Hardware Based Security

Gang Qu
University of Maryland, College Park
gangqu@umd.edu

Electronic Design Process Symposium
Milpitas, California, USA
October 3, 2019

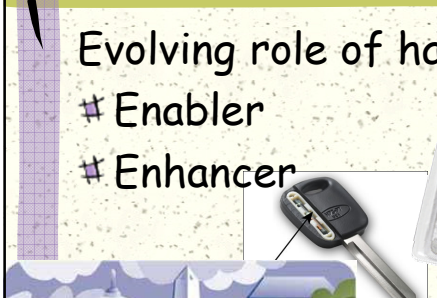
What You Will Hear in This Talk?

- ~~Hardware vulnerabilities, backdoors, IP piracy, Trojans, side channel, fault injection, untrusted supply chain, etc.~~
- Role of hardware in (cyber)security
- Hardware based security
  - Secure the hardware
  - Protect design and IP
  - Hardware security primitives
  - Case studies

Hardware in Security and Trust

Evolving role of hardware in security

- Enabler
- Enhancer



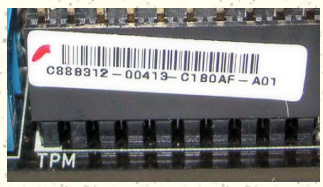
MeshSec Lab

2

Hardware in Security and Trust

Evolving role of hardware in security:

- Enabler
- Enhancer
- Enforcer



MeshSec Lab

Dr. Gang Qu (gangqu@umd.edu)

3

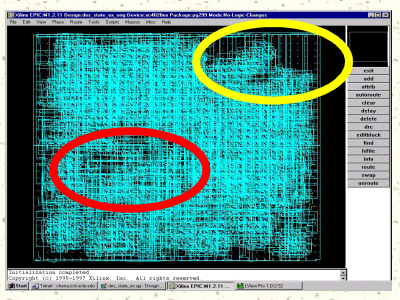
No Secure Hardware by Design

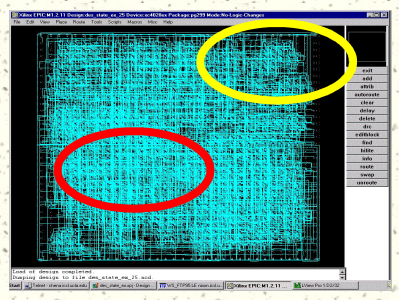
- Physical attacks
- Backdoors
- Side channels
  - Power, current, timing, EM, cache memory, scan chain, output signals, …
- Fault injection attacks
- Recommendations for secure hardware design

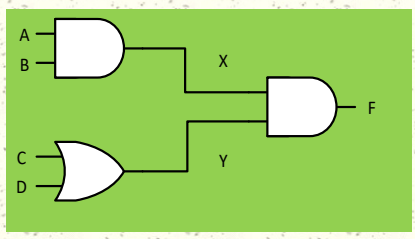
Design IPs Need to be Protected

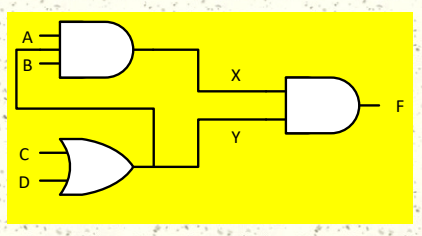
- Unlawful practices:
  - IP stealing, reverse engineering (with bad intend), counterfeiting, overbuilding, …
- Recommendations for IP protection:
  - Law enforcement and legal protection
  - Deterrent techniques
  - Mitigation methods

Digital Watermark & Fingerprint









MeshSec Lab Dr. Gang Qu (gangqu@umd.edu) 6

Hardware Security Primitives

- Trust platform module (TPM)
- Physical unclonable function (PUF)
  - Key generation and storage
  - xRNG
  - Many applications
- Lightweight authentication
  - Applications: IoT devices, embedded systems, mobile devices, sensors, …
  - Target: device, user, data, computation, …

MeshSec Lab Dr. Gang Qu (gangqu@umd.edu) 7

Device Authentication by VoS

- Voltage over-Scaling
  - Reducing V_{dd} is common for reducing power
    - $P=P_{stat}+P_{dyn}=C_{eff}V_{dd}^2f+V_{dd}(I_{sub}+I_{gate})$
    - Quadratic Dependence of Power to V_{dd}
  - Critical Voltage
  - Scaling Below Critical Voltage
    - Error due to path delay
    - Increased delay mean and deviations, causing incorrect computation

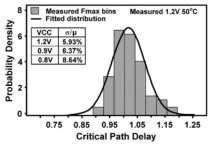
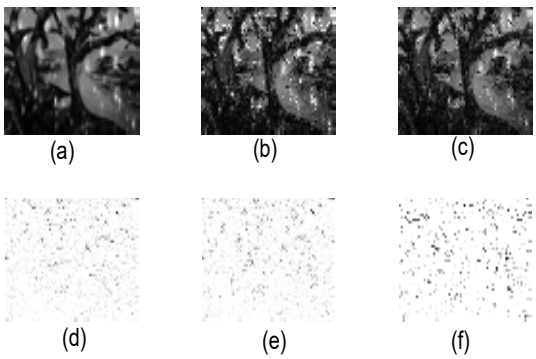
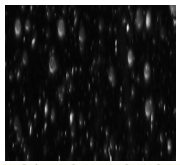


Figure 1: Impact of voltage scaling on path delay distribution. Mean and sigma of delay distribution and number of paths failing to meet target delay increase (80-core processor in 65nm [2]).

Device Authentication by VoS

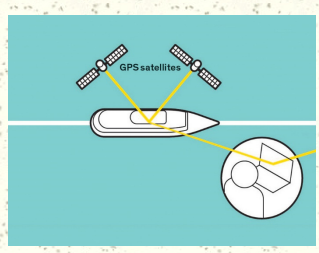
- Elevating variation to high level: VOLtA: Voltage Over-scaling Based Lightweight Authentication





Data Authentication: GPS Spoofing

- GPS spoofing: an effective attack
  - June 2013: *White Rose*



Source: IEEE Spectrum, 2016

  - 2012: *Phasor measurement units in smart grid.*
  - 2011: *Lockhead RQ-170 military drone spoofed and captured by a foreign country*

GPS Spoofing: Protection

- Cryptography
  - Needs decryption or decoding
- Signal-distortion detection
  - Additional signal processing and hardware
- Direction-of-arrival sensing
  - Off-line signal processing hours → 6 seconds
  - Assumes a single attacker

Source: IEEE Spectrum, 2016

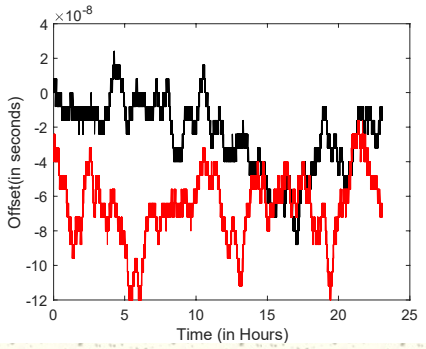
Hardware based Mitigation

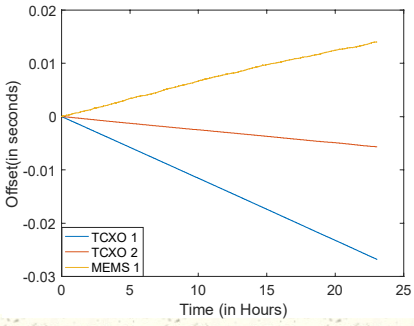
- Idea: Cross-validate with "something" "true" or trusted. → local clock
- 3-phase mitigation
  - Measure the physical properties of a local free-running oscillator/clock.
  - Detect spoofing attack when internal states of the local clock have "sudden" changes.
  - Survive the attack with synchronization solution for timing critical systems.

Why Crystal Oscillators?

- Availability on all GPS receivers
- Intrinsic unclonability
  - Piezo-electric Quartz Crystal
  - Common cutting methods (AT cut, SC cut) are imperfect, → cutting variations → *time offset* that is physically unclonable
- TCXOs (temperature controlled crystal oscillators) are used to correct timing errors due to temperature changes.

Why Crystal Oscillators?



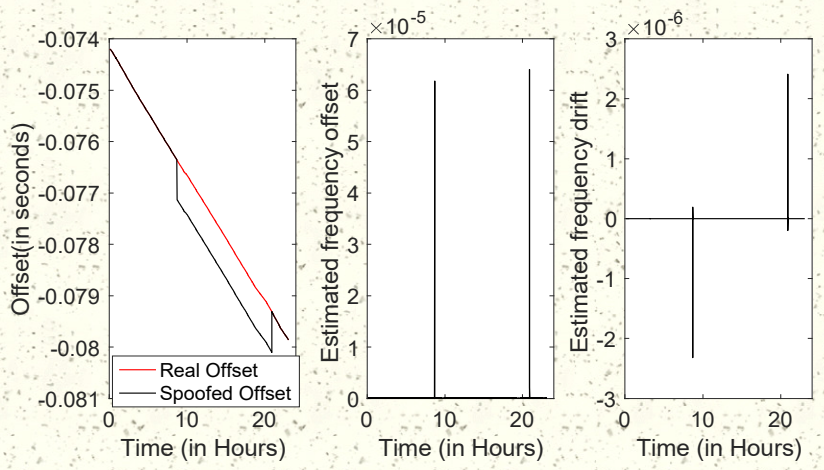


Time offset from two terrestrially received GPS signals (compared with Rubidium clock).

Time offset of commercial crystal oscillators compared with GPS

Key idea: measure this drift (unclonable) against the received GPS signal (untrusted) to detect spoofing.

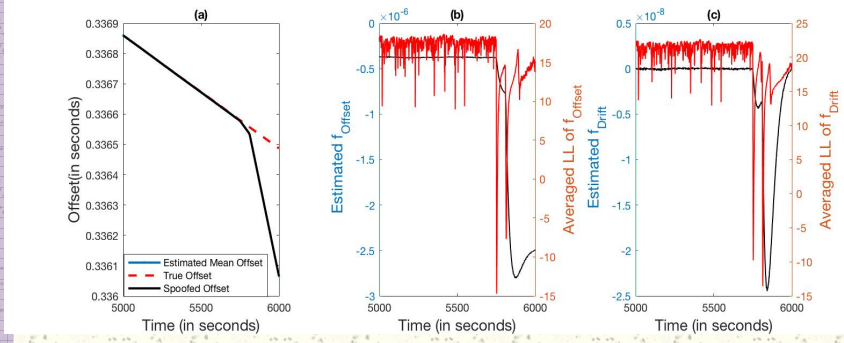
Temporal Shift Injection Attack



Attacker changes the timestamp of the GPS signal by 1%, there will be a significant jump in the free-running local clock (offset and drift).

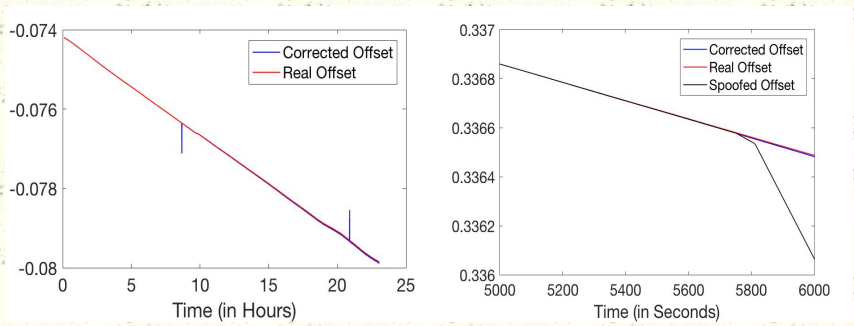
Replay and Meaconing Attack

- Example PMU attack (UT Austin)



(a) Spoofing attack is initiated at 5130 seconds. (b) Estimation of the frequency offset (black curve) and the LL of the frequency offset(red curve) (c) Similar estimation of frequency drift and the LL of the frequency drift. Attack detected when the red curve goes under a given threshold.

Attack Survival



Reconstructing GPS Signal during temporal shifting attack

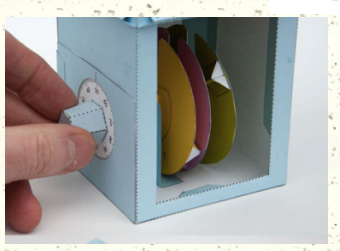
Reconstructing GPS Signal during replay and meaconing attack

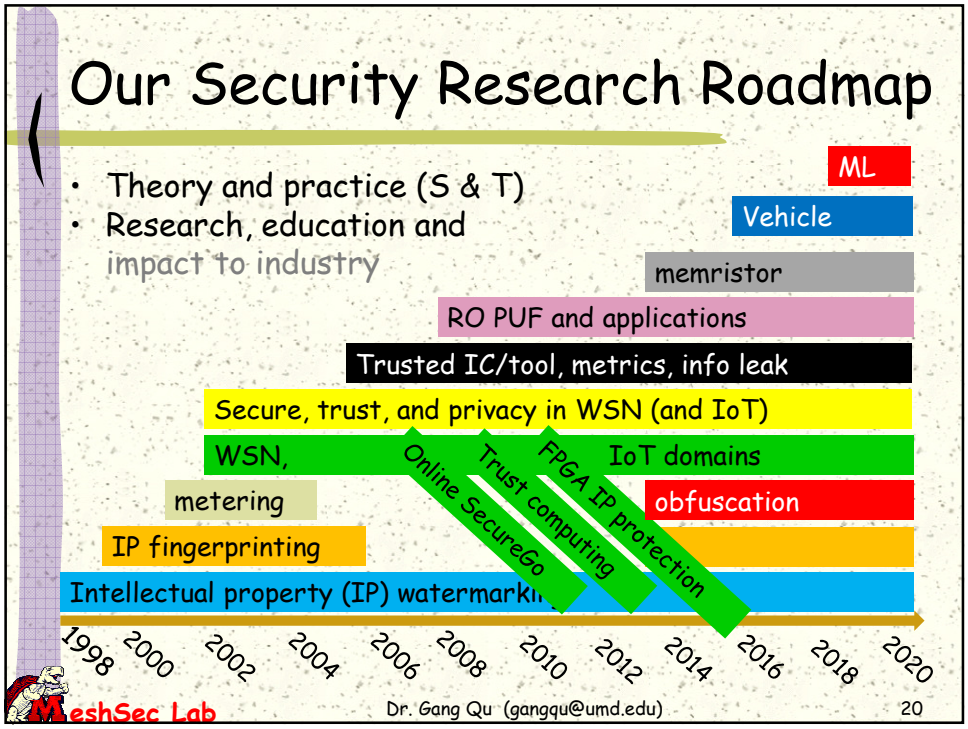
Conclusion: Nobody Is An Island

- Security, privacy, trust issues remain as long as currency exists
- Attacking surface grows faster than countermeasures
- No system is an island,
  - a holistic approach to build secure system
  - Cryptography, software, hardware, network, communication, device, USER, …
- Hardware is the root of security, trust, privacy

Enabler, Enhancer, Enforcer

Conclusion




Our Security Research Roadmap
Theory and practice (S & T)
Research, education and impact to industry
ML
Vehicle
memristor
RO PUF and applications
Trusted IC/tool, metrics, info leak
Secure, trust, and privacy in WSN (and IoT)
WSN,
IoT domains
Online SecureGo
Trust computing
FPGA IP protection
metering
obfuscation
IP fingerprinting
Intellectual property (IP) watermarki
1998
2000
2002
2004
2006
2008
2010
2012
2014
2016
2018
2020
MeshSec Lab
Dr. Gang Qu (gangqu@umd.edu)
20


Thank You!
This work is sponsored in part by NSF under grant CNS1745466, AFOSR MURI, NIST, and by a research agreement between the University of Maryland and the Laboratory for Physical Sciences.