HARDWARE-ENABLED AI FOR EMBEDDED SECURITY: A NEW PARADIGM

Charles THOORIS
Chief Sales Officer & Director Secure-IC Pte Ltd
Secure-IC
Charles.thooris@secure-ic.com
Cyberspace: Are humans thrown on scrapheap?

DARPA's Cyber Grand Challenge: World's first automated network defence tournament
HARDWARE-ENABLED AI FOR EMBEDDED SECURITY

INTRODUCTION

New trends, new risks, new strategy?
- Manpower: short on cybersecurity professionals
- Cyber-attack: “Zero-day attacks” are on the rise
- Physical-attack: IoT - Internet of things VS Internet of threats/targets

Sword and shield dialectic: find the right balance to stay ahead of the threat

“Are we going to be able to predict every attack? No. Are we going to be better about predicting trends and threats so that we’re ahead of the game? Yes.”

Terry Halvorsen
Chief Information Officer, U.S. Department of Defense
HARDWARE-ENABLED AI FOR EMBEDDED SECURITY

INTRODUCTION

New trends, new risks, new strategy?

- Manpower: short on cybersecurity professionals
- Cyber-attack: “Zero-day attacks” are on the rise
- Physical-attack: IoT - Internet of things VS Internet of threats/targets

Sword and shield dialectic: find the right balance to stay ahead of the threat
HARDWARE-ENABLED AI FOR EMBEDDED SECURITY

AGENDA

INTRODUCTION: New risks, new strategy?

ML-ENHANCED SECURITY ANALYSIS
- ML-based Side-Channel Analysis
- Secure-IC’s CTZ: Analysis booster
- ML-enhanced Cache timing attack

AI-ENABLED CYBER-PHYSICAL SECURITY
- Context & Motivations
- Secure-IC’s SMART MONITOR: Features & Benefits
- Roadmap

CONCLUSION: Trustworthy AI
HARDWARE-ENABLED AI FOR EMBEDDED SECURITY

AGENDA

INTRODUCTION: New risks, new strategy?

ML-ENHANCED SECURITY ANALYSIS
- ML-based Side-Channel Analysis
- Secure-IC’s CTZ: Analysis booster
- ML-enhanced Cache timing attack

AI-ENABLED CYBER-PHYSICAL SECURITY
- Context & Motivations
- Secure-IC’s SMART MONITOR: Features & Benefits
- Roadmap

CONCLUSION: Trustworthy AI
Hardware-Enabled AI for Embedded Security

ML-Enhanced Security Analysis

ML-based Side-Channel Analysis

- Profiling-based attacks when leakage model unknown
- ML = alternative to traditional statistical tools;
- Ad-hoc metrics for cyber-security such as Data Confusion Factor, etc.

A wealth of ML algorithms

- E.g. Support Vector Machines (SVM), Random Forest (RF), Rotation Forest (RTF), MultiBoost
- Complex and crucial parameter tuning

---

Side-Channel Analysis and Machine Learning: A Practical Perspective

Stjepan Picek\textsuperscript{1,}, Annelie Heuser\textsuperscript{1,}, Alan Jovic\textsuperscript{1,}, Simone A. Ludwig\textsuperscript{1,}, Sylvain Guillaume\textsuperscript{1,}, Domagoj Jakobovic\textsuperscript{1} and Nele Mentens\textsuperscript{1,}\textsuperscript{*}

\textsuperscript{1}KU Leuven-ESAT/PSI and imec, Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium

\textsuperscript{1}IRISA/CNRS, Rennes, France

\textsuperscript{1}University of Zagreb, Faculty of Electrical Engineering and Computing, Croatia

\textsuperscript{1}Department of Computer Science, North Dakota State University, Fargo, ND, USA

\textsuperscript{1}TELECOM-ParisTech, Paris, France and Secure-IC S.A.S., Rennes, France
Hardware-Enabled AI for Embedded Security

ML-Enhanced Security Analysis

Secure-IC’s CTZ: Analysis booster

- **Reveal**
  - Signal Processing
  - Pattern Recognition

- **Locate**
  - Features Extraction
  - Leakage Detection

- **Extract**
  - Data Mining
  - Machine Learning

Outputs
HARDWARE-ENABLED AI FOR EMBEDDED SECURITY

ML-ENHANCED SECURITY ANALYSIS

Secure-IC’s CTZ: Analysis booster

Target: Elliptic Curve Cryptography (ECC) from a widely used encryption library
Attacked Operation: Point Multiplication during an authentication in an advanced system (smartphone, complete SoC)

Goal: Extract the crypto-processor signal and relate it to the code executed

Problems: Highly challenging attack on classical tools:
• Large, high frequency and very noisy measures
• Only one measure available!
Hardware-Enabled AI for Embedded Security

ML-Enhanced Security Analysis

Secure-IC’s CTZ: Identification, Classification and Extraction of Secret

- Apply Data Mining and Machine Learning on the new data representation

**Hardware-Enabled AI for Embedded Security**

**ML-Enhanced Security Analysis**

**ML-enhanced Cache Timing attack**

- Cache miss & Cache hit patterns could reveal sensitive information (leakage)
- Deep-learning on cache access patterns
- E.g. OpenSSL ECDSA - Nonce LSB recovery using convolutional neural networks
HARDWARE-ENABLED AI FOR EMBEDDED SECURITY

AGENDA

INTRODUCTION: New risks, new strategy?

ML-ENHANCED SECURITY ANALYSIS
- ML-based Side-Channel Analysis
- Secure-IC’s CTZ: Analysis booster
- ML-enhanced Cache timing attack

AI-ENABLED CYBER-PHYSICAL SECURITY
- Context & Motivations
- Secure-IC’s SMART MONITOR: Features & Benefits
- Roadmap

CONCLUSION: Trustworthy AI
HARDWARE-ENABLED AI FOR EMBEDDED SECURITY

AI-ENABLED CYBER-PHYSICAL SECURITY

Motivations: Security at OSI Level – Our Vision

- Software: cyber security
- Hardware: physical security
  - TRNG
  - PUF
  - Active shield

Cryptographic stack

Operators / cloud
Report
IoCs
Suicide
Reboot
Motivations: Security at OSI Level – Our Vision

- Cryptanalysis → quantum-safe
- CVEs → formal methods

Cryptographic stack
- Tunable: lightweight / fast
- Standard / regional

- Cache attacks → constant time
- RowHammer attacks → detection
- Laser, EM inj. → Key Techs

Software: cyber security
- Zero-days → property check
- ROP, stack smashing → online detection

OS-level: Cyber-CPU
- For secure-boot, datacenters, etc.

Hardware: physical security
- EM-injection → TRNG → open-loop design
- Enough entropy, reliability → PUF → stochastic models
- Backside-attacks → Active shield → physical+logical

Caption: attacks/threats in red, innovative solutions by SIC in blue.
Hardware-Enabled AI for Embedded Security

AI-enabled Cyber-Physical Security

- Secure-IC’s SMART MONITOR: AI for embedded systems

Create collective intelligence between IPs and other whistleblowers
- Sources of information are diverse, abundant
- Signals could come from on-chip analog sensors, digital sensors, software reports…
- … or from opportunistic media (weak signals) = Indice of Compromission (IoC)

By leveraging diversity and complementary
- Sensitive to physical vs logical malfunctions
- Able to detect permanent problems vs transient issues
- Instantiated multiple times
HARDWARE-ENABLED AI FOR EMBEDDED SECURITY

AI-ENABLED CYBER-PHYSICAL SECURITY

- Secure-IC’s SMART MONITOR: AI for embedded systems

**Gain assurance in Threat Detection**
- Additional signals are aggregated for security event detection: multimodal analysis
- Learning phase to “lock down the perimeter” of attack
- Confidence & Robustness - Reduce false alarms and false positive event

**The right decision at the right time in full knowledge**
- Anatomy of an attack (nature, temporality, locality, intensity, attack phase…)
- Gain advantage over attackers (attack diagnosis): reverse the advantage
- Built an on-chip security Headquarter to react properly – Security strategy

**Business Intelligence**
- Know your device’s every-day life
- Attack typology and statistics for ≠ device categories, geographic areas, technology nodes…
Global Architecture: Supervisor – Command and control center

- **1. Learn/Train**
  - Acquisition campaign
  - Qualified data
  - Security & Performance metrics

- **2. Classify**
  - 10,000 bits of data (status) are processed each nano-second (10 Tb/s)
  - HW acceleration
  - Trustworthy implementation

**FAULT INJECTION ATTACKS**

**SMART MONITOR™**

- **Learn/Train**
  - Security Model (e.g., 100+ support vectors)

- **Classify**
  - Threat Identification
  - Security Diagnostic

**3. Decide**

- Better react w.r.t. threat
- Raise an alarm
- Security Policy (defensive, offensive, deceptive, ...)
- Business Intelligence

**Gain the advantage over attackers**

- **Fleet of Digital Sensors™**
  - All-in-one fault injection detector, entirely digital
HARDWARE-ENABLED AI FOR EMBEDDED SECURITY

AI-ENABLED CYBER-PHYSICAL SECURITY

- Use-case: ML-enhanced EM Fault Injection Detection

  A Fleet of Digital Sensors (DS) + HW AES on multiple targets (FPGA, ASIC)

  Individually, each DS allows to detect local variation of propagation time along a delay chain...

  ... but sensitivity is small, for internal activity or low power EMFI.
**HARDWARE-ENABLED AI FOR EMBEDDED SECURITY**

**AI-ENABLED CYBER-PHYSICAL SECURITY**

- Use-case: ML-enhanced EM Fault Injection Detection
  - A Fleet of Digital Sensors (DS) + HW AES on FPGA

Collectively, DS status aggregated and interpreted by Secure-IC’s Smart Monitor allow to improve notably the detection efficiency.
HARDWARE-ENABLED AI FOR EMBEDDED SECURITY

AI-ENABLED CYBER-PHYSICAL SECURITY

- Smart Monitor Roadmap

  - Trade-off between performances & security: RAM cost, input signal rate, #classes, code size, etc..
  - Study differential ageing of sensors / effect of sensor breakdown: a model per year?
  - Dynamical feedback on the model (to adapt it) // AI
  - Hardware, Software or a combination of both, depending whether reactivity or flexibility is most important
HARDWARE-ENABLED AI FOR EMBEDDED SECURITY

AGENDA

INTRODUCTION: New risks, new strategy?

ML-ENHANCED SECURITY ANALYSIS
- ML-based Side-Channel Analysis
- Secure-IC’s CTZ: Analysis booster
- ML-enhanced Cache timing attack

AI-ENABLED CYBER-PHYSICAL SECURITY
- Context & Motivations
- Secure-IC’s SMART MONITOR: Features & Benefits
- Roadmap

CONCLUSION: Trustworthy AI
CONCLUSION

Our convictions

- Bridging the gap between Hardware security and Cyber-security

  Not just “patch and pray” but “security by design”

- AI is a real paradigm shift regarding cyber-protection… not just a new tool or an additional IP
- Make the hardware becoming a trust partner and not (another) attacker’s accomplice

Trustworthy AI

- Designing secure AI systems
- Validate and verify the safety and security of decision making systems (DMS)
- Adversarial ML

Importance of Standardization

New SC 42 at ISO/IEC JTC 1 on AI (Trustworthiness = topic)
THANKS FOR YOUR ATTENTION

CONTACT

EUROPE sales-EU@secure-IC.com
APAC sales-APAC@secure-IC.com
JAPAN sales-JAPAN@secure-IC.com
AMERICAS sales-US@secure-IC.com