HOST: HOST Oriented Security and Trust

Lok Yan

Senior Computer Engineer, Ph.D.

AFRL/RIGA

Photo by Lok Yan

host (n):
Any computer attached to a network

Def 6. (computing, internet). https://en.wiktionary.org/wiki/host#Noun Retrieved: 15 ARP 2016

computer (n):
A programmable electronic device that performs mathematical calculations and logical operations
…

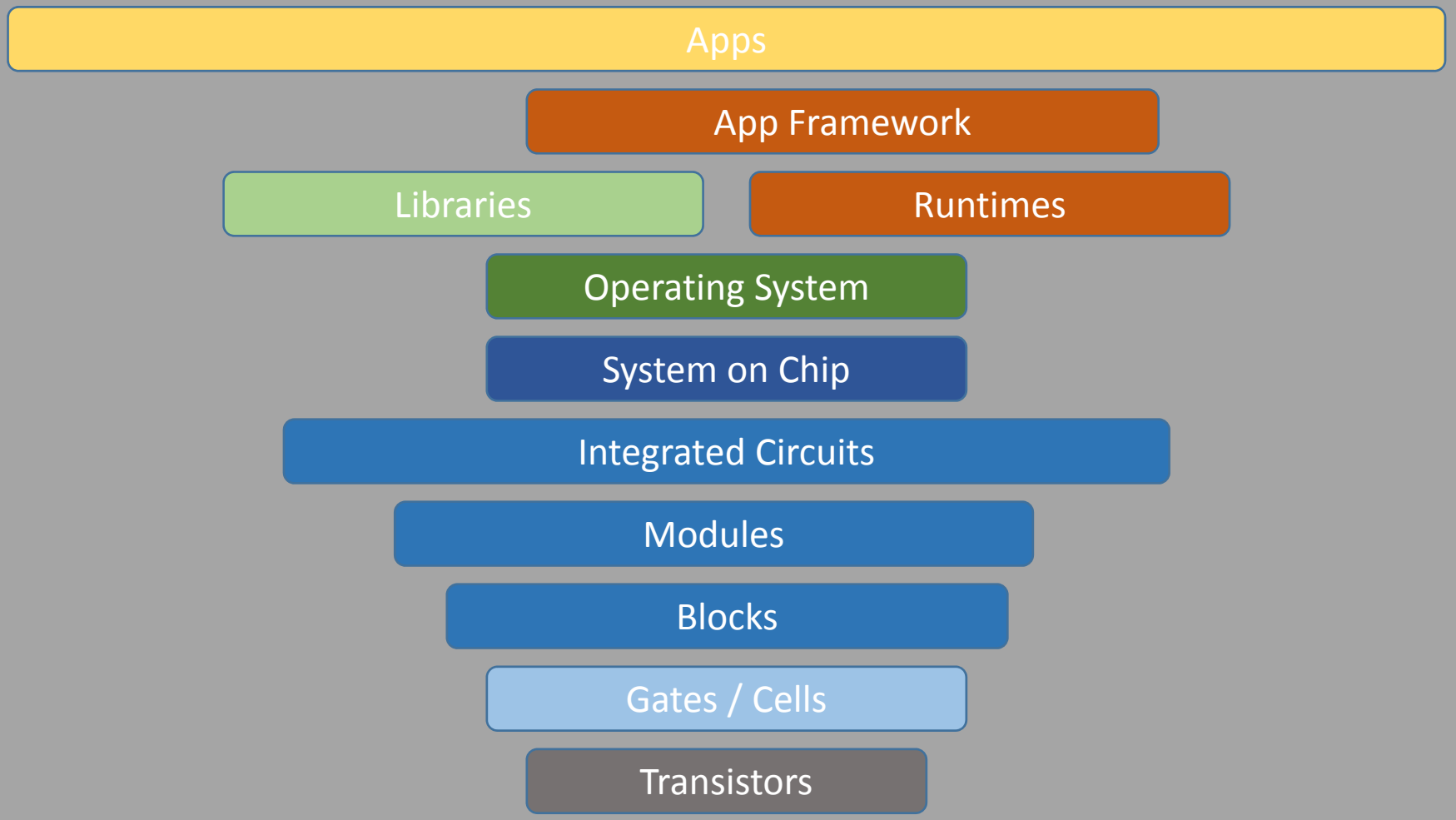
Def 3, https://en.wiktionary.org/wiki/computer#Noun Retrieved: 15 ARP 2016

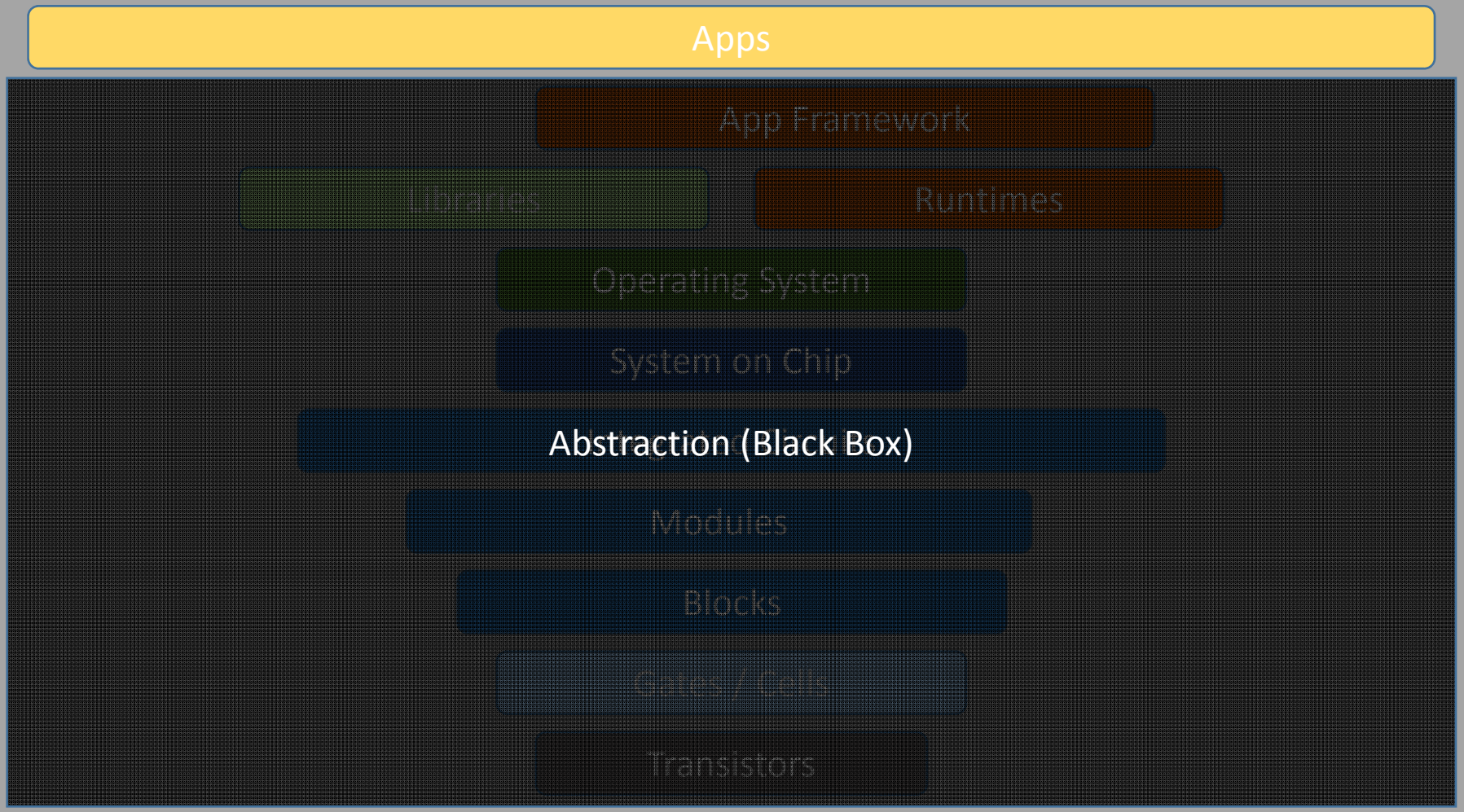
network (n):
Multiple computers and other devices connected together to share information

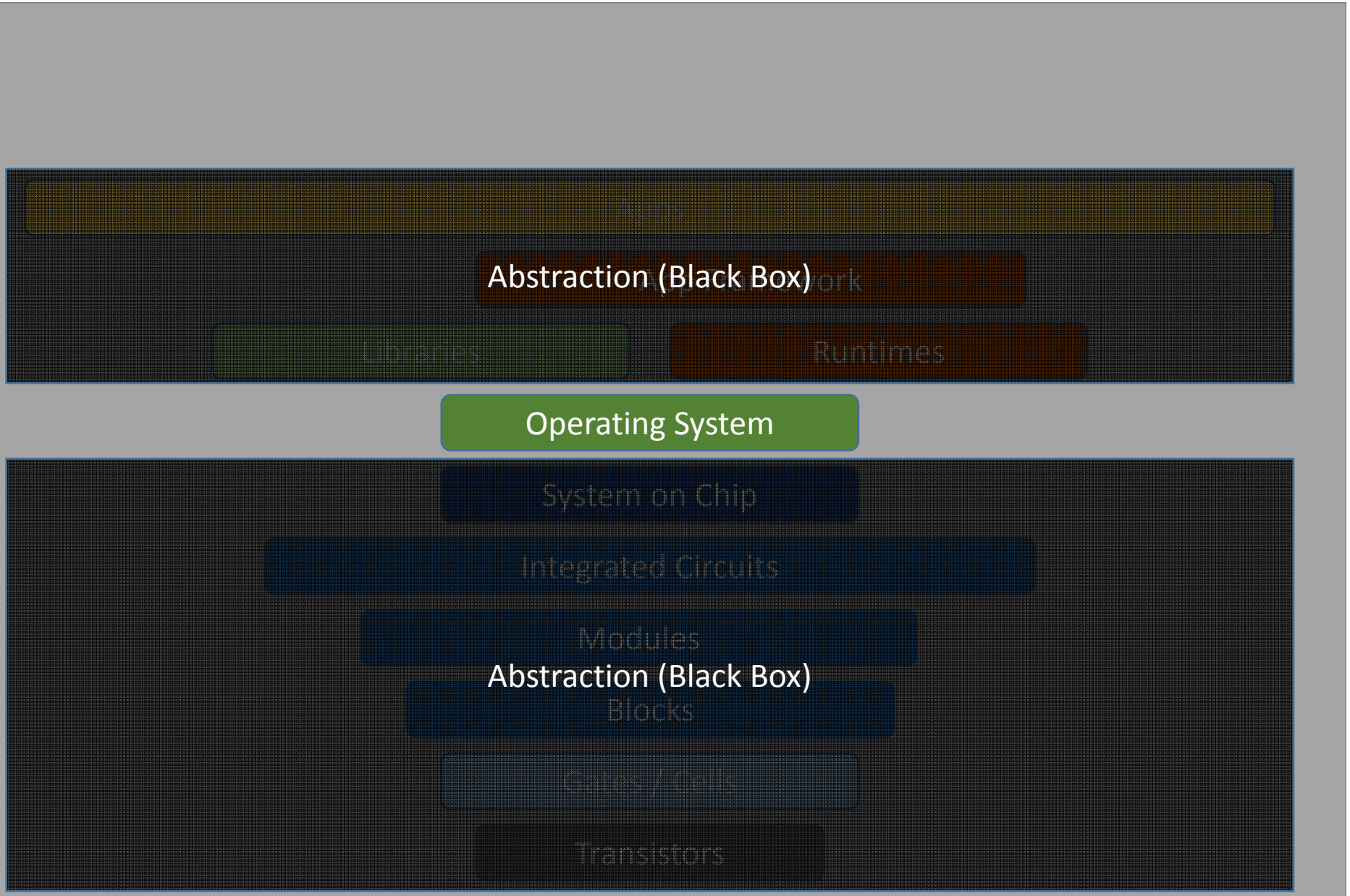
Def 5 (computing). https://en.wiktionary.org/wiki/network#Noun Retrieved: 15 APR 2016

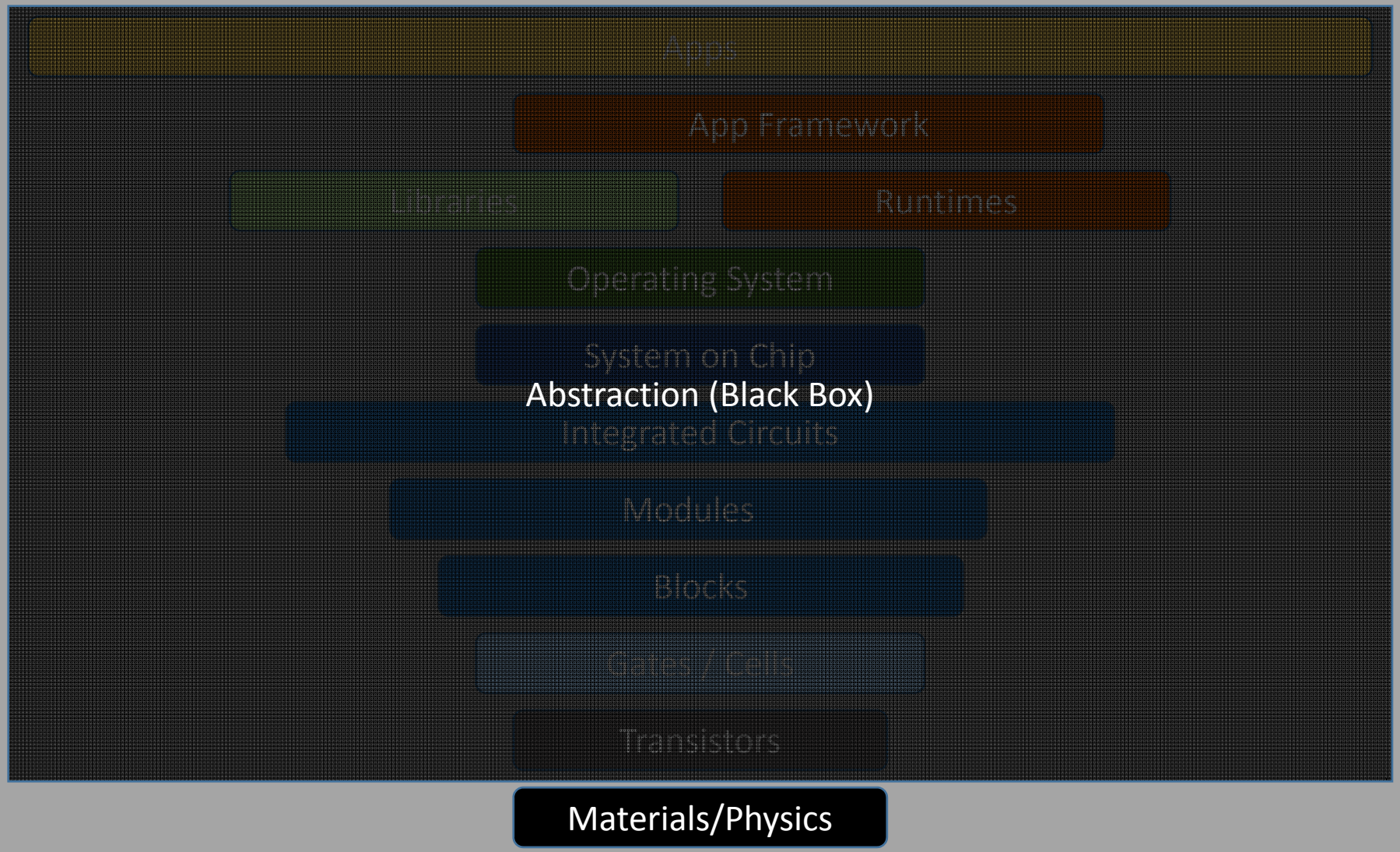
HOST: A holistic approach to security and trust

Hardware
Software
Wetware
Social/Net/…ware









Side Channel Attacks

What is the value of *ecx*?

1. mov $0, %eax;
2. mov $0xCAFEBABE, %ecx;
3. bsf %eax, %ecx

What is the value of *ecx*?

1. mov $0, %eax;
2. mov $0xCAFEBABE, %ecx;
3. bsf %eax, %ecx

UNDEFINED

"If the content of the source operand is 0, the content of the destination operand is undefined"[1]

[1]"Intel 64 and IA-32 Architectures Software Developer's Manual. Volume 2A: Instruction Set Reference, A-M." December, 2015. http://www.intel.com/content/dam/www/public/us/en/documents/manuals/64-ia-32-architectures-software-developer-vol-2a-manual.pdf

What is the value of *ecx*?

1. mov $0, %eax;
2. mov $0xCAFEBABE, %ecx;
3. bsf %eax, %ecx

0xCAFEBABE

*From testing

What is the value of *x*?

1. int32_t x = 0xFFFFFFFF;
2. x++;

What is the value of *x*?

1. int32_t x = 0xFFFFFFFF;
2. x++;

UNDEFINED

What is the value of *x*?

1. int32_t x = 0xFFFFFFFF;
2. x++;

0x0

*From testing on i386

CVE-2009-1897

Exploiting the Unexploitable

```
1. void func(int *param)
2. int localParam = *param;
3. if (!param)
4.     return;
5. …
```

See figure 2 from: Wang, X., Zeldovich, N., Kaashoek, F., and Solar-Lezama, A. "Towards Optimization-Safe Systems: Analyzing the Impact of Undefined Behavior." ASPLOS 2012. https://people.csail.mit.edu/nickolai/papers/wang-stack.pdf for further details.
Also see: Corbet, J. "Fun with NULL pointers, part 1." http://lwn.net/Articles/342330/

CVE-2016-0777,0778

Roaming through the OpenSSH client

1. tempKey = malloc(…)
2. fgets(privateKeyFile, tempKey)
3. authenticateUsingKey(tempKey)
4. zero(tempKey)
5. free(tempKey)

Qualys Security Advisory. “Roaming through the OpenSSH client: CVE-2016-0777 and CVE-2016-0778.” https://www.qualys.com/2016/01/14/cve-2016-0777-cve-2016-0778/openssh-cve-2016-0777-cve-2016-0778.txt

Photo by Lok Yan

Follow the specs!

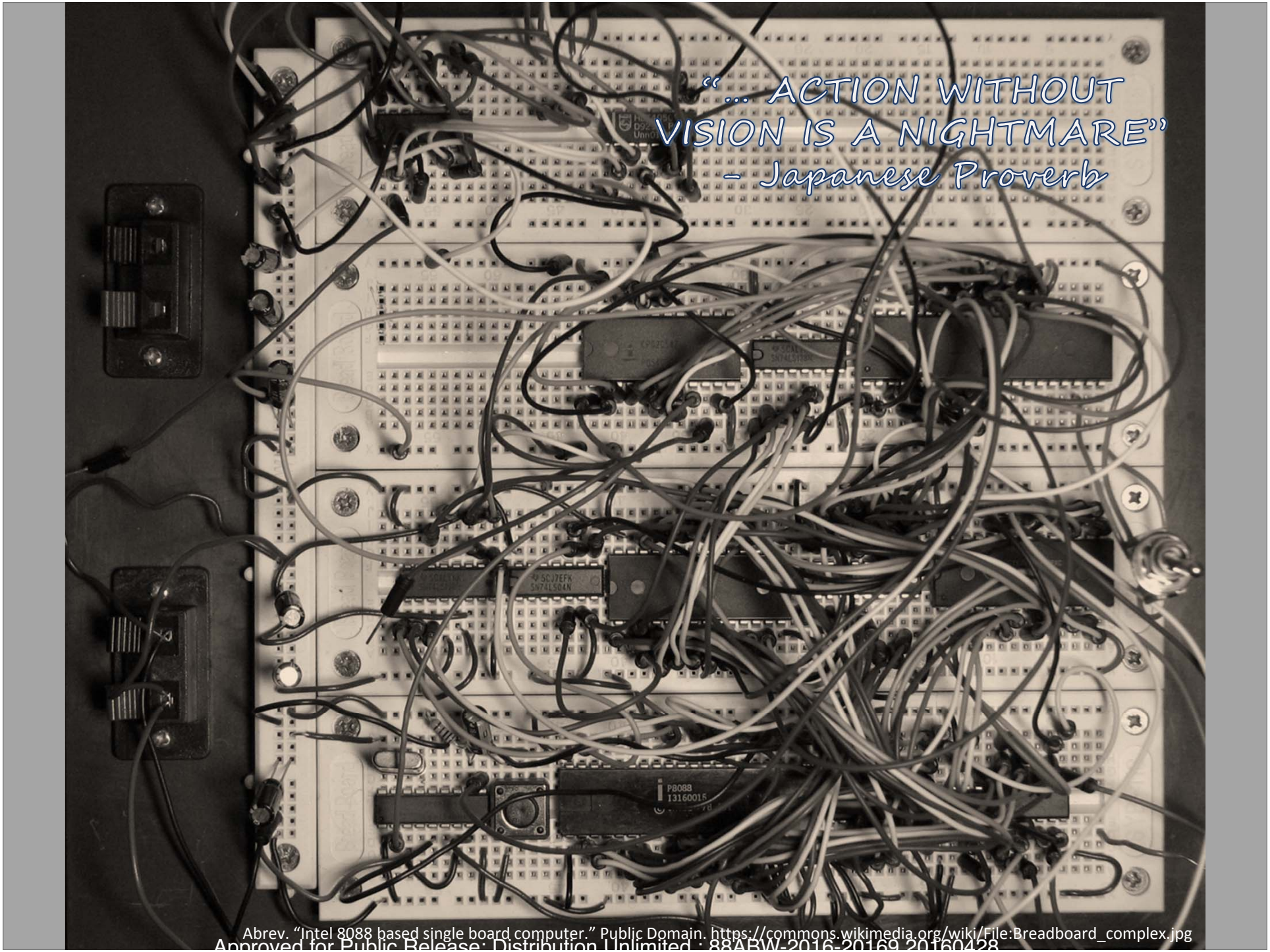
“Only the ARMv6 version on the imx31 platform of seL4 has a correctness proof.”

“It does not cover machine code, compiler, linker, boot code, cache and TLB management. “

https://github.com/seL4/seL4/blob/master/CAVEATS-generic.txt
seL4 is released under the BSD 2-Clause (https://github.com/seL4/seL4/blob/master/LICENSE_BSD2.txt) and GPL V2 Licenses (https://github.com/seL4/seL4/blob/master/LICENSE_GPLv2.txt)

"The proof shows that the seL4 C code implements the abstract API specification of seL4, and that this specification satisfies the following high-level security properties: [integrity, confidentiality, intransitive non-interference]"

"The security property proofs depend on additional assumptions on the correct configuration of the system."



Abrev. "Intel 8088 based single board computer." Public Domain. https://commons.wikimedia.org/wiki/File:Breadboard_complex.jpg

Vision:
Remove Abstractions

Power of Competition

AES

1997 – 2000 (Rijndael)

"The call indicated
NIST's goal that the AES would specify an unclassified, publicly disclosed encryption algorithm, available royalty-free, worldwide"[1]

SHA-3

2007 – 2012 (Keccak)

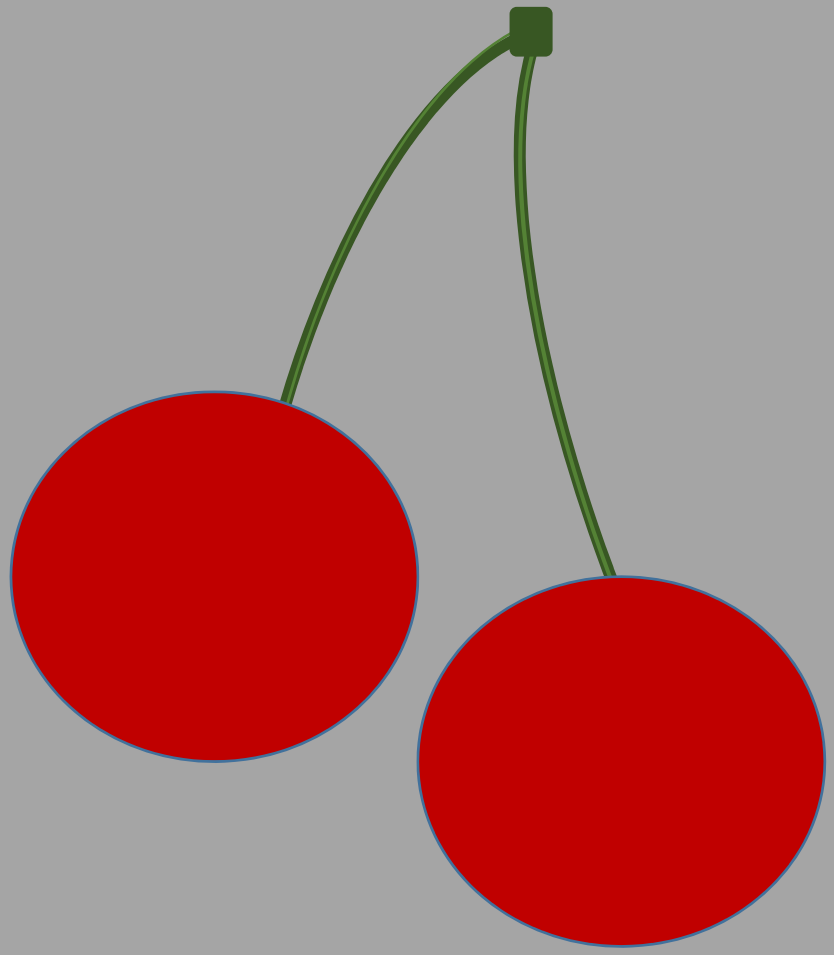
"Should my submission be selected for SHA–3, I hereby agree not to place any restrictions on the use of the algorithm, intending it to be available on a worldwide, non-exclusive, royalty-free basis."[2]

Security
Cost
Algorithm/Implementation

[1]Nechvatal, J. "Report on the Development of the Advanced Encryption Standard (AES)." October, 2, 2000. http://csrc.nist.gov/archive/aes/round2/r2report.pdf
[2]"Federal Register." Vol. 72, No. 212. http://csrc.nist.gov/groups/ST/hash/documents/FR_Notice_Nov07.pdf

DARPA CRASH
Clean-slate Design of Resilient, Adaptive, Secure Hosts

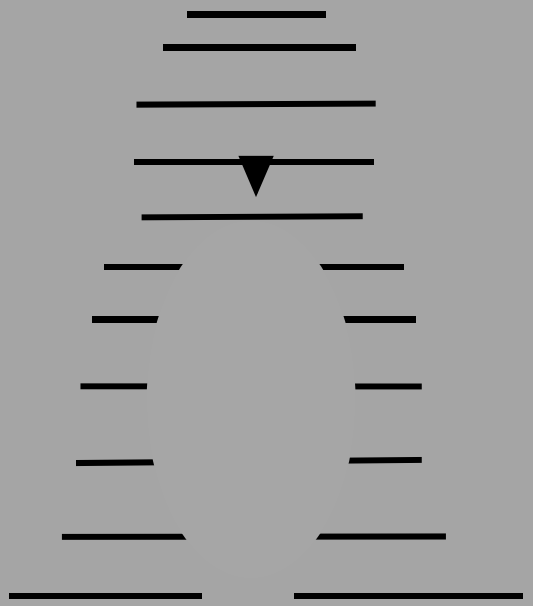
http://opencatalog.darpa.mil/CRASH.html



https://www.cl.cam.ac.uk/research/security/ctsrd/cheri/
https://www.cl.cam.ac.uk/research/security/ctsrd/beri/

1. Market / Adopt

Strength of One



Project Zephyr (IoT), 2016[5]

Raspberry Pi Model A, 2012

Android Donut, 2008[2]

Raspberry PI Founded 2006[4]

Linux breaks 50% of Supercomputers, 2004[1]

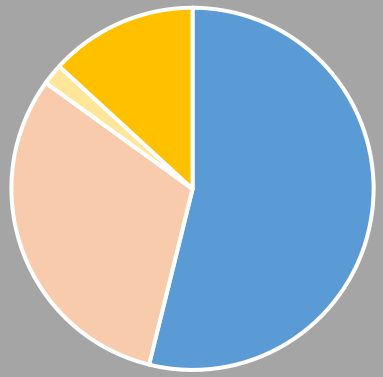
Android Inc. Founded, 2003[2]

KDE 1.0 & Gnome 1.2, 2000[3]

Linux was born, 1991[3]

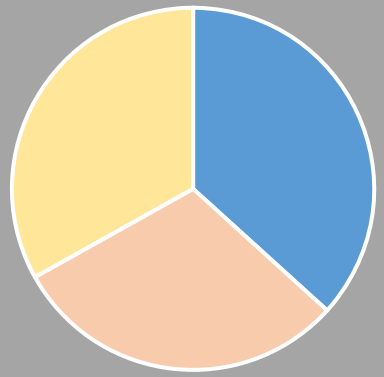
[1]https://en.wikipedia.org/wiki/Usage_share_of_operating_systems, [2]https://en.wikipedia.org/wiki/Android_(operating_system), [3]http://www.techradar.com/us/news/software/operating-systems/the-history-of-linux-how-time-has-shaped-the-penguin-1113914/1, [4]https://www.raspberrypi.org/about/, [5]http://www.linuxfoundation.org/news-media/announcements/2016/02/linux-foundation-announces-project-build-real-time-operating-system

Mobile



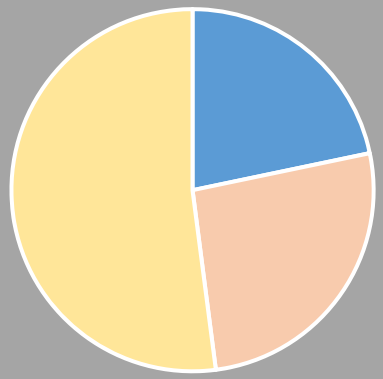
Android iOS Windows Other

Server



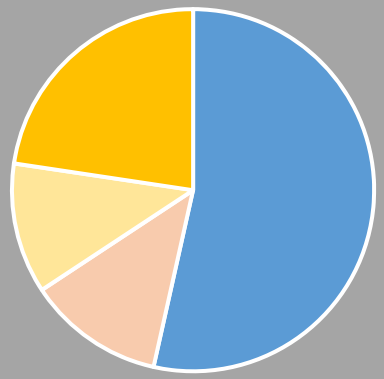
Linux Unix/BSD Windows Other

Desktop



Linux Unix/BSD Windows Other

Device Shipments



Linux Unix/BSD Windows Other

Source data from https://en.wikipedia.org/wiki/Usage_share_of_operating_systems Retrieved: 15 APR 2016

2. Advance

Hardware/Software Co-design &
Co-synthesis &
Co-verification &
Co …

Have Template Will Generate

Genesis 2

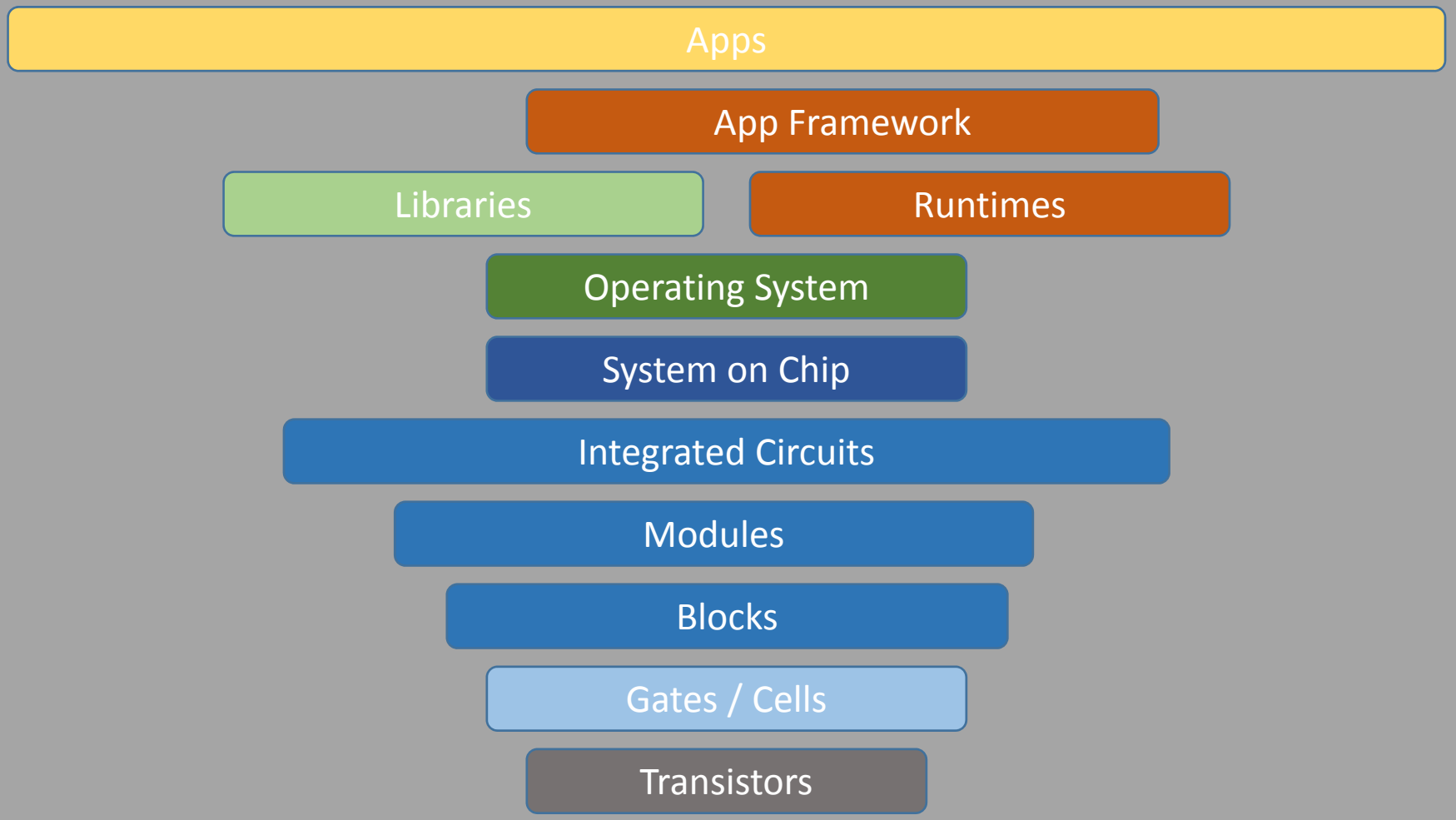
http://genesis2.stanford.edu/mediawiki/index.php/Main_Page

SISC – Security Instruction Set Computing

FISC – Formal Instruction Set Computing

AISC – Application-specific Instruction Set Computing

…



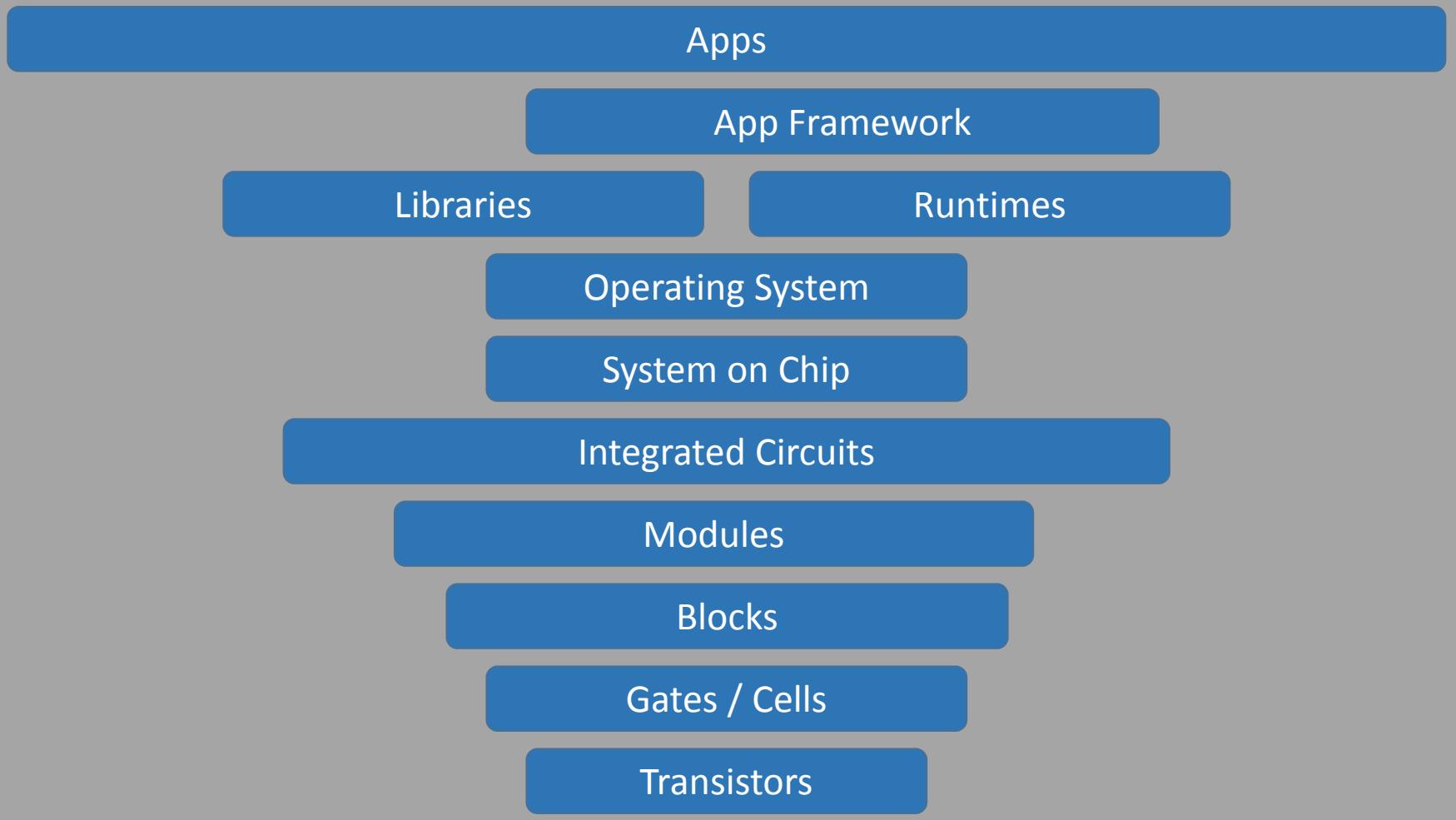


Photo by Lok Yan