DSbD Programme – Digital Catapult Cohort 2 Tier 1



KATLAS TechnologyWEB3 - Privacy wallets

Marcos Mayorga CTO at KATLAS Technology



KATLAS network

- Cryptocurrency protocol. Settlement.
- Smart wallets with trading role-2-role trading protocols.

Source Code



https://github.com/root1m3/plebble

Android App



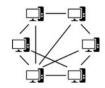
KATLASNET

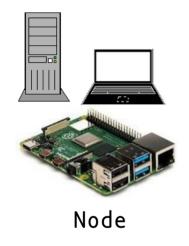


21:20 ₺ 1 ▲ 日 Document date: ~Wed Jun 29 2022 21:18:35 UTC basket_hash: 3Cbcbr1ewczXZrKoB1YRPpdKino7 fields: product units price/unit reward/unit info: Transaction successfully relayed. message: trade_THFU7UJ8UKfGApJWgKjYxx1YHYD pay_amount: 7510 pay_coin: 9PPteEVCPt25Ognnn3pfJsS2YNO reward_amount: 230 reward_coin: 4ZF1BsR2QDpxE9fDSBmQYFRC71WM trade id: THELIZITISHIK/GAn IWaKIYyy1VHVD tv: 8a74cuvDw2N58au5k7D8dU5K2AUVVOEvoKud97D7DA7iHGBc WOLINSWITNI JUSER 7005 Odd N10 Dul cu 2 v 7 T Hogo I GTdmodd 2 gu 3 K B wu9cVV14r1aaVTmbNYTfAvaKk2X1RVdOOA6YvTi1on6B73TiAxx5l kzFEDpriR6n9mJDxSXsj9pjqbSLxnaTTdLhGpqHBBC26trv3pFxLzo3 QmVrcHddJtM5HQ6vqvqc6q8PNdAvGDaxV3sFnMeVPi4RoqdqCwC MEBeC3TQu9GD1QNtkNarFXYVkRFhZuxu9xVfqs7kotQ8qZttkEcPQ zmPgx2Cupg7aCw3FweuDy4KUkQQTtNo3FtyV6nQfjcX9GbQXRC3 basket serial 1, 1 items * 3qRd49QNBqpH6XzPyug67fQBuufe 1 7510 230 exec time: 1656533915477118241 ~Wed Jun 29 2022 20:18:35 section #0. coin 9PPteEVCPt25Qgnnn3pfJsS2YNQ address: 2MSaYUAqWawK8XKgFhUrDwpqHda aCkCHFk4oZT8gVCcyUDx5TNGNU9jxBw79ArPJmjP2Uw sig 3rbW9vn8ikuiZFitgWiAn9rZVw9zLa7SiBJDziNV5eAG3ZDwhc3Zahf UuqSKyDiJmb8cnXZhdtfLSbRK4R6cKNtz address: 4ZF1BsR2QDpxE9fDSBmQYFRC71WM amount: 7510 section #1, coin 4ZF1BsR2QDpxE9fDSBmQYFRC71WM address: 4ZF1BsR2QDpxE9fDSBmQYFRC71WM unlock with: [!ts] s0{i o 0 } s1{i 0 o } pub 26iX4STsARGvD22CM5SqqFhDvG7cvfJ8urBurfsntBrra sig 2aZwe12cLHENeH6bZY3k2vgweUNbRmvwLjXiUP91EGWTXGfhHRt s8Gv8irWmr9rHVUG66BXn1.JdWEDMBrr36Dnis address: 2MSaYUAqWawK8XKqFhUrDwpqHdah amount: 230 /-transaction-Transaction is complete Signed by: 3V5q5zKFVqCKt2ELQPvsfXQKNMCF 2AUzenb2ZoewBER13eFHtMmVuuGZmRYfNs5TDveG3BUzq Signature: 3AgkWcYHiQSDYxRu2fDSE6RsuvmApdr2LZ2cu96u4Hk4 RG2AUgBU4TNc3zL67u3wSkekfXv5kogsXR9m9y7yJR1K Cryptographic verification SUCCEED. Data is legitimate. - END OF DOCUMENT

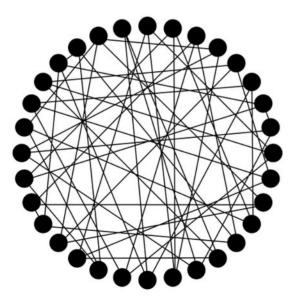


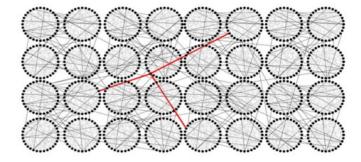
KATLAS network





P2P Network

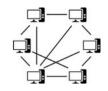


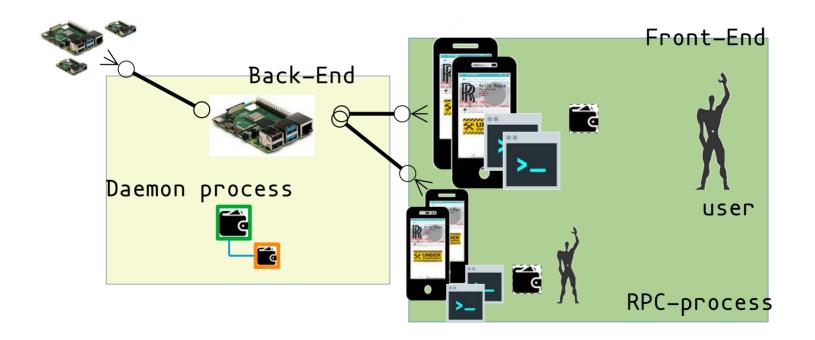






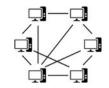


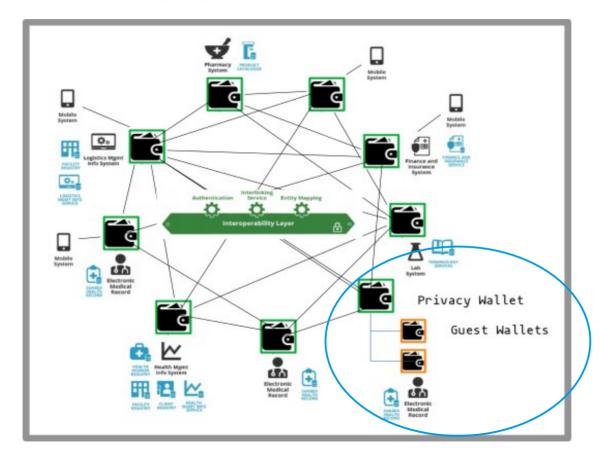






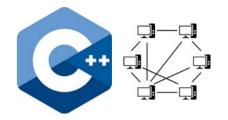
Ewallet











Daemon - user private data

- 1- User authentication → 64 bit id → Worker thread.
- 2- API request → Access to user wallet → Response

Risks:

- Code flaw could leak data from other user's wallet.
- Today's flawless code could contain a flaw tomorrow.



System tests – purecap ~50K LoC



- RPC API calls
- Threads
- TCP/IP sockets
- Cryptography (ECC, DSA, AES, HASH)
- B58 Encoder/decoder. Binary serialization.
- String manipulation (trim, split, replace, ...)



Detected transmission of pointers via IPC. Got provenance failure exception.

Once fixed...







package zstd

Morello

- root@cheripleb:~ # zstd /etc/motd.template
- zstd: error 11 : Allocation error : not enough memory
- morello/cheribsd
- qemu-riskv64-purecap/cheribsd



cheribuild.py - riscv



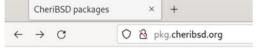
git clone https://github.com/CTSRD-CHERI/cheribuild

./cheribuild.py run-riscv64-purecap -d

root@cheribsd-riscv64-purecap:~# **pkg64c install** git

Error fetching

http://pkg.CheriBSD.org/CheriBSD:20220828:riscv64c/Latest/pkg.txz



CheriBSD packages

Morello CheriABI packages:

- · CheriBSD:20220314:aarch64c
- CheriBSD:20220511:aarch64c
- CheriBSD:20220828:aarch64c

Morello hybrid ABI packages:

- CheriBSD:20220314:aarch64
- CheriBSD:20220511:aarch64
- CheriBSD:20220828:aarch64

Only aarch64/aarch64c ports are available









Risks we'd like to reduce using compartmentalization:

- Code flaw could leak data from other user's wallet.
- Today's flawless code could contain a flaw tomorrow.

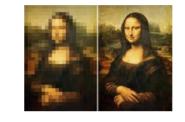
- How to guarantee that users can only access the right wallet...
- Even when evil users take advantage of current (or future) flaws in the code, gaining -anyhow- access to other's wallet.



Compartmentalization models



Shared library compartments.
 We need more granularity → C++ Objects.



- Enclaves, Protection domains, trampolines
 Requires a significant software refactoring effort.
 - → allocators, sealed capabilities



 We are figuring out how to achieve a model that: mitigates aforementioned risks minimizes development effort, easiest change

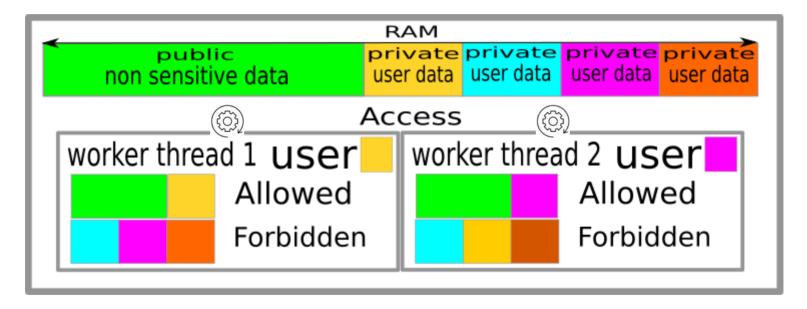












Coloured compartments

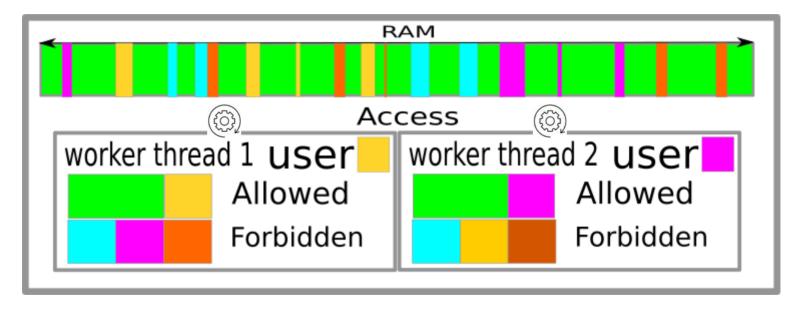








Ewallet



Coloured fragmented compartments

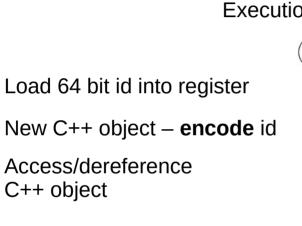


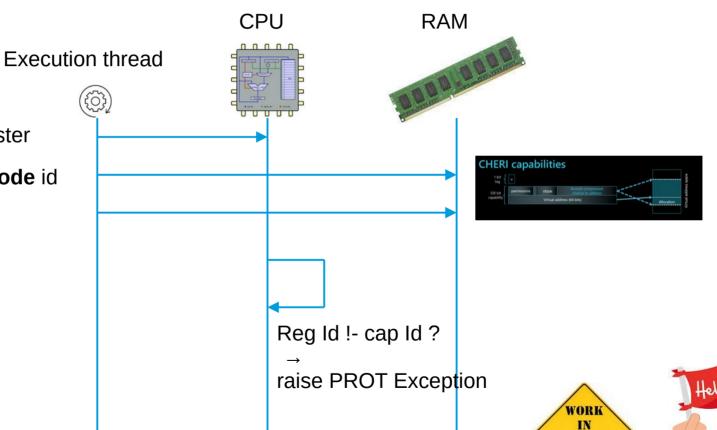












PROGRESS



Continuity

Privacy++ wallets
 featuring compartmentalized wallets with CHERI



KATLAS W3 Privacy router.

Internet router + P2P Node + family/business wallets in one computer.



