# Building Hardware We Are Proud Of

Jon Callas
CTO and co-founder
Silent Circle / Blackphone

# Welcome!

- We are here because of new beginnings on hardware

# The Future is Bright

- We are all here to build hardware we're proud of

- Our devices will be connected everywhere

- We have to do security right

# I want to share

- How we have been successful with Blackphone

- Privacy-friendly, security-friendly Android phone

- How this adapts to what you're doing

# Hardware is Hard

- Compared to software

  - Long lead times

  - Capital investment
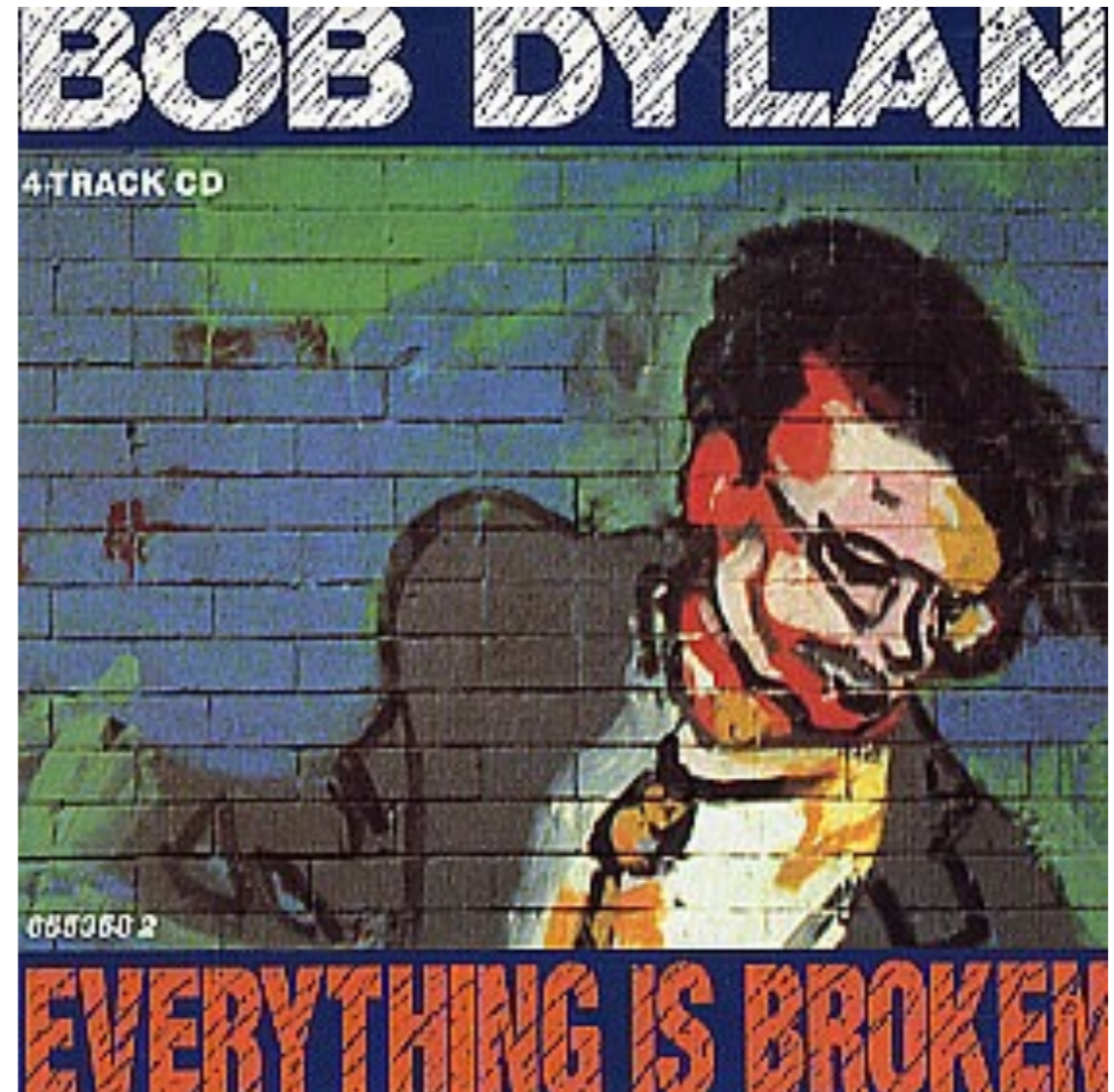
  - Hard to update and improve

# Software is Easy

- But we still get it so wrong

- Getting better all the time from cloud services

# Hardware is Software

- Many "hardware" devices are just a Linux box

- "IoT" devices are network devices

- The complexity, power of them is amazing

# Everything is Broken

# All Bugs are Security Bugs

# Today's HW Tomorrow's Bugs

- We're *all* shipping software with bugs that…

  - We didn't create

  - We don't know about

- Examples — Heartbleed, Stagefright, NTP, bash, etc.

# If Everything is Broken…

# Nothing is Broken

# If Every Bug is a Security Bug…

# No Bugs are Security Bugs

# So Just Accept It!

# Make your devices fixable!

# When We Started

- We decided we have an obligation to our customers

- We're more capable of protecting them than anyone else

# The First Thing We Did

- We started with Over-The-Air Updates

# If You Can Fix It…

# It Matters Less If It's Broken!

# Attitude

- Care about the users

- Just fix the bug. All bugs are security bugs.

- Just update the system.

- Process of development, you have to care

# Obviously…

- Deming was still right

  - It's always cheaper to fix something earlier

- In the wrong hands, this can be a reason to throw things over the wall that aren't done.

  - But no one's perfect and humans suck

# Back to the point!

# This Isn't Defending a Castle

- It's desert warfare

- Must keep moving, evaluating, testing

# Framework

- Make sure the device can't be bricked

- Make it get OS updates from the net

- Make it application updates from the net

- All this can get re-used to the next device

# Security of OTA

- Network security — Network encryption, certificate pinning, etc.

- Data security — signed packages

# Other Decisions

- Tradeoffs:

    - Security of the device

    - Openness of the device

- If you want to build an unhackable device, people aren't going to be able to hack it!

# Most of all…

- Start with updates

  - It makes your life easier

  - It makes beta, testing, etc. easier

  - It makes everything cheaper

# You can fix your mistakes

# You can fix other people's mistakes!

# You can deliver new features

# You make your customers happy

# You'll make us all proud!