Karen Shay West
9 Shannon Marie Way, North Easton, MA 02356

508-844-9776 http://www.linkedin.com/in/karenshaywest KarenWest15@gmail.com

SUMMARY OF RECENT ONLINE TECHNICAL COURSE WORK – Software and Hardware Security– see my Linked In Project Section for details and github links to files:

- **Topics and Projects Covered in Software Security:**
  - **1. Memory Security:** layout, memory-based attacks, stack smashing, buffer overflow, code injection, format string vulnerabilities and attacks, stale memory access attacks.
  - **2. Memory and Type Safety Languages:** immune from memory based attacks, Defenses: stack canaries, data execution protection (DEP), address space layout randomization (ASLR), undertstand how attacks based on return-oriented-programming (ROP) work, understand the concept of control-flow Integrity (CFI) and how it can defeat ROP-based attacks.
  - **3. Web: HTTP (hypertext transfer protocol), HTML (hypertext markup language), SQL (standard query language), Javascript programming language:** vulnerabilities: exploitation, defense: SQL injection attacks, web session state, using cookies and hidden form fields, Session hijacking, Cross-site Request Forgery (CSRF) attacks, browser-executed Javascript programs exploits leading to Cross-site Scripting (XSS) vulnerabilities. Avoid flaws and bugs that introduce these vulnerabilities with input validation and sanitization.
  - **4. Flaws and bugs -** Secure design, threat modeling (Architectural risk analysis), security requirements, avoiding flaws with principles, like favor simplicity, trust with reluctance, and defend in depth, monitoring/traceability, real-world examples of good and bad designs.
  - **5. Testing and validation phases:** automated tools assist developers, testers in finding important security bugs- 2 technologies: static analysis (SA) (including flow analysis with and without adding sensitivity, and context sensitve analysisand symbolic execution (SE) as search and the rise of solvers, the basics and their precision and scalabiltiy. SE is often used as the core of a penetration testing technology called white box fuzz testing.
  - **6. Penetration testing:** tools using these technologies and their techniques. Focus: whitebox fuzz testing, a technique that attempts to find potentially security-relevant software failures.
- **Topics Covered in Hardware Security:**
  - **1. Digital System Design:** Basics and Vulnerabilities: understand how digital system is specified, implemented, and optimized; learn what are sequential systems and how they are designed, identify the don't care conditions introduced during the design process; know that there exist security and trust vulnerabilities in hardware
  - **2. Intellectual Property Protection:** self-protection techniques for design IPs: watermarking, fingerprinting, metering assess the trade-off among security, cost and performance
  - **3. Physical Attacks and Modular Exponentiation:** understand the vulnerability to a system from hardware (physical attacks) learn the available countermeasures to physical attacks perform security evaluation for the hardware implementation of security modules modular exponentiation in cryptography, various ways to evaluate it and the security vulnerability, Montgomery Reduction.
  - **4. Side Channel Attacks(SCA) vulnerabilities and information leaks:** study in-depth the

following SCAs: cache attacks, power analysis, timing attacks, scan chain attacks. Learn countermeasures from software, hardware, and algorithm design. Implement security primitives such as RSA securely, Modified Modular Exponentiation. System engineering approach of building secure systems in all phases of the design.

- **5. Hardware Trojan:** (additions or modifications of the circuit with malicious purposes) and trusted integrated circuit (IC) design(does exactly what it is asked for, no less and no malicious more). Hardware Trojan taxonomies based on different criteria, how hardware Trojans work, approaches to detect. Illustrate by design space analysis, hardware Trojan prevention to build trust in ICs.
- **6. Emerging Hardware Security Topics:** trust platform module (TPM), physical unclonable function (PUF) and a RO Reliability PUF, FPGA Implementation of Crypto,Vulnerabilities and Countermeasures, Role of Hardware in Security and Trust.