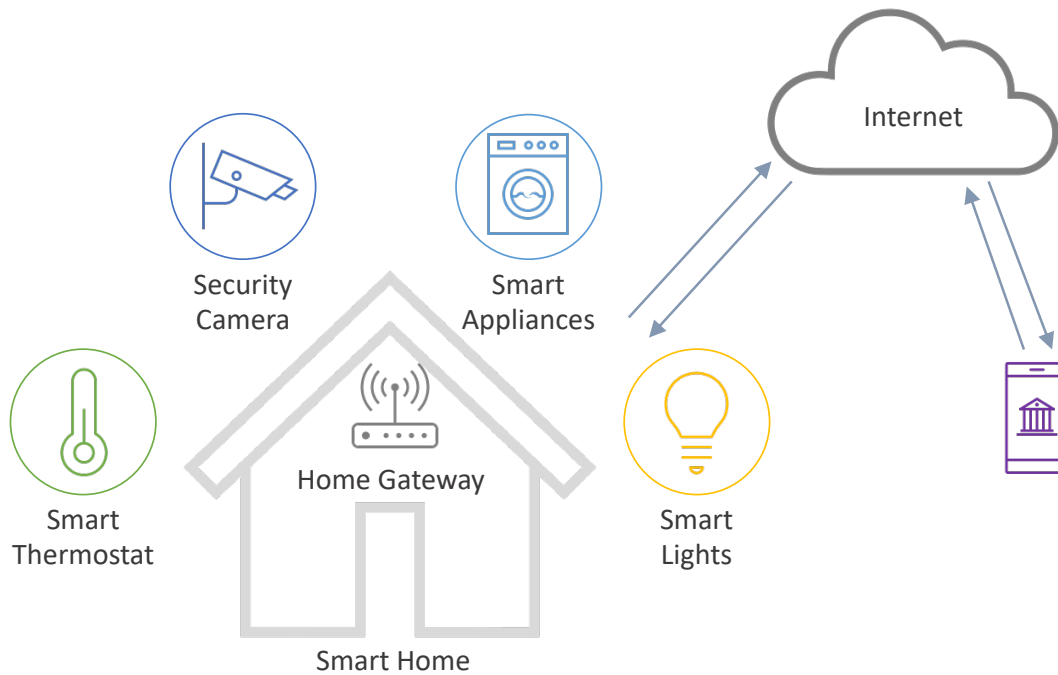


University of Arizona
ECE 509 – Cybersecurity: Concept, Theory, and Practice
Fall 2023

Homework 01
Due Tuesday, September 12, 2023, 11:59 PM
Upload to D2L as a PDF file

Apply threat modeling to the smart home architecture shown below.



Follow all the steps in threat modeling (except step 4: validate), identify 5 potential threats, apply STRIDE, and DREAD models, identify the impacted assets, and impacted entry points, and describe the mitigation strategy to handle each threat. Use the following tables as guidelines.

Threat Description	Threat Category (STRIDE)					
	<i>Spoofing</i>	<i>Tampering</i>	<i>Repudiation</i>	<i>Information Disclosure</i>	<i>Denial of Service</i>	<i>Elevation of Privileges</i>

Threat Description	Threat Risk Assessment (DREAD)					
	<i>Damage</i>	<i>Reproducibility</i>	<i>Exploitability</i>	<i>Affected Users</i>	<i>Discoverability</i>	<i>DREAD Score</i>

Threat Description	Impacted Assets						
	<i>Compute Resource</i>	<i>Physical Safety</i>	<i>Availability</i>	<i>Integrity</i>	<i>Data Integrity</i>	<i>Data Availability</i>	<i>Data Privacy</i>

Threat Description	Impacted Entry Points					Mitigation Strategies
	<i>Embedded HW/SW</i>	<i>Communication Channels</i>	<i>Admin Tools</i>	<i>Remote Application Interface</i>	<i>Deployment Infrastructure</i>	