FIPS 140, Quo Vadis?

Apostol Vassilev, Ph.D.
Research Lead - STVM, CSD, NIST

(Washington, DC, March 24, 2016)

Acknowledgments

- **Many of the ideas in this presentation are the result of close collaboration with my NIST colleagues**

  - **Michael Cooper**
  - **Melanie Cook**

Some facts about FIPS 140

- FIPS 140-1 was issued on January 11, 1994
  - developed by a government and industry working group
  - NIST established the Cryptographic Module Validation Program

The New York Times

Essay; Sink the Clipper Chip

By WILLIAM SAFIRE
Published: February 14, 1994

Of Privacy and Security: The Clipper Chip Debate

By PETER H. LEWIS
Published: April 24, 1994

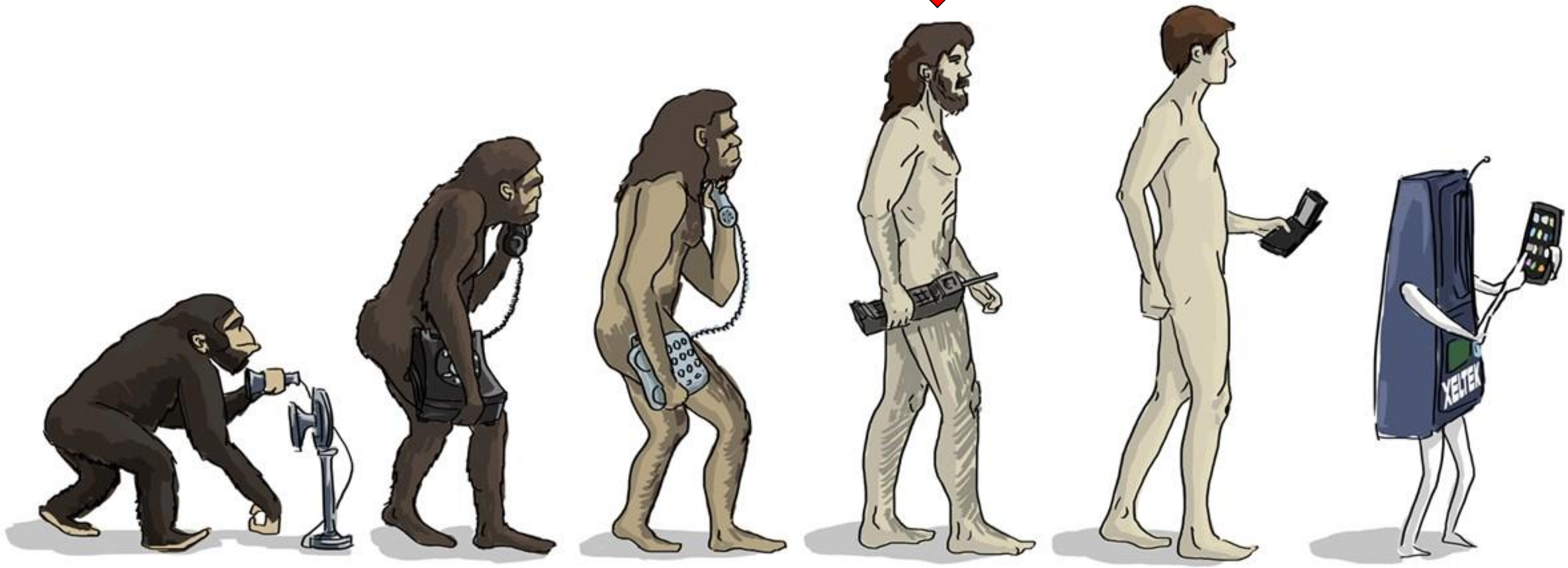
FLAW DISCOVERED IN FEDERAL PLAN FOR WIRETAPPING

By JOHN MARKOFF
Published: June 2, 1994

Battle of the Clipper Chip

By Steven Levy;
Published: June 12, 1994

1994



More facts about FIPS 140

- **FIPS 140-2 was issued on May 25, 2001**
  - **only very modest changes compared to predecessor**
  - **same year when AES became a standard**
- **FISMA-2002 removed the statutory provision that allowed agencies to waive mandatory FIPS**

Observation

It is hard for an essentially unchanged security standard and validation program to capture well the incredibly fast evolving domains of cybersecurity and cryptography.

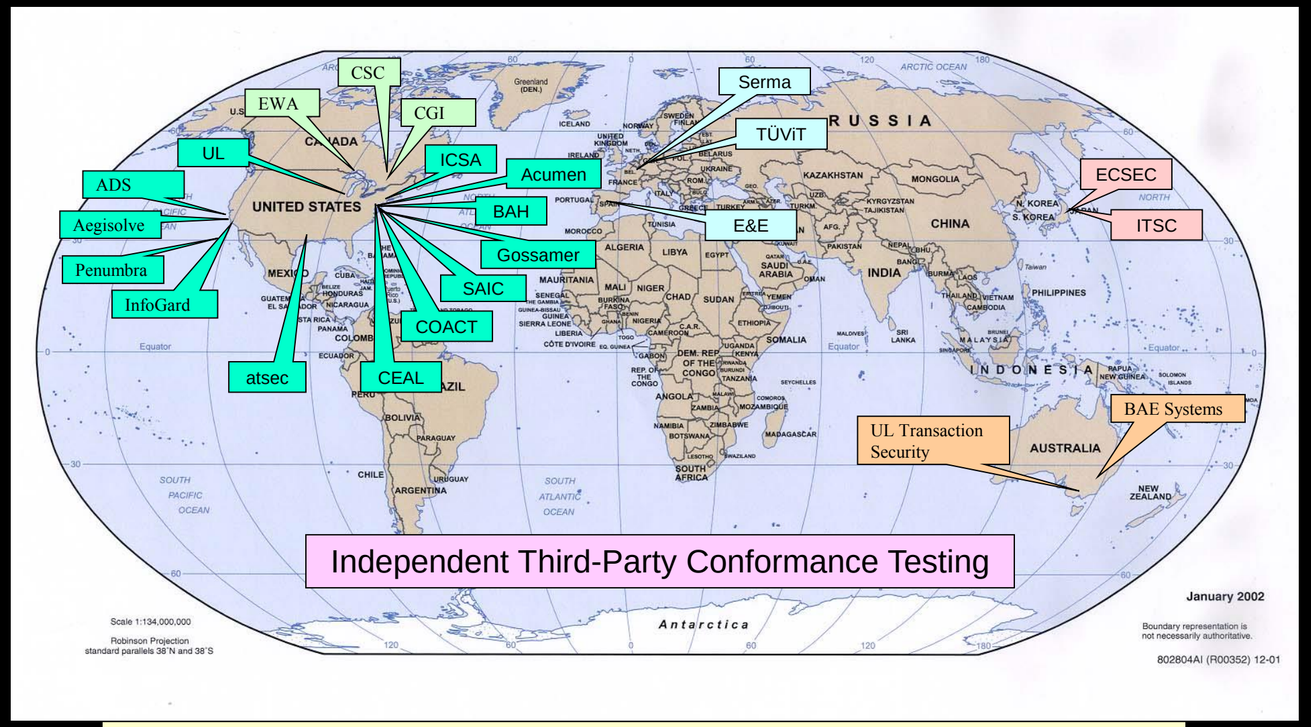
Some background on the CMVP

MISSION:

Improve the security and technical quality of cryptographic modules employed by Federal agencies (U.S. and Canada) and industry by

- **developing standards;**
- **researching and developing test methods & validation criteria;**
- **leveraging accredited independent third-party testing laboratories**

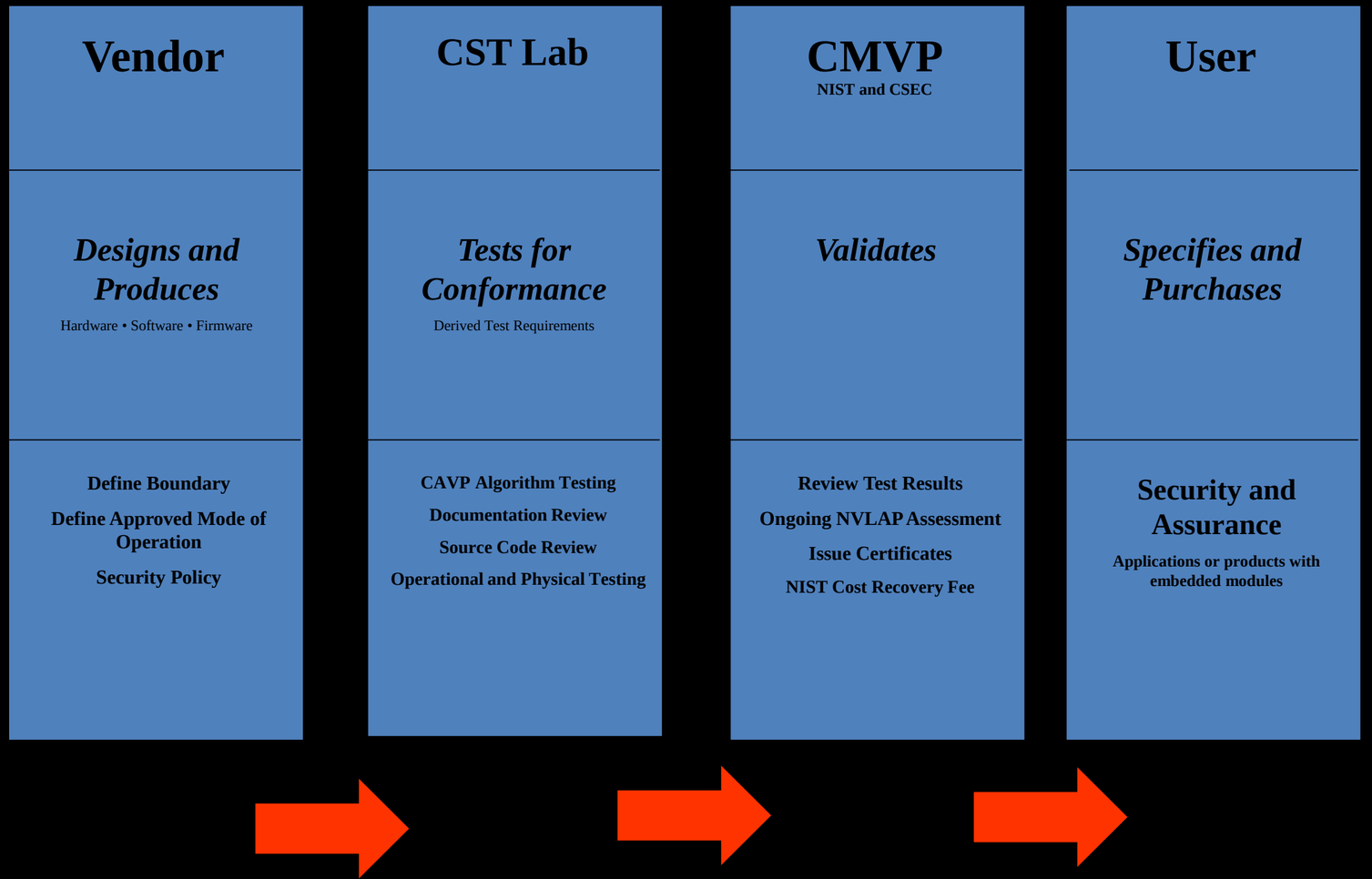
International footprint of CMVP



Development of standards, test artifacts, proficiency exams and training

NVLAP HB 150-17: Cryptographic and Security Testing

CMVP Testing and Validation



The party of four

Govt. Agencies

CMVP

FIPS 140-2 Validation Certificate

The National Institute of Standards and Technology of the United States of America

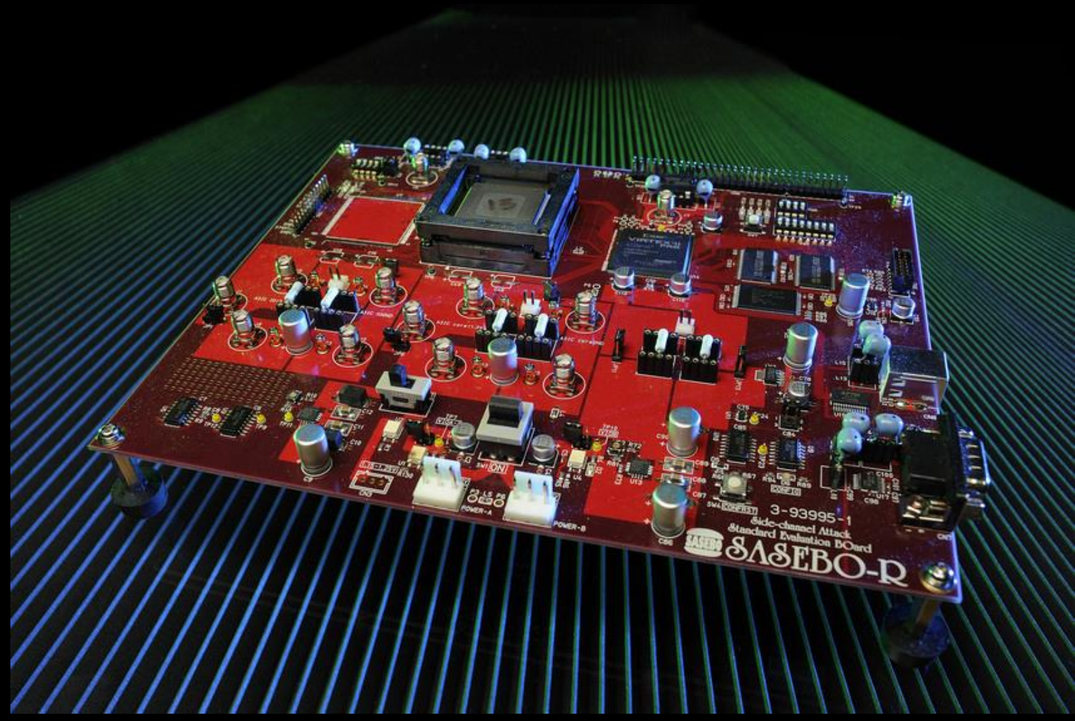
Certificate No. xxx

The Communications Security Establishment of the Government of Canada

CST Labs

Industry perspectives on CMVP

- long review cycles
  - well beyond product cycles
  - costly and rigid
    - updating validated modules is hard
    - automating review workflow helps but not enough
- security test requirements
  - software is <u>not</u> covered well
  - hardware security testing has not kept up with state-of-the-art e.g., <u>low-cost</u> fault injection



- relationship w/ other Government Programs
  - e.g., NIAP and CC

CMVP and CST Labs

- **Labs burdened with labor-intensive and ineffective test methodology**
  - **having trouble testing in depth, according to the state-of-the-art in security testing**
  - **the English essay model**

- **Concerns with Labs' competency in challenging technical areas, e.g.,**
  - **entropy & physical security testing**
    competency <u>unevenly</u> distributed among labs

- **Concerns with Labs' ability to avoid conflicts of interest**

The metamorphosis effect

Module validated <u>without</u> a single implementation change

Test report review uncovers <u>significant</u> discrepancies

documentation-only metamorphosis

A systemic problem casting doubts on security assurances due to lack in trust in laboratory testing

Agencies and CMVP

- long review cycles
  - slowing down adoption of latest technology

- difficult-to-use validation results
  - difficult-to-read validation certificates
    - caveats, operational environment versioning, etc;
    - some improvements help but more is needed
  - confusing configuration instructions in Security Policies

- inability to get FIPS 140-2 compliance assurance on platforms of interest
  - tested module configurations do not match real platforms

A look at the challenges ahead

- **The economy of cybersecurity slow to emerge**

a market failure in cybersecurity
www.economist.com/sites/default/files/20140712_cyber-security.pdf

<u>main reason</u> - the way computer code is produced

Automotive industry experience

- A useful example

  - turning car safety into a competitive advantage

the Volvo effect

IT SHOULDN'T TAKE AN ACT OF CONGRESS TO MAKE CARS SAFE.

Volvo was committed to safety long before it became mandatory.

In 1956, for example, we installed padded dashboards: 12 years before the government insisted on them.

In 1959, Volvo became the first mass-produced car in the world with safety belts as standard equipment. Nine years later all cars had safety belts, inspired by Federal regulations.

We don't just settle for the legal minimum, either:

The law says all cars must have two brake circuits. Volvos have two *triangular* circuits, each controlling three wheels. So if one circuit fails, you still have about 80% of your braking power.

Volvos also have many safety features not required by law:

Like front and rear ends which absorb the impact of collisions. Four-wheel disc brakes with a pressure-proportioning valve to reduce the chances of rear-wheel lock-up. Child-proof rear doors. Rear window defrosters.

Now who would you rather buy a car from?

A company that builds a safe car because someone else made them do it?

Or a company that builds a safe car because their conscience made them do it?

VOLVO

Putting it all together

- Monty Python:
  The Royal Society for putting things on top of other things

Changing standards

- **NIST is considering adopting ISO 19790 as FIPS 140-3**
  - **comment period closed on September 28, 2015**

  - **currently analyzing the received feedback**

- **Provides a <u>rare</u> opportunity to reorganize the CMVP**

Changing the CMVP

NIST intends to continue to specify the cryptographic modules, modes and key management schemes that are acceptable for use by the U.S. Government

Tackle depth and scope of testing

- **leverage mature industrial security development processes like**

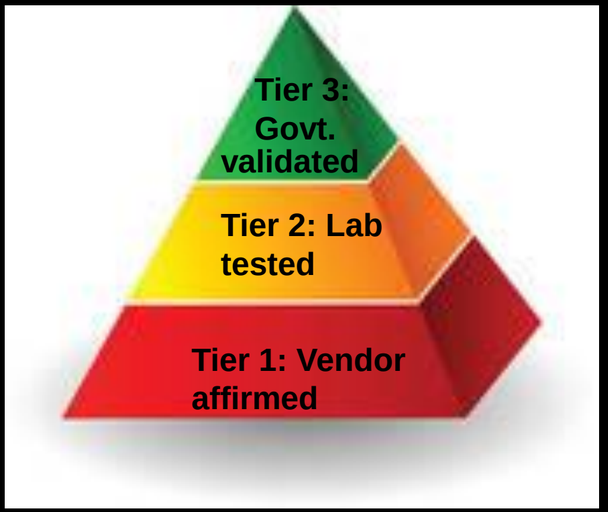
  ISO/IEC 27034 Information technology — Security techniques — Application security

- **reuse vendor test evidence in government validations**
  - **require laboratories to verify evidence, not recreate it 100% independently**
  - **refocus laboratories on testing beyond what is already tested by vendors**

- **develop a measurement criteria for reusing test evidence**

Tackle length of validation testing

- introduce a three-tier assurance model with trusted vendors



- allow companies with mature security development process to participate in Tier 1
  - if not in Tier 1, a company must work with Labs for Tier 2
  - the Volvo effect?
- allows the industry to enter early markets that require Tier 1 or 2
- focused lab testing would help shorten Tier 2 timespan
  - without sacrificing depth and scope of testing

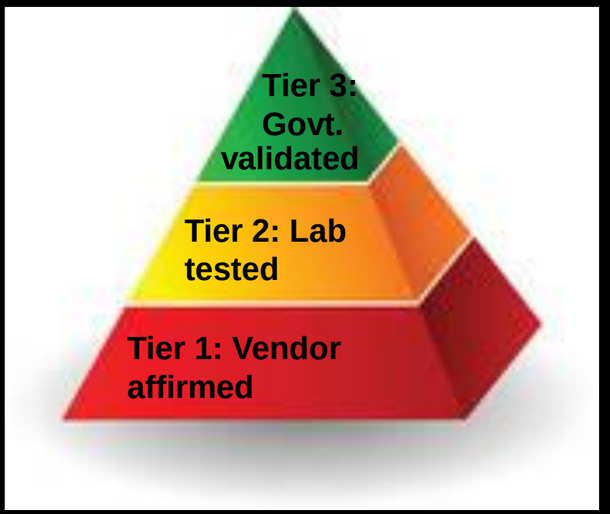
Automate as much as possible

- Reduce the validation cycle length
- Enable Just-In-Time validations
- Reduce the cost of validations

Powerful economic incentives for the industry

3-tier assurance in Federal Govt.

- allows for risk management in timely adoption of new technology



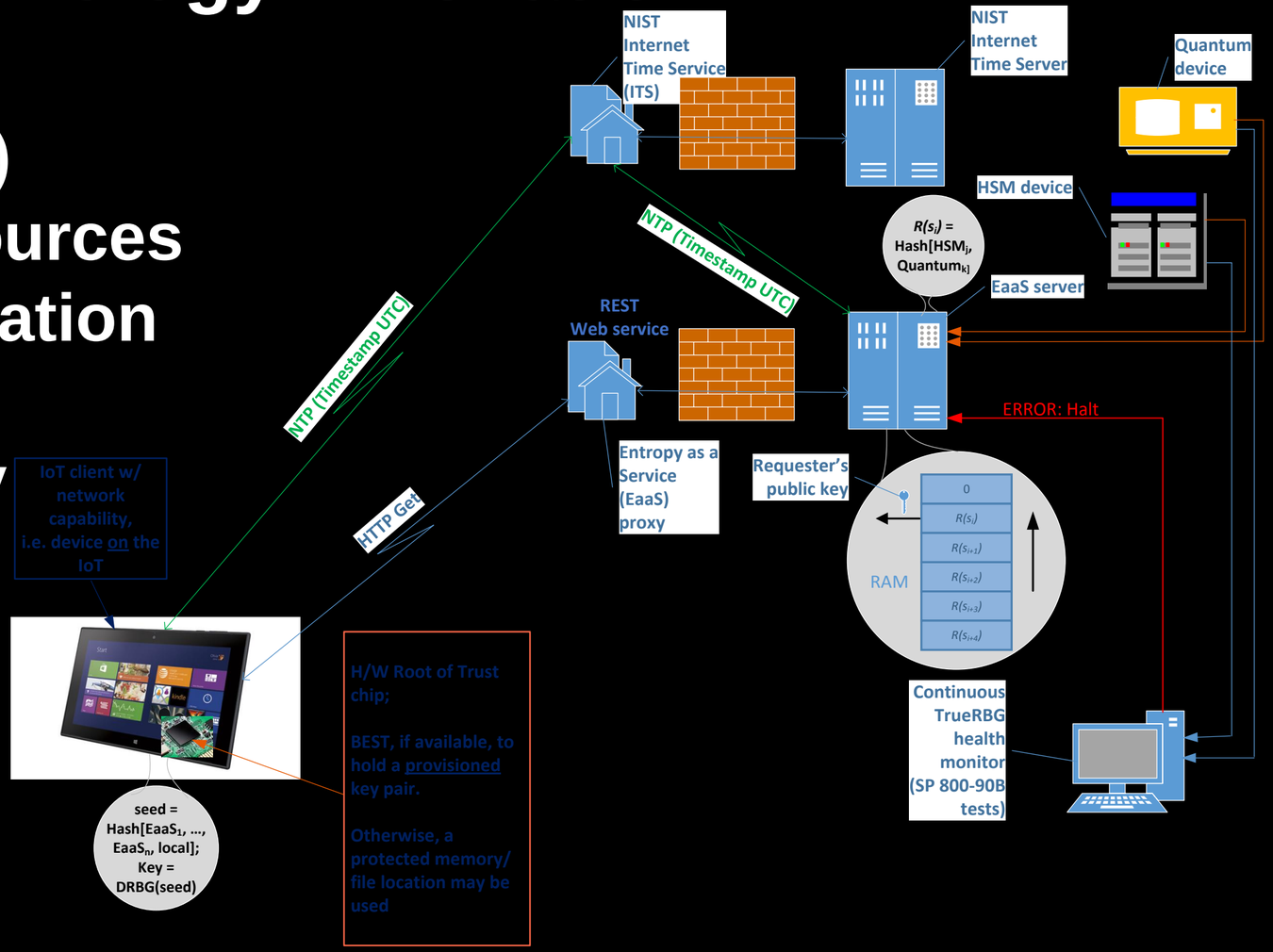
- allows for much shorter cycles of patching validated modules
- promotes proper differentiation of government and national security priorities vs. commercial applications
  - Tier 3 intended for U.S. govt. & national security systems
  - Tier 1 and 2 could be used in other markers where FIPS 140-2 validations are <u>voluntarily</u> used today

Research and Innovation

- **Help the industry meet difficult security requirements through technology innovation**

  - Entropy as a Service (EaaS)
    - leverages known good sources
    - eliminates complex estimation
  - Advanced physical security
  - Working w/ leading academic institutions

    University of Maryland
    KU Leuven, Belgium
    University of Florida



Internationalization of the CMVP

- **Help US industry access to international markets**

  - **Leverage adoption of the ISO standard to establish <u>bilateral</u> partnerships with other validation programs from Asia & Europe**

    - **allow companies to choose the validation authorities they want to target**
    - **<u>not</u> like the mutual recognition in Common Criteria**
    - **retain independence of US program**
  - **Align cryptographic module testing w/ NIAP PP’s**

Where are we today?

- Started an Industry Working Group in December 2015
  - a mix of industry and government participants
  - 36 members so far
    - 17 companies and Open-Source entities, 2 Govt. agencies
  - organized in several working areas led by industry participants
    - great level of participation from all
- Making progress towards the desired goals
  - Proof of concept development and demonstration
    - Automated Cryptographic Validation System
      - demo at ICMC 2016 in May
      - joint effort between NIST and the industry (Cisco)

Questions?