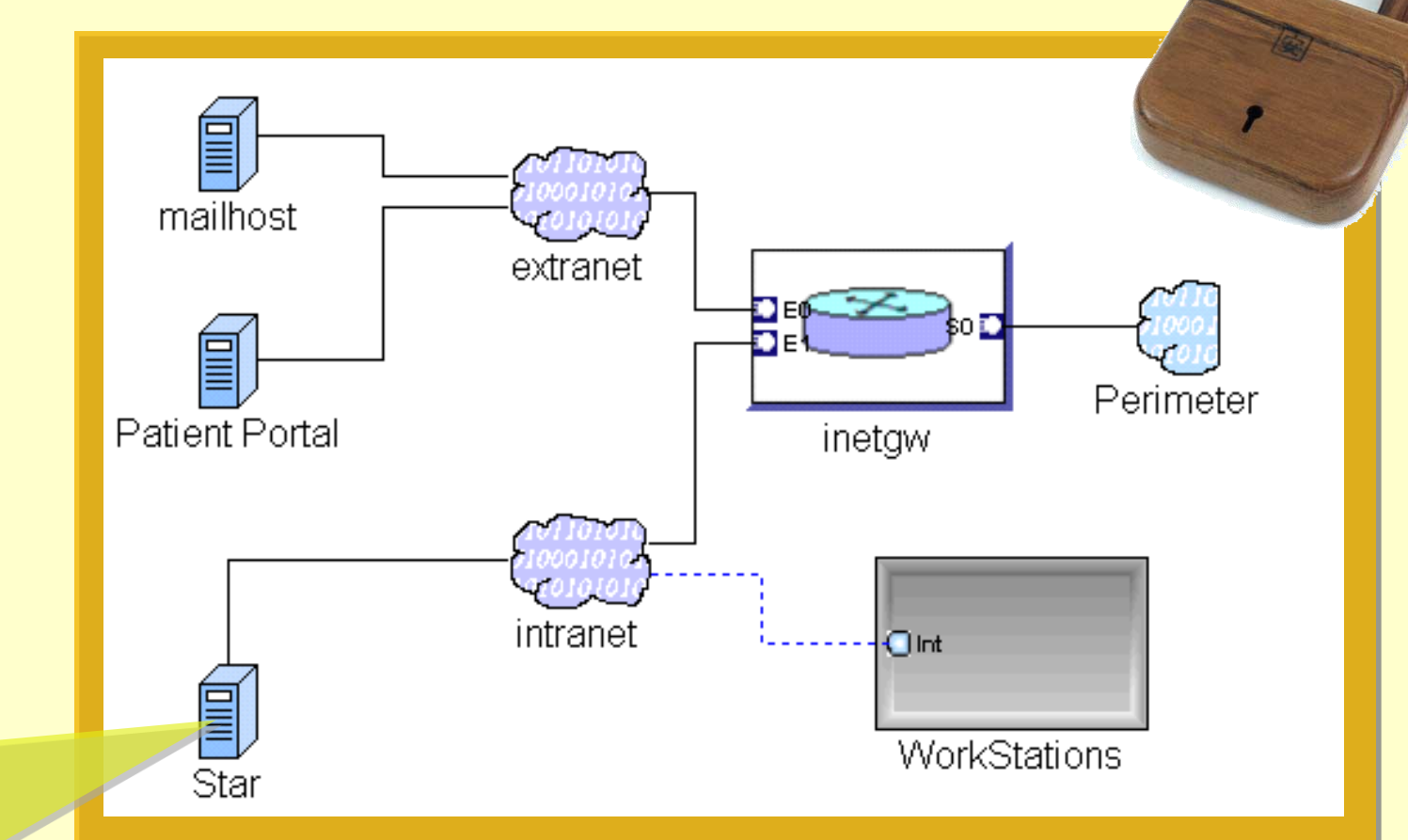
Machine Service

Deployment Models

Deployment models represent the network infrastructure

- Servers and workstations
- Secure sessions
- Access control

Network Architecture



Conclusions

- Domain experts confirmed the expressiveness of the abstractions in our language
- With our abstractions we created realistic models of a patient portal
- Modeling interactions within HIS requires multiple aspects to capture diverse considerations

Future Work

- Extend work beyond patient portals to include other components of HIS
- Compare implementation models
 - Effects of privacy policies
 - Effects of security measures