When Cryptography Meets Metrology

Carlos Galhardo* · Luís T. A. N. Brandão[†] · René Peralta

Cryptographic Technology Group, Computer Security Division, National Institute of Standards and Technology

Legal Metrology

In each country, the structure of regulations and enforcement applied to metrology affects the confidence in measurement results.

Legal Metrological Control

Examples of measuring instruments under legal control:

Instrument	Measured quantity	Units	Area
Gas pump	Gasoline volume	m^3	A
Speed trap	Vehicle speed	m/s	B
Gas analyzer	Air pollutant concentration	ppmv	C
Thermometer	Body temperature	K	D

A. Trade   **B.** Safety   **C.** Environment   **D.** Health

Gasoline volume   Vehicle speed   Air pollutant concentration   Body temperature

Image credits (CC BY): A (Anthony Inswasty); B (DeFacto @ wikipedia.org); C (Emmanuel Kwizera); D (NeferJanah Meistrup).
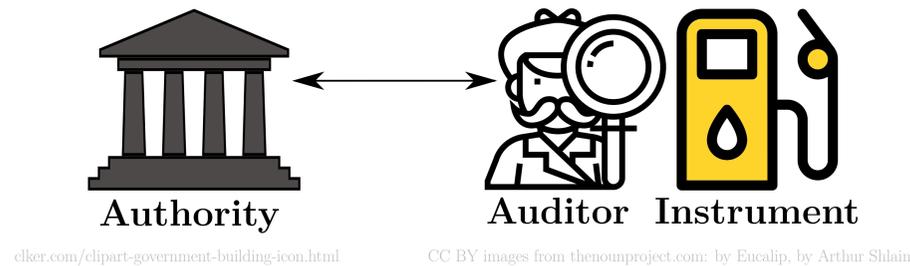
Confidence in measurements

Measurements under legal metrological control should be:

- **Accurate:** agrees with corresponding standard.
- **Reliable:** stable against environmental changes.
- **Incorruptible:** impervious to malicious manipulation.

Metrological verifications

A metrological authority sends auditors to verify instruments in use.

Authority   **Auditor**   **Instrument**

clker.com/clipart-government-building-icon.html   CC BY images from thenounproject.com: by Eucalip, by Arthur Shlain
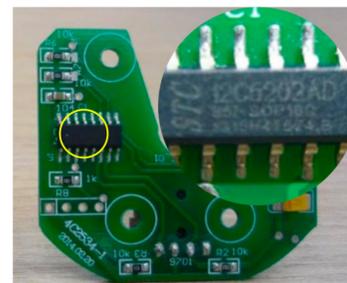
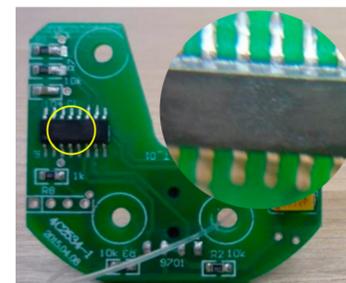## Tampering of measurement sensors

An example seized by auditors during verification (Inmetro, 2019):

- Two circuits of a gas pump volume sensor.
- The only difference is the micro-controller and its **software**.

Source: NIT-Sinst-002 (Inmetro)

(a) Original   (b) Counterfeit

Enhancing verifications

Improved attestation of possession of the original software:

- **Confidentiality:** auditor does not learn the software.
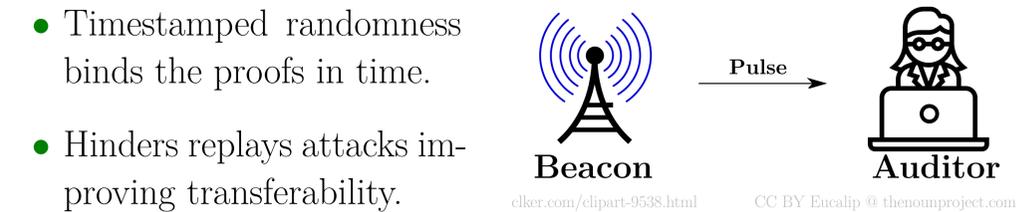- **Freshness:** guarantee timeliness of verifications.

Time for a change of approach

Software replacement is the most recent attack vector. Cryptography technology is available to mitigate them.

Zero-knowledge Device Attestation

Challenge → Response

Auditor   **Instrument**

CC BY images from thenounproject.com: by Eucalip, by Arthur Shlain

- Zero-Knowledge Proof of Knowledge of Discrete Log.
- Proof is transferable, so the authority can check it.

Attestation with the randomness beacon

- Timestamped randomness binds the proofs in time.
- Hinders replays attacks improving transferability.

Pulse →

Beacon   **Auditor**

clker.com/clipart-9538.html   CC BY Eucalip @ thenounproject.com

Social impact

Auditability   **Anti piracy**   **Engagement**

Citizen

clker.com/clipart-consultants.html   clker.com/clipart-15524.html   clker.com/clipart-smartphone-excitement-2.html

The authority can spot malicious auditors.   Counterfeits cannot construct a proof.   Any citizen can use the beacon to act as an auditor.