Descrizione Attività di Ricerca: Secondo Evento De Cifris – 22 Gennaio 2018

Andrea VISCONTI

Dipartimento di Informatica
Università degli Studi di Milano

1. Key Derivation Functions

Studio delle KDF:

- Applicazioni reali (Full Disk Encryption, WPA/WPA2, Mobile Devices, IoT)
- Ottimizzazioni degli algoritmi e delle loro implementazioni
- Vulnerabilità (teoriche e pratiche)
- Robustezza degli algoritmi/Crittoanalisi

Pubblicazioni:

1. *On the Weaknesses of PBKDF2.* CANS 2015, LNCS 9476, Springer-Verlag, 2015.
2. *What Users Should Know About Full Disk Encryption Based on LUKS.* CANS 2015, LNCS 9476, Springer-Verlag, 2015.
3. *Exploiting a Bad User Practice to Retrieve Data Leakage on Android Password Managers.* IMIS 2017, LNCS 612, Springer-Verlag, 2017.

2. High Speed Cryptography

Tecniche di High Speed Cryptography:

- Ottimizzazione delle componenti lineari di un algoritmo crittografico
- Applicazioni di queste tecniche ai block cipher (ottimizzazione delle prestazioni SW e HW)
- Crittoanalisi
- Moltiplicazione polinomiale

Pubblicazioni:

1. *Polynomial multiplication over binary finite fields: new upper bounds.* https://eprint.iacr.org/2018/091
2. *Improved upper bounds for the expected circuit complexity of dense systems of linear equations over GF(2).* https://eprint.iacr.org/2017/194
3. *Exploiting an HMAC-SHA-1 optimization to speed up PBKDF2.* https://eprint.iacr.org/2018/097

3. Miscellanea

3. Sicurezza e privacy (IoT/smartphone):
   - Protocolli crittografici (SSL/TLS) e loro implementazioni
   - Protocolli di autorizzazione (OAuth2)
4. Blockchain per la protezione del diritto d'autore
5. Codici correttori utilizzati per migliorare il tempo medio di vita dei dispositivi ottici

Pubblicazioni:

1. *The Dangers of Rooting: Data Leakage Detection in Android Application Mobile Information Systems.* Mobile Information Systems, Hindawi, 2018.
2. *Preserving cultural heritage: A new approach to increase the life expectancy of optical disc.* Journal of cultural heritage, 2018, in press.