Thierry Laurion

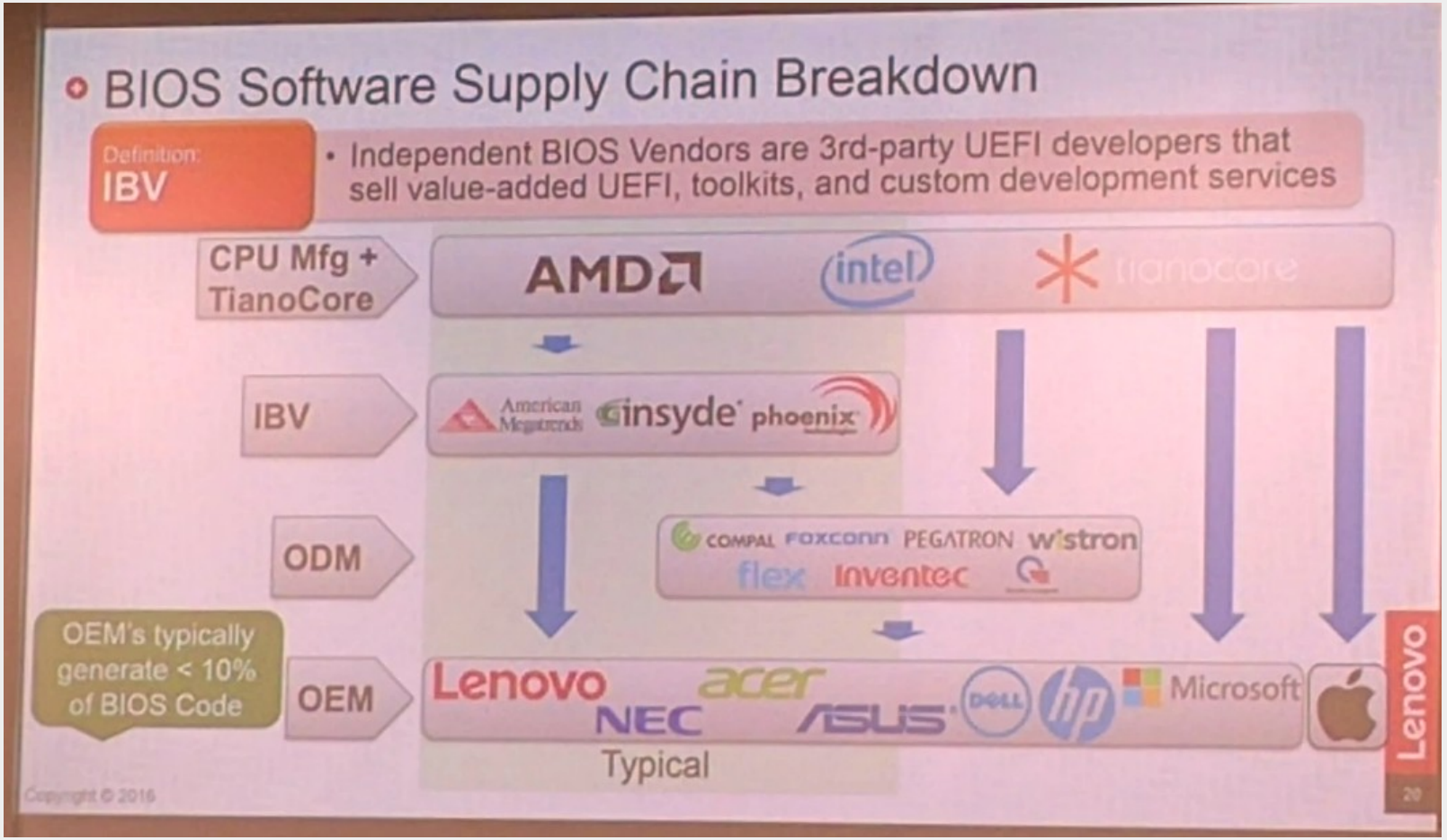
- **Insurgo Open Technology founder and CEO.**
- Former Security Analyst/Psychology Bachelor/Security Researcher and Developer.
- Now freedom defender as a open source firmware researcher/developer/integrator.

- Past collaborator to Libreboot, QubesOS contributor and Heads collaborator/reviewer.
- **Currently main Heads maintainer.**

- Started Insurgo Open Technologies in 2017.
- Made the PrivacyBeast X230 certified by QubesOS in July 2019.
- Nlnet grantee for the Accessible Security project in April 2019.
- *Nlnet grantee once again for Authenticated Heads (Heads-OpenPGP) project.*

Insurgo's mission is to **facilitate accessibility to security and confidentiality** to the masses.

Closed source firmware / BIOS Supply chain



Heads today


[heads-tests] QEMU
qemu-coreboot-fbwhiptail-tpm1-hotp | Heads Boot Menu
2023-02-01 16:39:28 UTC
TOTP: 593928 | HOTP: Success
Default boot
Refresh TOTP/HOTP
Options -->
System Info
Power Off

What is Heads?

- Heads as a **payload:**
    - **runtime environment**
        - **bootloader (kexec)**
        - **Recovery environment (Linux shell and tools)**
- Heads as a **build system**

Heads as runtime environment

Heads is:

coreboot + Linux Kernel in ROM

(plus Security research and tools)

Heads as a build system

- Heads is basically a ‘Make’ project
  - Global Makefile https://github.com/osresearch/heads/blob/master/Makefile
    - ‘make BOARD=board_name [module_name.statement options]’
      - **board** https://github.com/osresearch/heads/tree/master/boards
        - Relies on linux/coreboot/modules **configuration** files https://github.com/osresearch/heads/blob/master/config
      - **modules** (OSS): https://github.com/osresearch/heads/tree/master/modules
      - **patches** to be applied after module verification + extraction: https://github.com/osresearch/heads/tree/master/patches
  - Produces
    - Artifacts :
      - **coreboot rom(s) images** stitching the following (but produced independently):
        - **BzImage** (compiled kernel + in-kernel modules)
        - **initrd.cpio.xz**
          - **tools.cpio** (compiled modules stripped binaries)
          - **modules.cpio** (compiled as modules kernel drivers to be loaded on demand)
          - **heads.cpio** (scripts and config files generated at build time linked to board config and https://github.com/osresearch/heads/tree/master/initrd content)
      - **hashes.txt** file containing individual packed files, cpios, initrd.cpio.xz and coreboot roms

Insurgo Benefits as Partner

- Heads as a *coreboot payload* = “linuxboot”, aka linux as bootloader
  - More eyes on the code (linux kernel, std libraries, libraries and tools)
  - More eyes on applied security policies
- Heads as a *build system*
  - More eyes on the build system, more efficiency
  - More awareness on reproducible builds
- Better sustainability of the project (sustainable *money* stream from subscriptions)

- Get home message:
  - ***Better collaboration into Heads, knowledge sharing***
  - ***Expend the OSFW ecosystem: its features, its reach and its support***