



There are only 10 types  
of people in the world:  
Those who understand binary,  
and those who don't

(Who + What) && (Where + When) == Why

# APPLICATION SECURITY FOR THE MASSES

# Perché la solita minestra?

Application Security = SQL INJECTION e i suoi fratelli

Bah. Roba vecchia, le faceva mio nonno nel '98

<#1> Interessa solo perchè una banda di Lamer ha fatto casino nel 2011.

<#2> E' **la** solita tecnica per vendere qualche scatolone in più.

<#3> Basterebbe avere programmatori che sanno fare il loro dovere.

<#4> Se avessi gestito io quella roba lì non sarebbero mai entrati.

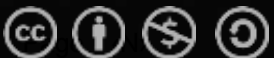
# Limiti dell'Application Security





PESCARA 24+25+26.08.2012  
<http://moca.olografix.org>

# The Contenders ■■■

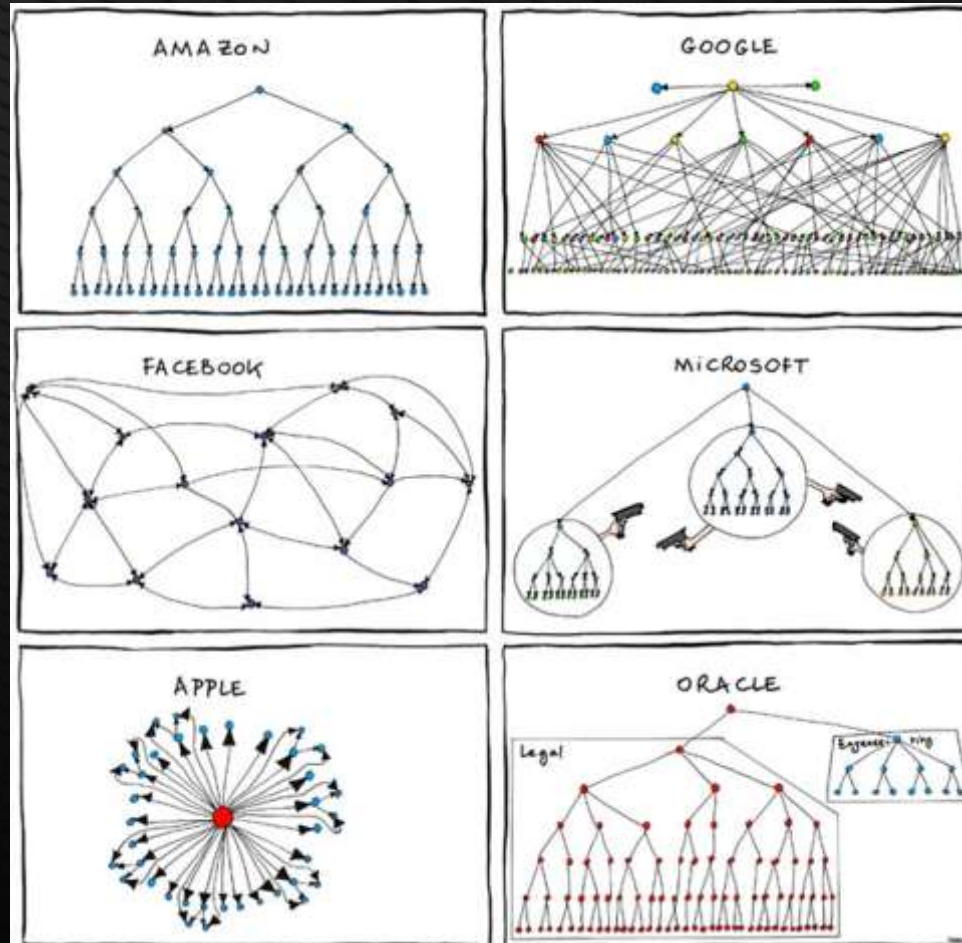


Except where otherwise noted, this work is licensed under  
<http://creativecommons.org/licenses/by-nc-sa/3.0/>

**Andrea Pompili**  
apompili@hotmail.com – Xilogic Corp.



# L'Azienda e la sua Organizzazione





MOCA  
2012  
fino alla fine del mondo

PESCARA 24+25+26.08.2012

<http://moca.olografix.org>

# Gli Hacker dell'IKEA

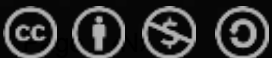
Learn How to Become a  
**COMPUTER  
HACKER**  
in 15 MINUTES!

**TeachMeToHackOnline.com**

Class designed by the Worlds No. 1 Hacker Gregory Evans

CLEAR CHANNEL

000156



Except where otherwise noted, this work is licensed under  
<http://creativecommons.org/licenses/by-nc-sa/3.0/>

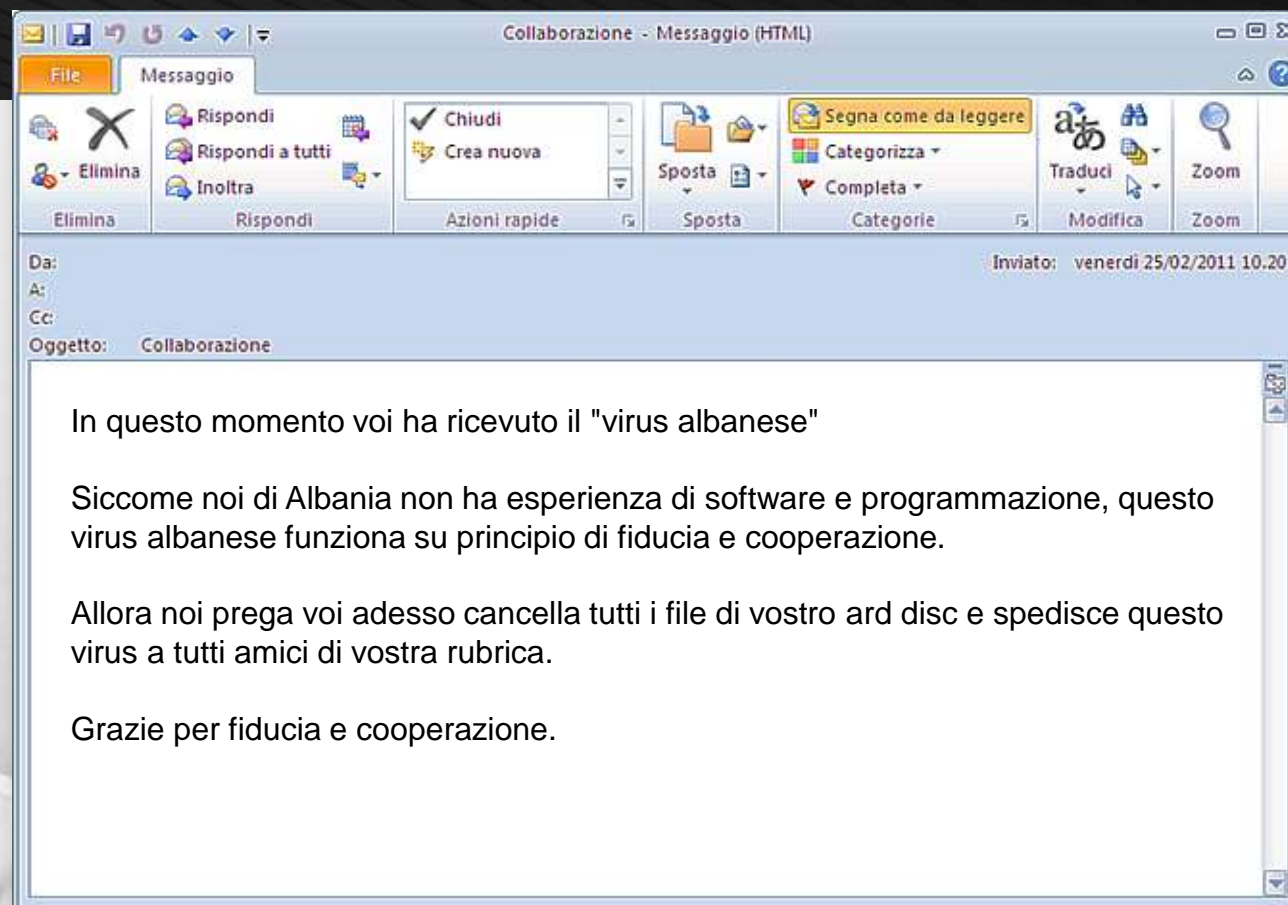
Andrea Pompili

apompili@hotmail.com – Xilogic Corp.





Seguici su [Twitter](#) per avere tutte le indicazioni necessarie in tempo reale. Visita la nostra [pagina web](#) per avere altri tool utili al NetStrike.

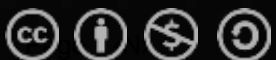






PESCARA 24+25+26.08.2012  
<http://moca.olografix.org>

# The Motivation ■■■



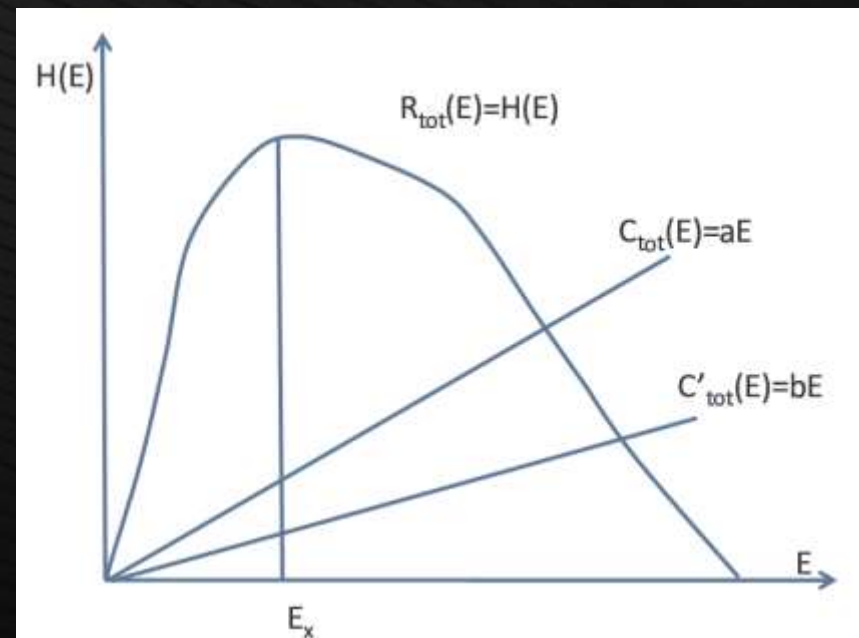
Except where otherwise noted, this work is licensed under  
<http://creativecommons.org/licenses/by-nc-sa/3.0/>

**Andrea Pompili**  
apompili@hotmail.com – Xilogic Corp.

# Il business del lato Oscuro della Forza

Example of a Typical Campaign	Mass Phishing Attack (Single Campaign)	Spearphishing Attack (Single Campaign)
(A) Total Messages Sent in Campaign	1,000,000	1,000
(B) Block Rate	99%	99%
(C) Open Rate	3%	70%
(D) Click Through Rate	5%	50%
(E) Conversion Rate	50%	50%
<b>Victims</b>	<b>8</b>	<b>2</b>
Value per Victim	\$2,000	\$80,000
<b>Total Value from Campaign</b>	<b>\$16,000</b>	<b>\$160,000</b>
Total Cost for Campaign	\$2,000	\$10,000
<b>Total Profit from Campaign</b>	<b>\$14,000</b>	<b>\$150,000</b>

Source: Cisco - "Email Attacks: This Time It's Personal" – 30/06/2011



Source: "A Profitless Endeavor: Phishing as Tragedy of the Commons" – 2008

$H(E)$  = Curva della raccolta di denaro sostenibile in funzione dell'effort sostenuto

# La Contestazione Sociale nel XXI secolo

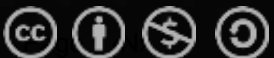






PESCARA 24+25+26.08.2012  
<http://moca.olografix.org>

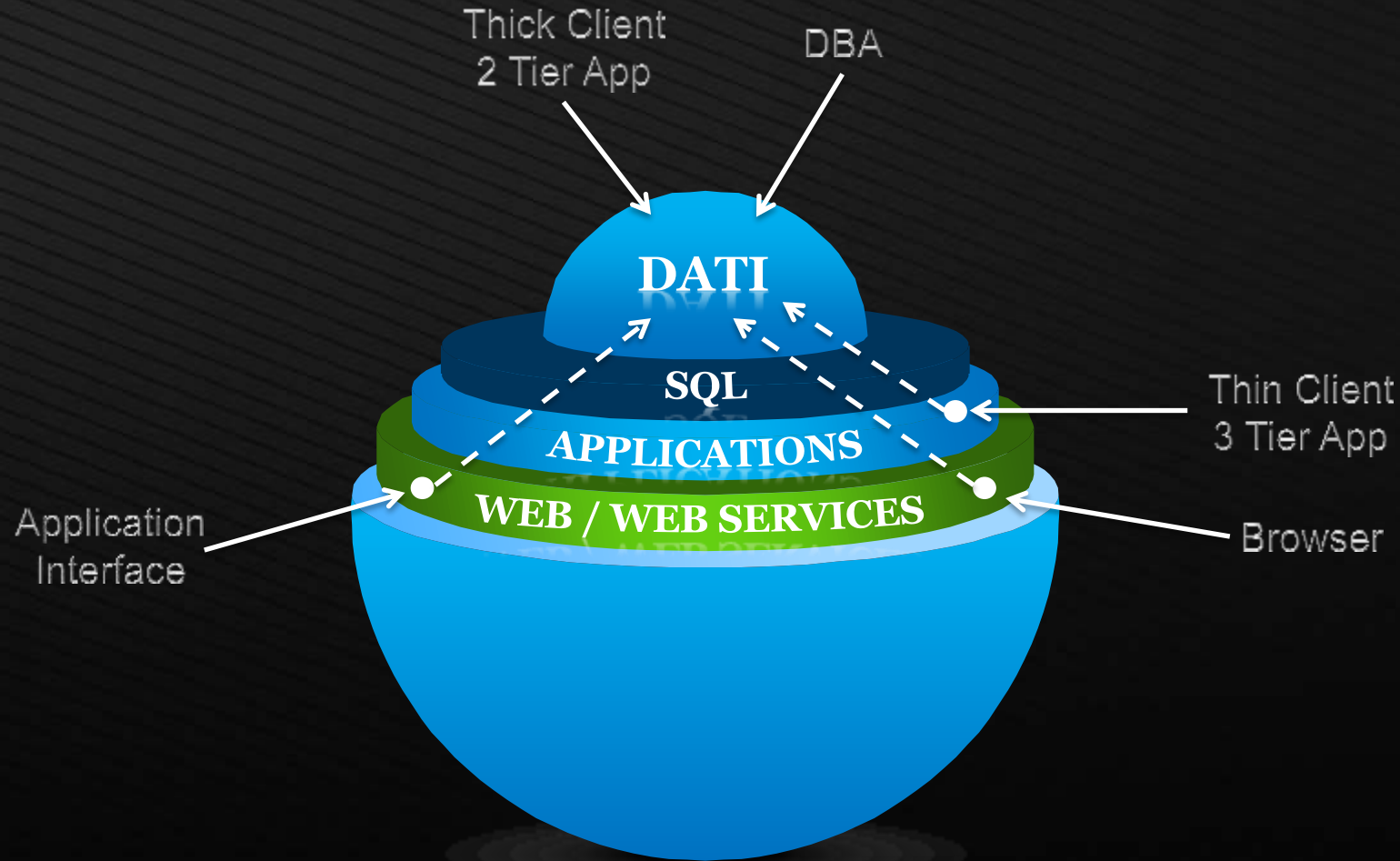
# The Battlefield ■■■



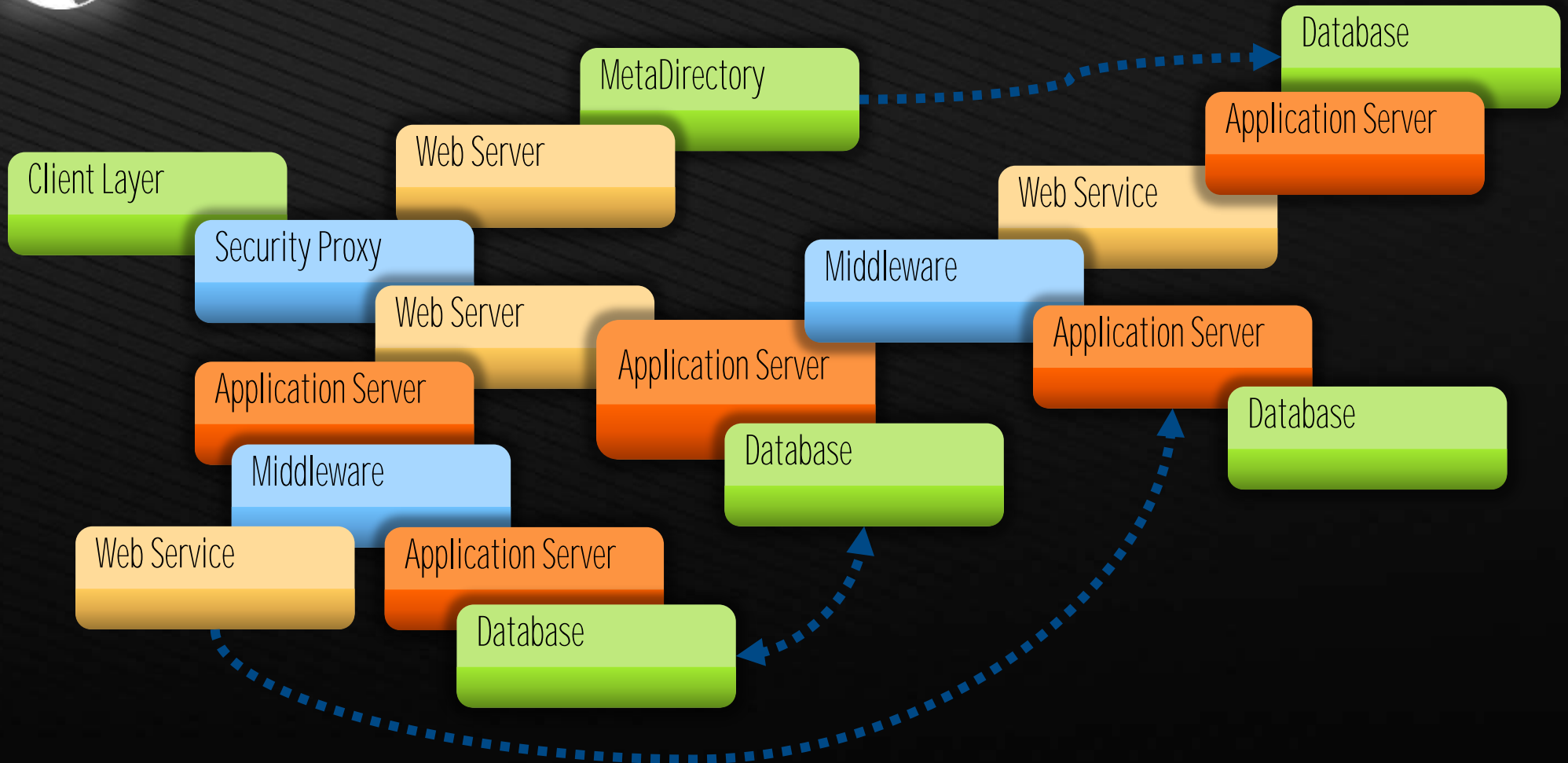
Except where otherwise noted, this work is licensed under  
<http://creativecommons.org/licenses/by-nc-sa/3.0/>

**Andrea Pompili**  
apompili@hotmail.com – Xilogic Corp.

# The Onion Application Framework



# ... and its Current Evolution







PESCARA 24+25+26.08.2012

<http://moca.olografix.org>

# To Code or not to Code



Giallo a Parigi, mobilitati i servizi di sicurezza

## Pirata nel computer della Difesa francese

Quali segreti è riuscito a rubare?

Hacker nel sito dell'Onu

### "Non uccidete i bambini"

Pacifisti protestano on line contro Usa e Israele

Pirati informatici scatenati: blog nel mirino

Tre assalti in un mese per il forum virtuale de "Il Giornale del Passato"



This work is licensed under <https://creativecommons.org/licenses/by-nc-sa/3.0/>

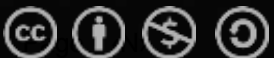
**Andrea Pompili**

[apompili@hotmail.com](mailto:apompili@hotmail.com) – Xilogic Corp.



PESCARA 24+25+26.08.2012  
<http://moca.olografix.org>

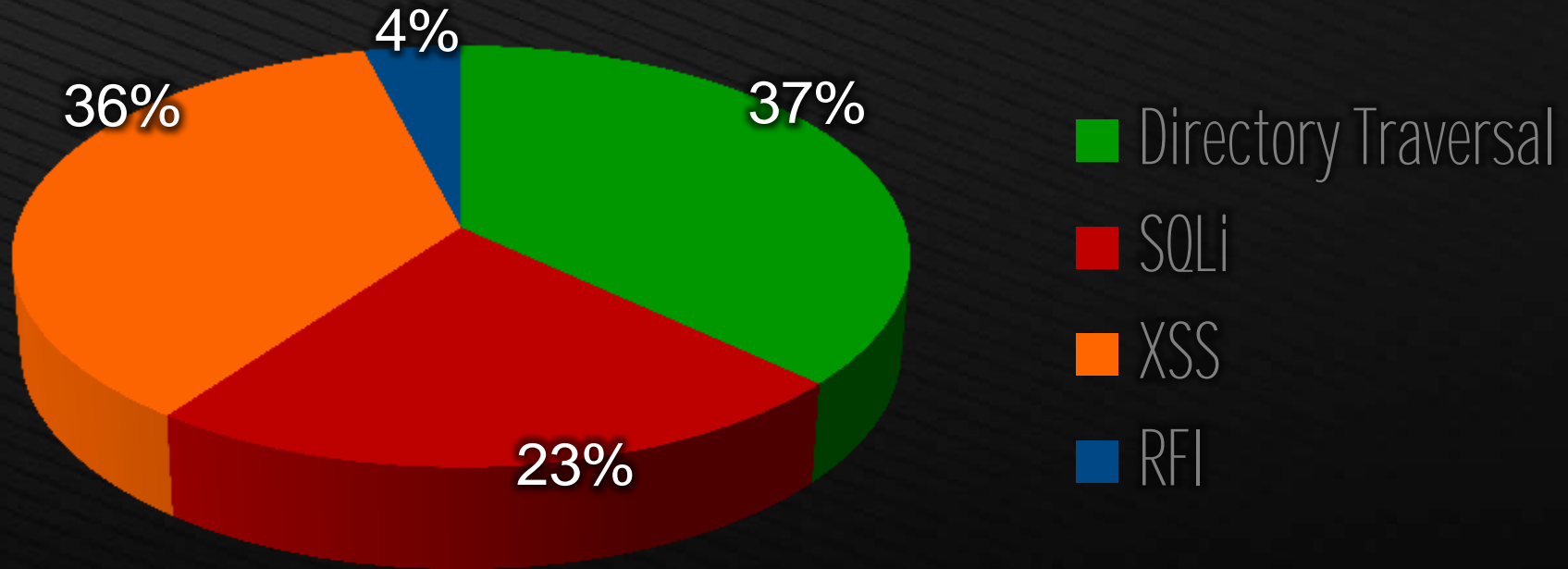
# The Weapons? ■■■■



Except where otherwise noted, this work is licensed under  
<http://creativecommons.org/licenses/by-nc-sa/3.0/>

**Andrea Pompili**  
apompili@hotmail.com – Xilogic Corp.

# Il mondo dei Fantastici 4



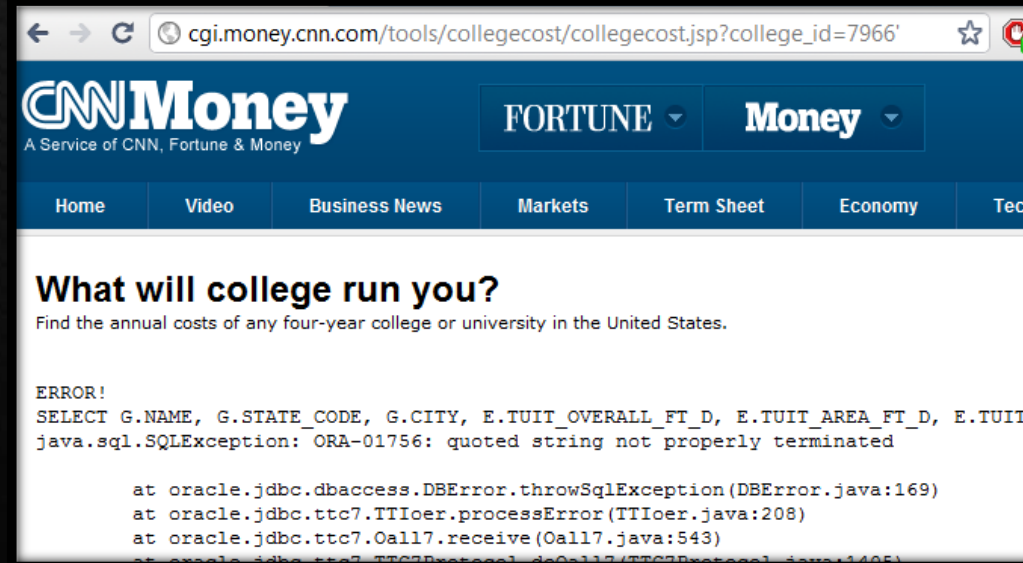


# Sua Maestà SQL Injection e i suoi sudditi

Def. «Le Injection Flaws, come SQL Injection, XML Injection, e LDAP Injection, si verificano quando dati non validati vengono inviati come parte di un comando o di una query al loro interprete. Il dato infetto può quindi ingannare tale interprete, eseguendo comandi non previsti o accedendo a dati per i quali non si ha l'autorizzazione».

<http://www.blackhat.com/presentations/bh-europe-09/Guimaraes/Blackhat-europe-09-Damele-SQLInjection-slides.pdf>

<http://www.modsecurity.org/archive/amit/blind-xpath-injection.pdf>



# A World of SQL Injection...

## <01> INBAND SQL INJECTION

Visto che ci sei aggiungimi anche i risultati di questa **SELECT...**

## <02> ERROR BASED SQL INJECTION

Siccome sei bravo a mostrare gli errori, fammi questa piccola conversione...

## <03> BOOLEAN-BASED BLIND

Quando la risposta dipende dal numero di risultati della **SELECT...**

## <04> TIME-BASED BLIND

Quando il Database è anche bravo ad aspettare...

# Perché conviene?

**Nel 2009, 94% di tutte le violazioni dei dati sono hanno coinvolto i Database o hanno compromesso applicazioni**

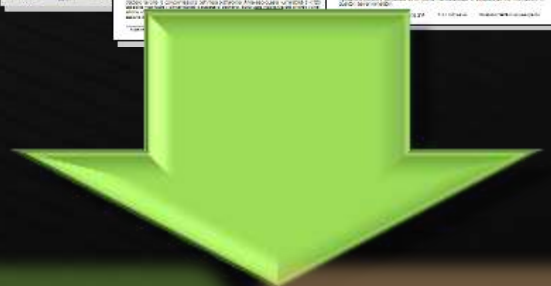
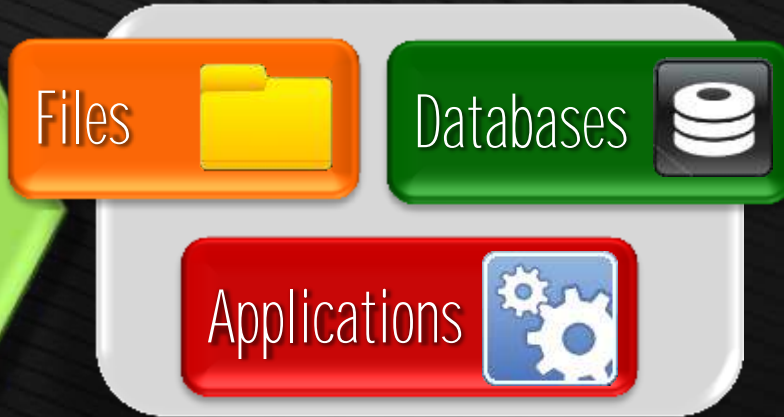
Asset Attacked	Volume of Data Stolen
Database	74%
Application	19%
Other	7%



**Ancora una volta, piu' del 90% dei \$16B spesi in sicurezza nel 2009 e' stato "altro"**



# The way to Application Security



Development



ICT Operations



IT Security

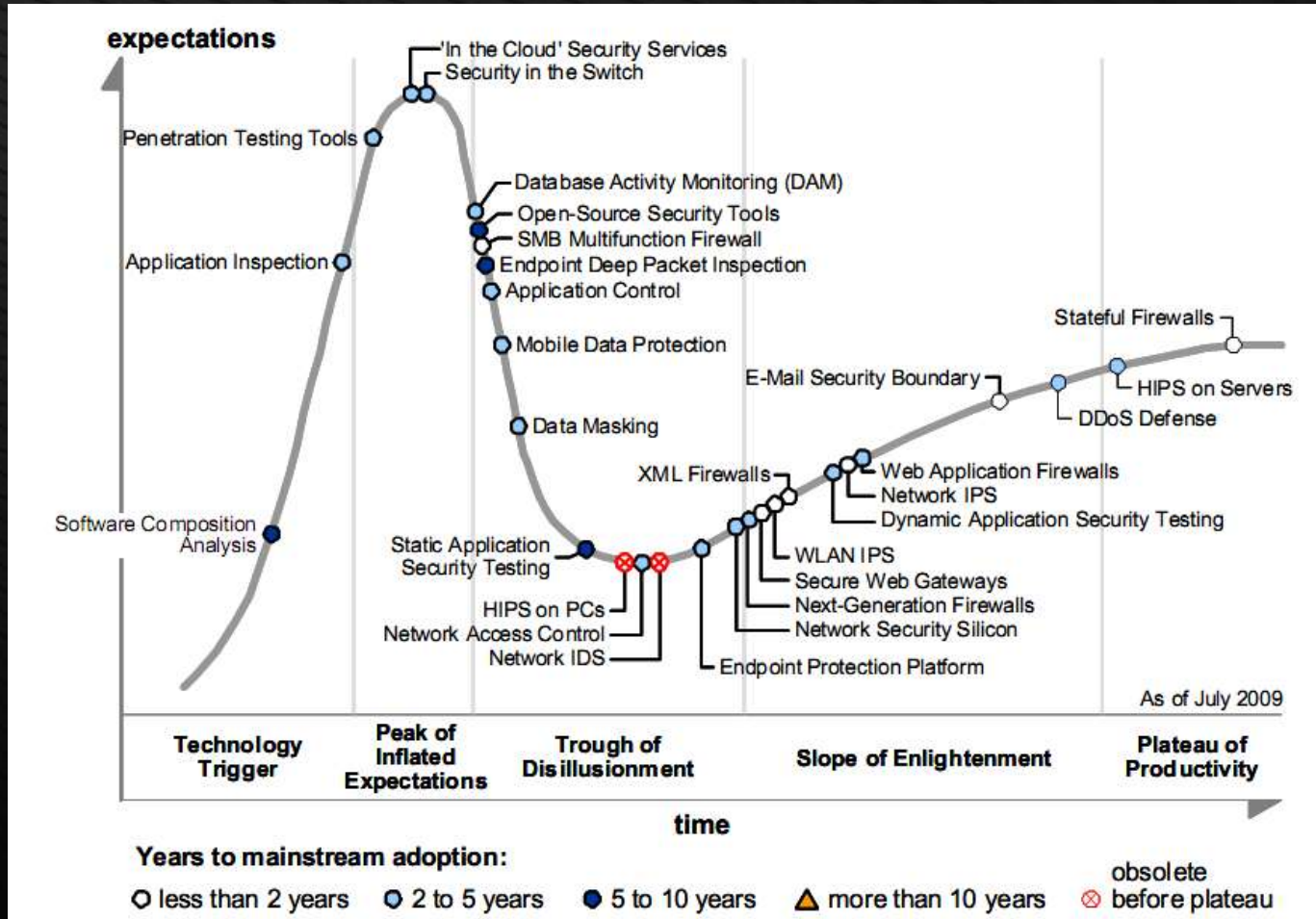


# ... e perché non funziona





# Current Application Security market







PESCARA 24+25+26.08.2012

<http://moca.olografix.org>

# #2 Choices and #1 Combined Approach

## <01> SOURCE CODE AUDITING

I Bambini imparano più facilmente da piccoli...

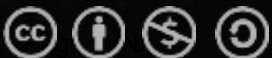
## <02> APPLICATION SECURITY INFRASTRUCTURE

Il Neoclassico della sicurezza informatica...

Apparentemente...

**Andrea Pompili**

[apompili@hotmail.com](mailto:apompili@hotmail.com) – Xilogic Corp.



Except where otherwise noted, this work is licensed under  
<http://creativecommons.org/licenses/by-nc-sa/3.0/>

# The Idea of a Self-Enforcement Environment



FAM

DAM



WAF

DLP  
Classificazione

IAM  
Autenticazione  
Autorizzazione

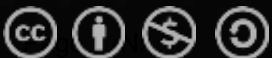
Usage Policy  
Interne



PESCARA 24+25+26.08.2012  
<http://moca.olografix.org>

# LESSON #1

## INPUTS & BACKDOORS ■■■■



Except where otherwise noted, this work is licensed under  
<http://creativecommons.org/licenses/by-nc-sa/3.0/>

**Andrea Pompili**  
apompili@hotmail.com – Xilogic Corp.



# Attacco a Poste Italiane

Posteitaliane

HACKED  
XIVELIC

Niente in tasca - Tutto in testa

La pagina sul server <http://www.poste.it> riporta:



Le Poste italiane sono state oscurate ?!

Perché questo atto di forza?

Per dimostrare a milioni di Italiani

che i loro dati sensibili non sono al sicuro!

Sembra pazzesco eppure tutta la sicurezza garantita

nei servizi on-line di e-commerce è solamente apparente.

Per vostra fortuna noi siamo persone non malintenzionate,

perciò i vostri dati ed i vostri accounts non sono stati toccati;

Ma cosa succederebbe se un giorno arrivasse qualcuno

con intenzioni ben peggiori delle nostre?

Con questo gesto quindi, invitiamo i responsabili ad occuparsi

della grave mancanza di sicurezza nei servizi on-line delle Poste s.p.a .

Mr.Hipo and StutM

OK

# Application Firewall

**x'; DROP TABLE  
users; --**

POST <http://www.sito.it/vulnpage.php> HTTP/1.1  
username: test  
password: **x'; DROP TABLE users; --**



**Virtual  
Patch**

**Applications**



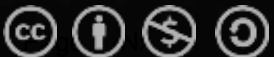


MOCA  
2012  
fino alla fine del mondo

PESCARA 24+25+26.08.2012  
<http://moca.olografix.org>

# LESSON #2

## THE GOOD OF ERRORS



Except where otherwise noted, this work is licensed under  
<http://creativecommons.org/licenses/by-nc-sa/3.0/>

**Andrea Pompili**  
apompili@hotmail.com – Xilogic Corp.



# Ricariche e Contatori elettrici



AAA - Fornitori

**Enel**  
L'ENERGIA CHE TI ASCOLTA.

Azienda **Clienti** Reti Impianti Media e Investor Eventi e News Carriere

Cerca...

Famiglie - Aziende - Condomini - Promozioni e Novità - **Enel Servizio Elettrico**

Home / Clienti / Enel Servizio Elettrico / Servizi SMS / **Autolettura sms**

RSS Invia Bookmark Stampa

La tua bolletta  
Il tuo contratto  
Il tuo contatore  
Tariffe

**Servizi SMS**

- **Autolettura sms**
- SMS Informativi
- Moduli sms
- Copia fattura sms
- Banche sms
- Infowatt sms

Moduli on line  
Diritti del Cliente  
Piano Salva Black-out (Data Enel Distribuzione)

**Enel Servizio Elettrico**  
Maggior Tutela

## AutoLettura SMS

Da oggi comunicare la lettura è più semplice!

**AutoLettura SMS** è il nuovo servizio ENEL SERVIZIO ELETTRICO per la comunicazione della lettura attraverso l'invio di un SMS dal tuo cellulare.

Visualizza la guida

Invia un SMS al numero **3202043438** digitando:

**LETTURA** il tuo **Numero Cliente** e la **lettura del contatore**

**LETTURA** corrisponde al codice identificativo del Servizio di comunicazione lettura.

Il **Numero Cliente** è il numero di 9 cifre che identifica la tua fornitura di energia elettrica. Lo puoi trovare in alto a destra sulla bolletta.

La **lettura del contatore** corrisponde alle cifre della lettura riportate sul contatore.

Se hai un **contatore di tipo tradizionale** leggi tutte le cifre che visualizzi sulla finestra trasparente relative ai tuoi consumi.

Se hai un **contatore di tipo elettronico** premi il pulsante fino a che sul display

I nostri servizi on-line

- La tua bolletta
- Il tuo contatore
- Il tuo contratto
- Scopri l'autolettura

Strumenti

Condividi

Info

Enel Do

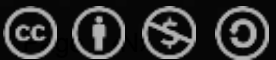




PESCARA 24+25+26.08.2012  
<http://moca.olografix.org>

# LESSON #3

## CONTROL YOUR FILES ■■■■



Except where otherwise noted, this work is licensed under  
<http://creativecommons.org/licenses/by-nc-sa/3.0/>

**Andrea Pompili**  
apompili@hotmail.com – Xilogic Corp.



MOCA  
2012  
fino alla fine del mondo

PESCARA 24+25+26.08.2012

<http://moca.olografix.org>

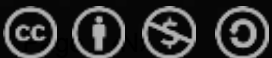
# Il caso Wikileaks



We open governments.



Wikileaks



Except where otherwise noted, this work is licensed under  
<http://creativecommons.org/licenses/by-nc-sa/3.0/>

**Andrea Pompili**  
apompili@hotmail.com – Xilogic Corp.



# File Security & Monitoring

- 1**
- Crawl File Systems
    - Find name, type, owner, permissions...
  - Apply Classification Policies
    - Owner, Org, Location
    - Automatic content classification

**2 Build Data/Permission Map**

Who	Group	What	Class
Joe, IT	Fin-CC	Read cc.xls	Financials
Jim, HR	HR-Exec	Read PII.doc	PII

**3 Enforce Policies**

Who	What	Action
Non Finance	Update Financials	Block
Any	Read PII	Audit

Joe, IT



Jim, HR



OK



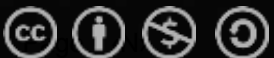
**Audit Log**

Who	What	When	Action
Joe	Read CC.xls	1/1/2010 12:50	Block
Jim	Read PII.doc	1/1/2010 12:51	Audit



# LESSON #4

## SELF-DESTRUCTION APPS ■■■







www.mywifisite.it

Prepagato   Abbonamento   Trova Hot-Spot

**Wi-Fi ZONE**

## Il tuo Wi-Fi pubblico

Wi-Fi Area è il servizio per navigare in internet con PC portatile, palmare e Smart Phone con funzionalità wi fi, ad **alta velocità e senza fili**, nei luoghi pubblici coperti dal Wi-Fi, in Italia e all'estero.

Scegli la proposta più adatta a te. Wi-Fi Area risponde alle diverse esigenze di navigazione, offrendo la flessibilità del prepagato per un uso occasionale e l'abbonamento per collegamenti frequenti.

**Prepagato**  
Se cerchi un servizio wi fi flessibile, scegli la carta prepagata di Telecom Italia. È disponibile nei formati da 1 ora, 5 ore, 24 ore e 7 giorni

- ▶ scopri di più
- ▶ acquista ora

**Abbonamento**  
Il servizio Wi-Fi Area in abbonamento, riservato ai clienti Telecom Italia, è ideale per collegarsi in rete quanto vuoi, in modalità Wi-Fi, anche lontano da casa o dall'ufficio.

- ▶ residenziali

**Gestione account Wi-Fi**

- il tuo account @wifiana.it
- recupera account @wifitecom.it
- abilita il tuo account @kie.it
- modifica password

**Navigare negli Hot Spot Wi-Fi Area?**  
Semplice, usa le tue credenziali My Wi-Fi





# Database Security & Monitoring

## Chi, Dove, Come e Quando

SKO URM 1 - Effective Rights Raw Data

Filter: Account Department is [RnD] and Object Category is [credit cards] and Sensitive...

Select Columns | Showing records 1-3 out of 3 available | Show Paths

Account Name	Department	Priv Type	System Priv.	Object Name	Schema Name	Object Type	Sensitive Object	Object Category	Object Last Used
acourtney	RnD	SELECT	Normal Priv.	fulcustomerdata	skotrain	Table	Sensitive	credit cards	2009-12-31
atloton	RnD	SELECT	Normal Priv.	fulcustomerdata	skotrain	Table	Sensitive	credit cards	2009-12-31
eho	RnD	SELECT	Normal Priv.	fulcustomerdata	skotrain	Table	Sensitive	credit cards	2009-12-31

Chi

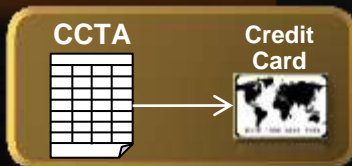
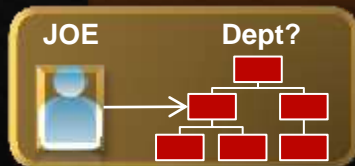
Come

Dove

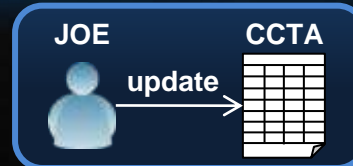
Cosa

Quando

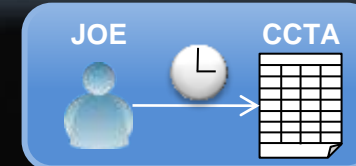
**DAS**  
Who Is? Sensitive?



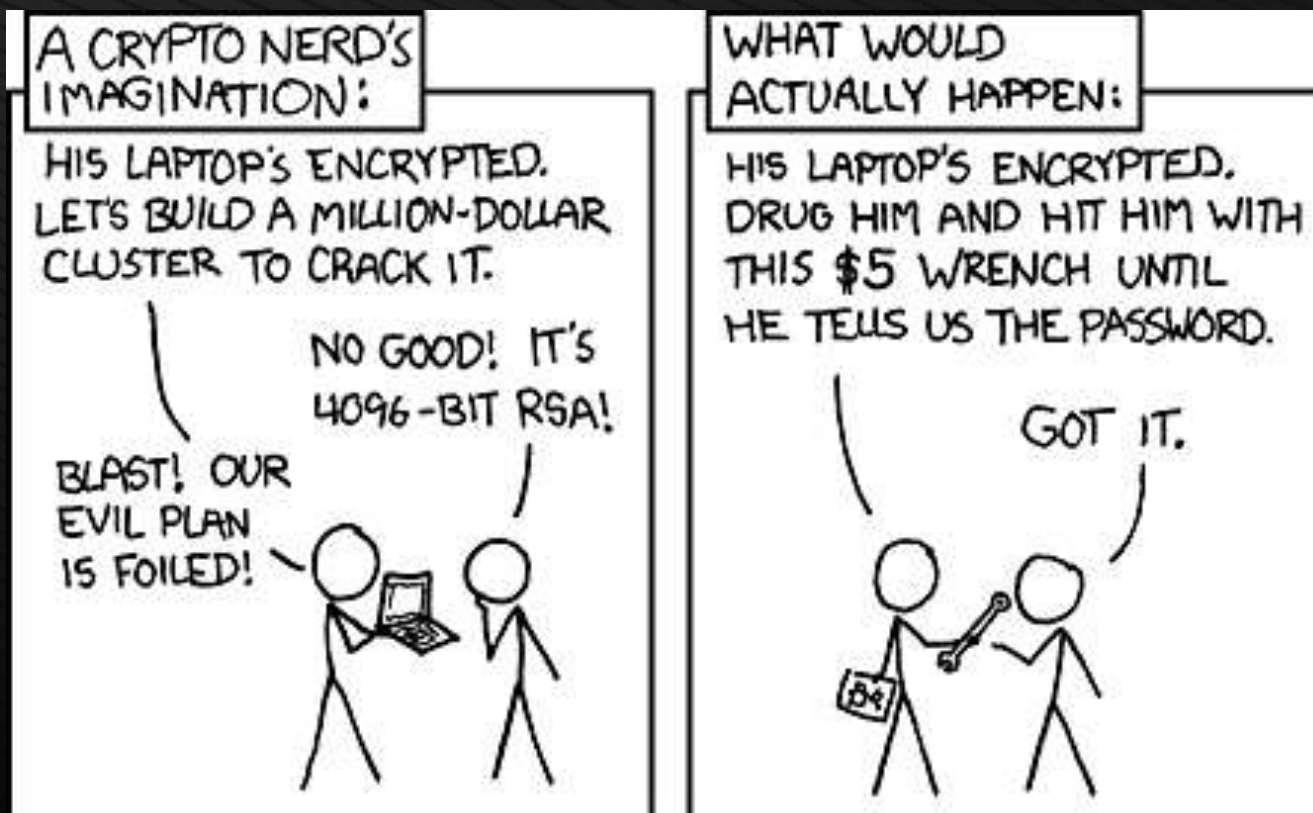
**URM**  
What Rights?



**DAM**  
When Used?  
Is it dormant?



# La naturale conclusione...





Questions?

English

¿Preguntas?

Spanish

مَطَالِبُ آيَّة

Arabic

вопросы?

Russian

Domande?

Italian

Ερωτήσεις?

Greek

Ḡorncyrin

Sindarin

tupoQghachmey

Klingon

質問

Japanese