securosys

“Why Switzerland?”

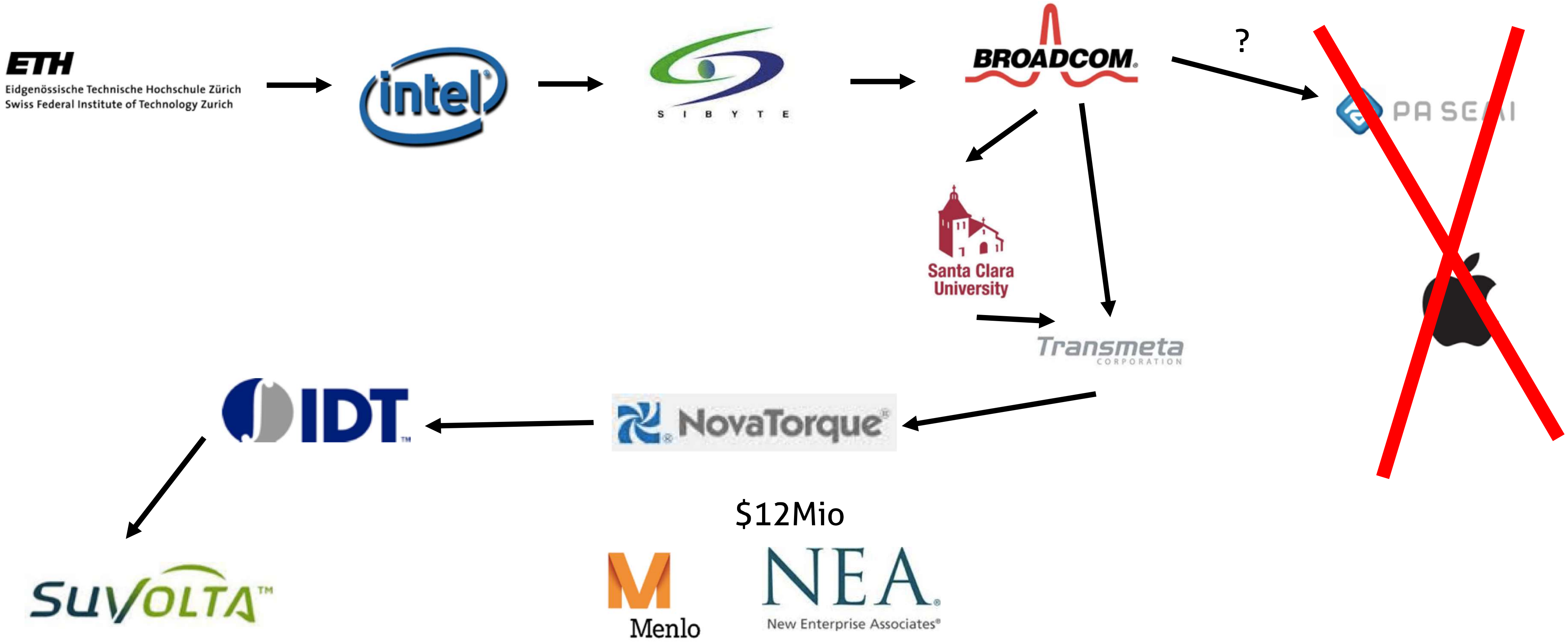
How to build secure systems in Switzerland

Robert Rogenmoser

Swiss Cyber Storm Conference

Bern, October 30, 2018

From Switzerland to Silicon Valley ..


ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich
intel
SIBYTE
BROADCOM
?
PA SEMI
Santa Clara University
Transmeta
CORPORATION
NovaTorque
IDT
SUVOLTA
Menlo
NEA
New Enterprise Associates

$12Mio

.. and after 17 years back to Switzerland

Where is a need? Securing Industrial Communications

Source: 3mschweiz

Lesson 1 for Startups: When opportunity knocks, pivot!

Securosys was founded in April 2014

- Founders Andreas Curiger and Robert Rogenmoser
- Let’s protect all power generation, distribution, and consumption

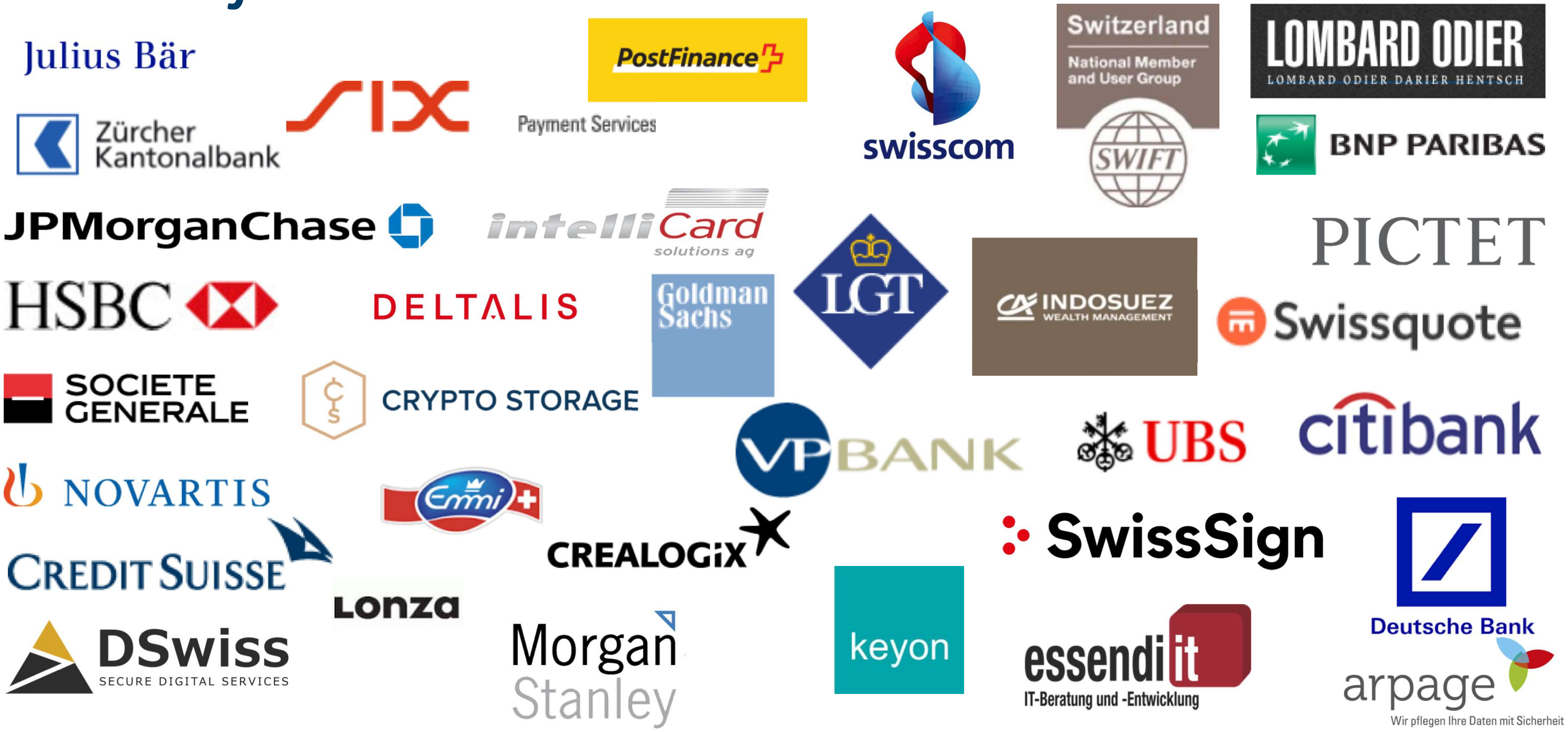
June 2014: Opportunity knocks

- We get a call: Can you build a HSM – a Hardware Security Module
- Who is asking: SIX and the SNB
- After reflecting for 2ns: YES

Execution!

- Delivery of prototypes in April 2015
- First shipment of production version December 2015
- Everybody switched over: June 2017

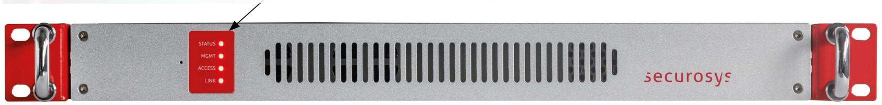
Securosys Customers



Why did the SNB and SIX choose Securosys?

What’s in the box?

- This is a critical infrastructure of Switzerland
  - Transactions of over CHF/$/€ 100 Billion every day
- We want to review all blueprints
- We want to review all the source code
  => The crypto group of the Swiss DoD reviewed everything

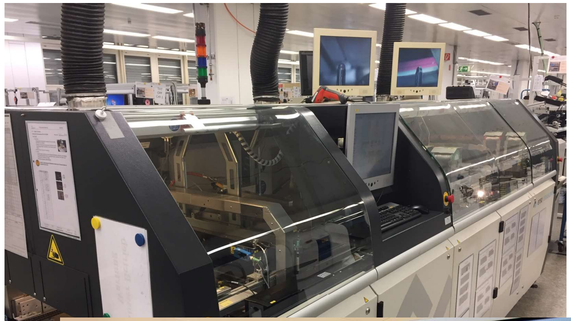


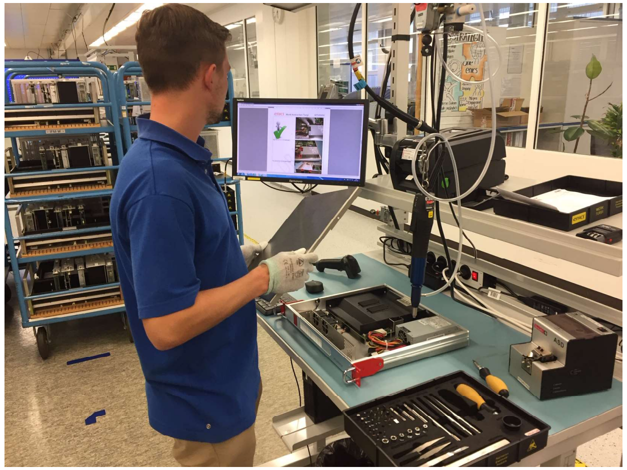
Design and manufacture in Switzerland

- Swissness is the USP
- Control of the supply chain from design to factory to customer

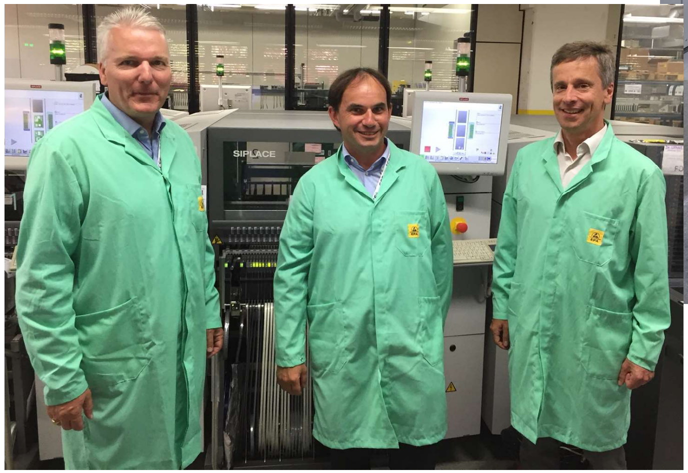
Manufacturing in Switzerland: Our Partners

enics





CCS Group



Importance of Good Encryption Keys

Encryption keys are an easy way for backdoors

- User cannot verify that a 256 bit key has only 40 bits of randomness

Backdoor examples:

- RSA Security random number generator Dual_EC_DRBG
- Random number generators inside Intel CPUs
- Fast Prime in Infineon Smart Cards

Generation of encryption keys is of utmost importance

- Software is deterministic and cannot generate good encryption keys
- True random number generators are required
  - Physical noise sources like thermal noise or diode noise
  - Quantum noise sources (superset of above)
- Guardrails to ensure proper random bit generation
  - A very cold thermal noise source is not that random anymore

Securosys Primus HSM have two TRNG based on physical noises sources

Trusted Supply Chain

How to keep the supply chain secure to the customer?

- Edward Snowden:
  - NSA intercepts shipment to end customer
- How can we protect our customers?
  - Tamper protection
- Think further: Digital Seal
  - Our equipment is active even without power!

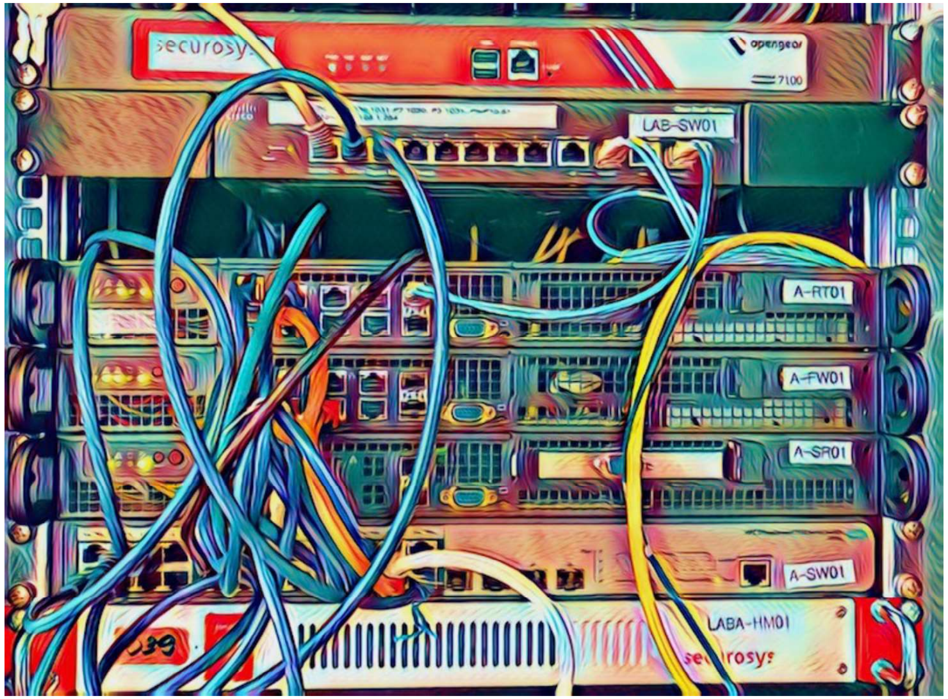
New Threats: Spectre and Meltdown

Spectre and Meltdown make servers unsafe – for years to come

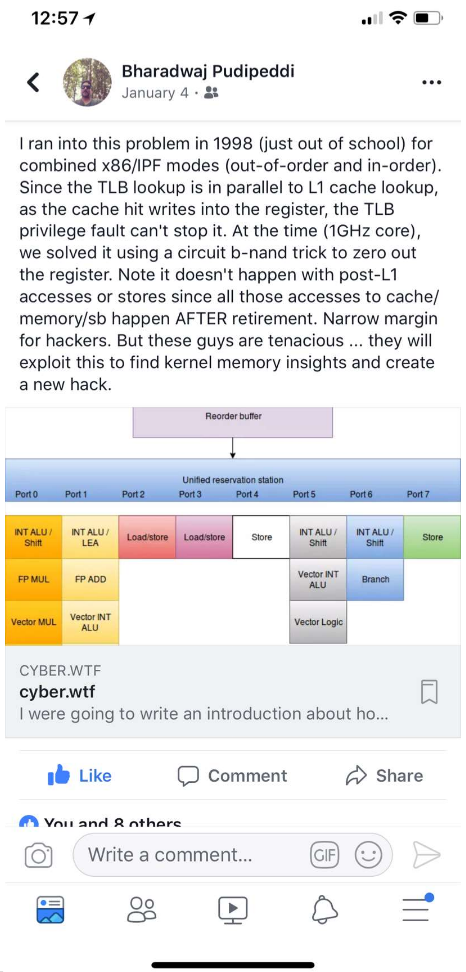
- Servers cannot keep critical data secure – other programs can access critical information
- Needs to be fixed at the chip level
  This will take years!
- Other hidden vulnerabilities

Passwords and encryption keys must be stored in a HSM

- Securosys HSM do not allow external code to be executed



Insider: I worked at Intel designing microprocessors

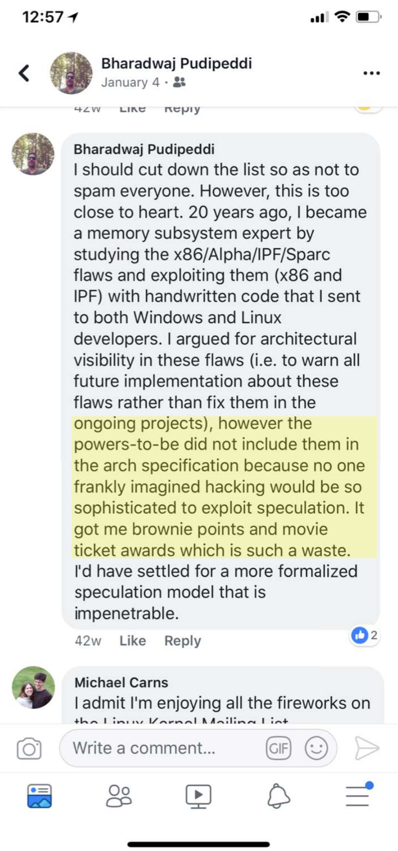


12:57

Bharadwaj Pudipeddi
January 4 ·

I ran into this problem in 1998 (just out of school) for combined x86/IPF modes (out-of-order and in-order). Since the TLB lookup is in parallel to L1 cache lookup, as the cache hit writes into the register, the TLB privilege fault can't stop it. At the time (1GHz core), we solved it using a circuit b-nand trick to zero out the register. Note it doesn't happen with post-L1 accesses or stores since all those accesses to cache/memory/sb happen AFTER retirement. Narrow margin for hackers. But these guys are tenacious ... they will exploit this to find kernel memory insights and create a new hack.

CYBER.WTF
cyber.wtf
I were going to write an introduction about ho...



12:57

Bharadwaj Pudipeddi
January 4 ·

42w Like Reply

Bharadwaj Pudipeddi
I should cut down the list so as not to spam everyone. However, this is too close to heart. 20 years ago, I became a memory subsystem expert by studying the x86/Alpha/IPF/Sparc flaws and exploiting them (x86 and IPF) with handwritten code that I sent to both Windows and Linux developers. I argued for architectural visibility in these flaws (i.e. to warn all future implementation about these flaws rather than fix them in the ongoing projects), however the powers-to-be did not include them in the arch specification because no one frankly imagined hacking would be so sophisticated to exploit speculation. It got me brownie points and movie ticket awards which is such a waste. I'd have settled for a more formalized speculation model that is impenetrable.

42w Like Reply 2

Michael Carns
I admit I'm enjoying all the fireworks on the Linux Kernel Mailing List

https://www.securosys.ch/blog/spectre-and-meltdown-make-servers-unsafe-years-come

Why Switzerland?

Switzerland is not the best place for a startup

- Lots of money, but not enough venture funding
- Very good engineers, but not enough hungry engineers
- Lucrative market, but simply too small

Switzerland is the best place to start a cyber security company

- Clear regulation and jurisdiction
- Not 3-letter agency forcing you to include backdoors for them

Where are we going?

Crypto Currencies and Blockchain Systems

- Securosys has the best solution to generate, manage, and control access to keys
- Multi-signature solution to provide enterprise grade solutions

Trusted Execution Platform / Trusted Execution Environment

- Control where you run your code
- Virtualization, while practical, has many dangers

IoT Key Management

- Securosys Primus HSM can already handle millions of keys
- For IoT, we need more, much more

Make Securosys an Internationally Recognized Brand

- Subsidiaries in key markets
- Worldwide marketing

How can we finance this?

Fundraising the Modern Way: ICO

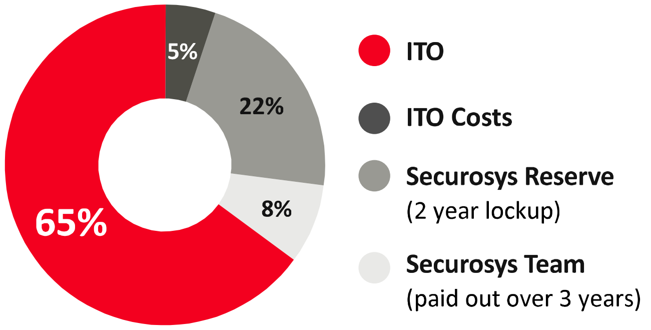
Initial Coin Offering instead of Venture Capital round

- Securosys is targeting this market with its products – compound effect!
- Actually, we are doing an STO, a Security Token Offering:
  - Token have dividend rights
  - Token can be exchanged in company shares
  - Company shares already reserved for tokens

TOKEN ECONOMICS

Ticker	SET
Token type	ERC20
Hard Cap	3,049,045 SET
PPT (Price per token)	CHF 5.00
Minimum investment	CHF 5k / 50k / 0.5M / 1M+
Discounts	0-15 / 10-20 / 25 / 30%
Lockup periods	0 / 3 / 6 / 6 months

TOKEN DISTRIBUTION



Take aways

Networking!

- Work on your connections and relationships
- Even more when you leave or go abroad!

Stay hungry – be nimble

- Challenge: To be ready at the right place and the right time

Better make sure where your secrets are

- Use CPU Power wherever
- Control your digital keys and identities

Why not Switzerland?

Thank You!

To participate in the Securosys Token Offering please visit:

https://ico.securosys.ch

Förrlibuckstrasse 70
8005 Zürich
Switzerland

info@securosys.ch

www.securosys.ch
+41 44 552 31 00