HW 1 Answers – Question 1

CSCI-UA.0480-63

September 29, 2025

1. Threat modeling for Citi Bike

We propose three security policies for New York's Citi Bike system, each targeting a distinct adversary type (thieves, terrorists, trolls). For each policy, we specify concrete enforcement mechanisms and rationale.

Policy A (Thieves): Ensure bikes cannot be used or resold if unlawfully removed

Goal: Reduce economic incentive by making stolen bikes valueless and hard to monetize.
Mechanisms:

- *Tamper-resistant electronic locks with authenticated release*: Require station or on-bike lock to perform mutual authentication with backend before unlock; deny offline unlocks; sign unlock events to enable audit. Implement geo-fencing so a bike that leaves a service area without an authorized session hard-locks. (Defense-in-depth policy/mechanism separation discussed in Notes 2025.01.01.)

- *On-bike immobilizer with cryptographic pairing*: Pair controller to per-bike keys; if controller or battery is replaced without re-provisioning via service tool, firmware refuses to engage motor/gears. (Avoid security by obscurity; rely on secret keys rather than hidden design; cf. Kerckhoffs principle, Notes 2025.01.04.)

- *Active recovery and deterrence*: GPS/Cellular beaconing with periodic attestations; stolen-mode triggers brighter lighting patterns and server-side location beacons for recovery in collaboration with NYPD.

Why it works: Removes resale utility and increases recovery likelihood, shifting attacker utility (Notes 2025.01.01 on attacker/defender utilities).

Policy B (Terrorists): Maintain rider safety and rapid incident response

Goal: Preserve safety and availability in the face of attempts to cause violent disruption.
Mechanisms:

- *Station and fleet integrity monitoring*: Backend analytics for simultaneous abnormal unlocks, sudden mass rebalancing anomalies, or tamper alerts indicating coordinated sabotage; automated incident playbooks to disable unlocks in affected zones.

- *Physical hardening and surveillance at high-risk sites*: Bollards, tamper-evident fasteners, and CCTV coverage at major transit hubs to deter placement of hazards and to support forensics.

- *Emergency broadcast and geo-fenced shutdown*: Capability to pause rentals and push safety notices within a radius; integrate with city emergency systems for coordinated response.

Why it works: Defense-in-depth across detection, prevention, and response reduces likelihood and impact (Notes 2025.01.01 on defense-in-depth).

Policy C (Trolls): Maintain service availability and fair access

Goal: Limit nuisance attacks (dock blocking, false reports, mass reservation griefing).
Mechanisms:

- *Strong user authentication and rate-limiting*: Bind accounts to verified payment tokens; apply per-user and per-IP quotas on reservations, unlock attempts, and incident reports; require proof-of-ride (e.g., short post-unlock movement) to keep a dock reserved.
- *Anomaly scoring and graduated friction*: Add friction (CAPTCHAs, SMS recheck) when behavior deviates from normal usage to deter automated griefing.
- *Dock occupancy attestation*: Use on-dock sensors plus bike IMU to verify a dock is truly occupied; auto-release ghost holds.

Why it works: Increases attacker cost for nuisance actions while minimizing friction for legitimate riders (Notes 2025.01.01 on policy vs. mechanism and attacker utilities).

References to provided Notes

- Notes 2025.01.01: Introduction & threat modeling; policy vs. mechanism; defense-in-depth; attacker/defender utilities. Example passages used for rationale.
- Notes 2025.01.04: Kerckhoffs's principle and avoiding security by obscurity; adversary models.

Selected excerpts (for traceability)

- Security Text 2025.01.01.txt, around line 1:
  Chapter 1: Introduction & threat modeling Suggested reading: • Security Engineering, Chapter 1
- Security Text 2025.01.01.txt, around line 3:
  • Security Engineering, Chapter 1 • Tools & Jewels Chapter 1 • An introduction to approachable threat modeling • Attack trees Case study:
- Security Text 2025.01.01.txt, around line 10:
  Security is fundamentally a contest between an attacker and defender. Defenders have security policies they wish to enforce and attackers, for various reasons, aim to undermine those policies.

  Security engineering is about designing mechanisms for defenders to prevent attackers from causing harm. Defenders also must balance competing requirements such as a budget, ease-of-use and compliance with the law.

  The most challenging aspect of security engineering is that attackers adapt and evolve over time. Security engineers continually try to predict what attackers will do in response to a new system being deployed so they can build in security in advance.
- Security Text 2025.01.01.txt, around line 45:
  The distinction between the two notions is not binary. Some security measures provide both. For example, locking your door when you arrive home provides some feeling of protection from the outside world. It also actually makes it more difficult for potential intruders to get inside (though in most cases probably far less than people believe). Deceptive security mechanisms: security theater and deterrents

While almost everybody understands rationally that sleeping under a blanket provides no real security, sometimes elaborate security mechanisms are designed to appear effective to the general public although security engineers know they have little effect. This is called security theater (as coined by Bruce Schneier) or sometimes placebo security. Airport security is often cited as an example of security theater. An infamous example was the use of “puffer machines” (ETPs) in the US in the mid-2000s. They were consistently found to have no effectiveness at bomb detection under real operating conditions. It’s been speculated they were kept in operation for years because the high-tech-looking machines helped ease public fear about flying after September 11th.

- Security Text 2025.01.01.txt, around line 47:
  Deceptive security mechanisms: security theater and deterrents

  While almost everybody understands rationally that sleeping under a blanket provides no real security, sometimes elaborate security mechanisms are designed to appear effective to the general public although security engineers know they have little effect. This is called security theater (as coined by Bruce Schneier) or sometimes placebo security. Airport security is often cited as an example of security theater. An infamous example was the use of “puffer machines” (ETPs) in the US in the mid-2000s. They were consistently found to have no effectiveness at bomb detection under real operating conditions. It’s been speculated they were kept in operation for years because the high-tech-looking machines helped ease public fear about flying after September 11th.

  Deception about the effectiveness of a security mechanism can also be useful if potential attackers don’t understand the true effectiveness and are scared off. This is called a deterrent effect. A common example is shops which mount fake security cameras to deter shoplifters. Or more classically, scarecrows or plastic owls can scare away unwanted birds.

- Security Text 2025.01.01.txt, around line 49:
  While almost everybody understands rationally that sleeping under a blanket provides no real security, sometimes elaborate security mechanisms are designed to appear effective to the general public although security engineers know they have little effect. This is called security theater (as coined by Bruce Schneier) or sometimes placebo security. Airport security is often cited as an example of security theater. An infamous example was the use of “puffer machines” (ETPs) in the US in the mid-2000s. They were consistently found to have no effectiveness at bomb detection under real operating conditions. It’s been speculated they were kept in operation for years because the high-tech-looking machines helped ease public fear about flying after September 11th.

  Deception about the effectiveness of a security mechanism can also be useful if potential attackers don’t understand the true effectiveness and are scared off. This is called a deterrent effect. A common example is shops which mount fake security cameras to deter shoplifters. Or more classically, scarecrows or plastic owls can scare away unwanted birds.

  Finally, the security industry is also littered with snake oil: products deceptively claiming to provide security which in fact are useless. These may fool the owner, but not potential attackers. The ADE 651 machine was widely sold in Iraq, though it literally did nothing except look like a bomb detector. Many argue that anti-virus software in the modern era is largely snake oil. Snake oil might offer some psychological benefit as security theater. The distinction is that with security theater the operator knows the mechanism is ineffective; with snake oil they’ve been deceived.