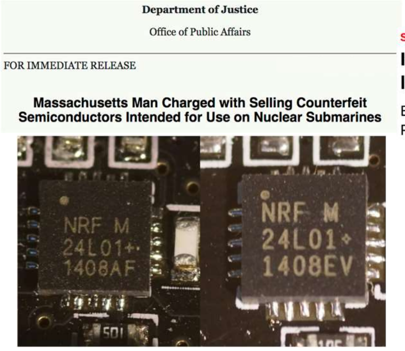
ECE 592-080 (Fall 2018)
Cryptographic Engineering and Hardware Security

Instructor: Aydin Aysu, aaysu@ncsu.edu

Objective/Description: Trusted computing in hardware is fundamental for information security practices. The basis of security guarantees in digital systems ultimately boils down to a set of cryptographic operations executing in a hardware root-of-trust. When this root-of-trust is compromised, security enforcement/isolation mechanisms at higher abstraction levels will inevitably fail. This course is on *how to establish trust in hardware*. It covers information leaks from a wide-array of hardware vulnerabilities of critical cyberinfrastructure. The course will involve hands-on experiments to teach the applications of these attacks and study state-of-the-art countermeasures to mitigate them. The goal of the course is to equip the participants with an understanding of implementations of cryptographic hardware, potential exploits, and associated defenses.



Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Massachusetts Man Charged with Selling Counterfeit Semiconductors Intended for Use on Nuclear Submarines

NRF M 24L01+ 1408AF
NRF M 24L01+ 1408EV

Security

COMPUTERWORLD FROM IDG

IoT worm can hack Philips Hue lightbulbs, spread across cities

Easy chain reaction hack would spread across Paris, boffins say

PHILIPS
PHILIPS

COMPLETELY BROKEN —

Millions of high-security crypto keys crippled by newly discovered flaw

Factorization weakness lets attackers impersonate key holders and decrypt their data.

DAN GOODIN - 10/16/2017, 6:00 AM

EESTI VABARIIK REPUBLIC OF ESTONIA

DIGITAALNE ISIKUTUNNISTUS DIGITAL IDENTITY CARD

JURVETSON

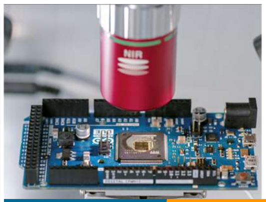
STEPHEN

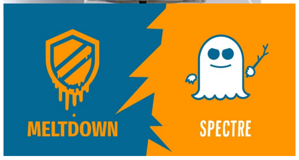
KEHTIV KUNI / DATE OF EXPIRY 02.12.2017

DOKUMENDI NUMBER / DOCUMENT NUMBER N01

ISIKUKOOD / PERSONAL CODE 367030100

AINULT ELEKTROONILISEKS KASUTAMISEKS ELECTRONIC USE ONLY





Prerequisites: ECE-564 or prior background on RTL coding. Familiarity with assembly language. Background on cryptography is not necessary but is helpful.

Textbook: There is no single textbook that the class relies on. “Handbook of Applied Cryptography” by Menezes et al., “Physically Unclonable Functions: Constructions, Properties and Applications” by Roel Maas, “Power Analysis Attacks” by Mangard et al., and “Post-quantum Cryptography” by Bernstein et al. are among the books that will be used for the course. Proceedings of conferences such as CHES, HOST, DATE, DAC, CCS, and S&P will also be used.

Topics:

- Design and implementation of cryptographic primitives: symmetric- and public-key systems, hash functions, and random number generators
- Implementation attacks on cryptography (physical side-channels and fault attacks)
- Securing electronic supply-chain and counterfeit detection via Physical Unclonable Functions
- Hardware backdoors and Trojans
- Next-generation cryptosystems (post-quantum cryptography, lightweight cryptography, and cryptocurrencies)
- Trusted computing bases: Intel SGX, ARM Trustzone, and academic proposals
- Micro-architectural vulnerabilities, side- and covert-channels in computer architectures

Grading: Bi-weekly reading assignments/presentations/critiques; monthly hands-on project assignments; one final research project and presentation;