On-Site Inspections \textit{from} a Distance

The Application of Virtual Proofs of Reality to Nuclear Safeguards And Arms Control Verification

Sébastien Philippe, CVT Associate, Princeton University
2016 Consortium on Verification Technology Workshop, October 19, 2016
CHALLENGES OF NUCLEAR INSPECTIONS

BACKGROUND

TREATIES REQUIRE CREDIBLE INFORMATION-GENERATING MECHANISMS

On-site inspections are a key mechanism for nuclear verification. Often (if not always) a contentious point of negotiations: what is to be inspected and measured? Frequency of inspections? (Political & cultural differences also affect the outcome.)

FINDING ACCEPTABLE TECHNICAL SOLUTIONS IS DIFFICULT

Physical measurements in sensitive locations require trusted equipment. Classical approaches to distant remote verification require classical tamper-proof hardware, cryptographic keys and digital signatures. Requirement of protecting sensitive information.
CHALLENGES OF NUCLEAR INSPECTIONS

BACKGROUND

TREATIES REQUIRE CREDIBLE INFORMATION-GENERATING MECHANISMS

On-site inspections are a key mechanism for nuclear verification.

Often (if not always) a contentious point of negotiations: what is to be inspected and measured? Frequency of inspections?

(Political & cultural differences also affect the outcome.)

FINDING ACCEPTABLE TECHNICAL SOLUTIONS IS DIFFICULT

Physical measurements in sensitive locations require trusted equipment.

Classical approaches to distant remote verification require classical tamper-proof hardware, cryptographic keys and digital signatures.

Requirement of protecting sensitive information.
“Virtual Proofs of Reality offer a way to prove physical statements remotely without using classical tamper-resistant hardware and cryptographic keys.”
How to Construct Virtual Proofs of Reality?
Step 1: Turning Sensors into Physical One-Way Functions
PHYSICAL UNCLONABLE FUNCTIONS (PUFs) ARE THE PHYSICAL EQUIVALENT OF ONE-WAY FUNCTIONS

\[ R = f_{\text{PUF}}(C) \]

Properties
Easy To Evaluate But Hard To Predict
Easy To Manufacture But Hard To Duplicate
PHYSICAL UNCLONABLE FUNCTIONS
CAN BE EITHER ELECTRONIC OR NON-ELECTRONIC


PHYSICAL UNCLONABLE SENSORS

TURNING PUFS INTO SENSORS - OR VICE VERSA

Physical Quantity (e.g. temperature) \( \theta \)

Challenge \( C \) \( \rightarrow \) PUF \( \rightarrow \) Response \( R \)

\[ R = f_{PUF}(C, \theta) \]

By turning PUFs into Physical Sensors, we can create Challenge-Response pairs dependent on physical quantities.
Step 2: Use Sensor-PUFs in an Interactive Protocol
GENERAL ASSUMPTIONS
INTERACTIVE PROOF BETWEEN PROVER AND VERIFIER IN TWO DIFFERENT LOCATIONS

\[ S_1 \quad \text{Prover} \quad \text{Communication Channel} \quad \text{Verifier} \quad S_2 \]

VIRTUAL PROOF PROTOCOL
SET-UP PHASE

A) For each $k$ prepares $\mathcal{L} = (R_j^i, C_j^i, \Theta_j)$
Where Challenge-Response pairs are constructed for a given physical quantity $\Theta_j$ as

$$R_j^i = F_{WO_k}(C_j^i, \Theta_j)$$
VIRTUAL PROOF PROTOCOL

PROOF PHASE

Transfer Custody of the Witness Object to Prover
VIRTUAL PROOF PROTOCOL

PROOF PHASE

Prover Sends $\theta$

Verifier Sends $C$

Prover Sends $r$

if $r = R^i_j$

$\theta = \Theta_j$

$L = (R^i_j, C^i_j, \Theta_j)$

$c = C^i_j$

Accept Proof

$r = F_{WO_1}(c, \Theta_j)$

OK!
Example 1
A Virtual Proof of Temperature
THE BI-STABLE RING PUF CAN BE TURNED IN A TEMPERATURE SENSOR

A Simplified 4 Inverter Ring Example

Ring forced in unstable state

Stable state A

Stable state B

64-bit BR-PUF

Xilinx Artix-7 FPGA
VP OF TEMPERATURE PROTOTYPE

EXPERIMENTAL RESULTS CONFIRMED PROOF-OF-PRINCIPLE

Example 2
Example 2
A Virtual Proof of Neutron Non-Irradiation
VP OF NEUTRON NON-IRRADIATION
PROVING AN OBJECT HAS NOT BEEN EXPOSED TO NEUTRON

- **Set-up Phase (Verifier):**
  - Preload detector
  - Create CRP-list
  - Transfer detector to Prover

- **Proof Phase:**
  - Prover claim detector hasn’t been exposed to neutrons
  - Verifier send challenge \((z,\theta)\)
  - Prover shine laser at \((z,\theta)\) and send response to Verifier
  - If response sent = expected response from CRP-list, Verifier accept the proof
What Are Potential Applications for Virtual Proofs?
SOME RELEVANT AND POTENTIAL APPLICATIONS

CHALLENGE INSPECTIONS FROM A DISTANCE
Remote and trusted physical measurements (potentially constant monitoring).

CHAIN OF CUSTODY AND CONTINUITY OF KNOWLEDGE
Have treaty accountable items stored in a room been displaced? (freeze scenario)

PERIMETER CONTROL
Have radiation sources or plutonium been taken out of a room/building? (dismantlement)

DATA COMMITMENT
Allowing the Host to review the data first (facilitating imaging protocols)
BEYOND ARMS CONTROL
TRUSTED SENSOR NETWORKS AND IOT
On-site inspections are a key mechanism for nuclear verification. But they are often hard to negotiate. Setting-up remote verification is an alternative but is limited by the ability to insure that data are trustworthy.

Virtual Proofs of Reality offer a way to prove physical statements remotely without using classical tamper-resistant hardware and cryptographic keys. They have potentially important applications in nuclear verification.

TAKE AWAY
ACQUIRING DATA IN PLACES WHERE WE HAVE NO ACCESS
MORE

nuclearfutures.princeton.edu/projects/
sebastienphilippe.org

ACKNOWLEDGEMENTS

U. Rührmair, A. Glaser, B. Barak, M. Kütt & M. McKeown