Sicurezza delle reti e crittografia

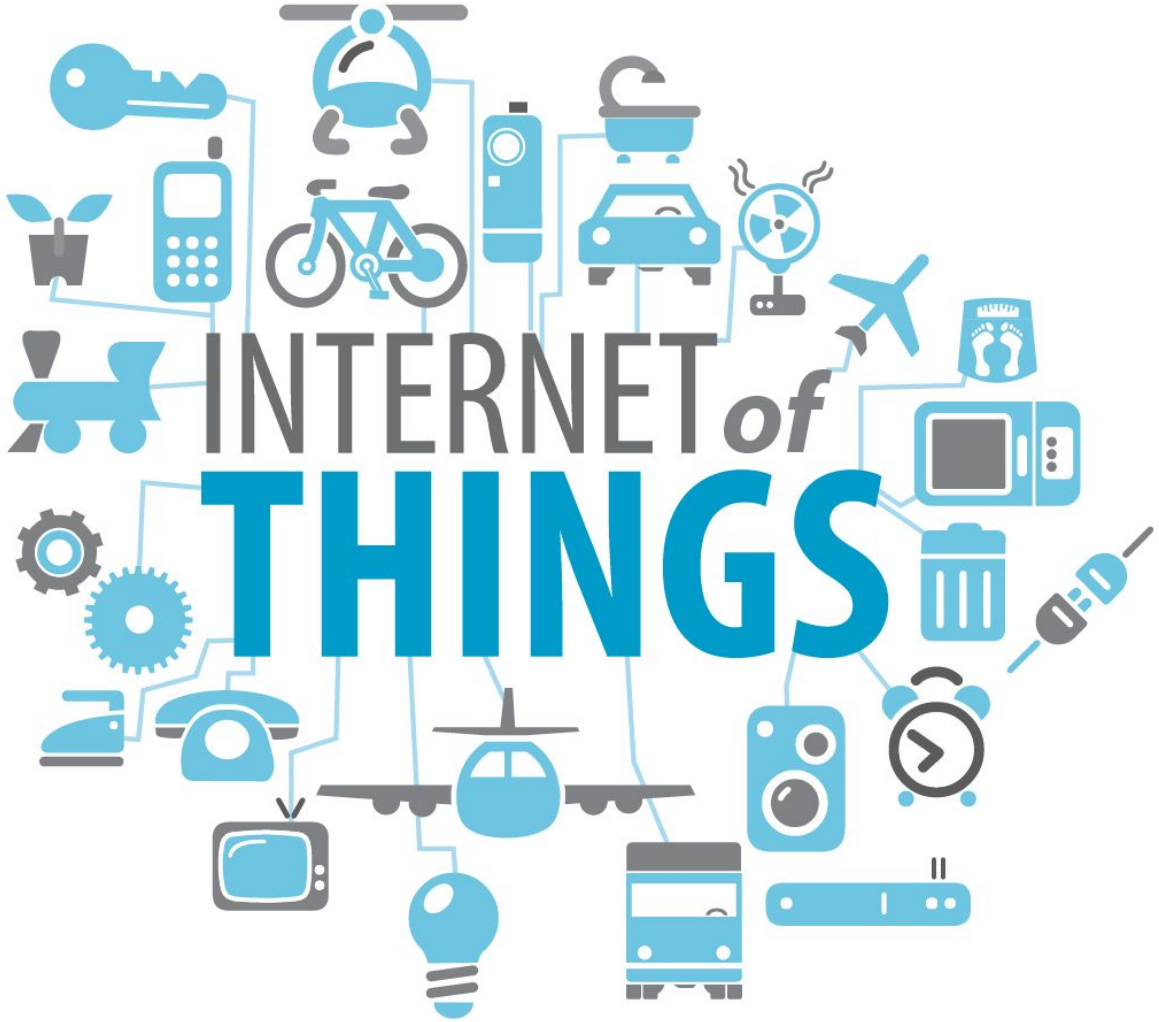
Riccardo Focardi

Università
Ca'Foscari
Venezia

Università Ca' Foscari Venezia
Cryptosense, Paris

8 Novembre 2016

IoT = tutto è connesso



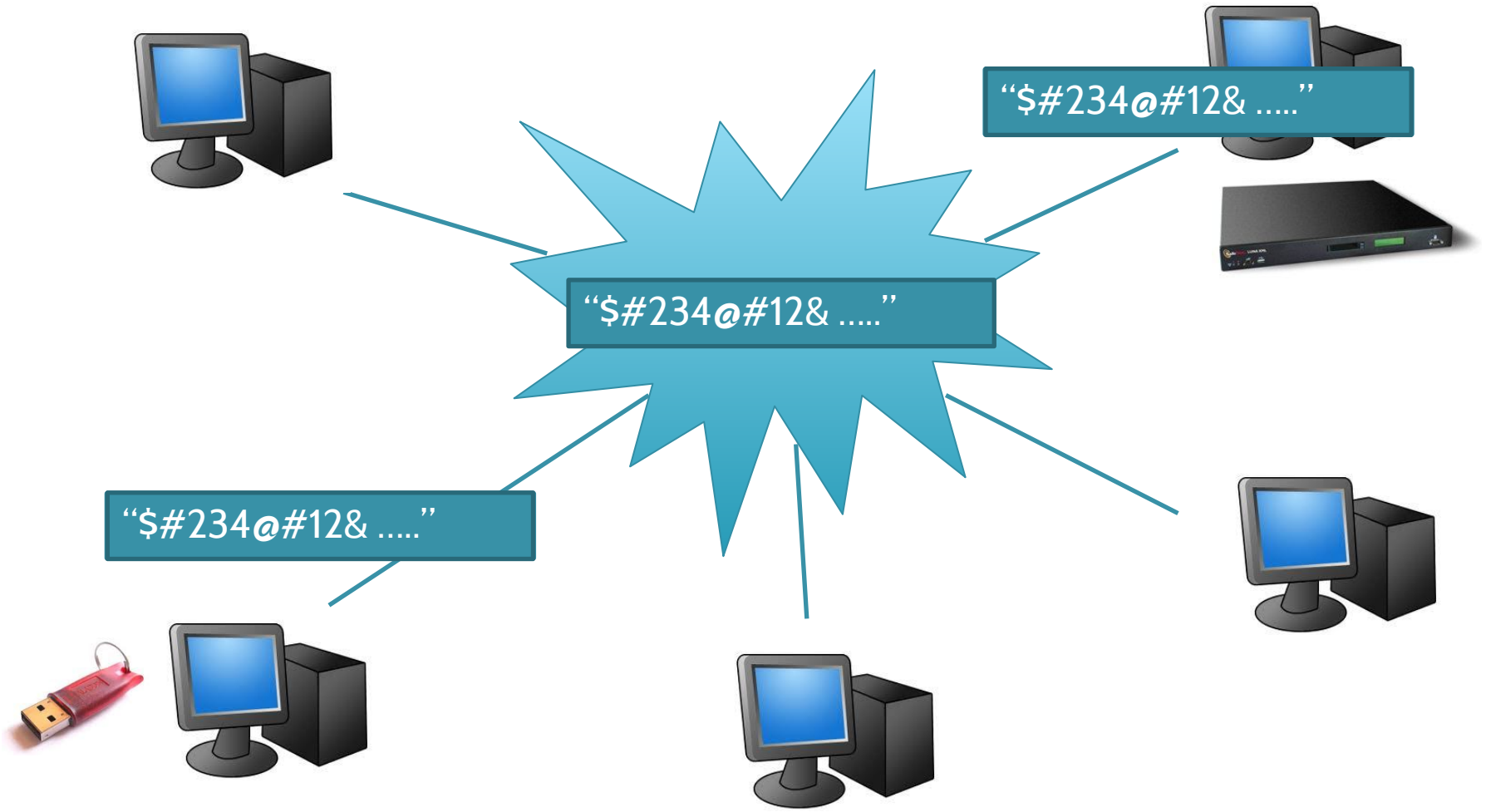
Sicurezza fisica e sicurezza digitale

La sicurezza digitale richiede

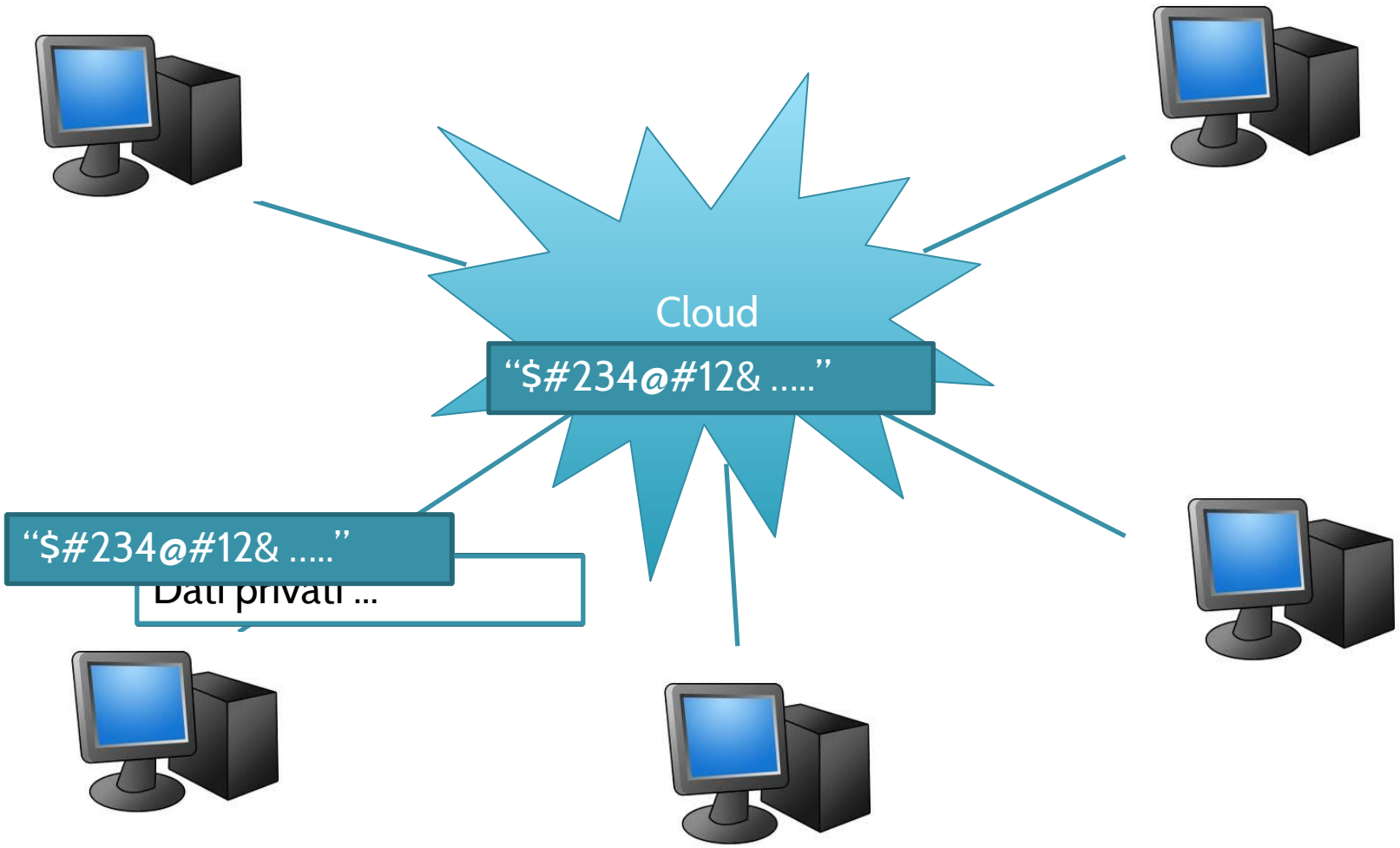
- Solide "mura" che separino ciò di cui ci fidiamo dal mondo esterno

- Protezione anche al di fuori delle "mura"

Il mondo esterno: Internet



Cloud o non cloud ...



La crittografia, o *scrittura nascosta*

Un testo viene trasformato in modo da non essere comprensibile

Cifrario di Cesare: ogni lettera è sostituita con quella 3 posizioni più avanti nell'alfabeto.

Brute force e crittoanalisi

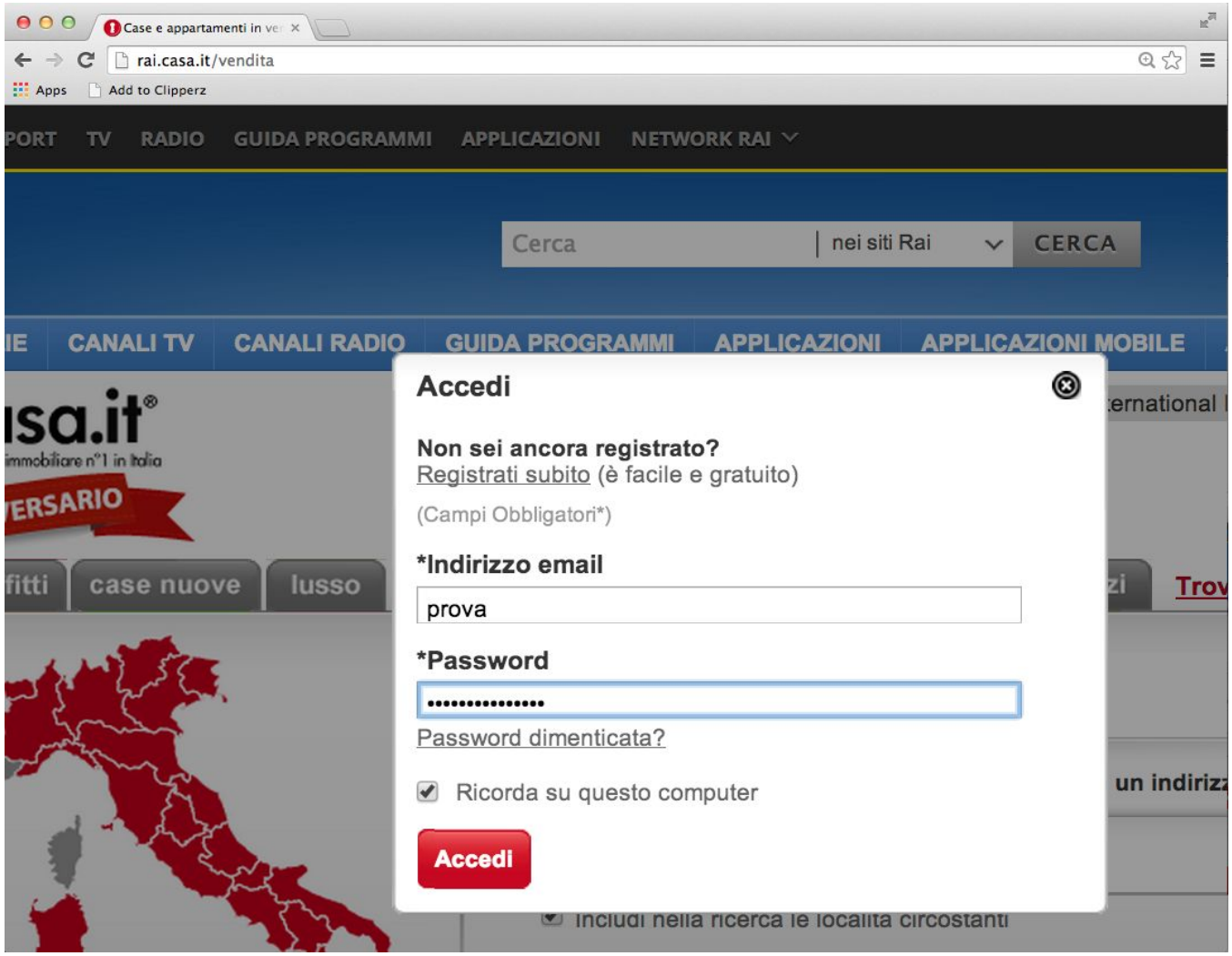
Il cifrario di Cesare ha solo 21 varianti … si possono **provare tutte**!

Lettere uguali sono cifrate **allo stesso modo**: è semplice individuare le vocali e le doppie

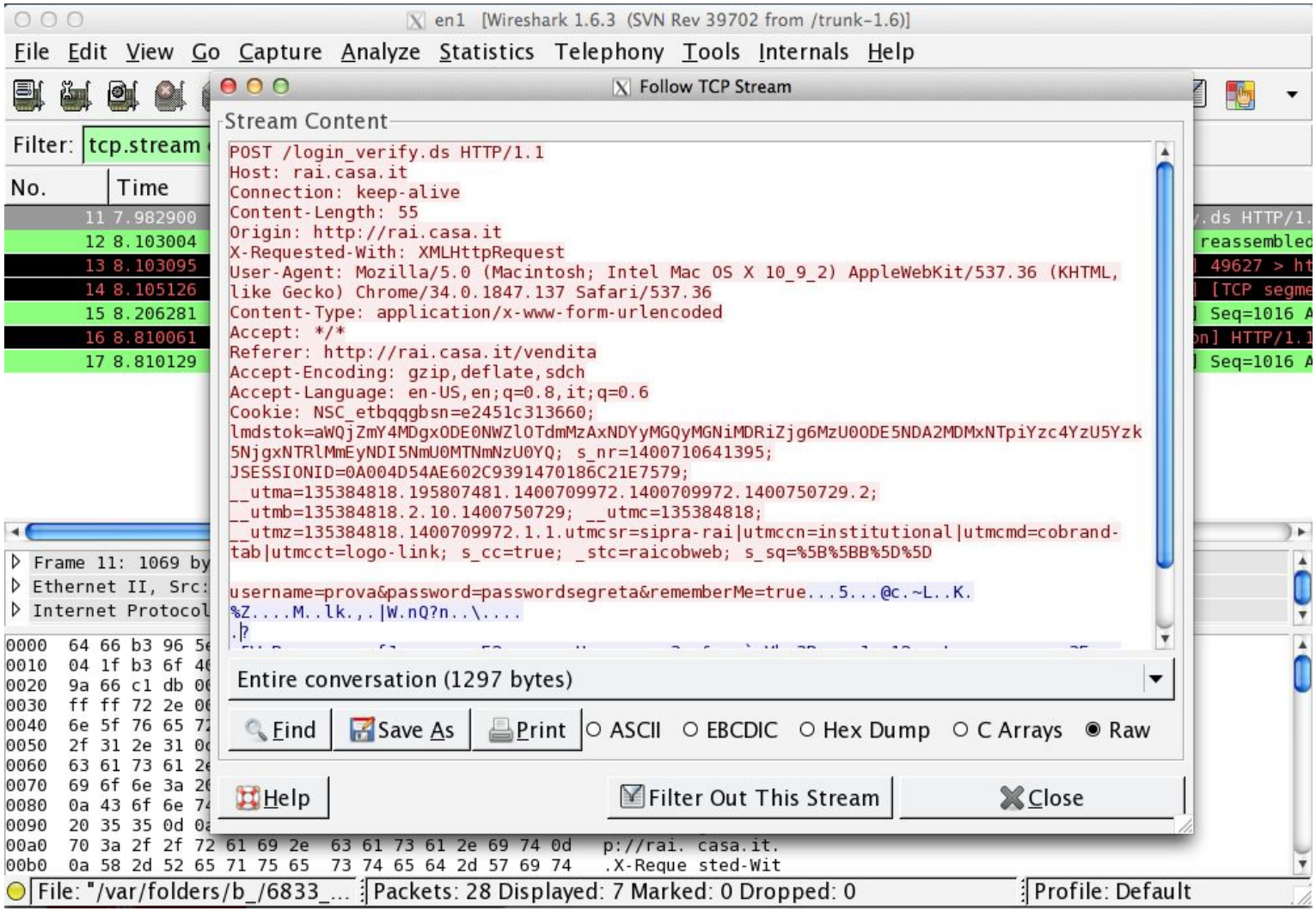
I cifrari moderni sono estremamente complessi e utilizzano *chiavi* di grandi dimensioni:

circa $\mathbf{3.40282367 \times 10^{38}}$ chiavi differenti

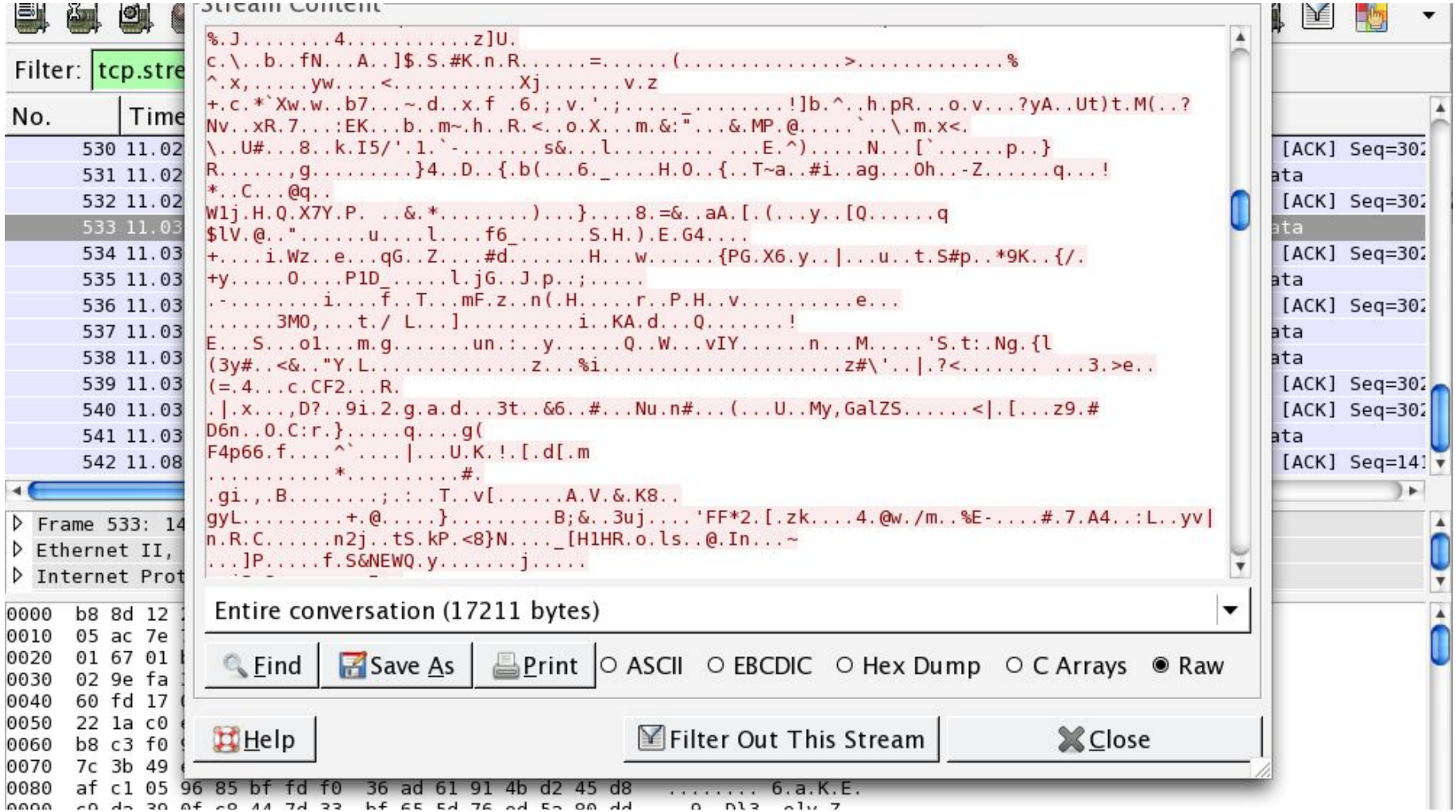
Crittografia sul Web: http e https



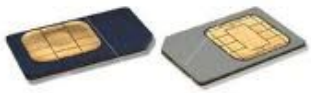
http: nessuna protezione!

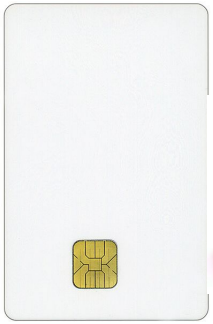


https: tutta la comunicazione è cifrata



Cryptography … of things!





Crittografia nelle banche

Pagamenti elettronici, bancomat, trasferimenti inter-bancari, ...

Hardware Security Module (HSM)

Costo 5k-20k € e mercato di circa 200M € annui

… non sempre le cose funzionano

Device		Supported Functionality						Attacks found				
Brand	Model	s	as	cobj	chan	w	ws	wd	rs	ru	su	Tk
Aladdin	eToken PRO	✓	✓	✓	✓	✓	✓	✓				wd
Athena	ASEKey	✓	✓	✓								
Bull	Trustway RCI	✓	✓	✓	✓	✓	✓	✓				wd
Eutron	Crypto Id. ITSEC		✓	✓								
Feitian	StorePass2000	✓	✓	✓	✓	✓	✓	✓	✓	✓		rs
Feitian	ePass2000	✓	✓	✓	✓	✓	✓	✓	✓	✓		rs
Feitian	ePass3003Auto	✓	✓	✓	✓	✓	✓	✓	✓	✓		rs
Gemalto	SEG		✓		✓							
MXI	Stealth MXP Bio	✓	✓		✓							
RSA	SecurID 800	✓	✓	✓	✓				✓	✓	✓	rs
SafeNet	iKey 2032	✓	✓	✓		✓						
Sata	DKey	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	rs
ACS	ACOS5	✓	✓	✓	✓							
Athena	ASE Smartcard	✓	✓	✓								
Gemalto	Cyberflex V2	✓	✓	✓		✓	✓	✓				wd
Gemalto	SafeSite V1		✓		✓							
Gemalto	SafeSite V2	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	rs
Siemens	CardOS V4.3 B	✓	✓	✓		✓				✓		ru

Attacchi reali!

20 febbraio 2013

35 000 000 € rubati in **meno di 10 ore**

L'attacco Heartbleed

Vulnerabilità di OpenSSL che implementa https

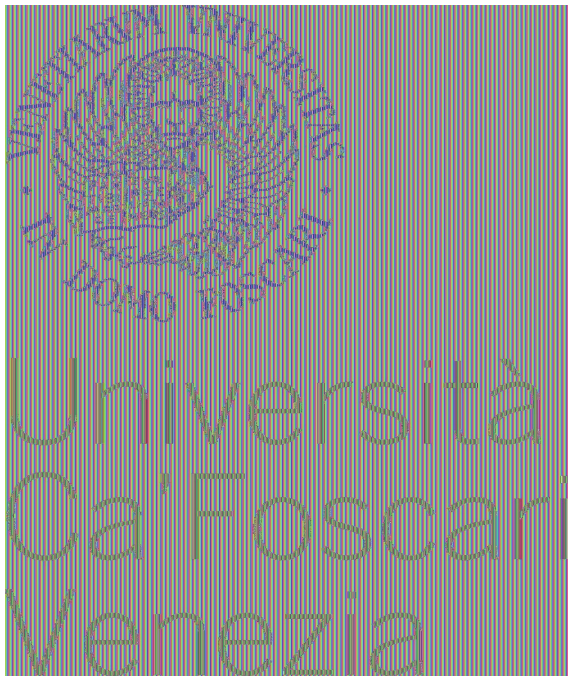
Un *over-read* permette di accedere a una parte di memoria del server che contiene le **chiavi crittografiche**

Tramite le chiavi è possibile decifrare **tutta la sessione Web**

Cattivo utilizzo di cifrari sicuri

Un cifrario sicuro usato in modo errato può essere facilmente attaccabile

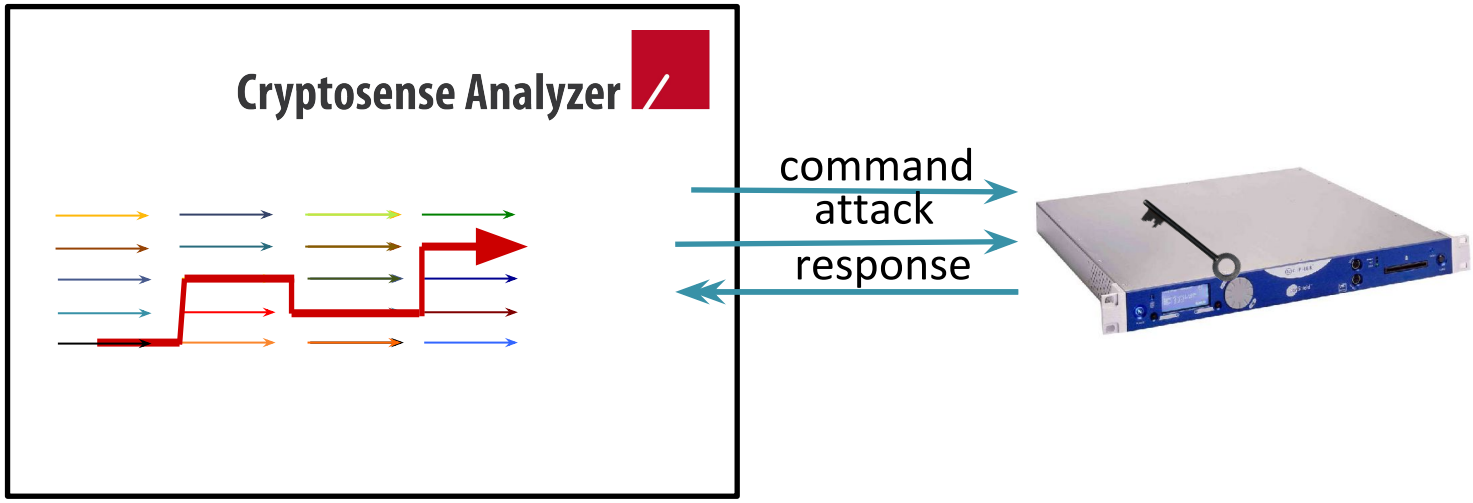
Università
Ca'Foscari
Venezia



Lo spin-off Cryptosense

Spin-off di INRIA e Ca' Foscari

Fondato a Settembre 2013 in Agoranov (Parigi)



Efficacia e impatto sulle aziende

Utilizzato da due **agenzie** per la sicurezza nazionale, due **banche** Europee, un **produttore** di smartcard

Adottato da ANSSI come tool standard per HSM

Database contenente svariate vulnerabilità su HSM e smartcard

Business plan

Prodotti

Java Crypto Tracer
Crypto Discovery
Java Crypto Training

Obiettivi futuri

Web service APIs
Web app APIs
Databases
etc.

Vision: analizzare tutta la crittografia *enterprise*

Grazie per l'attenzione!

Maggiori informazioni

http://www.dais.unive.it/~focardi
http://cryptosense.com

Twitter @rfocardi
email focardi@unive.it

Riferimenti bibliografici

Attacchi su crittografia "embedded":

- R. Verdult, F. D. Garcia and B. Ege. **Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer**. USENIX Security 2013
- R. Bardou, R. Focardi, Y. Kawamoto, L. Simionato, G. Steel, J. Tsay. **Efficient Padding Oracle Attacks on Cryptographic Hardware**. CRYPTO 2012
- M. Bortolozzo, M. Centenaro, R. Focardi, G. Steel. **Attacking and fixing PKCS#11 security tokens**. ACM CCS 2010
- F. D. Garcia, P. van Rossum, R. Verdult and R. Wichers Schreur. **Wirelessly Pickpocketing a Mifare Classic Card**. IEEE S&P 2009