ECS 235B Module 33 Break-the-Glass Policies

Break-the-Glass Policies

- Motivation: when security requirements conflict, some access controls may need to be overwritten in an unpredictable manner
  - Example: a doctor may need access to a medical record to treat someone, yet that person is unable to give consent (without which access would be denied)
- User overrides the denial
  - Controls notify some people about the override
  - Controls log override for later audit

Example: Rumpole

- Implements a break-the-glass policy
- *Evidential rules*: how to assemble evidence to create context for request
- *Break-glass rules*: define permissions
    - Includes constraints such as obligations to justify need for actions
- *Grant policies*: how rules are combined to determine whether to grant override

Example: Rumpole Enforcement Model

- *Request*: subject, desired action, resource, obligations acceptable to subject
- Decision point:
  - Grants request
  - Denies request
  - Returns request with set of obligations subject must accept; subject then can send a new request with that set of obligations, if they are acceptable