

# Security for Building Automation Systems

Carl A. Gunter and Nikita Borisov  
University of Illinois at Urbana-Champaign



## Risk Mitigation in Multi-Tier Systems

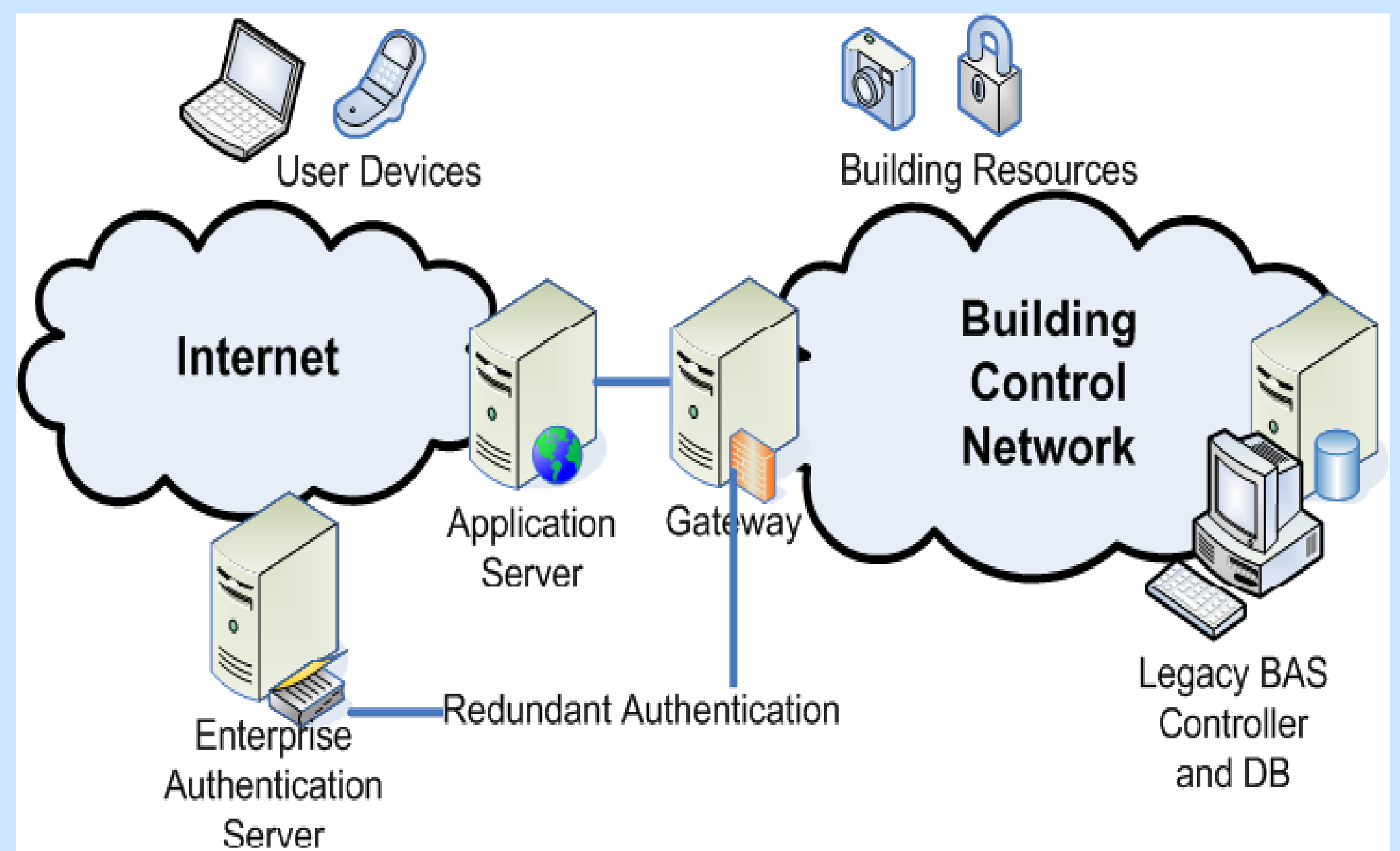
- Multi-tier systems are commonly used to protect back-end resources
- Front-end access to back-end is too broad, a security risk in case of compromise
- Permissions should be limited to those required for operation on behalf of current users

## Building Automation Systems

- Multi-tier critical infrastructure example
- Building Automation systems control building systems such as HVAC and door locks
- Protected by isolation from production networks
- Isolation prohibits open applications and access
- Applications and network exposure for applications requires risk mitigation through security protocols

## Approach: Redundant Authentication

- Requests are validated with non-repudiable authentication tokens from currently active users
- Limits scope of compromise of front end
- Leverages enterprise authentication systems



## Approach and Impact

### New approach

- Multi-tier protection for connection to enterprise network
- Redundant authentication

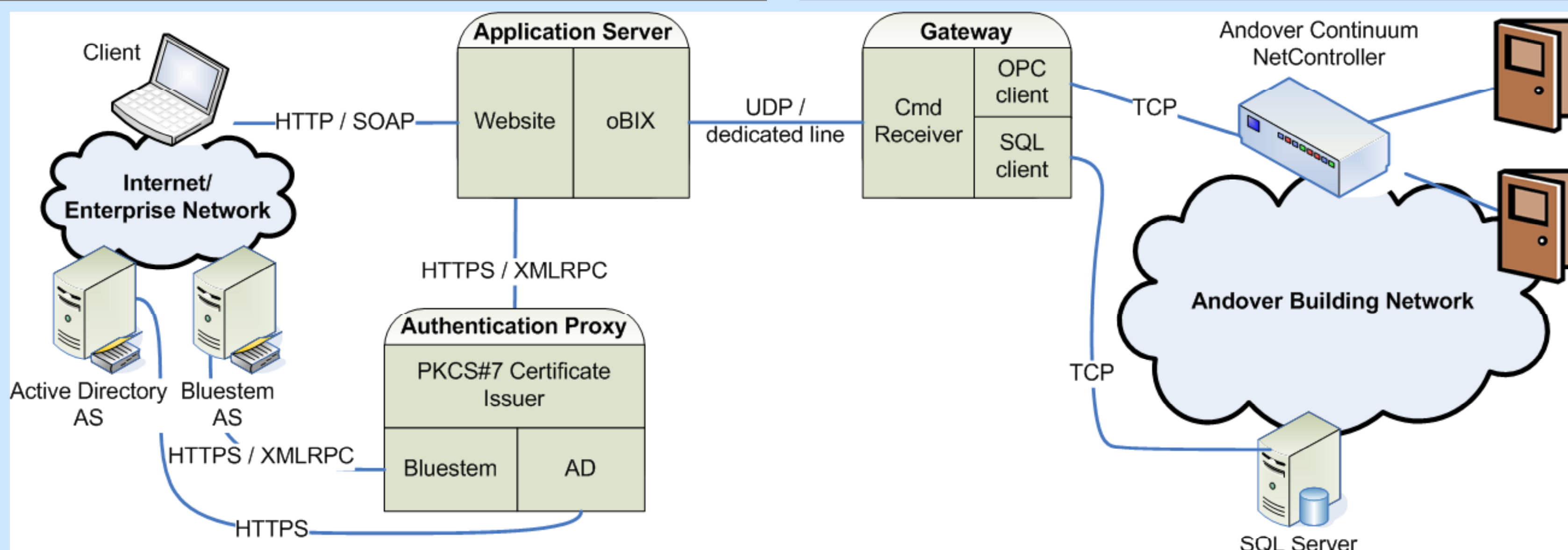
### Research Impact

- Methodologies for securing multi-tier systems
- Exposure of previously closed automation systems
- A new protocol for risk mitigation

## Building Automation Middleware (BAM)

- BAM is a middleware web services implementation of redundant authentication for the Siebel Center
- BAM API permits applications on the building
  - Automated delegation of access rights to doors
  - Mobile unlocking doors with phones, web, etc.
- BAM leverages existing network authentication protocols and BAS systems

- BAM uses several industry standards:
  - oBIX for the API
  - OPC and SQL to abstract the building systems
- The gateway enforces the following policy
  - Requests must be made by an authenticated client
  - Clients can only perform actions on rooms to which they already have access



## Research Directions

- APIs for new applications
- Intrusion detection systems for a networked BAS
- Discretionary, user controlled, data access systems
- Deployment in Siebel Center

Reference: Improving Multi-Tier Security Using Redundant Authentication. Boyer, Hasan, Olson, Borisov, Gunter, Raila. ACM Computer Security Foundations Workshop (CSAW '07) Fairfax, VA, November 2007

To learn more: Google "UIUC BAM"