دانشگاه صنعتی امیرکبیر
(تهران پلی تکنیک)

عنوان مقاله:

1.FIRMRES: Exposing Broken Device-Cloud Access Control in IoT Through Static Firmware Analysis

2.Towards Shielding 5G Control Plane Functions

ارائه دهنده: فاطمه حسنی

استاد: آقای دکتر زرندی

زمستان ۱۴۰۳

فهرست

1.FIRMRES: Exposing Broken Device-Cloud Access Control in IoT Through Static Firmware Analysis

مقدمه

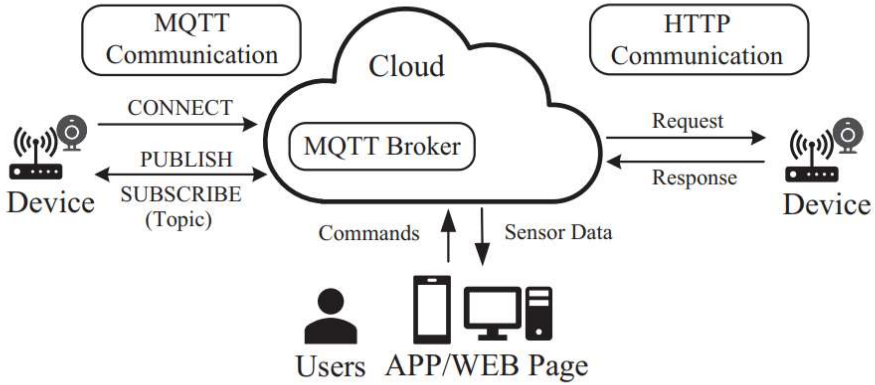
- نقش کلیدی رابط دستگاه-ابر (Device-Cloud Interface) در IOT
- رابط دستگاه-ابر چیست؟
- عملکرد ۳ قسمتی
  - ثبت دستگاه
  - مدیریت از راه دور
  - انتقال داده

مقدمه

- ارائه و معرفی ابزار FIRMRES
- استفاده از روش تحلیل ایستا
- بازسازی پیام‌ها از Firmware دستگاه IOT، بدون نیاز به شبیه‌سازی یا اجرای واقعی

پیشینه تحقیق

- ۳ بخش اصلی سیستم‌های IOT
- HTTPو MQTT پروتکل‌های اصلی



پیشینه تحقیق

- تعامل دستگاه با ابر شامل دو مرحله Binding و Business
- عناصر کنترل دسترسی در پیام‌ها:
  - Dev-Identifier: شناسه دستگاه
  - Dev-Secret: اطلاعات محرمانه دستگاه
  - User-Cred: اطلاعات کاربری
  - Bind-Token: توکن اتصال

پیشینه تحقیق

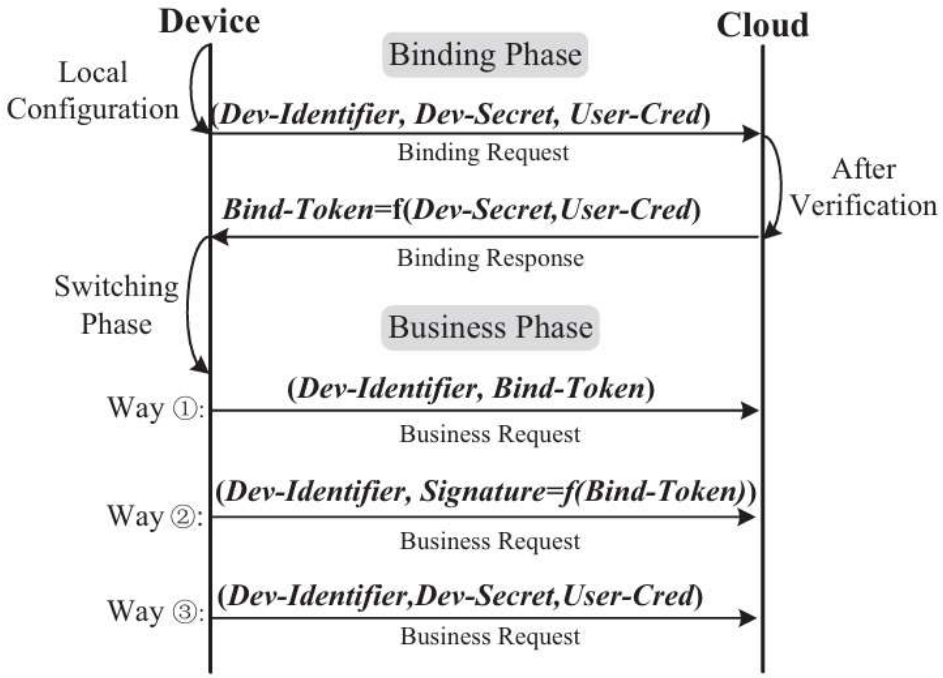
- مرحله Binding

هدف: تایید هویت و اصالت دستگاه

- مرحله Business

هدف: تأیید اتصال دستگاه به یک کاربر و اجازه دسترسی به منابع ابری

پیشینه تحقیق

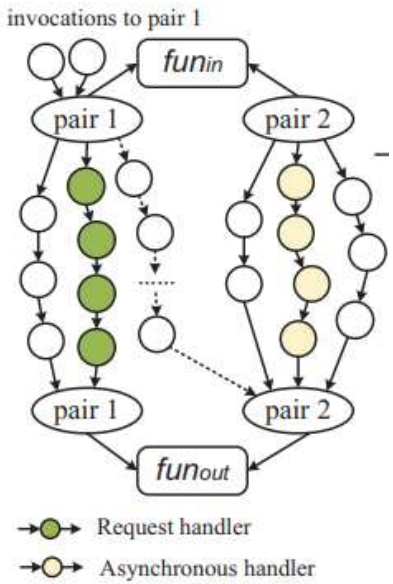


رویکرد اصلی

- ارائه FIRMRES
- یک ابزار نوآورانه، استفاده از تحلیل ایستا
- شناسایی آسیب‌پذیری‌های مرتبط با کنترل دسترسی در رابط های دستگاه-ابر:
  - فقدان فیلدهای ضروری
  - مقادیر سخت کدشده
- ۵ گام اصلی

Pinpointing Device-Cloud Executables

- شناسایی برنامه‌های (فایل‌های اجرایی) دستگاه-ابر
- فایل‌ها مسئول ارسال و دریافت پیام‌های بین دستگاه و ابر
- شناسایی هندلرهای درخواست
- شناسایی هندلرهای ناهمگام



Identifying Message Fields

- شناسایی فیلدهای پیام
- Taint source: اطلاعات اولیه پیام
- Taint sink: ذخیره و پردازش اطلاعات پیام

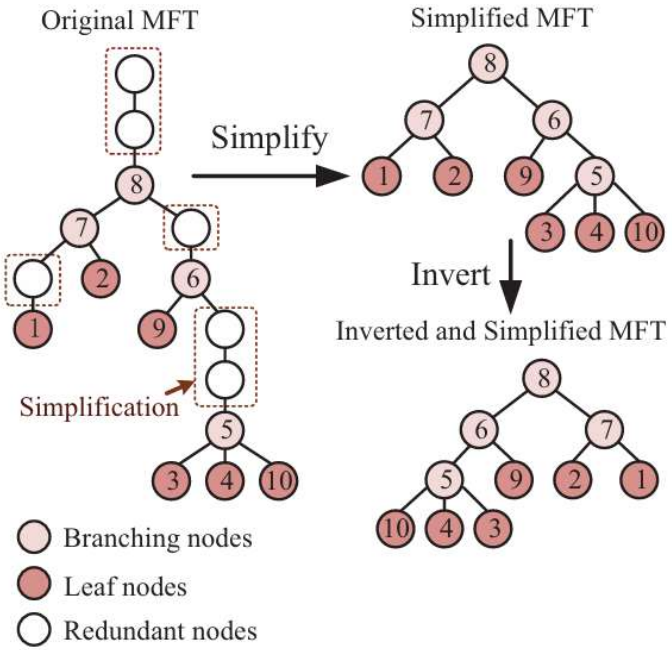
Identifying Message Fields

- تحلیل جریان داده (Data flow analysis)
- تحلیل به صورت عقب گرد
- استفاده از ابزار Ghidra، یک ابزار متن‌باز برای تحلیل مهندسی معکوس نرم‌افزار
- قانون انتشار (propagation rule)

Recovering Field Semantics

- ترمیم معنای فیلدها
- استفاده از مدل یادگیری عمیق
- ایجاد درخت (Message field tree)
- ایجاد code slice برای هر مسیر

Concatenating Message Fields



- بازسازی پیام‌ها از فیلدهای شناسایی شده
- گروه بندی کدها
- ساده سازی و معکوس کردن درخت

Assessing Access Control Implementations

- ارزیابی کنترل دسترسی
- تحلیل خودکار
- تایید دستی

نتایج

- بازسازی پیام‌های دستگاه-ابری را از فریمور دستگاه‌های اینترنت اشیا به صورت خودکار
- مقایسه با دو ابزار LEAKSCOPE و IOT-APISCANNER
- تفاوت در ورودی‌ها، سرویس های ابری هدف و روش تحلیل
- پایین بودن دقت در بازسازی پیام ها به دلیل تحلیل ایستا

مراجع

- [1] WANG, X., SUN,Y.,NANDA, S., AND WANG, X. Looking from the mirror: Evaluating {IoT} device security through mobile companion apps. In 28th USENIX security symposium (USENIX security 19), pp. 1151–1167, 2019.
- [2] WRIGHT, C., MOEGLEIN, W. A., BAGCHI, S., KULKARNI, M., AND CLEMENTS, A. A. Challenges in firmware re-hosting, emulation, and analysis. ACM Computing Surveys (CSUR) 54, 1 (2021), 1–36.
- [3] YAHYAZADEH, M., PODDER,P.,HOQUE, E., AND CHOWDHURY,O. Expat: Expectation-based policy analysis and enforcement for appified smart-home platforms. In Proceedings of the 24th ACM symposium on access control models and technologies (2019), pp. 61–72.
- [4] YUAN, B., JIA,Y.,XING, L., ZHAO, D., WANG, X., AND ZHANG, Y. Shattered chain of trust: Understanding security risks in {Cross Cloud}{IoT} access delegation. In 29th USENIX security symposium (USENIX security 20) (2020), pp. 1183–1200.
- [5] YUAN, B., WU,Y.,YANG, M., XING, L., WANG, X., ZOU, D., AND JIN, H. Smartpatch: Verifying the authenticity of the trigger-event in the iot platform. IEEE Transactions on Dependable and Secure Computing 20, 2 (2022), 1656–1674.
- [6] ZHANG,Y.,MA,S.,LI, J., GU, D., AND BERTINO, E. Kingfisher: Un veiling insecurely used credentials in iot-to-mobile communications. In 2022 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) (2022), IEEE, pp. 488–500.
- [7] ZHOU,W., JIA,Y.,YAO,Y.,ZHU, L., GUAN, L., MAO,Y.,LIU,P., AND ZHANG, Y. Discovering and understanding the security hazards in the interactions between {IoT} devices, mobile apps, and clouds on smart home platforms. In 28th USENIX security symposium (USENIX security 19) (2019), pp. 1133–1150.
- [8] ZHOU,X.,GUAN,J.,XING,L.,ANDQIAN, Z. Perils and mitigation of security risks of cooperation in mobile-as-a-gateway iot. In Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communica tions Security (2022), pp. 3285–3299.

2.Towards Shielding 5G Control Plane Functions

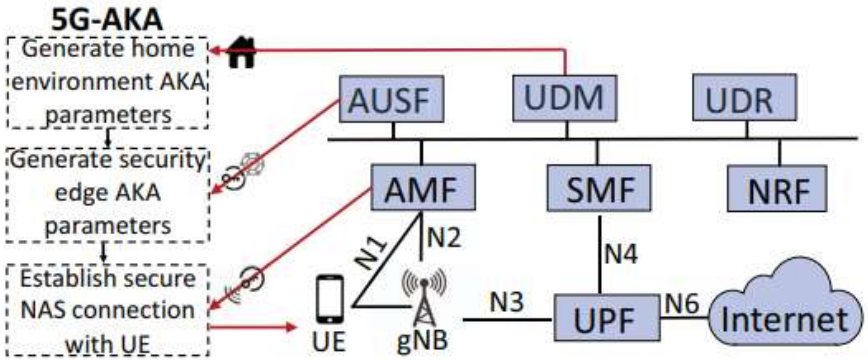
فهرست

مقدمه

- مزیت و چالش استفاده از فناوری مجازی سازی
- چالش‌های امنیتی
- استفاده از محفظه‌های اجرا سخت افزاری (HMEE)
- SGX یک فناوری سخت افزاری
- ایجاد یک محیط اجرایی ایمن و محافظت‌شده درون حافظه به اسم Enclave

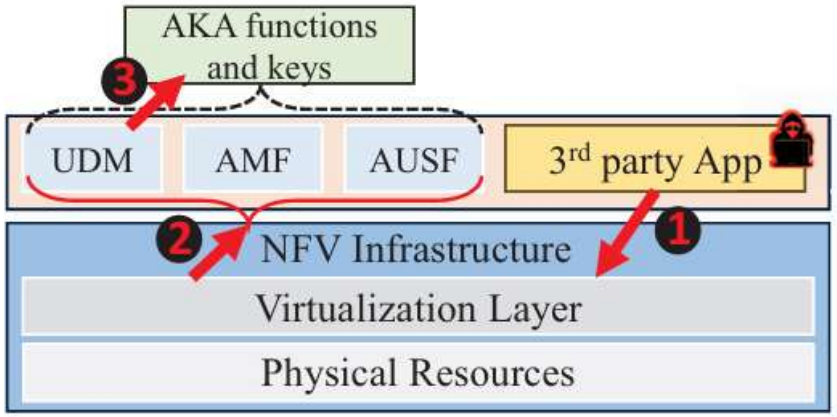
پیشینه تحقیق

- طراحی توابع مختلف شبکه به صورت ماژولار
- UDR: واحد ذخیره سازی اطلاعات
- UDM: واحد مدیریت داده
- AUFS: سرور احراز هویت



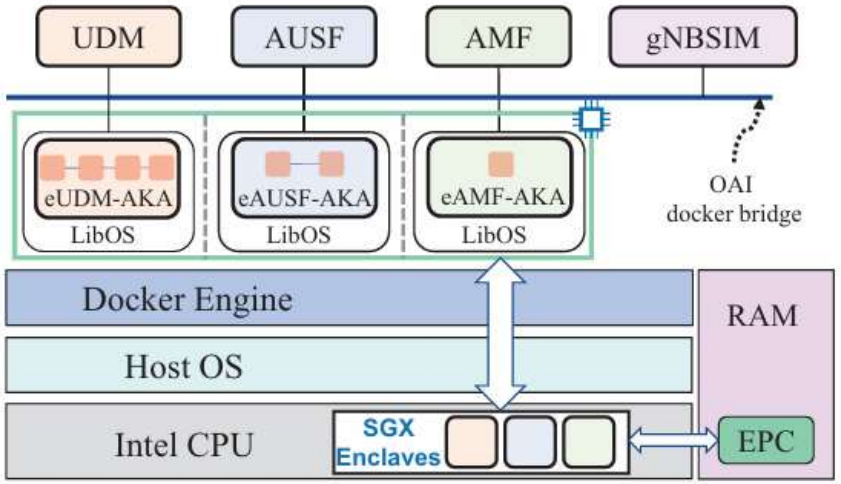
بیشینه تحقیق

- تعریف یک مدل تهدید
- استفاده از یک زیر ساخت شامل سخت افزار COTS (Commercial off-the-shelf)
- دسترسی به کل سیستم
- نفوذ به بقیه ماشین‌های مجازی



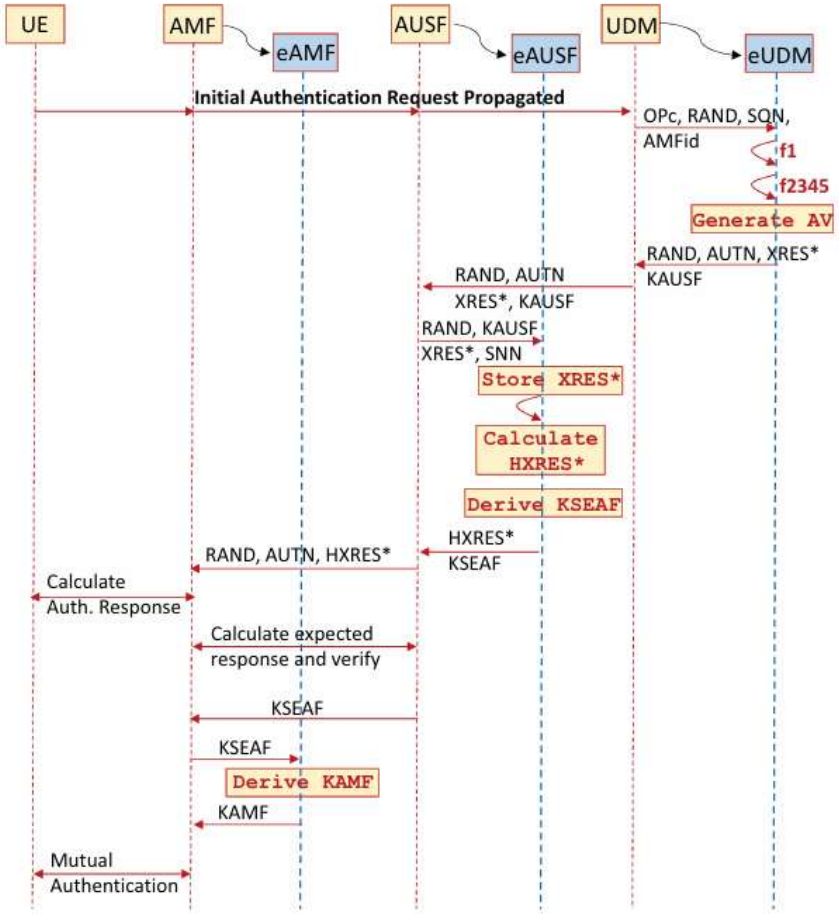
طراحی بستر آزمایش

- هدف: افزایش امنیت عملکردهای حیاتی در صفحه کنترل
- قرار گرفتن عملکردهای مختلف احراز هویت در کانتینرهای داکر
- استفاده از API برای ارتباط با هم
- LibOS: کتابخانه سیستم عامل
- EPC: بخشی از حافظه سیستم



طراحی بستر آزمایش

- احراز هویت دستگاه
- ذخیره اطلاعات در یک محیط امن
- استفاده از TLS: یک پروتکل امنیت برای ایجاد ارتباطات ایمن در شبکه

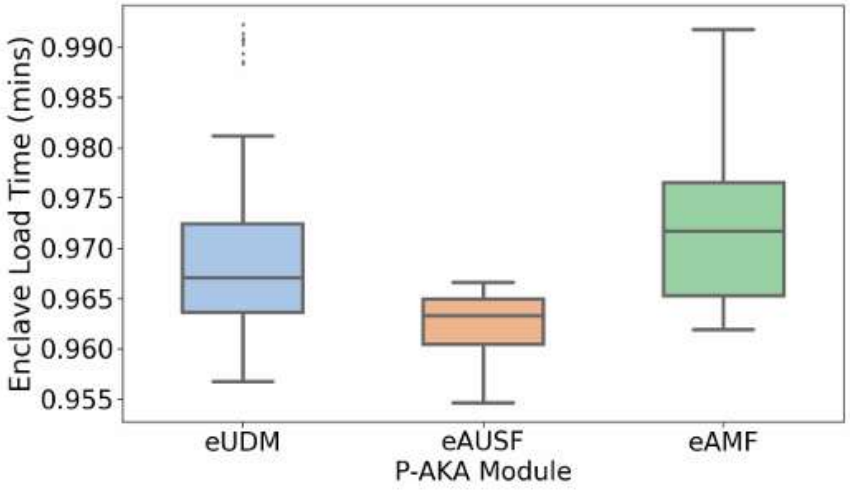


طراحی بستر آزمایش

- SGX یک تکنولوژی برای اجرا امن برنامه‌ها
- ایجاد تغییرات با استفاده از AMD-SEV و Intel-TDX:
  - فناوری امن برای ایجاد محیط‌های ایمن در سرورها
- استفاده از Gramine برای اجرا برنامه‌ها داخل SGX
- Gramine: یک لایه نرم افزاری

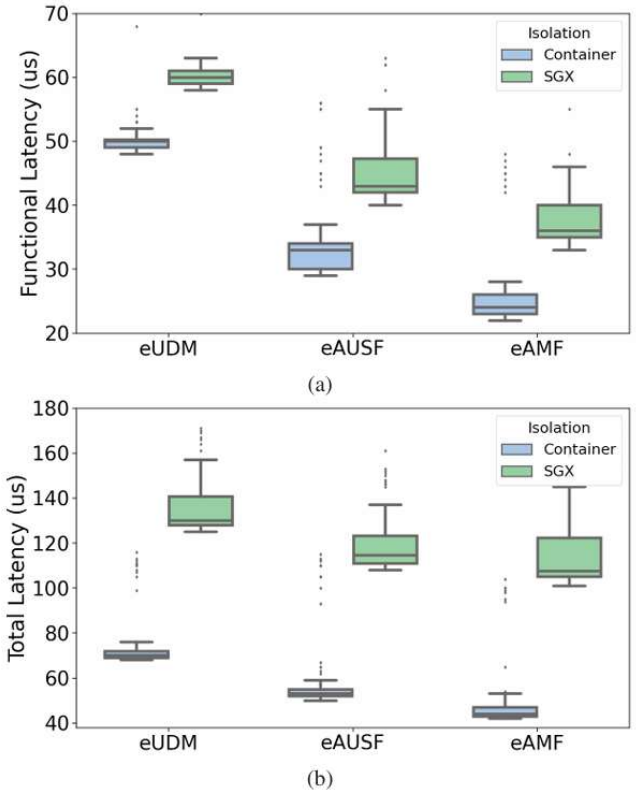
نتایج و آزمایش

- زمان بارگذاری Enclave برای ماژول‌های مختلف AKA
- افزایش زمان بارگذاری به دلیل Ocall
- Ocall: فراخوانی توابع از محیط Enclave به محیط غیر ایمن



نتایج و آزمایش

- بررسی تاخیر با استفاده از فناوری SGX
- افزایش تاخیر اتصال کاربر به شبکه (UE REgistration)
- افزایش تاخیر به دلیل فرایندهای امنیتی SGX



مراجع

- [1] M. Sabt, M. Achemlal, and A. Bouabdallah, “Trusted Execution Environment: What it is, and what it is not,” in 2015 IEEE Trustcom/BigDataSE/Ispa, vol. 1. IEEE, pp. 57–64, 2015.
- [2] N. C. Will and C. A. Maziero, “Intel software guard extensions applications: A survey,” ACM Computing Surveys, 2023.
- [3] M. Russinovich, “Azure Confidential Computing,” https://azure.micros oft.com/en-us/blog/azure-confidential-computing/, May 2018, (accessed November 30, 2023).
- [4] J. Han, S. Kim, J. Ha, and D. Han, “SGX-Box: Enabling Visibility on Encrypted Traffic using a Secure Middlebox Module,” in Proceedings of the First Asia-Pacific Workshop on Networking, pp. 99–105, 2017.
- [5] O. Weisse, V. Bertacco, and T. Austin, “Regaining lost cycles with HotCalls: A fast interface for SGX secure enclaves,” ACM SIGARCH Computer Architecture News, vol. 45, no. 2, pp. 81–93, 2017.
- [6] T. Dinh Ngoc, B. Bui, S. Bitchebe, A. Tchana, V. Schiavoni, P. Felber, and D. Hagimont, “Everything You Should Know about Intel SGX Performance on Virtualized Systems,” Proceedings of the ACM on Measurement and Analysis of Computing Systems, vol. 3, no. 1, pp. 1–21, 2019.
- [7] 3GPP, “Security Architecture and Procedures for 5G System,” 3rd Generation Partnership Project (3GPP), TS 33.501 V18.1.0 , Mar. 2023.
- [8] C.-C. Tsai, D. E. Porter, and M. Vij, “Graphene-sgx: A Practical Library OS for Unmodified Applications on SGX.” in USENIX Annual Technical Conference, pp. 645–658, 2017.
- [9] X. Gao, B. Steenkamer, Z. Gu, M. Kayaalp, D. Pendarakis, and H. Wang, “A Study on the Security Implications of Information Leakages in Container Clouds,” IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 1, pp. 174–191, 2021.

با تشکر از توجه شما!