Week 6 – Final Technical Report & Prototype Tool

1. Executive Summary

We analyzed five Alexa skills spanning account-linking and media playback. We captured mobile app traffic with mitmproxy, modeled threats with STRIDE/LINDDUN, and identified recurring risks at the OAuth boundary and in vendor APIs. We propose mitigations and present a lightweight prototype concept ('SkillLinkGuard') to automatically flag over-collection and OAuth weaknesses during testing.

2. Methodology

• Testbed: Android emulator + Alexa app routed through mitmproxy with generated CA.
• Procedure: enable skill → (if required) complete account linking → exercise minimal features → export HAR and screenshots.
• Analysis: search and filters in mitmweb (~u regex for sensitive fields; domain grouping), manual review of authorize/token exchanges, and mapping of flows to STRIDE/LINDDUN.
• Evidence management: saved HARs and screenshots per skill; masked any tokens in the report.

3. Findings (Cross- Cutting)

Area	Issue	Recommendation
OAuth Linking	Risk of excess scopes or weak state/PKCE verification	Mandate PKCE + strict state and redirect_uri checks in certification
Token Hygiene	Potential long-lived, broad tokens	Short TTLs, refresh rotation, proof-of-possession or DPoP where feasible
Over-collection	Email/name requested by simple skills	Progressive consent and runtime justification
Playback	Large audio segment sizes and CDN verbosity	Signed URLs, header minimization, size/time limits
Telemetry	Numerous analytics	Consolidate and document

	endpoints	collection; offer user toggles

4. Case Studies

Ask My Buddy

Account linking observed with Amazon accountLink/validate and vendor login journey; requires confirm of /token and post-link call to finalize evidence.

Philips Hue

Complete OAuth journey visible across account.meethue.com and auth.meethue.com; typical Auth Code with PKCE is expected; post-link API calls should carry Authorization: Bearer …

Question of the Day

No linking; minimal GETs to Alexa endpoints and potential audio playback; low privacy risk aside from analytics.

Cat Facts

No linking; standard invocation and content delivery.

Sleep Sounds

Media-only; repeated .ts segment retrieval from CDN; risks center on DoS and information disclosure from headers.

5. Ethical Implications

Testing must avoid accessing others' accounts or collecting unnecessary personal data. Disclosures should follow responsible reporting. Where risks reflect user misunderstanding (e.g., consent granularity), design-centric remedies should be prioritized alongside technical fixes.

6. Prototype Tool: SkillLinkGuard

SkillLinkGuard is a mitmproxy addon concept that automatically detects account-linking flows, extracts scopes/state/PKCE parameters, and flags over-collection or misconfigurations. It produces a Week-4/5-ready summary.

Prototype (concept) mitmproxy addon snippet:

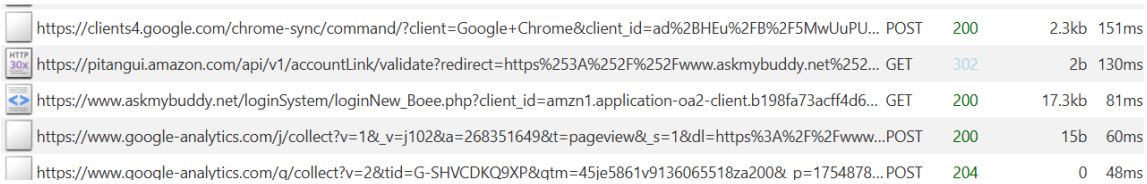
```
from mitmproxy import http, ctx
import re, json
```

```
OAUTH_AUTHZ = re.compile(r"/authorize\b")
OAUTH_TOKEN = re.compile(r"/token\b")
SENSITIVE = {"profile", "email", "name", "zip"}

class SkillLinkGuard:
  def __init__(self):
    self.findings = []
  def request(self, flow: http.HTTPFlow):
    url = flow.request.pretty_url
    if OAUTH_AUTHZ.search(url):
      qs = dict(flow.request.query)
      scopes = set((qs.get('scope','').split()) if 'scope' in qs else [])
      missing_state = 'state' not in qs
      pkce = ('code_challenge' in qs)
      overcollect = bool(scopes & SENSITIVE)

self.findings.append({"type":"authorize","url":url,"pkce":pkce,"missing_state":missing_state,
"overcollect":overcollect,"scopes":list(scopes)})
    if OAUTH_TOKEN.search(url):
      self.findings.append({"type":"token","url":url})
  def done(self):
    ctx.log.info(json.dumps(self.findings, indent=2))
addons = [SkillLinkGuard()]
```

7. Recommendations & Roadmap

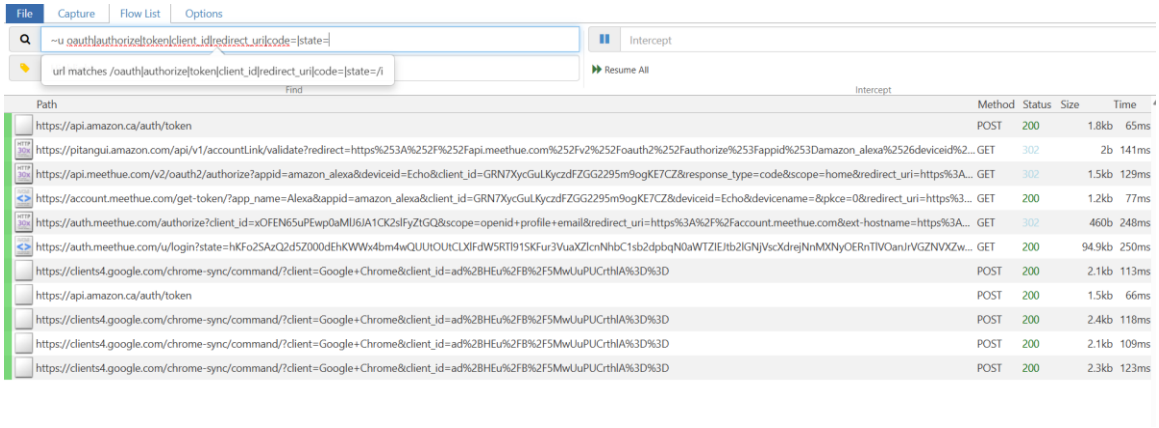
Short-term: add PKCE/state checks to certification, cap scopes, and validate signed media URLs.
Medium-term: publish a vendor linking guideline and lint rules for Alexa skill submissions.
Long-term: offer a user-visible permission dashboard with revocation and per-skill data usage summaries.

Appendix: Selected Screenshots

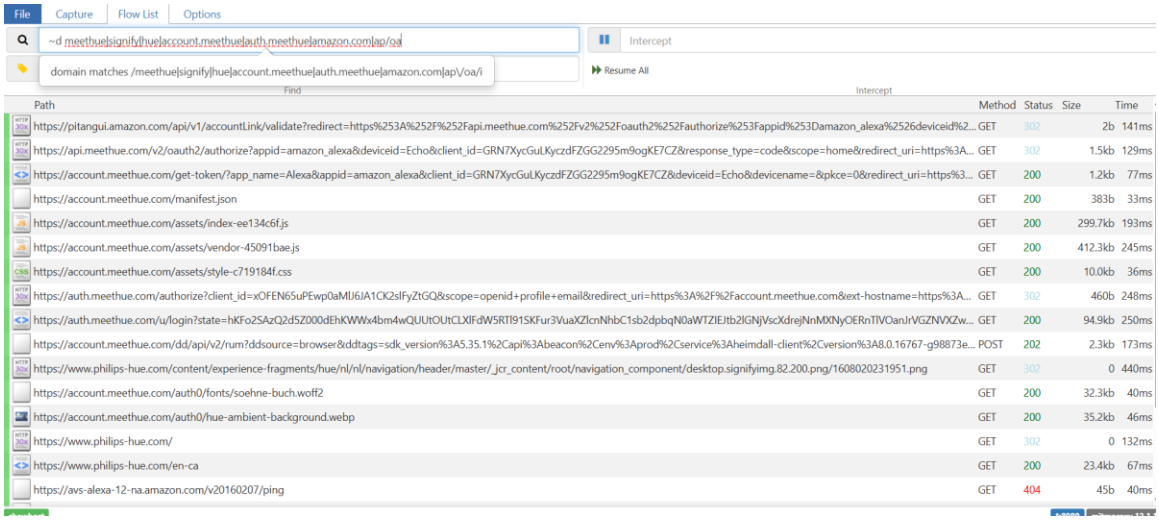


https://clients4.google.com/chrome-sync/command/?client=Google+Chrome&client_id=ad%2BHEu%2FB%2F5MwUuPU...	POST	200	2.3kb	151ms
https://pitangui.amazon.com/api/v1/accountLink/validate?redirect=https%253A%252F%252Fwww.askmybuddy.net%252...	GET	302	2b	130ms
https://www.askmybuddy.net/loginSystem/loginNew_Boee.php?client_id=amzn1.application-oa2-client.b198fa73acff4d6...	GET	200	17.3kb	81ms
https://www.google-analytics.com/j/collect?v=1&_v=j102&a=268351649&t=pageview&_s=1&dl=https%3A%2F%2Fwww...	POST	200	15b	60ms
https://www.google-analytics.com/g/collect?v=2&tid=G-SHVCDKQ9XP&gtm=45je5861v9136065518za200&_p=1754878...	POST	204	0	48ms

askbuddy skill.png



philips_hue1.png



philips_hue_oauth2.png

philips_hue_oauth3.png

Path	Method	Status	Size	Time
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean.m3u8?src=alexa&src_request_id=amzn1.echo-api.request.c7bab921-76ec-48db-8e2b-0b0a01781530	GET	200	1.9kb	30ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean0.ts	GET	200	890.8kb	213ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean1.ts	GET	200	890.2kb	190ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean2.ts	GET	200	891.0kb	190ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean3.ts	GET	200	890.4kb	1
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean4.ts	GET	200	890.1kb	192ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean5.ts	GET	200	891.2kb	188ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean6.ts	GET	200	890.1kb	188ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean7.ts	GET	200	890.4kb	187ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean8.ts	GET	200	890.6kb	188ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean9.ts	GET	200	890.6kb	187ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean10.ts	GET	200	890.2kb	189ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean11.ts	GET	200	890.4kb	188ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean12.ts	GET	200	890.6kb	188ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean13.ts	GET	200	890.6kb	198ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean14.ts	GET	200	890.4kb	192ms

sleep_soundspic.png

https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean15.ts	GET	200	890.4kb	190ms

showhost *:8080 mitmproxy 12.1.1

sleep_soundspic2.png