CRYPTOSAT
YAN MICHAELVSKY, CO-FOUNDER

CRYPTO-SATELLITES
- A CRYPTOGRAPHIC TRUSTED PARTY IN SPACE AND ITS APPLICATIONS
Yonatan Winetraub
Aerospace

2nd time founder. Founded SpaceIL - the first private moon-mission.

Yan Michalevsky
Crypto and Security

2nd time founder. Founded Anjuna - an enterprise security company in Confidential Computing.
Advisors

Prof. Dan Boneh
Ben Fisch
Juan Benet
Omer Shlomovits
We build satellites that power cryptographic and blockchain applications. Our goal is to create the most secure cryptographic root-of-trust in space to protect protocols.
SpaceTEE: Secure and Tamper-Proof Computing in Space using CubeSats

Yan Michalevsky
Stanford University
yanm2@cs.stanford.edu

Yonatan Winetraub
Stanford University, SpaceCell
yonatanw@stanford.edu

ABSTRACT
Sensitive computation often has to be performed in a trusted execution environment (TEE), which, in turn, requires tamper-proof hardware. If the computational fabric can be tampered with, we may no longer be able to trust the correctness of the computation. We study the wild and crazy idea of using computational platforms in space as a means to protect data from adversarial physical access. In this paper, we propose SpaceTEE – a practical implementation of this approach using low-cost nano-satellites called CubeSats. We study the constraints of such a platform, the cost of deployment, and discuss possible applications under those constraints. As a case study, we design a hardware security module solution (called SpaceHSM) and describe how it can be used to implement a root-of-trust for a certificate authority (CA).

KEYWORDS
SpaceTEE, TEE, CubeSats, SpaceHSM, Physical Security

1. SpaceHSM: Root-of-Trust (R) and crypto-accumulator

2. Ground-station (GS): delegates cert. sign. requests

3. Public, append-only certificate log (L)

4. Verifier (V): checks certificate validity
Use-cases

**HARDWARE SECURITY MODULE (HSM)**
Can we provide a better alternative to expensive and hard-to-operate HSMs that can still potentially be physically accessed and might be susceptible to side-channel attacks?

**TRUSTED SETUPS**
How to generate public parameters for cryptographic schemes securely? zkSNARKs, Threshold Signature schemes, etc.

**TRUSTED SOURCE OF ENTROPY**
How to obtain random bits we can trust to be random?

**TRUSTED PARTY FOR CRYPTOGRAPHIC PROTOCOLS**
Privacy-preserving aggregation, private voting, sealed-bid auctions
PHYSICALLY INACCESSIBLE & TAMPER EVIDENT
No side-channel attacks, a satellite can be destroyed but not captured. Any physical attack will be easily noticeable by national monitoring (e.g. NORAD)

ZERO INFRASTRUCTURE
Self-sufficient, no internet cables, no power source, anybody can set a personal ground station

TRANSPARENT
Satellites can guarantee that multiple parties see the same transmission. No split-world attacks.

PRACTICAL
<$100k to build, launch and maintain a satellite
Cube satellites are miniature satellites made from off the shelf components. The costs of building cube satellites and launching them into space has dramatically declined in the past decades and will continue to do so as the technology gains more widespread adoption. We believe they are ideally suited for applications requiring trust.
Architecture
(in a nutshell)

Our Ground Station Network
Trust model

Minimize trust

- **Assembly & Testing**
  Supply Chain Security
- **Security Checkpoint**
  Pick 1 of N Components to be Launched
- **Launch Pad & Launch**
  Moment of Inertia Measurement

Zero-trust

- **In Orbit**
  Hard to Reach Monitoring by NORAD
Milestones

- **ISS Experiment** (March 2022)
- **Crypto1 Launch** (May 2022)
- **2nd ISS Experiment** (December 2022)
- **Crypto2 Launch** (Jan 2023)
  - 30x compute power
- **Crypto3 In Design**
Cryptosat experiment aboard the International Space Station (ISS).

- DRAND (Distributed Random Beacon)
- Bitcoin transaction co-signing from space
- Tweets From Space
- and more...
Tweets From Space

GET YOU TWEET SIGNED ABOARD THE INTERNATIONAL SPACE STATION (ISS)

Tweet at @cryptosatbot, and we send back a certificate digitally signed in space.
Crypto1 and Crypto2
Crypto1 launch, May 25th 2022
Trusted Setup

TRUSTED SETUP IN SPACE FOR GROTH16 ZK-SNARKS

The proof system is used for collusion resistant voting in a DAO.
Crypto2 launch
Cape Canaveral, Florida
Jan 3rd 2023
Some of our partners
CRYPTOSAT VRF ORACLE

https://docs.cryptosat.io/cryptosat/random-beacon/verifiable-random-beacon
https://docs.cryptosat.io/cryptosat/random-beacon/verifiable-random-beacon
Trusted Setups for zkSNARKs
How Developers Interact with Cryptosat

https://simulator.cryptosat.io
Thank you

IN THE NEWS

Space Invaders
Crypto1 launch

TheBlock
Yahoo finance

PL + CRYPTOSAT

VDF announcement

VELAS + CRYPTOSAT

Random Beacon announcement

WHITEPAPER

SpaceTEE: Secure and Tamper-proof Computing in Space using Cubesats