Side Channel Attacks And Countermeasures For Embedded Systems
Side Channel Attacks And Countermeasures
The Untold Secrets of Operational Wi-Fi Calling Services: Vulnerabilities, Attacks, and Countermeasures TIAN XIE, Michigan State University GUAN-HUA TU, Michigan State University BANGJIE YIN, Michigan State University CHI-YU LI, National Chiao Tung University CHUNYI PENG, Purdue University MI ZHANG, Michigan State University HUI LIU, Michigan State University ...

Vulnerabilities, Attacks, and Countermeasures - arxiv.org
In cryptography, power analysis is a form of side channel attack in which the attacker studies the power consumption of a cryptographic hardware device (such as a smart card, tamper-resistant "black box", or integrated circuit). The attack can non-invasively extract cryptographic keys and other secret information from the device. Simple power analysis (SPA) involves visually interpreting power ...

Power analysis - Wikipedia
International Conference on PHYSICAL ASSURANCE and INSPECTION of ELECTRONICS (PAINE) July 23-24, 2019 Crystal City Marriott (Washington, D.C. area), USA About PAINE Physical attacks on electronics have grown significantly recently and is becoming a major threat to the chip designers, original equipment manufacturers as well as end users. The complex long life of the emergent ...

PAINE Conference 2019
To learn hardware security, we first need to learn how hardware is designed. This week's lectures give an overview of the basics on digital logic design, which is a semester-long course for freshmen and sophomores in most schools.

Hardware Security | Coursera
1000 Ways to Die in Mobile OAuth. OAuth has become a highly influential protocol due to its swift and wide adoption in the industry. The initial objective of the protocol was specific: it serves the authorization needs for websites.

Black Hat USA 2016 | Briefings
Technical Advisory: Private Key Extraction from Qualcomm Hardware-backed Keystores Vendor: Qualcomm Vendor URL: https://www.qualcomm.com/ Systems Affected: Listed ...

Private Key Extraction from Qualcomm Hardware-backed Keystore
While much of TEMPEST is about leaking electromagnetic emanations, it also encompasses sounds and mechanical vibrations. For example, it is possible to log a user's keystrokes using the motion sensor inside smartphones. Compromising emissions are defined as unintentional intelligence-bearing signals which, if intercepted and analyzed (side-channel attack), may disclose the information ...

Tempest (codename) - Wikipedia
At a high level, SGX is a new feature in modern Intel CPUs which allows computers to protect users' data even if the entire system falls under the attacker's control. While it was previously believed that SGX is resilient to speculative execution attacks (such as Meltdown and Spectre), Foreshadow demonstrates how speculative execution can be exploited for reading the contents of SGX ...

Foreshadow: Breaking the Virtual Memory Abstraction with ...
Security Analysis of Layer Two. Our security analysis of the mobile communication standard LTE (Long-Term Evolution, also known as 4G) on the data link layer (so called layer two) has uncovered three novel attack vectors that enable different attacks against the protocol. On the one hand, we introduce two passive attacks that demonstrate an identity mapping attack and a method to perform ...

alter-attack.net - Breaking LTE on Layer Two
Welcome to my webpage. I am a Professor in the Digital Security (DiS) group. I joined the institute
for Computing and Information Sciences at the Radboud University in August 2009. Before that I was a PhD student and PostDoc at the COSIC group, KU Leuven Belgium. Before that I worked as a cryptographer for Pijnenburg Securealink (later SafeNet B.V.) in The Netherlands.

Lejla Batina - Institute for Computing and Information ...  
Current state of security in smart manufacturing. • Survey of important reported attacks against smart manufacturing systems. • The fundamental differences between the IT and smart manufacturing security; discussion of existing vulnerabilities, types of attacks and adversaries.

Security of smart manufacturing systems - ScienceDirect  
The following is a developer-centric defensive cheat sheet for the 2013 release of the OWASP Top Ten Project. It also presents a quick reference based on OWASP Testing Project to help how to identify the risks. OWASP Top Ten Cheat Sheet

OWASP Top Ten Cheat Sheet - OWASP  
48 Dirty Little Secrets Cryptographers Don't Want You To Know. Over the past year, more than 10,000 people participated in the Matasano crypto challenges, a staged learning exercise where participants implemented 48 different attacks against realistic cryptographic constructions.

Black Hat USA 2014 | Briefings  
Dedicated to making data faster and safer, Rambus creates innovative hardware, software and services that drive technology advancements from the data center to the mobile edge.

Rambus. Data Faster Safer  
Conclusion. As a Pentester Check for Cross-Site WebSocket Hijacking attacks as soon as you notice any WebSocket based communication in the application you’re analysing. As a side note, in case you already find Origin header verification present in the application, try to bypass it from victim’s browser: When the server expects https://www.some-trading-application.com as the Origin, mount your ...

Cross-Site WebSocket Hijacking (CSWSH) - Christian Schneider  
Vulnerabilities have been found in the WPA3-Personal protocol that could allow adversaries to crack Wi-Fi passwords and gain access to encrypted traffic sent between a user’s devices. The ...

Flaws in WPA3 Wi-Fi Standard Allow Attackers To Crack ...  
The FBI's Weapons of Mass Destruction (WMD) Directorate uses a cohesive and coordinated approach to incidents involving nuclear, radiological, biological, or chemical weapons—with an overriding ...

WMD — FBI  
Return of Bleichenbacher's Oracle Threat - ROBOT is the return of a 19-year-old vulnerability that allows performing RSA decryption and signing operations with the private key of a TLS server.

The ROBOT Attack - Return of Bleichenbacher's Oracle Threat  
Computer security training, certification and free resources. We specialize in computer/network security, digital forensics, application security and IT audit.

SANS - Information Security Resources  
Security flaw lets attackers recover private keys from Qualcomm chips. Firmware patches have been released earlier this month, 46 Qualcomm chipsets impacted.