# Hardware Security -- Good Practice and Emerging Technologies

Cybersecurity Specialization

## What Do We Expect to Learn?

- Trust platform module (TPM)
- Physical unclonable function (PUF)
- FPGA and FPGA-based systems
- Conclusion: hardware's role in security and trust
- Background
  - Digital logic design basics
  - Physical attacks, IP protection, hardware Trojan, etc.

## Trust Platform Module (TPM)

- TPM refers to
  - the set of specifications for a secure crypto-processor, and
  - the implementation of these specifications on a chip.
- TPM chips
  - can be installed on the motherboard and is used in almost all PCs, laptops, and tablets; most smart phones.
  - Best to be used together with: firewall, antivirus software, smart card, biometric verification
  - Vendors: Atmel, Broadcom, Infineon, Sinosun, STMicroelectronics, Winbond, Toshiba, Intel, etc.

## Main Functions of TPM

- cryptographic key generation
- protection of cryptographic keys
- hardware pseudo-random number generation
- hardware authentication
- sealed storage (passwords, encryption keys and digital certificates)
- remote attestation

## TPM Keys

- Endorsement Key (EK)
  - An RSA key pair, required, created only once for the TPM's lifetime
  - Private key is inside TPM, never revealed or accessible outside the TPM
- Storage Root Key (SRK)
  - Created when system's ownership is created
  - Based on the EK and user provided password
  - Master wrapping key, stored inside TPM

## TPM Keys

- Attestation identity key (AIK)
  - Another pair of RSA keys, for attestation
  - Public key will be signed by EK and then sent to a trusted certificate authority (CA)
  - CA validates the EK and issues a certificate for the AIK, TPM authenticates itself w.r.t. this certificate
- Storage key
  - Asymmetric key, encrypt data or other keys (called wrapping)

## TPM Keys

- Signing key
  - Asymmetric key, sign data and message
- Bind key
  - Encrypt small amount of data or key on one platform and decrypt it on another
- Authentication key
  - Symmetric key, protect transport sessions
- Legacy key
  - Can be exported to another TPM, for signing and encryption

## Key Attributes

- Non-migratable keys (NMK)
  - Bound/unique to a single TPM, inside TPM
- Migratable keys (MK)
  - Generated inside or outside of a TPM
  - Integrated inside a TPM or move to another
  - Trusted by its creator
- Certified Migratable keys (CMK)
  - Generated inside a TPM, can move to another TPM, coordinated by a migration authority or migration selection authority

## TPM: Pros and Cons

- Pros:
  - Added security against physical theft and attacks
  - Convenience with the single sign-on
- Cons:
  - User privacy
  - Trusted hardware and vendors

## Useful Links

- TCG homepage: http://www.trustedcomputinggroup.org/
- Use TPM with Linux:
  - http://www.grounation.org/index.php?post/2008/07/04/8-how-to-use-a-tpm-with-linux
  - http://www.infond.fr/2010/03/trusted-platforms-module-tpm-openssl.html
- TPM and BitLocker in Windows 8 OS
  - http://threatpost.com/en_us/blogs/tpm-chip-windows-8-lays-foundation-widespread-enhancements-hardware-based-security-102612