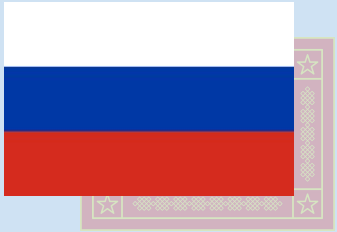
Trust, Transparency, and Simplicity

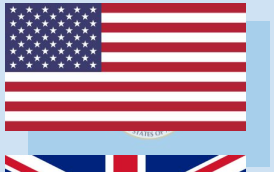
Eric Grosse ehg@google.com

2016-11-29 5th RISC-V Workshop, Mountain View CA

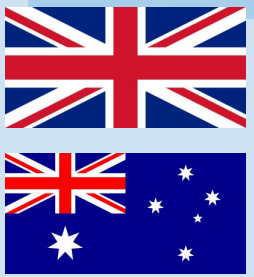
Focus on securing billions

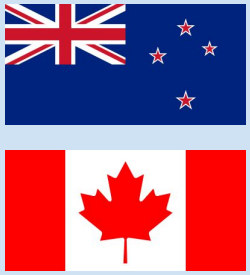
Know your adversary

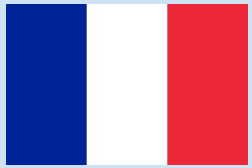




never discount sloth and ineptitude







Fix 1. secure communications

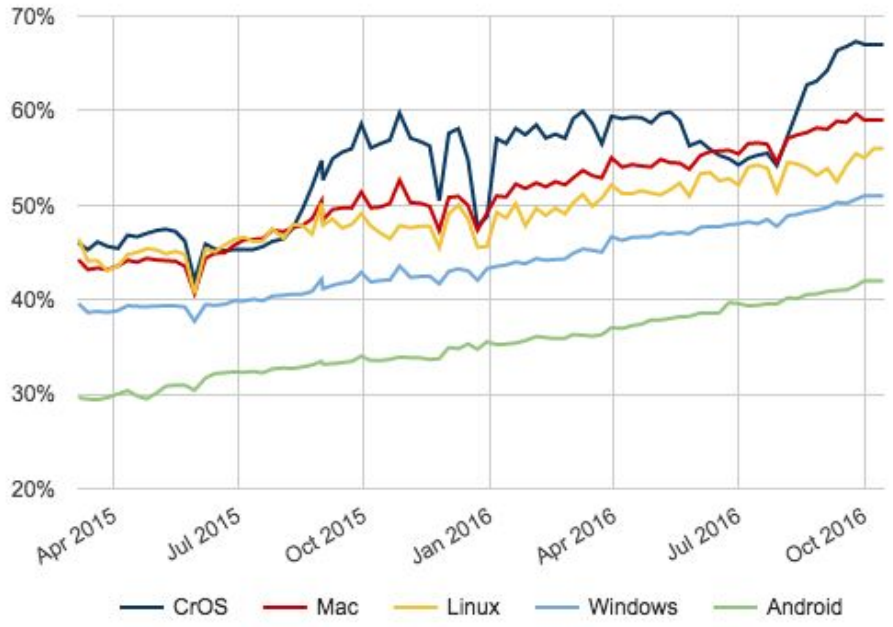
remarkable adoption of SSL

and PFS, LetsEncrypt, CT

less visible: encryption of internal links

end-to-end encryption

PGP, Signal, storage



HTTPS connections in Chrome

Fix 2. authentication

Lost credentials are the #1 way our users lose their data.

Passwords are too hard to use safely; public key crypto is stronger *and* easier to use.

You should already be using this technology!

latest: user *and* device *and* software stack.

Fix 3. patch

ref: SOUPS, googleonlinesecurity July 2015

Доверяй, но проверяй

Rowhammer and disclosure culture

Spray most of physical memory with page tables, then

```
code1a:
  mov (X), %eax  // Read from address X
  mov (Y), %ebx  // Read from address Y
  clflush (X)  // Flush cache for address X
  clflush (Y)  // Flush cache for address Y
  jmp code1a
```

https://googleprojectzero.blogspot.com/2015/03/exploiting-dram-rowhammer-bug-to-gain.html

Great BIOS lockdown of 2011

The need for simplicity and transparency

Rob Joyce, NSA TAO at Enigma 2016: Disrupting Nation State Hackers

"You know what technologies you intended to use. We know what is actually used." "We'll know the security functionality better than the people who developed the device."

Long-standing practitioners' wisdom: "Complexity is the enemy of security."

Our systems today are way too complicated and undocumented.

Open source and ruthless pruning are a partial answer. But what about the binary blobs in firmware and the mysterious chips?

Focus on securing friends and family

A paranoid's choice of CPU

x86 (but see Joanna Rutkowska, Intel x86 considered harmful, Oct 2015)

- Qubes-OS on NUC kit (tricky to get USB Security Key to correct VM)
- Coreboot, u-root on Asus KGPE-D16 motherboard

OpenPower

- Google servers
- "Talos Lockdown" on crowdsupply.com

RISC-V

- You have the critical advantage of openness; be sure to keep it.
- Please resist adding features lightly, or remove others in compensation.
- Consider CHERI security extension?


2 0TB
Seagate
WD