ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Cyber Security… non andrà tutto bene

La sicurezza informatica come forma mentis

Gabriele D'Angelo

<g.dangelo@unibo.it>

http://www.cs.unibo.it/gdangelo/

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Scaletta del webinar

- Sicuro?
  - *Cosa significa? L'analisi del valore delle risorse*
- Vulnerabilità dei sistemi o ingegneria sociale?
- La balcanizzazione del perimetro:
  - *Industria 4.0 (... ma non solo)*
- Senza fiducia non c'è sicurezza
- Pessimismo? **No, opportunità**

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Chi sono e da dove vengo

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Home | Curriculum vitae | Pubblicazioni | Didattica | Temi di ricerca | Collaborazioni | Contenuti utili | Avvisi

Gabriele D'Angelo

Ricercatore confermato
Dipartimento di Informatica - Scienza e Ingegneria
Settore scientifico disciplinare: INF/01 INFORMATICA

Nota biografica

Ricercatore confermato (a tempo indeterminato), per ricerca e didattica mi occupo di **Simulazione** e **Sicurezza informatica**. Vai al Curriculum

Contatti

E-mail: g.dangelo@unibo.it
Tel: +39 0547 338886

Altri contatti
Web: Vai al sito personale

Dipartimento di Informatica - Scienza e Ingegneria
Via dell'Università 50, Cesena - Vai alla mappa

Foto di Claudio Turci (Unibo Immagine)

“Cyber Security”

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

SICURO?

“Cyber Security”

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Twitter reveals that its own employee tools contributed to unprecedented hack

Twitter says hackers compromised high-profile accounts thanks to access to internal tools

By Nick Statt | @nickstatt | Jul 15, 2020, 11:42pm EDT

SHARE

Illustration by Grayson Blackmon / The Verge

Jason Koebler @jason_koebler · Jul 16, 2020

Replying to @jason_koebler

OK, we talked to another hacker. Were able to confirm how they got accounts: Twitter employee used internal tool to change email addresses associated with accounts. Twitter seems to have just confirmed this in tweets as well

Hackers Convinced Twitter Employee to Help Them Hijack Acco…
After a wave of account takeovers, screenshots of an internal Twitter user administration tool are being shared in the hackin…
vice.com

Jason Koebler
@jason_koebler

we spoke to two hackers and we were able to independently verify they were in control of hijacked accounts today. One of them said they paid the Twitter employee to help them take over accounts; not sure on the specifics here at the moment

4:50 AM · Jul 16, 2020

link

“Cyber Security”

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Cosa, da chi, perché?

Analisi del Valore

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Analisi del Valore

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Home | Curriculum vitae | Pubblicazioni | Didattica | Temi di ricerca | Collaborazioni | Contenuti utili | Avvisi

Gabriele D'Angelo

Ricercatore confermato

Dipartimento di Informatica - Scienza e Ingegneria
Settore scientifico disciplinare: INF/01 INFORMATICA

Nota biografica

Ricercatore confermato (a tempo indeterminato), per ricerca e didattica mi occupo di **Simulazione** e **Sicurezza informatica**. Vai al Curriculum

Contatti

E-mail: g.dangelo@unibo.it
Tel: +39 0547 338886

Altri contatti
Web: Vai al sito personale

Dipartimento di Informatica - Scienza e Ingegneria
Via dell'Università 50, Cesena - Vai alla mappa

Analisi del Valore

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

link

Vulnerabilità: hardware

Association for Computing Machinery @TheOfficialACM · 18 giu

Two separate academic teams reported two novel exploits that breach @intel Software Guard eXtension (SGX), enabling hackers to plunder #encryptionkeys and other sensitive data. Read more here via @arstechnica: bit.ly/3hg5MKN

Vulnerabilità: software

Security Bulletin VLC 3.0.11

```
Summary           : Multiple vulnerabilities fixed in VLC media player
Date              : June 2020
Affected versions : VLC media player 3.0.10 and earlier
ID                : VideoLAN-SB-VLC-3011
CVE references    : CVE-2020-13428
```

Details

A remote user could create a specifically crafted file that could trigger a buffer overflow in VLC's H26X packetizer

Impact

The affected code was only used by macOS/iOS hardware accelerated decoder (VideoToolbox), meaning other platforms are unaffected.

If successful, a malicious third party could trigger either a crash of VLC or an arbitratry code execution with the privileges of the target user.

While these issues in themselves are most likely to just crash the player, we can't exclude that they could be combined to leak user informations or remotely execute code. ASLR and DEP help reduce the likelyness of code execution, but may be bypassed.

We have not seen exploits performing code execution through these vulnerability

Threat mitigation

Exploitation of those issues requires the user to explicitly open a specially crafted file or stream.

Workarounds

The user should refrain from opening files from untrusted third parties or accessing untrusted remote sites (or disable the VLC browser plugins), until the patch is applied.

Solution

VLC media player **3.0.11** addresses the issue.

Vulnerabilità: humanware

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

One out of every 142 passwords is '123456'

The '123456' password was spotted 7 million times across a data trove of one billion leaked credentials, in one of the biggest password re-use studies of its kind.

By Catalin Cimpanu for Zero Day | July 1, 2020 -- 15:09 GMT (16:09 BST) | Topic: Security

MORE FROM CATALIN CIMPANU

Google
Chrome 84 released with support for blocking notification popups on spammy sites

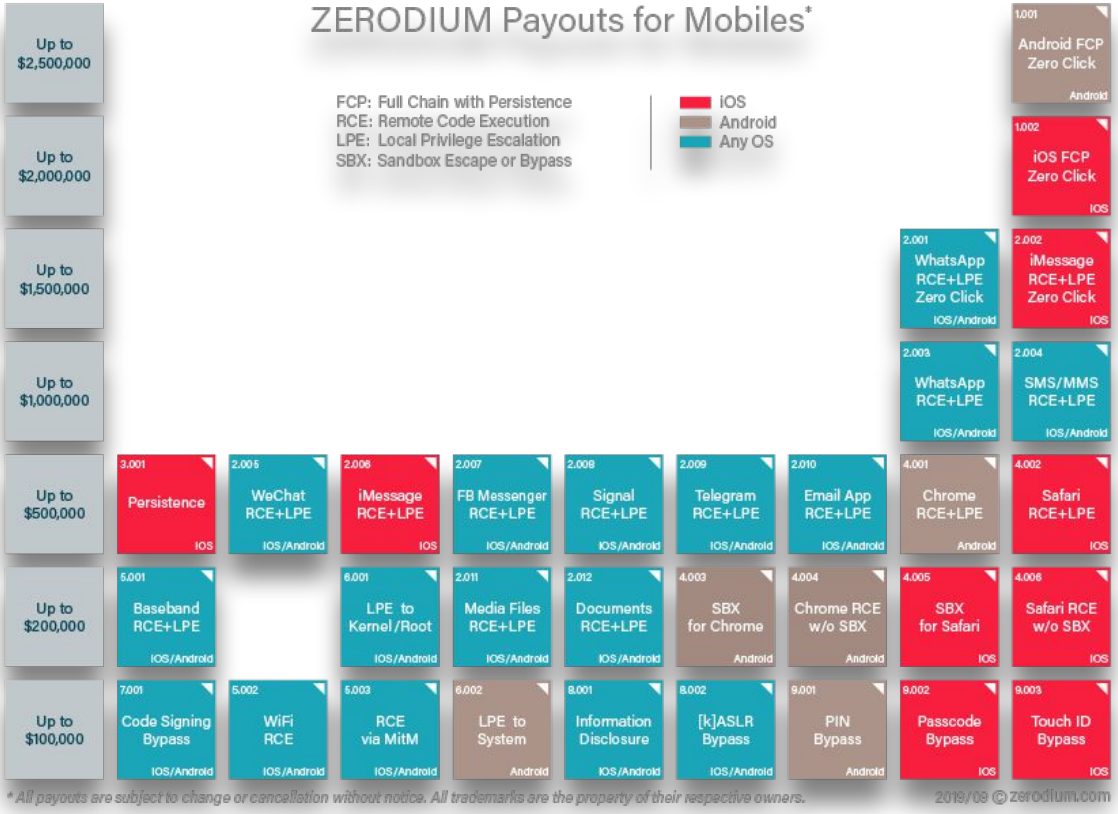
Security
Microsoft July 2020 Patch Tuesday fixes 123 vulnerabilities

Security
RECON bug lets hackers create admin accounts on SAP servers

Security
A hacker is selling details of 142 million MGM hotel

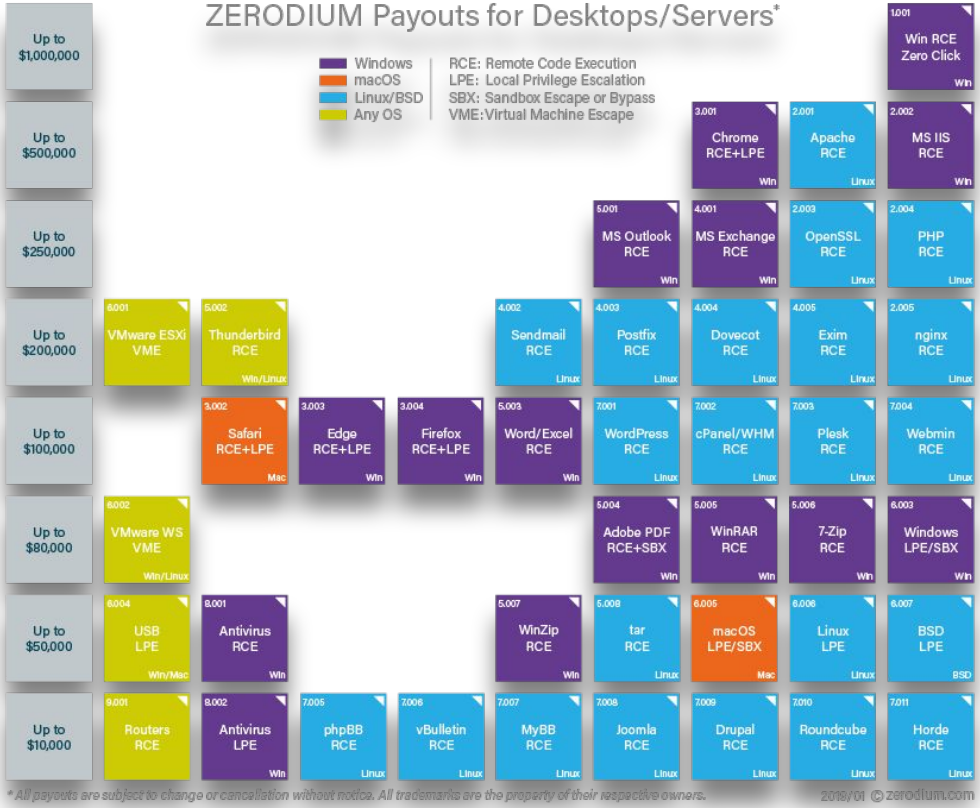
Vulnerabilità dei Sistemi

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA



Vulnerabilità dei Sistemi

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA



Social engineering e Stupidità

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

link

… “evil maid” attack

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

link

Balcanizzazione del Perimetro

link

Balcanizzazione del Perimetro

link

Balcanizzazione del Perimetro

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

link

Balcanizzazione del Perimetro

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

#ZeroTrust

Senza fiducia non c'è Sicurezza

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Non accettare caramelle dagli sconosciuti!

link

Senza fiducia non c'è Sicurezza

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

HUAWEI

AGI AGENZIA ITALIA

La Gran Bretagna ha escluso Huawei dalla rete 5G

ECONOMIA

Tim esclude Huawei dall'elenco dei potenziali fornitori per il 5G

La decisione, secondo quanto apprende l'AGI, che interessa Italia e Brasile, non ha nulla a che vedere con aspetti di natura politica ma riflette solo una scelta industriale che va nell'ottica della diversificazione dei partner

REUTERS

Prima Pagina Economia Mercati TV

PRIMA PAGINA 14 LUGLIO 2020 / 14:40 / AGGIORNATO 2 ORE FA

Regno Unito esclude Huawei da rete 5G

Cyber security Geopolitica

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

BBC Sign in | News | Sport | Reel | Worklife | Travel | Future

NEWS

Home | Video | World | UK | Business | Tech | Science | Stories | Entertainment & Arts

Business | Market Data | Global Trade | Companies | Entrepreneurship | Technology of Busir

Huawei finance chief Meng Wanzhou arrested in Canada

6 December 2018 Share

Meng Wanzhou was detained while transferring between flights in Vancouver

The New York Times

Extradition of Huawei Executive Clears a Major Legal Hurdle in Canada

A Vancouver court ruled that fraud charges against Meng Wanzhou in the United States would constitute a crime in Canada, opening the way for her extradition.

Cyber security Geopolitica

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

THE WALL STREET JOURNAL.

English Edition ▾ | July 16, 2020 | Print Edition | Video | Latest Headlines

Home World U.S. Politics Economy Business Tech Markets Opinion Life & Arts Real Estate WSJ. Magazine

WORLD | ASIA | CHINA

Two Canadians Detained in China Indicted on Espionage Charges

Cases of Michael Spavor and Michael Kovrig, first detained over 18 months ago, are seen as retribution for Canada's arrest of a Huawei executive

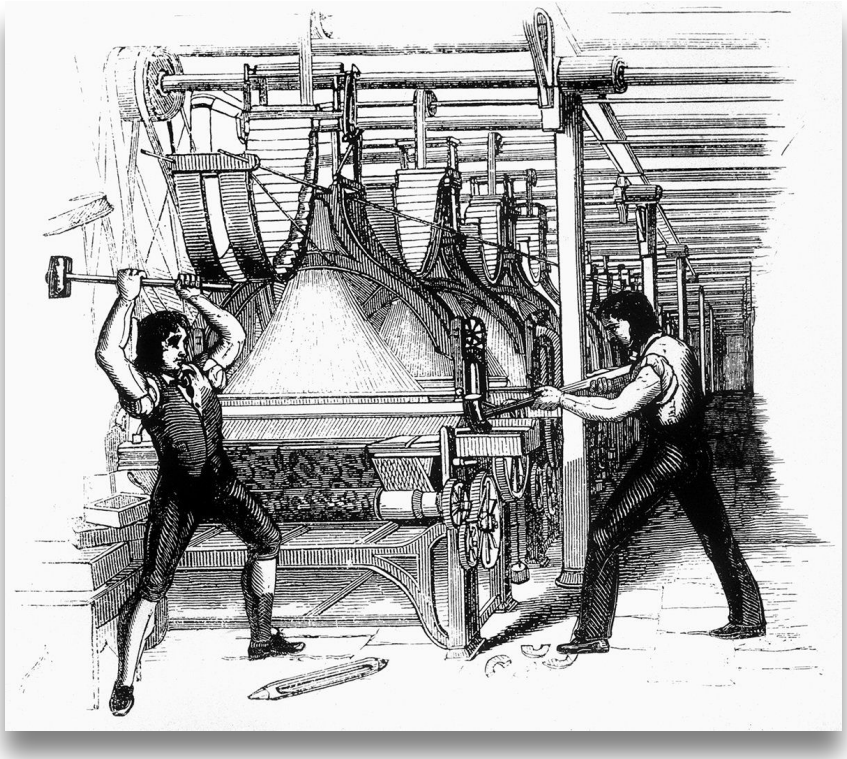
By Chun Han Wong
Updated June 19, 2020 1:50 pm ET

PRINT TEXT

HONG KONG—Chinese prosecutors have formally indicted two Canadian citizens on espionage charges more than 18 months after the men were first detained, advancing a pair of cases widely seen as retribution for Canada's arrest of a well-connected Chinese Huawei executive.

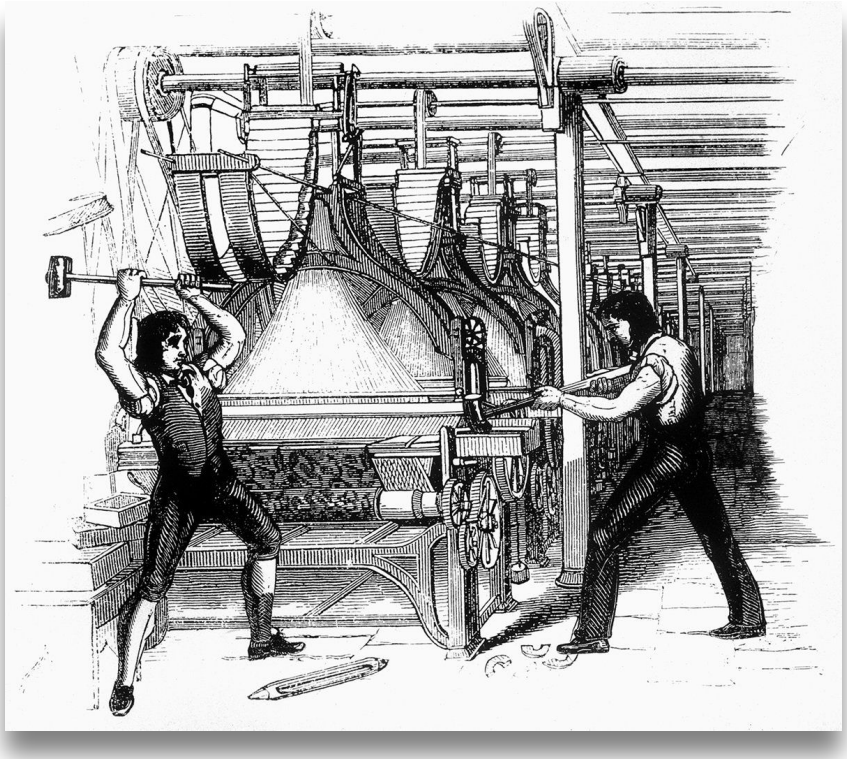
Michael Kovrig, a researcher and former Canadian diplomat, was charged with "probing into state secrets and intelligence" on behalf of foreign actors, while entrepreneur Michael

Pessimismo? Luddismo mon amour?



link

Pessimismo? Luddismo mon amour?



link

NO!

Opportunità

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

- Abbiamo **buoni strumenti** (anche se non perfetti)
- Dobbiamo (finalmente) capire che **efficienza ≠ riduzione**
- Servono **buoni investimenti** in
  - *tecnologia*
  - *humanware*

Conoscenza e Formazione

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

- **Conoscenza** approfondita del sistema
- **Ridondanza** (la sicurezza non è gratis)
- **Approccio proattivo**:
  - *non attendere la catastrofe*
  - *pianificare la gestione dell'incidente*
- **Formazione e aggiornamento** (componente umana)

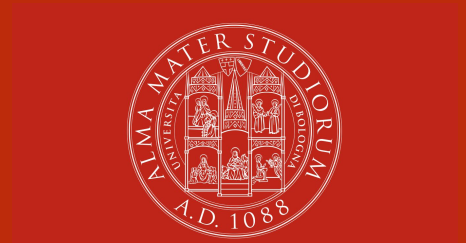
Attenzione ad ogni Dettaglio

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

"Only the paranoid survive"

(Andrew Grove)

link



ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Cyber Security...

non andrà tutto bene

Gabriele D'Angelo

<g.dangelo@unibo.it>

http://www.cs.unibo.it/gdangelo/

Cyber Security @ Bi-REX

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

"Cyber Security: protezione dei sistemi industriali e dei servizi"

32 ore di lezione, casi di studio ed esempi

- **"Modulo 1":** *introduzione alla sicurezza informatica*
- **"Modulo 2":** *strumenti e meccanismi di base per la protezione dei sistemi*
- **"Modulo 3":** *attacchi, contromisure e prospettive future*
- **"Modulo 4":** *quadro nazionale e regolamenti*