CE876 - Information Security Mng. & Eng.

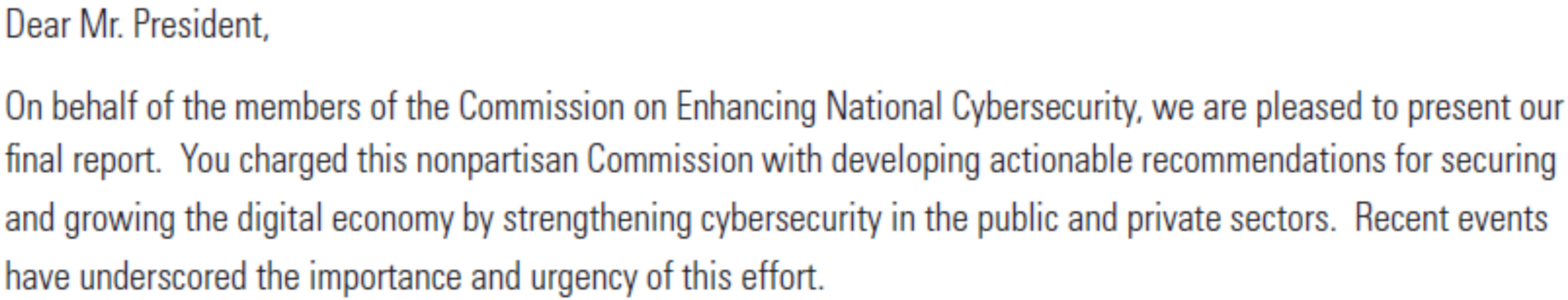
Lecture 2: Trust & Device Ownership

Department of Computer Engineering
Sharif University of Technology
Spring 1400

S4Lab

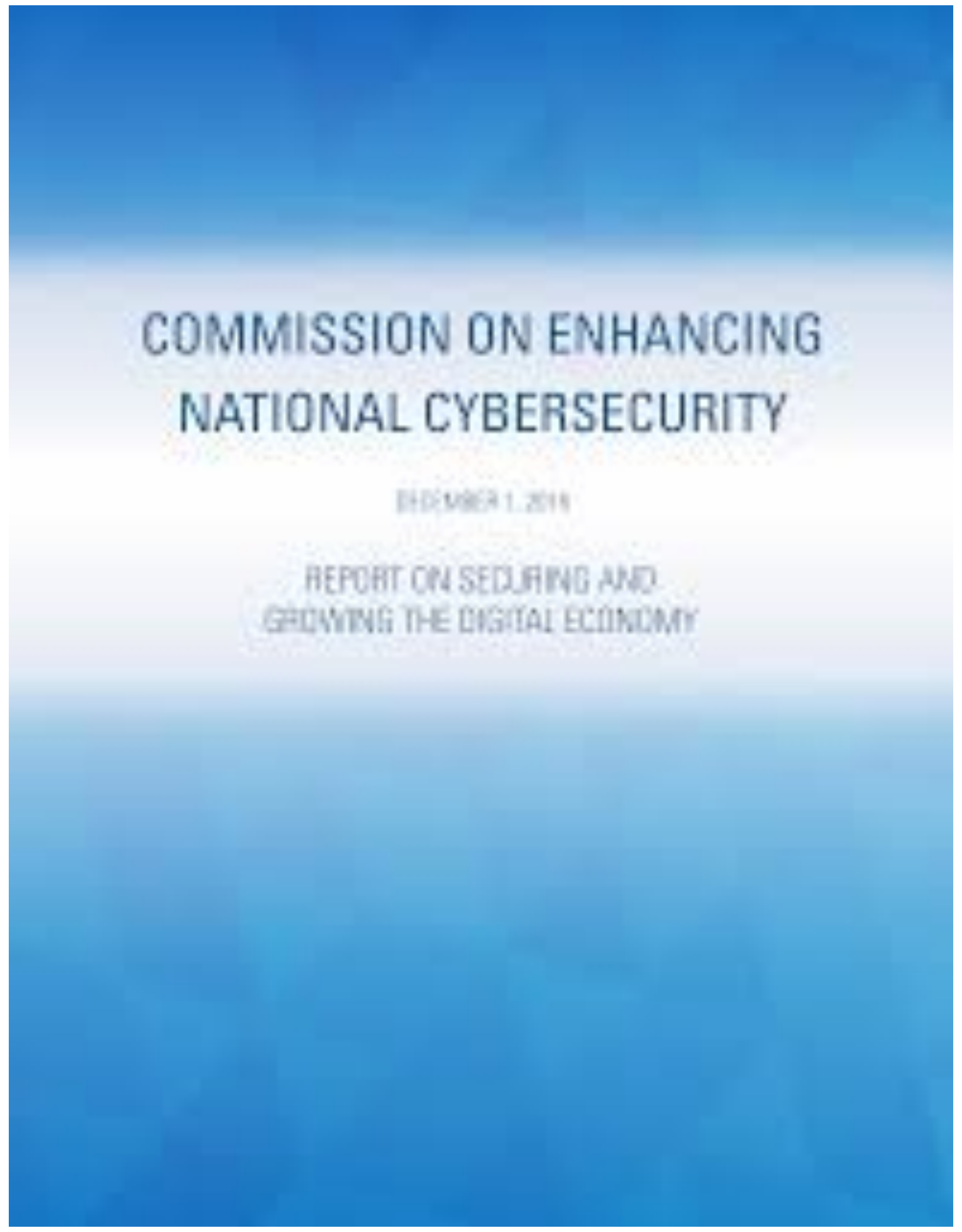
Acknowledgments: Some of the slides are fully or partially obtained from other sources. A reference is noted on the bottom of each slide to acknowledge the full slide or partial slide content. These slides were initially developed by Seyedeh Atefeh Musavi and Mehdi Kharrazi.

What is trust?



Dear Mr. President,

On behalf of the members of the Commission on Enhancing National Cybersecurity, we are pleased to present our final report. You charged this nonpartisan Commission with developing actionable recommendations for securing and growing the digital economy by strengthening cybersecurity in the public and private sectors. Recent events have underscored the importance and urgency of this effort.



COMMISSION ON ENHANCING
NATIONAL CYBERSECURITY

REPORT ON SECURING AND
GROWING THE DIGITAL ECONOMY

[https://www.nist.gov/cybercommission]

Trust is fundamental

- The success of the digital economy relies on
  - individuals and organizations trusting computing technology and,
  - trusting the organizations that provide products and services and,
  - trusting the organizations that collect and retain data.
- Recent incidents and breaches have weakened this trust.
- Concerns over misuse and compromise of corporate and personal data.
- Formation and Impact of the Cybersecurity Commission
  - Established by President Obama in Feb. 2016 via Executive Order 13718.
  - Commission released its report on December 1, 2016.
  - Recommendations aim to enhance cybersecurity across public and private sectors.

[https://www.nist.gov/cybercommission]

Why Trust

- Exploration of trust is going to start and end with security,
  - Because security is what you need when you don't have any trust.
- All complex ecosystems, biological like the human body, natural like a rain forest, social like an open-air market, or socio-technical like the global financial system or the Internet, are deeply interlinked.
- At the same time, all complex ecosystems contain parasites.
  - Within every interdependent system, there are individuals who try to subvert the system to their own ends.
- Society runs on trust. This is vital.
  - If the number of parasites gets too large, if too many people steal or too many people don't pay their taxes, society no longer works.

[Schneier, B., Liars and outliers: enabling the trust that society needs to thrive. John Wiley & Sons, 2012]

So let’s accept the complexity

- NY Times can helpfully spoof your email addresses when you refer an article to a friend, as can spammers in their unwanted mass mailings.
    - While spammers could be foiled by using identity based techniques, doing so would break the service provided by the NY Times and many other beneficial parasites.
- If we fix the Internet by simplifying it so that only those that create value can profit from it, then in such restricted environments, innovation and evolution are smothered and resources spent defending artificial restrictions rather than extending the ecosystem.
- In complex systems, like the Internet, parasites are accepted for what they are. Negative parasites are the price we pay for the benefits of positive parasites and the freedom to innovate.
- Remember: Internet is not broken -- just complex.

[http://web.archive.org/web/20130729211452id_/]
[http://itc.conversationsnetwork.org/shows/detail461.html]

How do parasites behave?

- Being a parasite is a balancing act:
  - Biological parasites do best if they don't immediately kill their hosts, but instead let them survive long enough for the parasites to spread to additional hosts.
  - Spammers do better if they don't clog e-mail to the point where no one uses it anymore
  - Rogue banks are more profitable if they don't crash the entire economy.
- All parasites do better if they don't destroy whatever system they've latched themselves onto. *Parasites thrive only if they don't thrive too well.*
- So this can be seen in a game theory model.
- Excepting the smallest and simplest cases, every society has parasites living inside it. And there is an evolutionary advantage to being a parasite as long as there aren't too many of them and they aren't too good at it.

[Schneier, B., Liars and outliers: enabling the trust that society needs to thrive. John Wiley & Sons, 2012]

In what we Trust?

S4Lab

- When we trust people:
  - Either trust their intentions or their actions.
- The first is more intimate:
  - When we say we trust a friend, that trust isn’t tied to any particular thing he’s doing.
- The second is less intimate: (sociologist Susan Shapiro calls it impersonal trust.)
  - When we don’t know someone, but we can trust that she won’t run red lights, or steal from us, or cheat on tests.
  - We don’t know if she has a secret desire to run red lights . Rather, we know that she is likely to follow most social norms of acceptable behavior because the consequences of breaking these norms are high.
  - You can think of this kind of trust—that people will behave in a trustworthy manner even if they are not inherently trustworthy—more as confidence, and the corresponding trustworthiness as compliance.
- In another sense, we’re reducing trust to consistency or predictability.

[Schneier, B., Liars and outliers: enabling the trust that society needs to thrive. John Wiley & Sons, 2012]

In what we Trust? (con’t)

- In which we trust more?
  - Systems or people.

[Schneier, B., Liars and outliers: enabling the trust that society needs to thrive. John Wiley & Sons, 2012]

Trusting technology

- These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.
- What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.

[Nakamoto, Satoshi, and A. Bitcoin. "A peer-to-peer electronic cash system." Bitcoin, 2008]

- Bitcoin is not a system that doesn't rely on trust it eliminates certain trust intermediaries but you have to trust Bitcoin whatever that means and in general what block chains do is they can change the nature of trust.
- Block chains shifts trust in people and institutions to stress on technology.
- Would you rather trust a human legal system or the details of some computer code that you probably do not have the expertise to audit.
- Trusting technology's harder than trusting people block chain doesn't necessarily reduce the cost of trust it shifts it around.

[keynote at Hyperledger Global Forum on “Security, Trust and Blockchain.”, 2018]

Why parasitic behaviors exists?

- The problem isn’t with people; the problem is with the dilemma.
- Societal dilemmas are choices between group interest and some competing individual interest.
- Society solves societal dilemmas by making it in people’s best interest to act in the group interest. (cooperator vs. defector)
- How?

[Schneier, B., Liars and outliers: enabling the trust that society needs to thrive. John Wiley & Sons, 2012]

How to solve societal dilemmas

- Pressures that increase the actual or perceived difficulty of defecting.
- Pressures that raise the consequences of defecting.
- Pressures that reduce the actual or expected benefits of defecting.
- Pressures that limit the damage caused by the defections that happen.
- Pressures that increase the benefits of cooperating,
- Pressures that lower the costs of cooperating.

[Schneier, B., Liars and outliers: enabling the trust that society needs to thrive. John Wiley & Sons, 2012]

Four categories to sort societal pressures

- Moral pressure
- Reputational pressure
- Institutional pressure
- Security systems

[Schneier, B., Liars and outliers: enabling the trust that society needs to thrive. John Wiley & Sons, 2012]

Different types of security systems

- Defenses: Physically stop potential defectors from doing whatever they're trying to do.
- Interventions: Other security measures that happen during the defection that either make defection harder or cooperation easier (e.g.obfuscation).
- Detection/response systems: Burglar alarms, IDS, RFID tags attached to merchandise.
- Audit/forensic systems: Primarily enhancements to institutional societal pressure.
- Recovery systems: Make it easier for the victim to recover from an attack.
  - A credit monitoring service or an insurance plan.
- Preemptive interventions: Operate before the attack, and directly affect the risk trade-off. Often punishments after an attack, but they can prevent a future attack, too. Incarceration is also a preemptive intervention as well as a punishment; there are entire categories of crimes that someone in jail simply can't commit.

[Schneier, B., Liars and outliers: enabling the trust that society needs to thrive. John Wiley & Sons, 2012]

Different kinds of Trust

- Three main approaches to trust in computer science :
  - Computational trust
  - Logical trust (Semantic web)
  - Trusted computing

Computational trust (reputation models)

S4Lab

- Used in supply chains, e-commerce, or Information Systems, psychology, economics, and sensor networks.
- A reputation system should:
  - Capture feedback
  - Guide trust decisions
  - Persist over time
- So there is a model to compute trust based on different feedbacks.
- An important indication: if Allice trusts Bob, I have also ….
- (Some) Implicit trust to Allice has been assumed.
- Implicit transitivity property for trust has been assumed.

Digikala example

S4Lab

پیشنهاد شگفت‌انگیز

۰۳ : ۲۷ : ۰۶

کفش پسرانه نیترو کد 7468

★ ۴ (۱۸) • ۱۹ دیدگاه کاربران • ۱ پرسش و پاسخ

برند : متفرقه   دسته‌بندی : کفش رسمی پسرانه

اندازه : ۳۴

ویژگی‌های کالا

- جنس: جیر، پارچه
- نحوه بسته شدن: یکسره

خدمات ویژه کاربران دیجی‌پلاس   شما هم عضو شوید

ارسال رایگان • ۳۰ روز بازگشت کالا • امکان ارسال فوری

بیش از ۱۰ نفر از خریداران این محصول را پیشنهاد داده‌اند

فروشنده:پویان

عملکرد: ۳.۳ از ۵ | ٪۱۰۰ رضایت از کالا

گارانتی اصالت و سلامت فیزیکی کالا

موجود در انبار دیجی‌کالا

ارسال دیجی‌کالا

قیمت فروشنده ~~۱۲۹,۰۰۰~~ ۳۵٪

۸۴,۰۰۰ تومان

بهترین قیمت ۳۰ روز گذشته

۹ امتیاز پس از فعال‌سازی دیجی‌کلاب و خرید این کالا

[digikala.com]

Digikala (con’t)

S4Lab

زیابی و رتبه بندی فروشندگان

شندگان براساس معیارهای ذکر شده در سه گروه خوب، متوسط و بد رتبه‌بندی می‌شوند و براساس رتبه‌ی کسب شده، نسبت به ادامه‌ی کاری ایشان با دیجی‌کالا تصمیم‌گیری می‌شود.

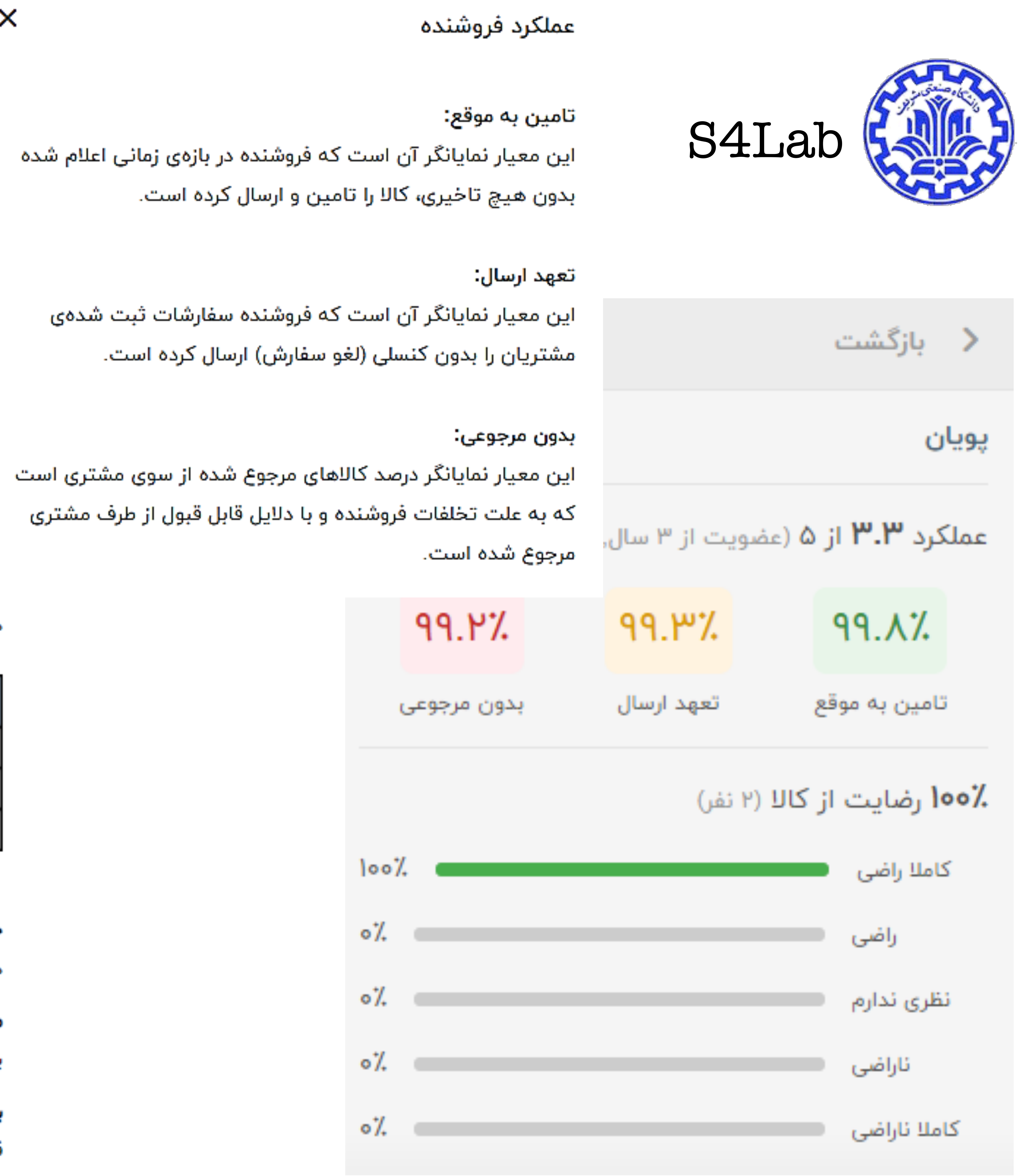
درجدول زیر جزییات نحوه‌ی رتبه‌بندی فروشندگان قابل مشاهده است:

	مرجوعی	لغو سفارش	تاخیر ارسال
خوب	کمتر و مساوی ۱٪	کمتر و مساوی ۱٪	کمتر و مساوی ۱٪
متوسط	بیشتر از ۱٪ و کمتر و مساوی ۲٪	بیشتر از ۱٪ و کمتر و مساوی ۲٪	بیشتر از ۱٪ و کمتر و مساوی ۳٪
بد	بیشتر از ۲٪	بیشتر از ۲٪	بیشتر از ۳٪

خوب: طبق این جدول، فروشندگانی که کمتر یا مساوی ۱% تاخیر در ارسال کالا، کمتر یا مساوی ۱% لغو سفارش و کمتر یا مساوی ۱% مرجوعی داشته باشند، دررده‌ی فروشندگان خوب قرارمی‌گیرند.

متوسط: فروشندگانی که بیشتراز ۱% و کمتر یا مساوی ۳% تاخیر درارسال کالا، بیشتراز ۱% و کمتر یا مساوی ۲% لغو سفارش و بیشتراز ۱% و کمتر یا مساوی ۲% مرجوعی داشته باشند، درردهٔی فروشندگان متوسط قرارگرفته و نیاز به بهبود عملکرد خود دراسرع وقت دارند.

بد: فروشندگانی که بیشتراز ۳% تاخیر درارسال کالا، یا بیشتراز ۲% لغو سفارش و یا بیشتراز ۲% مرجوعی داشته باشند، درردهٔی فروشندگان بد قرارگرفته و دیجی‌کالا ناچاربه خاتمه‌ی همکاری با ایشان است.



عملکرد فروشنده

تامین به موقع:

این معیار نمایانگر آن است که فروشنده در بازه‌ی زمانی اعلام شده بدون هیچ تاخیری، کالا را تامین و ارسال کرده است.

تعهد ارسال:

این معیار نمایانگر آن است که فروشنده سفارشات ثبت شده‌ی مشتریان را بدون کنسلی (لغو سفارش) ارسال کرده است.

بدون مرجوعی:

این معیار نمایانگر درصد کالاهای مرجوع شده از سوی مشتری است که به علت تخلفات فروشنده و با دلایل قابل قبول از طرف مشتری مرجوع شده است.

عملکرد ۳.۳ از ۵ (عضویت از ۳ سال،

تامین به موقع	تعهد ارسال	بدون مرجوعی
۹۹.۸٪	۹۹.۳٪	۹۹.۲٪

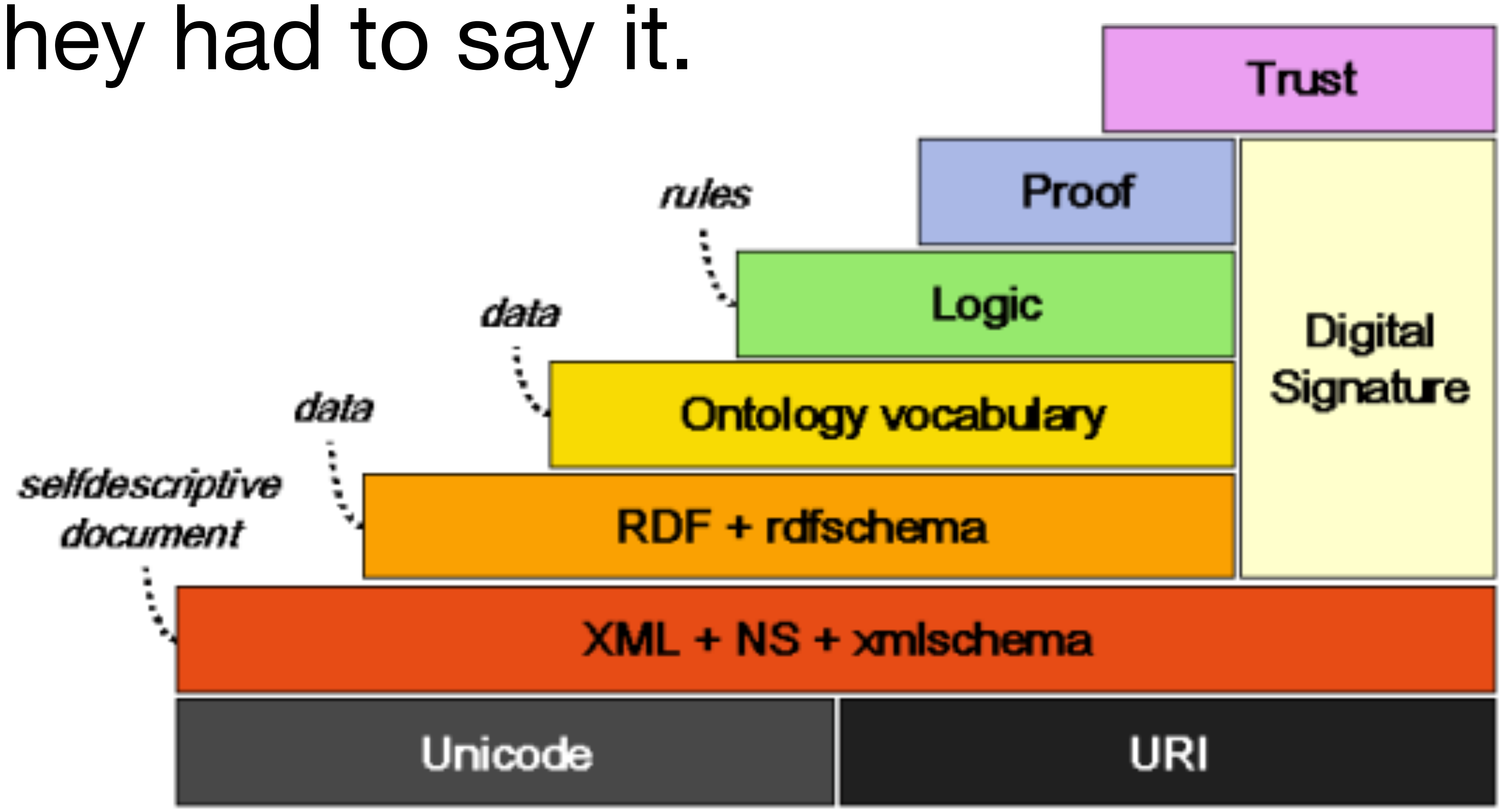
۱۰۰٪ رضایت از کالا (۲ نفر)

کاملا راضی	۱۰۰٪
راضی	۰٪
نظری ندارم	۰٪
ناراضی	۰٪
کاملا ناراضی	۰٪

[digikala.com]

Semantic web trust

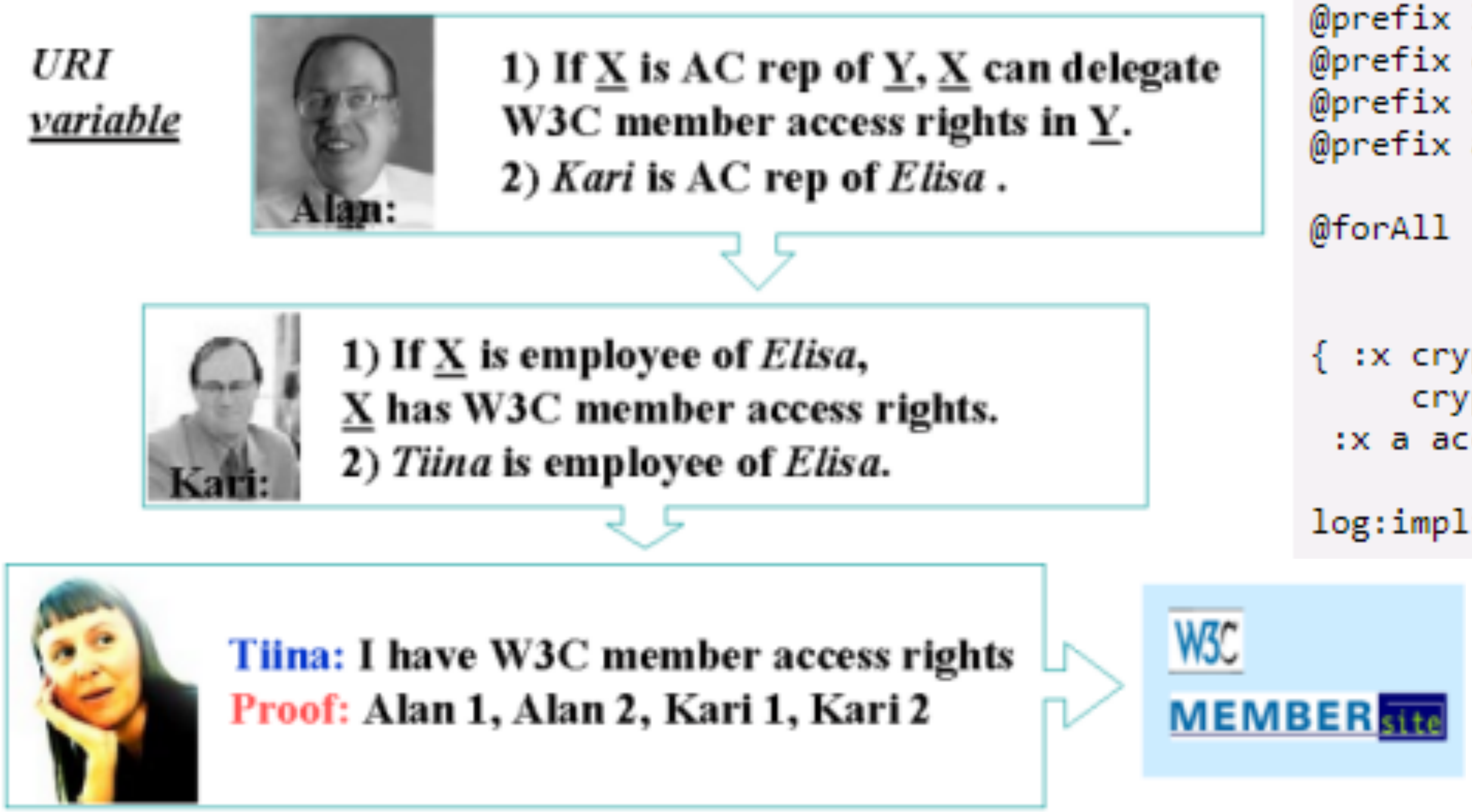
- Not everything found from the Web is true and the Semantic Web does not change that in any way.
- Truth - or more pragmatically, trustworthiness - is evaluated by each application that processes the information on the Web. The applications decide what they trust by using the context of the statements; e.g. who said what and when and what credentials they had to say it.
- The Semantic Web doesn't make that social problem much easier. When you have figured out a trust model, the Semantic Web allows you to write it down.



[https://www.w3.org/2001/12/semweb-fin/w3csw]

An example

S4Lab



URI
variable

Alan: 1) If X is AC rep of Y, X can delegate W3C member access rights in Y.
2) *Kari* is AC rep of *Elisa* .

Kari: 1) If X is employee of *Elisa*, X has W3C member access rights.
2) *Tiina* is employee of *Elisa*.

Tiina: I have W3C member access rights
Proof: Alan 1, Alan 2, Kari 1, Kari 2

```
#  Generate master key

@prefix : <#> .
@prefix log: <http://www.w3.org/2000/10/swap/log#> .
@prefix crypto: <http://www.w3.org/2000/10/swap/crypto#> .
@prefix string: <http://www.w3.org/2000/10/swap/string#> .
@prefix acc: <http://www.w3.org/2000/10/swap/test/crypto/acc.n3#>.

@forAll :x , :y.


{ :x crypto:keyLength "1024";
     crypto:publicKey :y } log:implies {
 :x a acc:MasterKeyPair; a acc:Secret.  :y a acc:MasterKey } .

log:implies a log:Chaff.
```

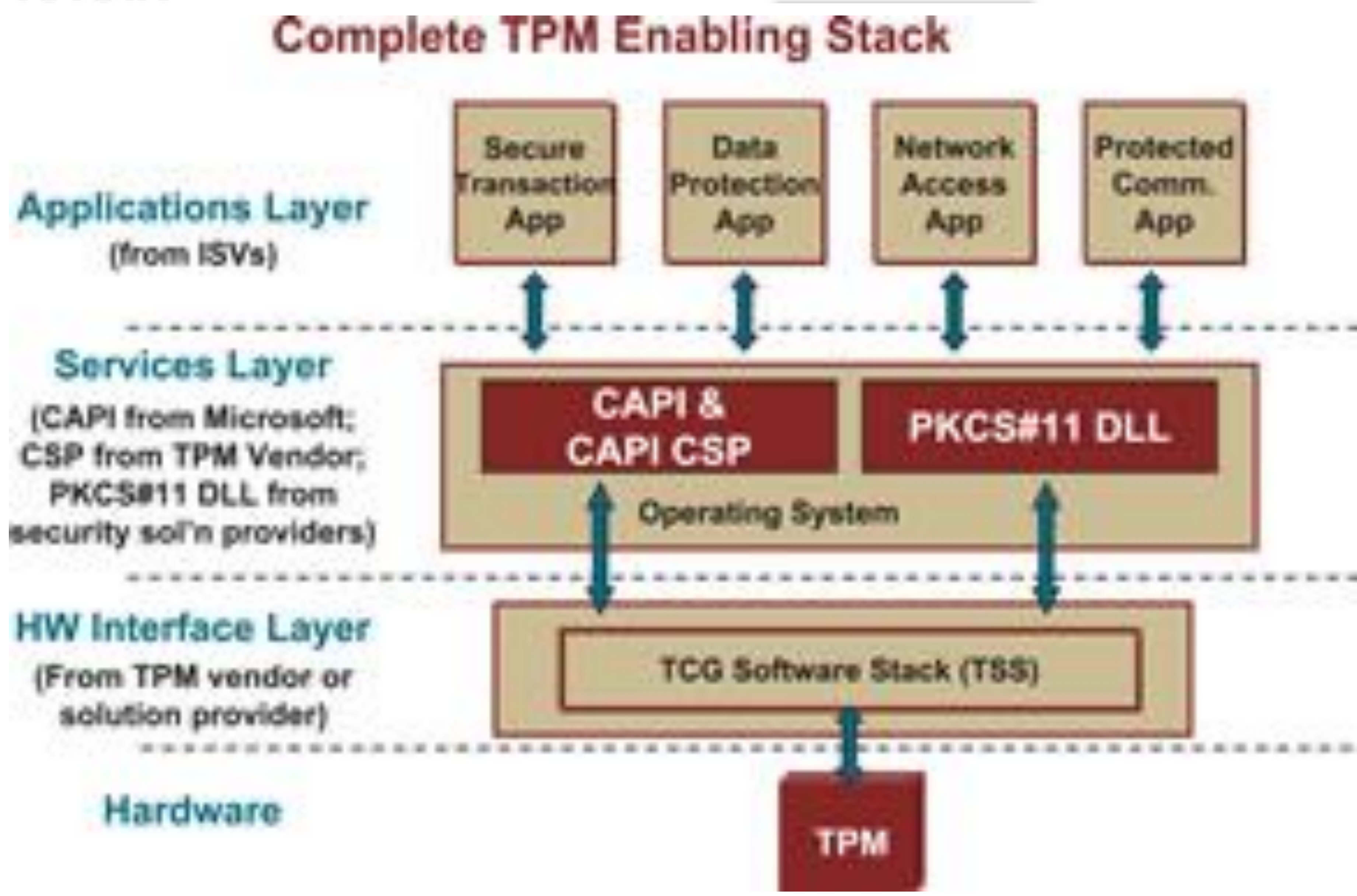
[https://www.w3.org/2000/10/swap/doc/Trust]

Trusted computing

S4Lab

AMD Cisco Dell Hewlett Packard Enterprise
hp HUAWEI IBM infineon
intel Juniper Networks Lenovo Microsoft
TOYOTA

- The Trusted Computing Group (TCG) is a not-for-profit organization formed to develop, define and promote open, vendor-neutral, global industry specifications and standards, supportive of a hardware-based root of trust, for interoperable trusted computing platforms.
- TCG's core technologies include specifications and standards for the Trusted Platform Module (TPM), Trusted Network Communications (TNC), and network security and self-encrypting drives.
- So what about the implementation ?
- There are specific vendors with TCG Vendor ID Registry
  - E.g. Infineon
  - There is a trend to make the implementation also open source by TPM 2.



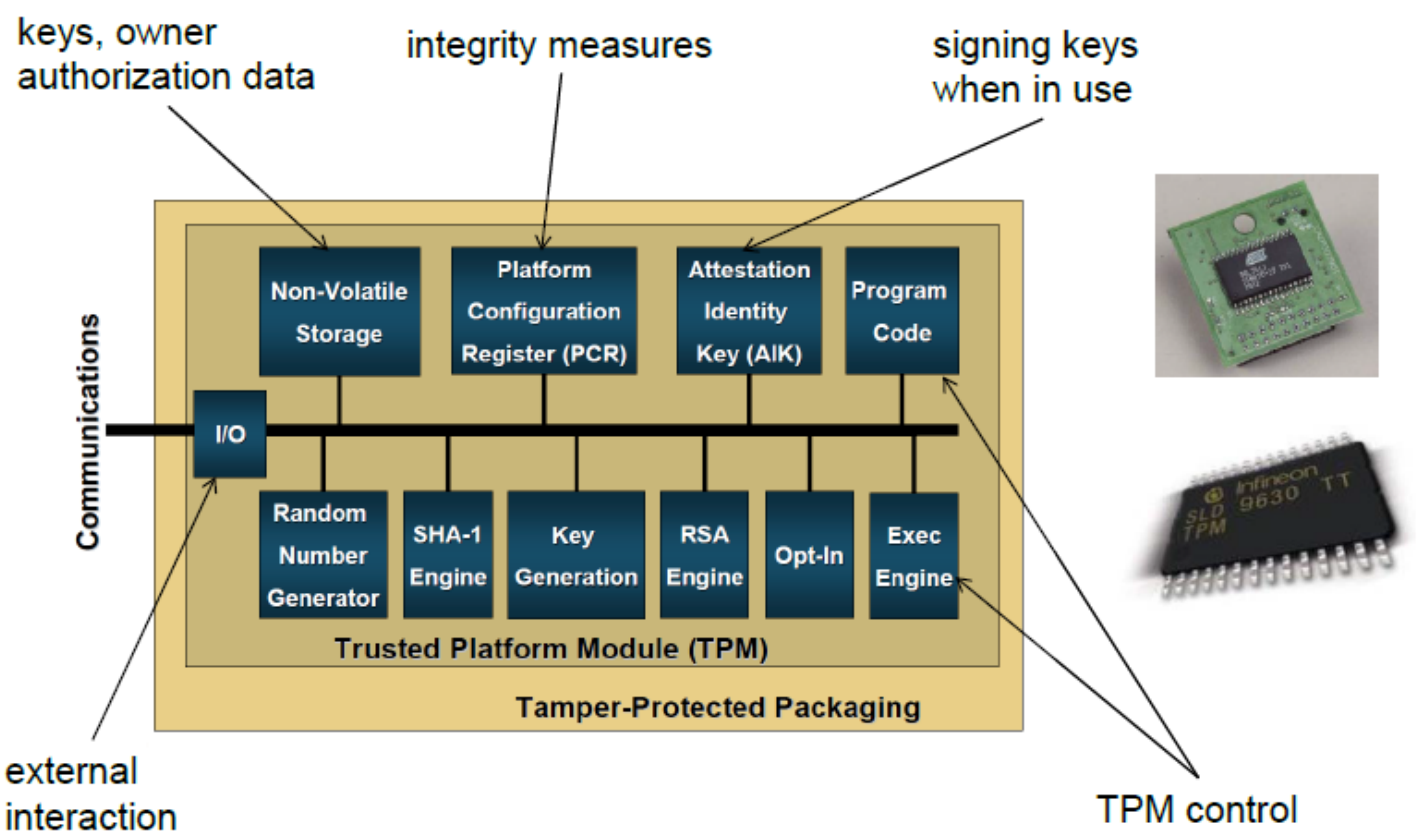
[https://trustedcomputinggroup.org/]

TPM (Trusted Platform Module)

- A TPM is a cryptographic co-processor with secure storage and hardware-enforced access control.
  - Commonly used for software attestation, cryptographic key storage, storing root certificates, full disk encryption, and as an anchor for trusted execution environments.
  - Said to be tamper-proof, but there has been multiple attacks against it!
  - Assume the TPM implementation is secure, not necessarily the platform on which it is attached.
- TC provides a computing platform on which you can't tamper with the application software.
  - Applications can communicate securely with their authors and with each other.
- The original motivation was digital rights management (DRM):
  - Disney will be able to sell you DVDs that will decrypt and run on a TC platform, but which you won't be able to copy.
- TC will also make it much harder for you to run unlicensed software

[https://www.cl.cam.ac.uk/~rja14/tcpa-faq.html]

TPM Internals

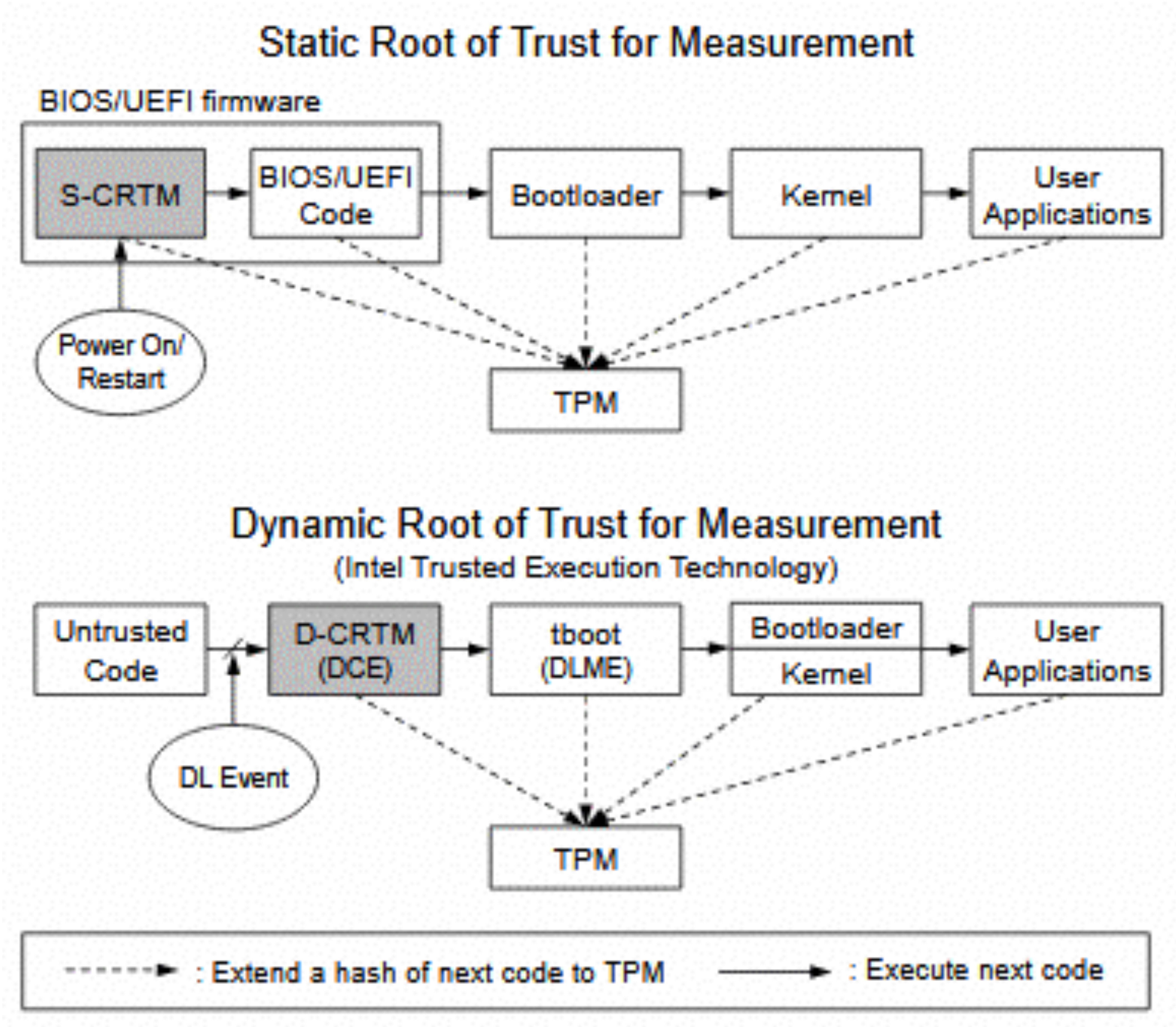


- Measure a component before executing it.
- Record the measurement as a hash value of the code/data (aka, fingerprint).
- Produces a hash chain by combining individual hash values.
- Changes in the executing code can be detected by comparing measurement of executing code against recorded value.
- The measurements themselves must be protected from undetected manipulation.
- At least 16 PCR registers, each register stores 20 bytes.

[https://courses.cs.vt.edu/cs5204/fall10-kafura-BB/Overheads/TPM.pptx]

How TPM works?

S4Lab



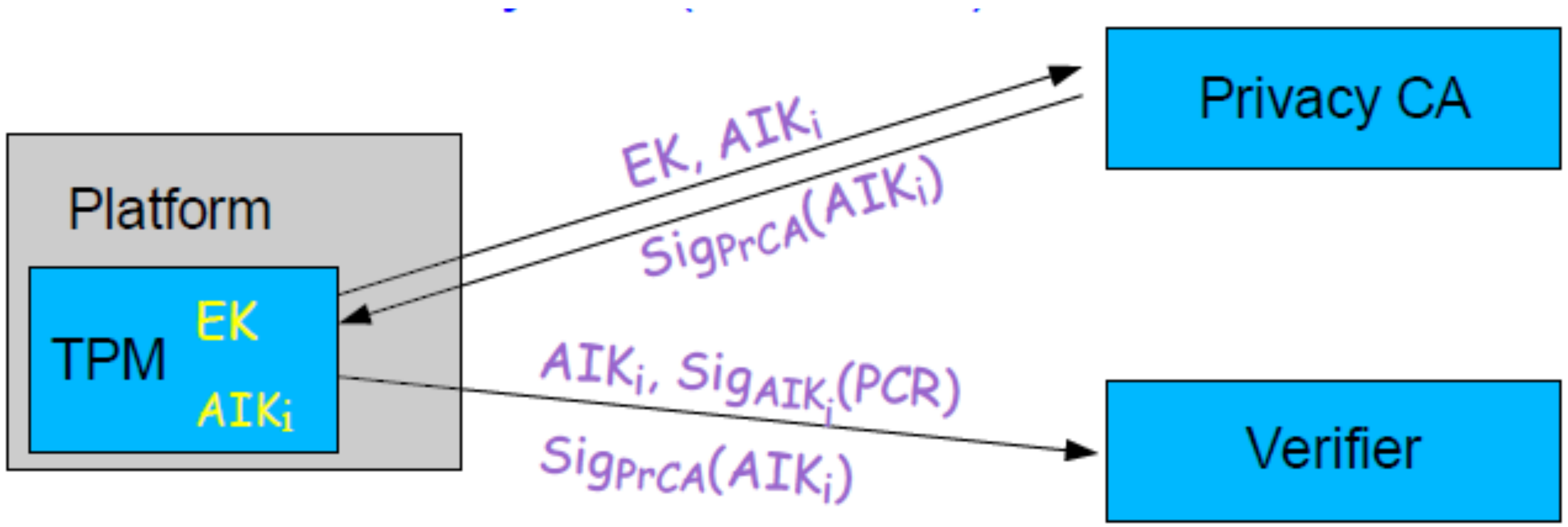
[https://www.bleepingcomputer.com/news/security/researchers-detail-two-new-attacks-on-tpm-chips/]

Attestation problem

- Attestation: To show this is a valid tpm, and has expected valid PCR values (w.r.t valid executed codes)
    - i.e., authenticate as valid TPM to third party verifiers and then provide signatures on PCR values

TPM 1.1 attestation protocol

S4Lab



- Use / generate different keys (AIKi) per verifier.
- Privacy CA needs to be involved in every transaction and thus highly available.
- Highly secured (CA) which contradicts availability.
- CA/verifier collusion?
- Privacy concerns.

[Camenisch, J., Direct anonymous attestation: Achieving privacy in remote authentication. In *ZISC Information Security Colloquium, 2004]*

Who owns your device?

Trusted Computing controversies

- When you think about a secure computer, the first question you should ask is "Secure for whom?" [Schnier]
- But the main question is that the device would be "Trusted to whom"?
- Although Large volume of the existing mechanisms for providing trusted platform use TPM-based ideas, there are serious controversies against it.

CBDTPA

S4Lab

Consumer Broadband and Digital Television Promotion Act (2002)

Technological enforcement is necessary because the rights owner does not necessarily trust the customer, yet they would like to have a reasonable level of assurance that the license terms will be complied with even though the content is stored and used on devices that they do not own or control.

[Reid, J., & Caelli, W., DRM, trusted computing and operating system architecture. *Proceedings of the 3rd Australasian Workshop on Grid Computing and e-Research and the 3rd Australasian Information Security Workshop, 2005]*

Consume But Don't Try Programming

☺

Hollings bill, while failing to mention TCPA anywhere in the text of the bill, was written with the specific technology provided by the TCPA in mind for the purpose of mandating the inclusion of this technology in all future general-purpose computing platforms, now that the technology has been tested, is ready to ship, and the BIOS vendors are on side.

[Lucky Green: http://cryptome.org/tcpa-fritz.htm]

Their definition of `security' is controversial; machines built according to their specification will be more trustworthy from the point of view of software vendors and the content industry, but will be less trustworthy from the point of view of their owners.

In effect, the TCG specification will transfer the ultimate control of your PC from you to whoever wrote the software it happens to be running. (Yes, even more so than at present.)

[Ross Anderson, `Trusted Computing' Frequently Asked Questions, 2003]

There's also a lot I don't like, and am scared of. My fear is that Pd will lead us down a road where our computers are no longer our computers, but are instead owned by a variety of factions and companies all looking for a piece of our wallet.

[Schneier, https://www.schneier.com/crypto-gram/archives/2002/0815.html]

Treacherous computing

S4Lab

- In the past, these were isolated incidents. “Trusted computing” would make the practice pervasive. “Treacherous computing” is a more appropriate name, because the plan is designed to make sure your computer will systematically disobey you.
  - In fact, it is designed to stop your computer from functioning as a general-purpose computer. Every operation may require explicit permission.
- The technical idea underlying treacherous computing is that the computer includes a digital encryption and signature device, and the keys are kept secret from you. Proprietary programs will use this device to control which other programs you can run, which documents or data you can access, and what programs you can pass them to.
  - These programs will continually download new authorization rules through the Internet, and impose those rules automatically on your work. If you don't allow your computer to obtain the new rules periodically from the Internet, some capabilities will automatically cease to function.

Richard Stallman

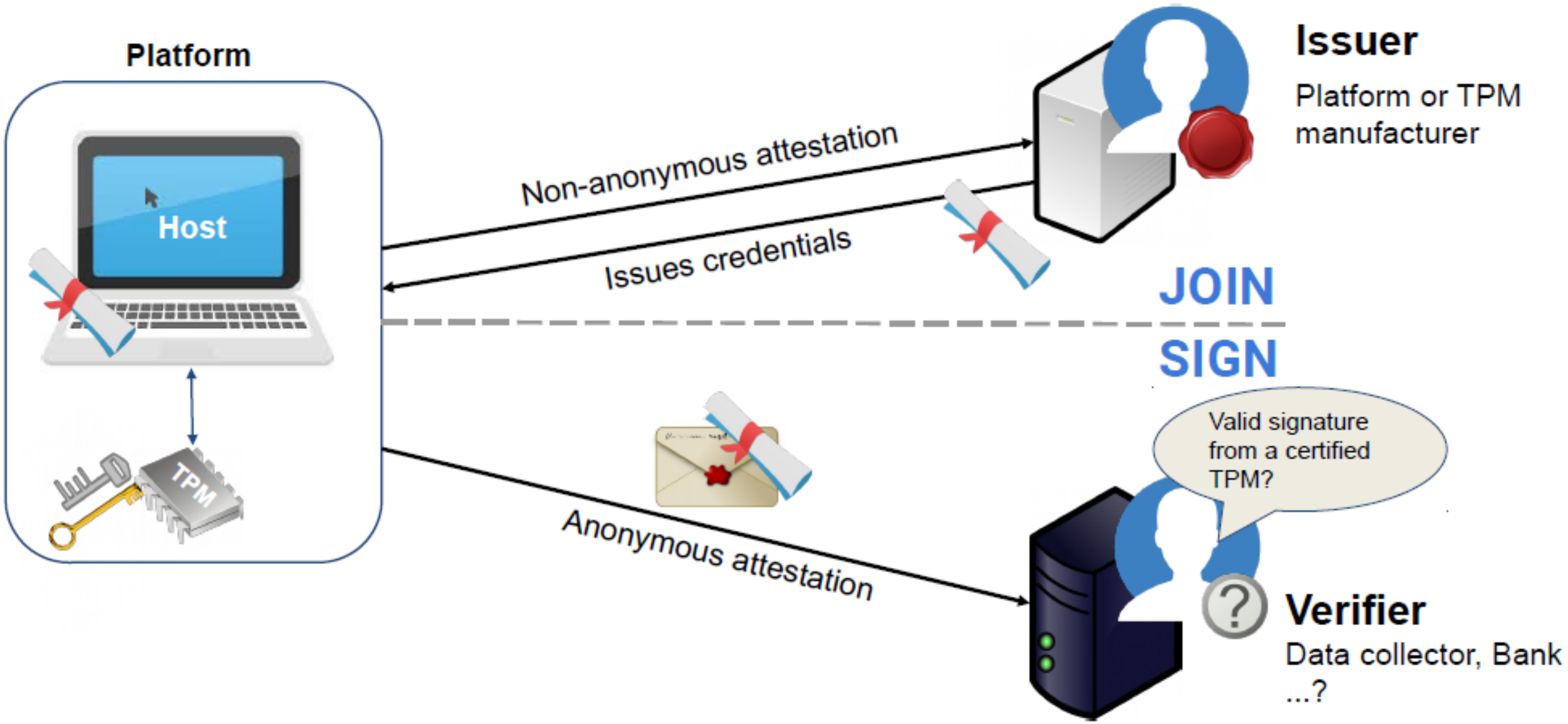
[https://www.gnu.org/philosophy/can-you-trust.en.html]

Direct anonymous attestation (DAA)

- A particular type of privacy-preserving authentication.
- ISO/IEC 20008 specifies anonymous digital signature mechanisms.
- Two categories of anonymous digital signatures mechanisms: using a group public key, and using multiple public keys.
- Common group public verification key associated with many (typically millions) of unique private signature keys.
- Properties of DAA:
  - User-controlled Anonymity
    - Identity of a user cannot be revealed from signature.
  - User-controlled Traceability
    - Host controls whether signatures can be linked

[Casey, M., et al., Direct Anonymous Attestation in the Wild. RWC, 2019]

Direct anonymous attestation (DAA)



[Casey, M., et al., Direct Anonymous Attestation in the Wild. RWC, 2019]

Direct anonymous attestation (DAA)

- TPM 1.2 (RSA-based)
  - ISO/IEC 20008-2 mechanism 2
- TPM 2.0 (pairing-based)
  - ISO/IEC 20008-2 mechanism 4 & ISO/IEC 11889
- Enhanced Privacy ID (EPID)
  - Used by Intel SGX
  - Improved revocation

[Casey, M., et al., Direct Anonymous Attestation in the Wild. RWC, 2019]

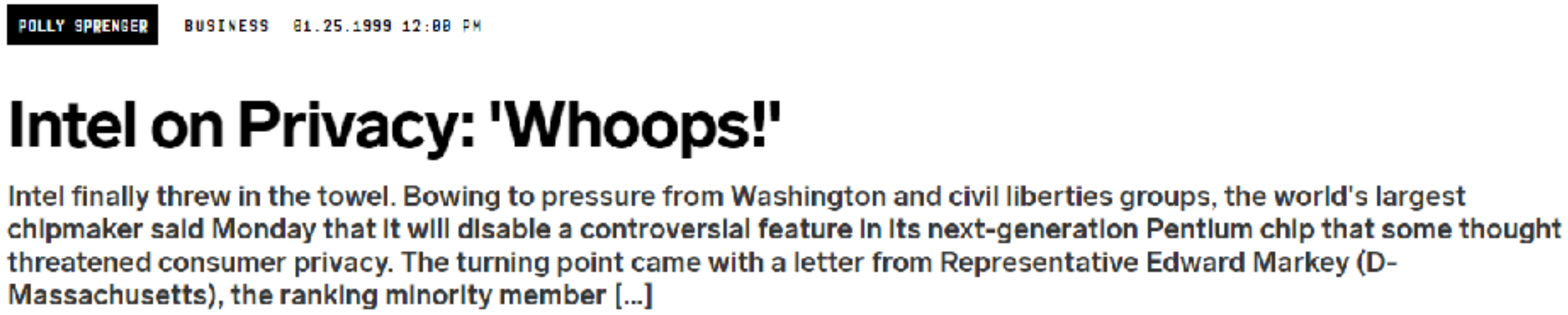
Privacy has cost…

- Because the TPM is a small chip with limited resources, a requirement for direct anonymous attestation was that the operations carried out on the TPM be minimal and, if possible, be outsourced to (software that is run on) the TPM's host.

[Camenisch, J., Direct anonymous attestation explained. IBM Research, 2007]

Intel’s EPID

- Enhanced Privacy Identification (EPID) is an extension of DAA phenomenon with added revocation and based on ISO 20008.
- Implemented by Intel after the Intel’s serial number controversy in 2008.
    - Provides device authentication in an Enterprise. Instead of forgeable MACs!
    - Intel fuses a 512 bit number directly into a submodule of the processor called the Management Engine.



POLLY SPRENGER BUSINESS 01.25.1999 12:00 PM

Intel on Privacy: 'Whoops!'

Intel finally threw in the towel. Bowing to pressure from Washington and civil liberties groups, the world's largest chipmaker said Monday that it will disable a controversial feature in its next-generation Pentium chip that some thought threatened consumer privacy. The turning point came with a letter from Representative Edward Markey (D-Massachusetts), the ranking minority member [...]

[https://www.wired.com/1999/01/intel-on-privacy-whoops/]

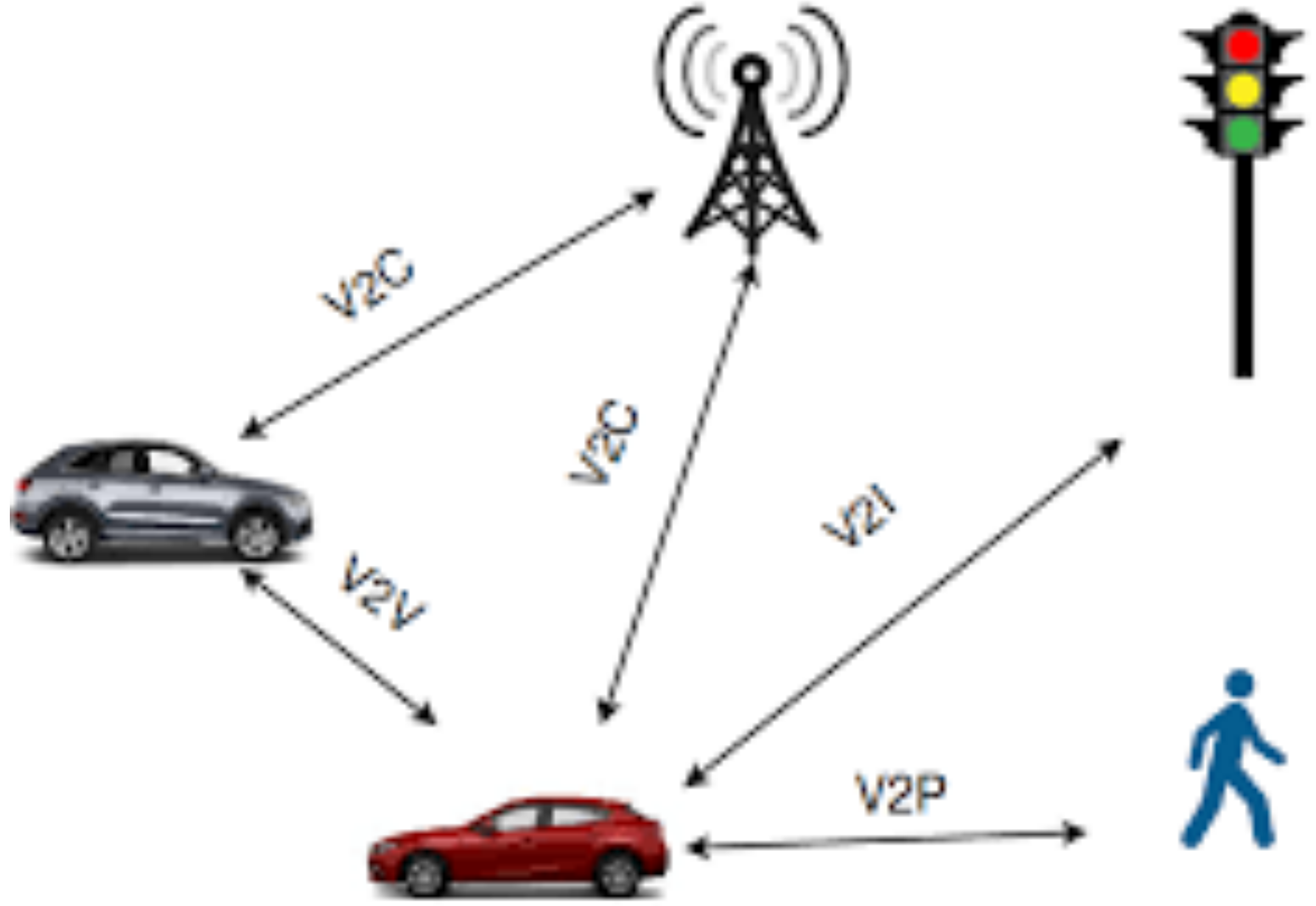
Intel’s EPID example use

- Device generates, stores, and uses keys in a protected environment.
- Used to establish login keys with many institutions.
- Institution knows that login keys are protected.
- Member knows that a compromise at one institution does not affect his security or privacy at any other institution.

[https://csrc.nist.gov/csrc/media/events/meeting-on-privacy-enhancing-cryptography/documents/brickell.pdf]

Are you still thinking only about your laptop?

- Important in V2X use-cases
- Crypto mining
- ....



[Image: https://itea3.org/project/appstacle.html]

Opt-in policy

- In 2005, the Trusted Computing Group (TCG) published guidance to preserve user privacy as well as user control of their computing platform environment, among other things.
- Vendors implemented opt-in for Trusted Platform Modules (TPMs) in a variety of ways, with several major vendors delivering platforms to end users with Trusted Platform Modules (TPMs) turned off.
- This inconsistency discouraged application developers from taking advantage of the TPM to enhance security in their products and systems.
- TPM 2.0 no Opt-in/Opt-out mechanism in specification.

[https://trustedcomputinggroup.org/resource/the-case-for-turning-on-trusted-platform-modules/]

Discrete vs integrated TPMs

- Historically, TPMs have been discrete chips soldered to a computer's motherboard.
- Such implementations allow the computer's original equipment manufacturer (OEM) to evaluate and certify the TPM separate from the rest of the system.
- Although discrete TPM implementations are still common, they can be problematic for integrated devices that are small or have low power consumption.
- Some newer TPM implementations integrate TPM functionality into the same chipset as other platform components while still providing logical separation similar to discrete TPM chips.
- Which is better?

[https://trustedcomputinggroup.org/resource/the-case-for-turning-on-trusted-platform-modules/]

TPM for the innocent secondary uses!

- As of 2015, treacherous computing has been implemented for PCs in the form of the “Trusted Platform Module”.
- For practical reasons, the TPM has proved a total failure for the goal of providing a platform for remote attestation to verify Digital Restrictions Management.
- Companies implement DRM using other methods.
- At present, “Trusted Platform Modules” are not being used for DRM at all, and there are reasons to think that it will not be feasible to use them for DRM.
- Ironically, this means that the only current uses of the “Trusted Platform Modules” are the innocent secondary uses—for instance, to verify that no one has surreptitiously changed the system in a computer.

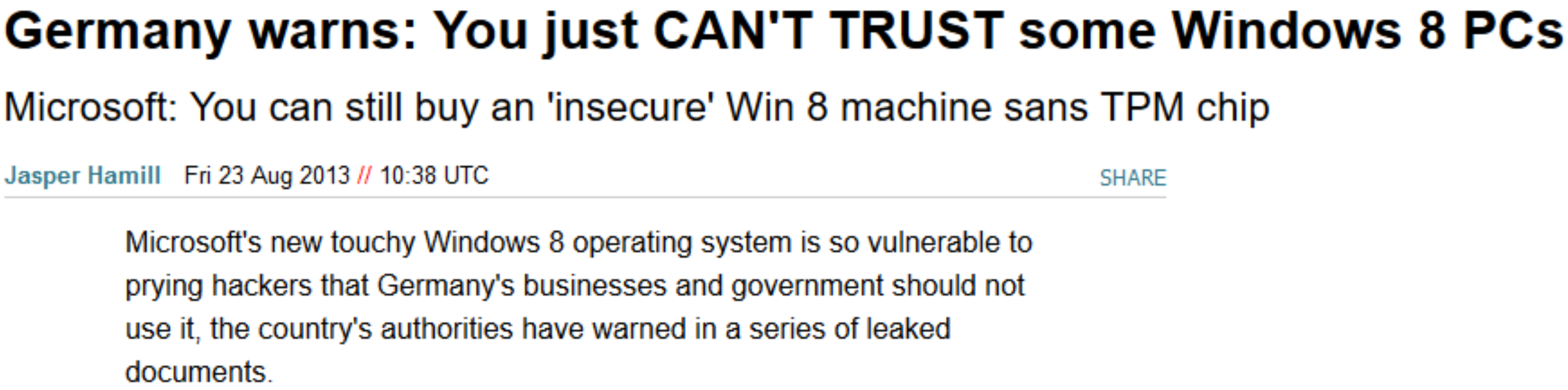
[https://www.gnu.org/philosophy/can-you-trust.en.html]

TPMs in the real world

- File/disk encryption: BitLocker, IBM, HP, Softex
- Attestation for enterprise login: Cognizance, Wave
- Client-side single sign on: IBM, Utimaco, Wave

[crypto.stanford.edu/cs155old/cs155-spring08/lectures/08-TCG.ppt]

Case of Germany



Germany warns: You just CAN'T TRUST some Windows 8 PCs

Microsoft: You can still buy an 'insecure' Win 8 machine sans TPM chip

Jasper Hamill Fri 23 Aug 2013 // 10:38 UTC SHARE

Microsoft's new touchy Windows 8 operating system is so vulnerable to prying hackers that Germany's businesses and government should not use it, the country's authorities have warned in a series of leaked documents.

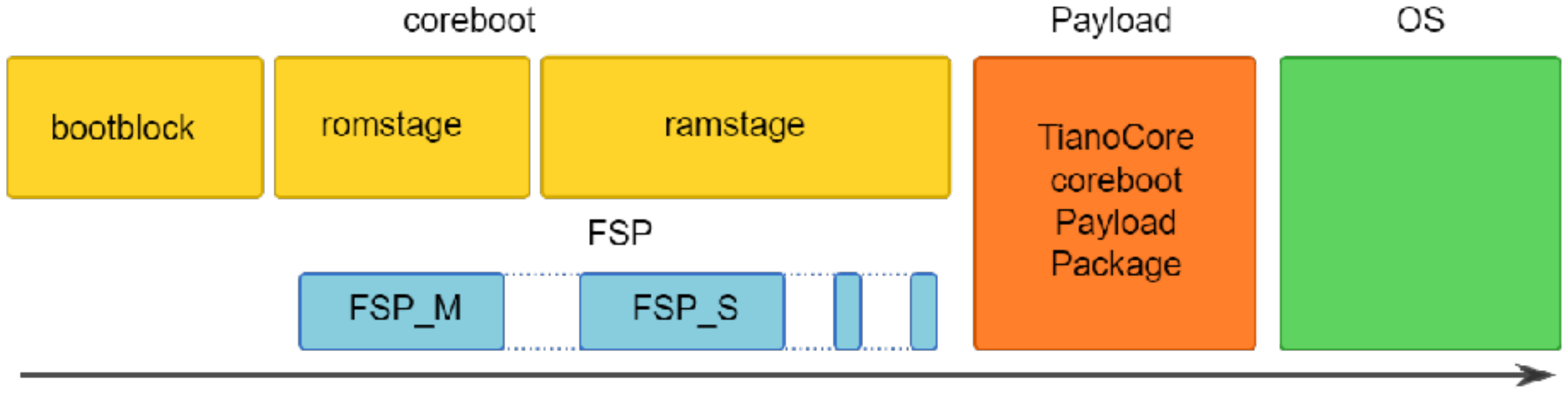
- The use of 'Trusted Computing' technique in this form...is unacceptable for the federal administration and the operators of critical infrastructure.
- BSI (i.e. Federal Office for Information Security):
  - The use of Windows 8 in combination with a TPM 2.0 is accompanied by a loss of control over the operating system and the hardware used.

[https://www.theregister.com/]

Other requirements to have a trusted platform?

- The basic idea for the trusted computing is that we can have trusted platform if we can verify/check that the system has been booted/initialized with a trusted state.
- So assuming the initialization is tamper-proof (which is not☹), what about other requirements?
  - OK, we trust that the stored boot code has been loaded, but how to trust to the initial firmware it self ??
  - How to provide run-time trust?

TianaCore story…



- No trust to Intel CPU boot process
  - proprietary Intel firmware
- Boot process is a multi-stage complex process.
- Usually requires firmware blobs for Chipset initialization and such other extremely low-level hardware specific code implemented by vendors.
- TianoCore is Intel's open source implementation of UEFI interfaces, good?
  - Only parts of the boot process are open sourced.
- So why don’t you use open source firmware alternatives?
- Unfortunately they also rely on these blobs!

[http://silicone.homelinux.org/2018/04/11/inside-an-open-source-bios/]

Really Trusted Boot process

S4Lab

- Need a true open-source board?
- Look for true open-source hardware!

27 Oct 2015 | 21:00 GMT

Novena: A Laptop With No Secrets

How we built a laptop with nothing but open-sourced hardware and software

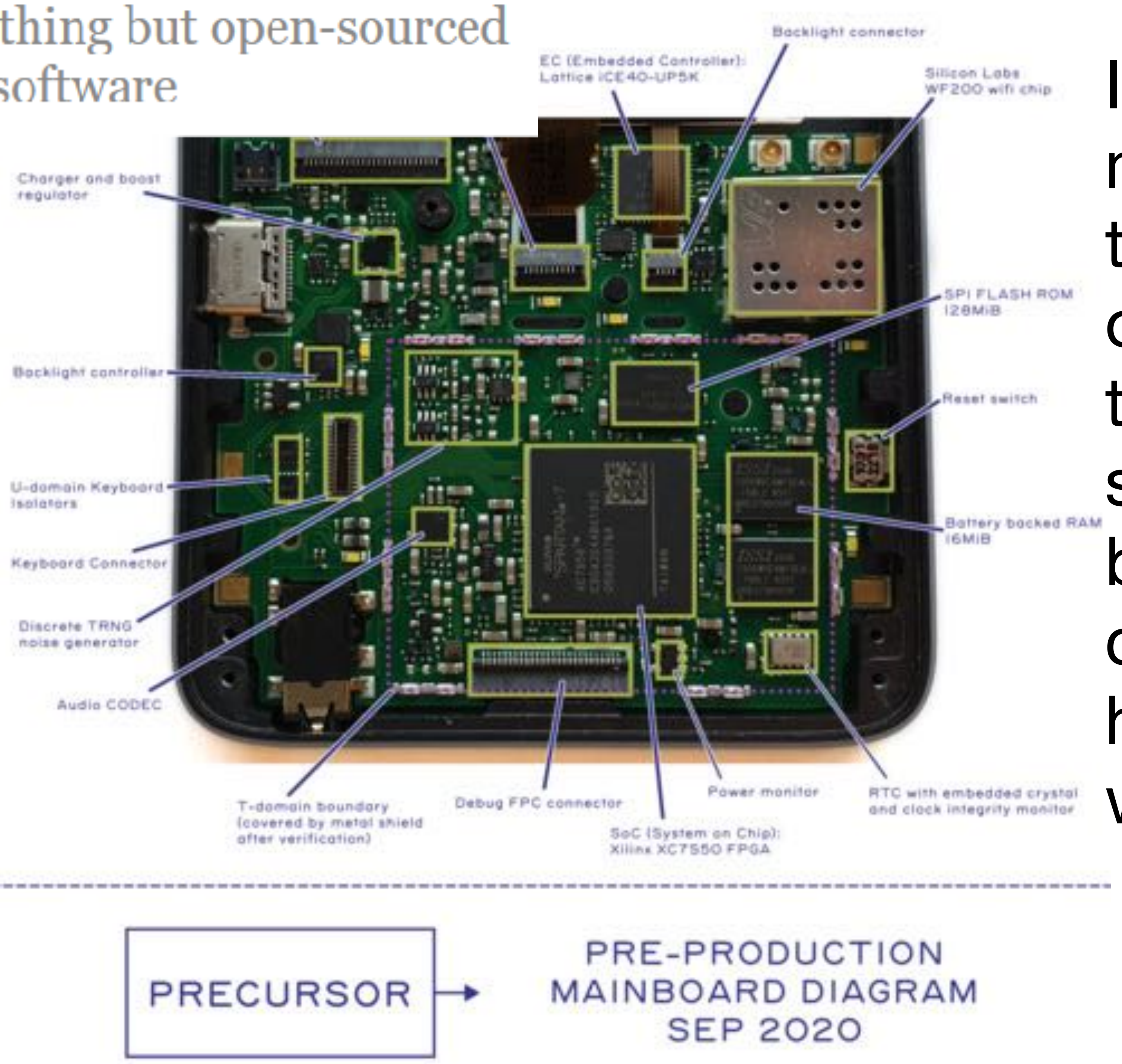
Librem 5 USA

$1,999.00

Librem 5 USA, a premium version of the
focuses on security by design and privac
default with a secure supply chain and el
USA. Outfitted with hardware kill switche
designed hardware, you are in control of
information. **Learn more about the Libr**

Place your order now, get in a few month
Librem 5 USA Announcement
Librem 5 Evergreen Update

Price. **$1,999.00**



PRE-PRODUCTION
MAINBOARD DIAGRAM
SEP 2020

If anything, the process of building Novena made me acutely aware of how little we could trust anything. As we vetted each part for openness and documentation, it became clear that you can't boot any modern computer without several closed-source firmware blobs running between power-on and the first instruction of your code. Critics on the Internet suggested we should have built our own CPU and SSD if we really wanted to make something we could trust

[https://www.bunniestudios.com/blog/?p=5706]

opentitan

- First open source project for silicon root of trust (RoT) chips.
- The lowRISC Ibex.

- Based on what you have learned (and read about precursor), what can you say about the processor?

opentitan

- First open source project for silicon root of trust (RoT) chips.
- The lowRISC Ibex.
- Based on what you have learned (and read about precursor), what can you say about the processor?

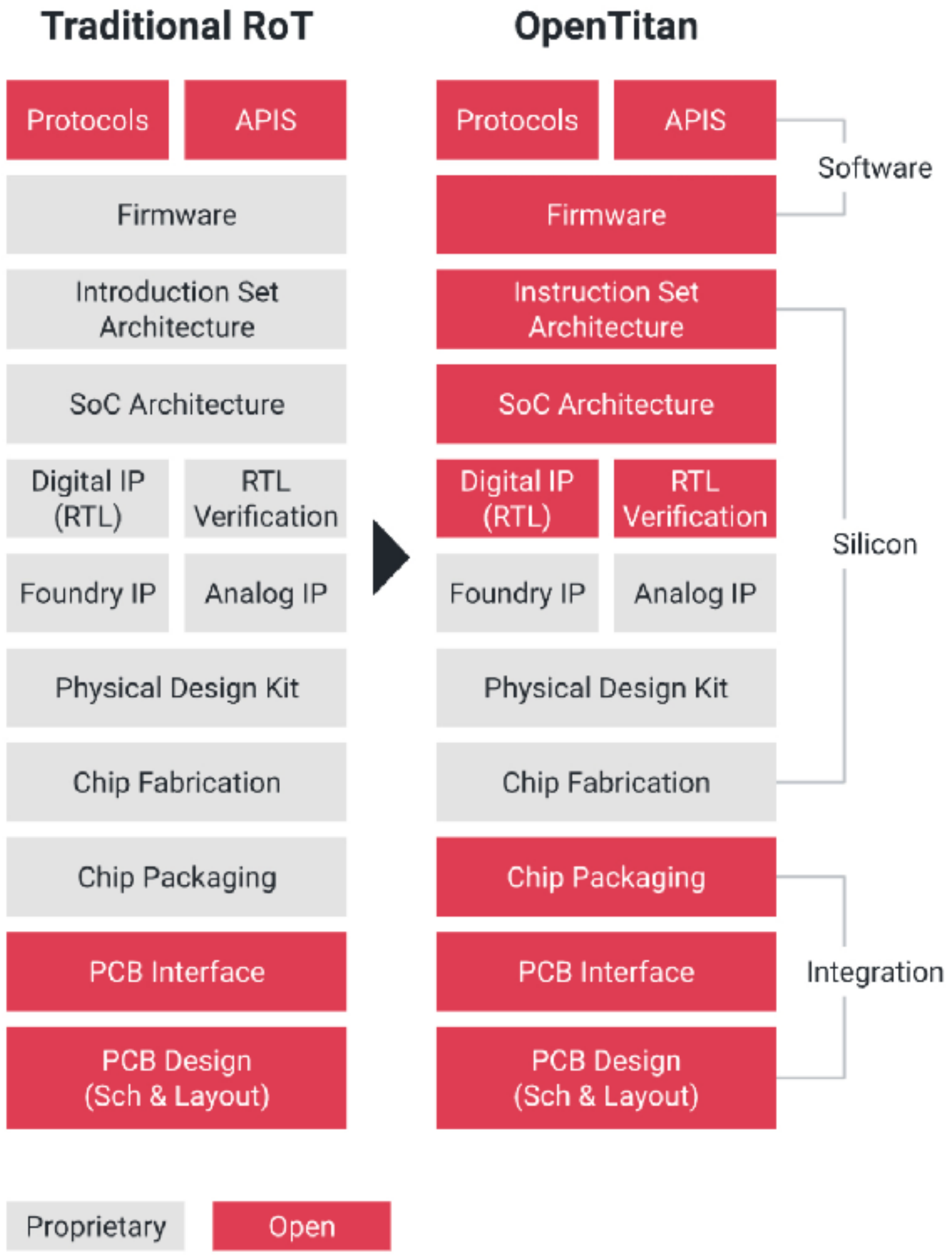
- Should have open ISA.
- RISC-V-based
- Fully open source?

[https://venturebeat.com/2019/11/05/google-announces-opentitan-an-open-source-silicon-root-of-trust-project/]

opentitan

- First open source project for silicon root of trust (RoT) chips.
    - The lowRISC Ibex.
- Based on what you have learned (and read about precursor), what can you say about the processor?

- Should have open ISA.
- RISC-V-based
- Fully open source? NO
- We will discuss further in supply chain session.



Traditional RoT	OpenTitan	
🟥 Protocols	🟥 Protocols	Software
🟥 APIS	🟥 APIS	
⬜ Firmware	🟥 Firmware	
⬜ Introduction Set Architecture	🟥 Instruction Set Architecture	Silicon
⬜ SoC Architecture	🟥 SoC Architecture	
⬜ Digital IP (RTL)	🟥 Digital IP (RTL)	
⬜ RTL Verification	🟥 RTL Verification	
⬜ Foundry IP	⬜ Foundry IP	
⬜ Analog IP	⬜ Analog IP	
⬜ Physical Design Kit	⬜ Physical Design Kit	
⬜ Chip Fabrication	⬜ Chip Fabrication	
⬜ Chip Packaging	🟥 Chip Packaging	Integration
🟥 PCB Interface	🟥 PCB Interface	
🟥 PCB Design (Sch & Layout)	🟥 PCB Design (Sch & Layout)	

⬜ Proprietary 🟥 Open

[https://venturebeat.com/2019/11/05/google-announces-opentitan-an-open-source-silicon-root-of-trust-project/]

Current State

S4Lab

- Current Trusted Computing technologies focus on establishing trust.
  - But how to maintain trust in dynamically changed environments still lacks deep-insight study.

[https://lists.aisnet.org/pipermail/aisworld_lists.aisnet.org/20170930/027582.html]

Reading

- Reardon, J., Basin, D., & Capkun, S., Sok: Secure data deletion. IEEE symposium on security and privacy, 2013.
- Bootkits: past, present & future, https://www.virusbulletin.com/virusbulletin/2014/11/paper-bootkits-past-present-amp-future

Questions?