

Sicurezza delle reti e crittografia

Riccardo Focardi

Università Ca' Foscari Venezia
Cryptosense, Paris



Università
Ca' Foscari
Venezia

8 Novembre 2016

IoT = tutto è connesso



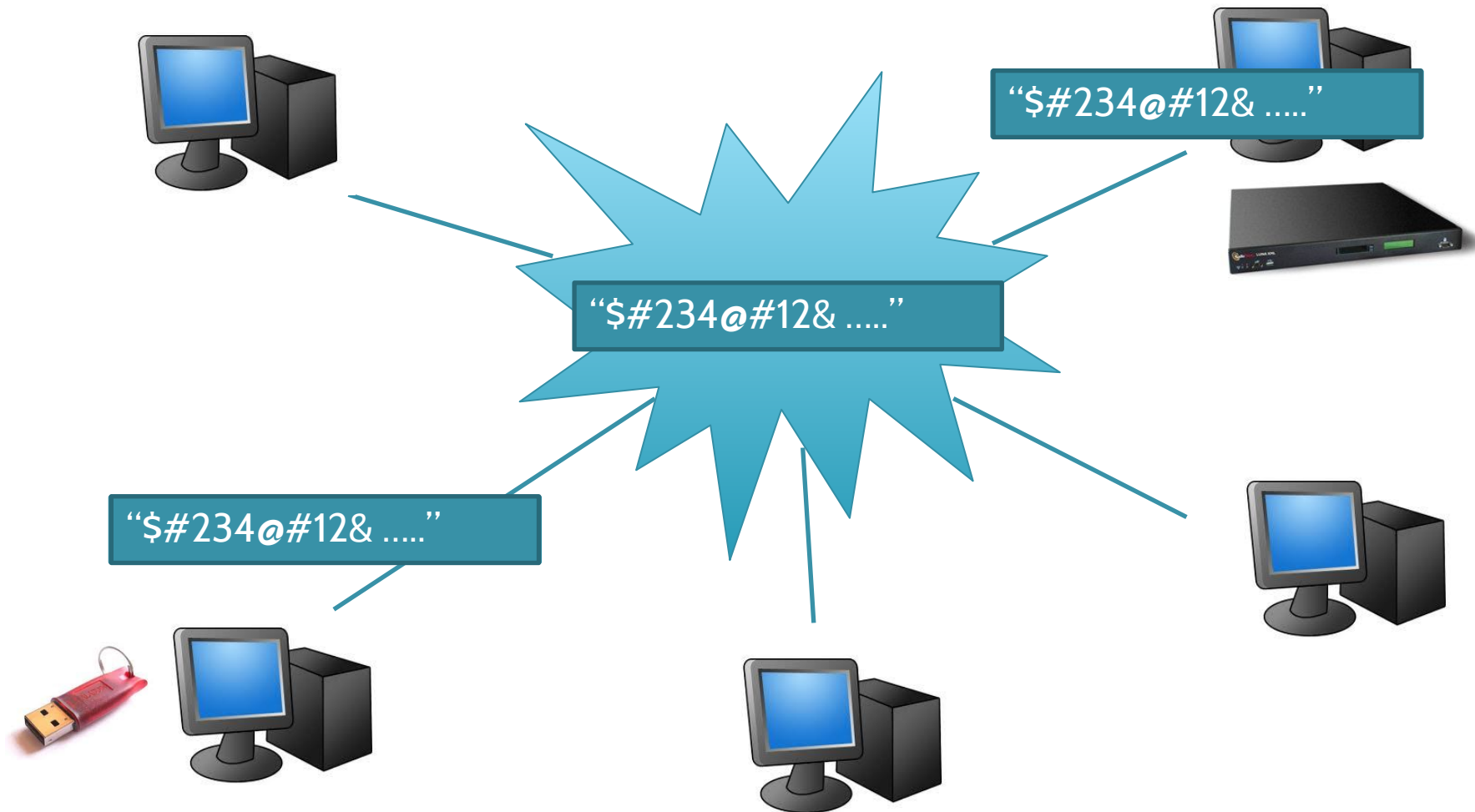
Sicurezza fisica e sicurezza digitale

La sicurezza digitale richiede

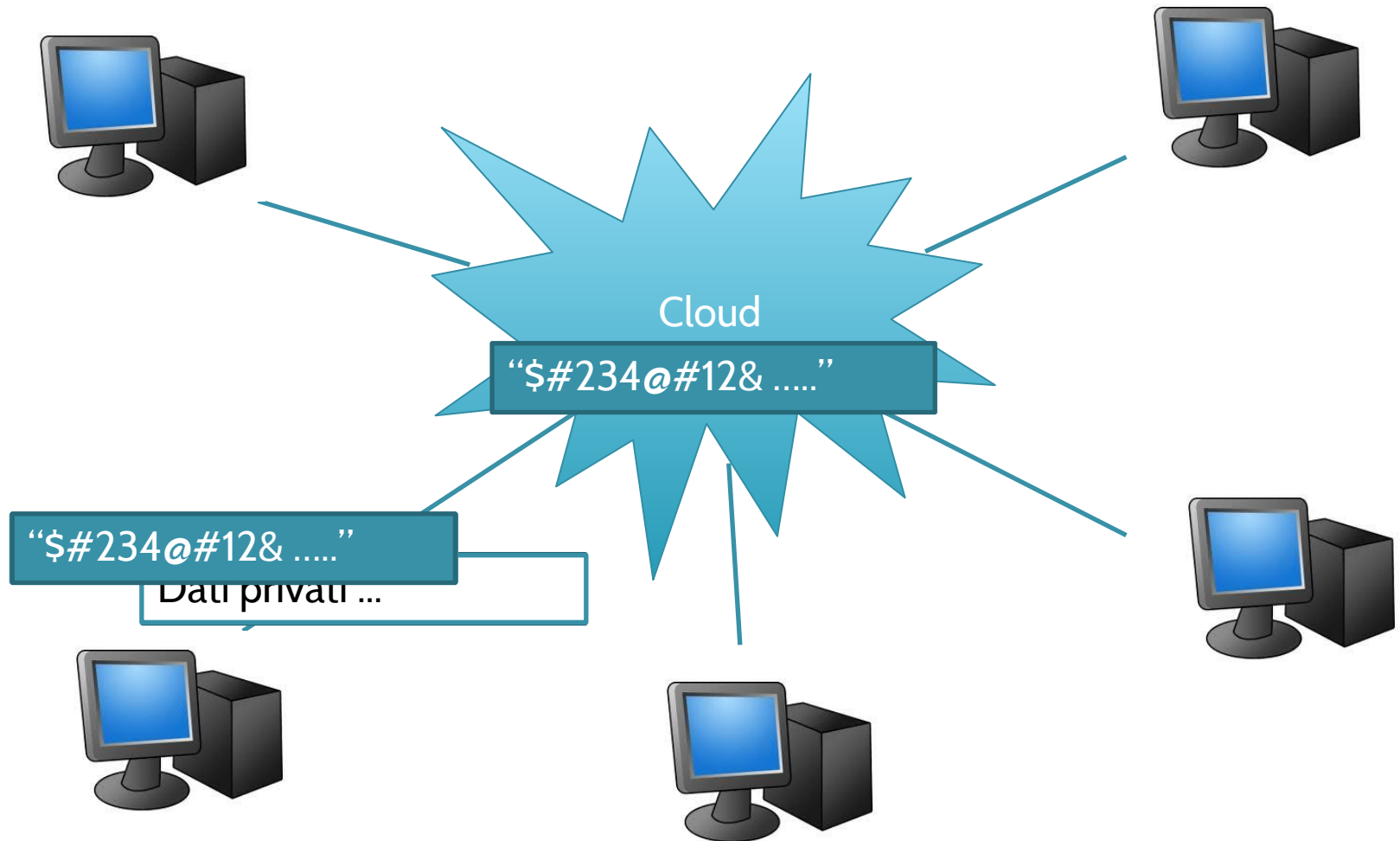
- Solide “mura” che separino ciò di cui ci fidiamo dal mondo esterno
- Protezione anche al di fuori delle “mura”



Il mondo esterno: Internet



Cloud o non cloud ...

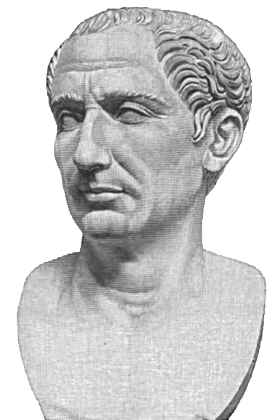


La crittografia, o *scrittura nascosta*

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.

GRPAV!



Brute force e crittoanalisi

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

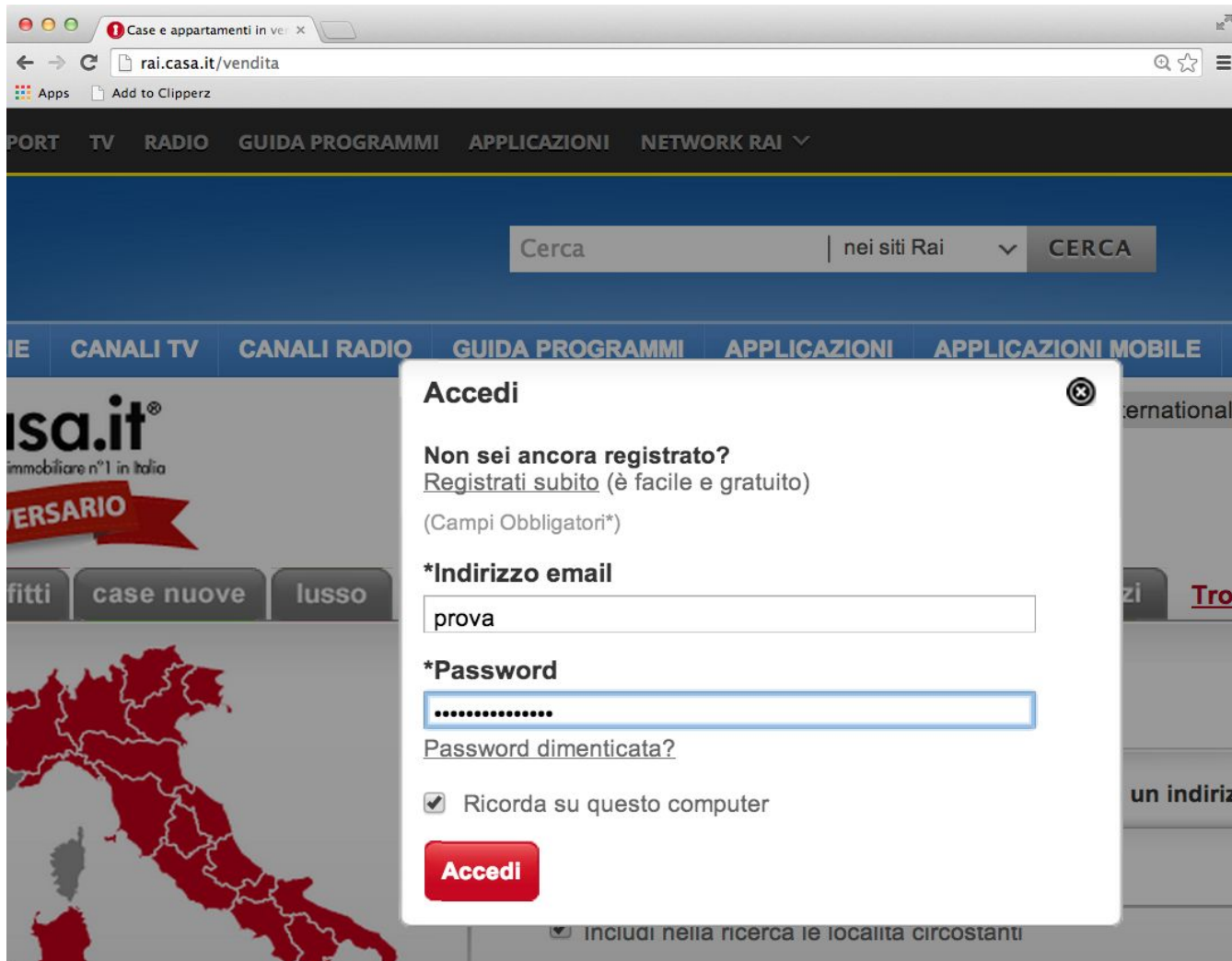
Lettere uguali sono cifrate **allo stesso modo**: è semplice individuare le vocali e le doppie

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

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



Crittografia sul Web: http e https



http: nessuna protezione!

en1 [Wireshark 1.6.3 (SVN Rev 39702 from /trunk-1.6)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp.stream

No.	Time
11	7.982900
12	8.103004
13	8.103095
14	8.105126
15	8.206281
16	8.810061
17	8.810129

Stream Content

```
POST /login_verify.ds HTTP/1.1
Host: rai.casa.it
Connection: keep-alive
Content-Length: 55
Origin: http://rai.casa.it
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_2) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/34.0.1847.137 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Referer: http://rai.casa.it/venedita
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US, en; q=0.8, it; q=0.6
Cookie: NSC_etbqqgbsn=e2451c313660;
lmdstok=aWQjZmY4MDgxODE0NWZlOTdmMzAxNDYyMGQyMGNiMDRiZjg6MzU0ODE5NDA2MDMxNTpiYzc4YzU5Yzk
5NjgxNTRlMmEyNDI5NmU0MTNmNzU0YQ; s_nr=1400710641395;
JSESSIONID=0A004D54AE602C9391470186C21E7579;
__utma=135384818.195807481.1400709972.1400709972.1400750729.2;
__utmb=135384818.2.10.1400750729; __utmc=135384818;
__utmz=135384818.1400709972.1.1.utmcsr=supra-rai|utmccn=institutional|utmcmd=cobrand-
tab|utmctt=logo-link; s_cc=true; _stc=raicobweb; s_sq=%5B%5BB%5D%5D

username=prova&password=passwordsegreta&rememberMe=true...5...@c.~L..K.
%Z...M..lk...|W.nQ?n.. \....
.P
```

Entire conversation (1297 bytes)

Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw

Help Filter Out This Stream Close

File: "/var/folders/b_/6833_..."; Packets: 28 Displayed: 7 Marked: 0 Dropped: 0; Profile: Default

https: tutta la comunicazione è cifrata

Filter: tcp.stre

No.	Time
530	11.02
531	11.02
532	11.02
533	11.03
534	11.03
535	11.03
536	11.03
537	11.03
538	11.03
539	11.03
540	11.03
541	11.03
542	11.08

Stream Content

```
%J.....4.....z]U.  
c.\..b..fN...A..]$S.#K.n.R.....=(.....>.....%  
^X,.....yw...<.....Xj.....v.z  
+c.*`Xw.w..b7...~.d..x.f..6.;v.';.....!b.^..h.pR...o.v...?yA..Ut)t.M(...?  
Nv..xR.7...:EK...b..m~.h..R.<..o.X...m.&:"...&.MP.@.....'\.m.x<.  
\..U#...8..k.I5/'..1..'.....s&...l.....E.^).....N...['.....p..}  
R.....g.....}4..D..{.b(...6...H.O..{.T~a..#i..ag...0h...-Z.....q...!  
*..C...@q..  
Wlj.H.Q.X7Y.P...&.*.....).....}.....8.=&.aA.[.(...y..[Q.....q  
$lV.@.."......u....l....f6.....S.H.)E.G4....  
+...i.Wz..e...qG..Z...#d.....H..w.....{PG.X6.y..|...u..t.S#p..*9K..{/..  
+y.....0....P1D.....l.jG..J.p.;.....  
..-.....i....f..T...mF.z.n(.H.....r..P.H..v.....e...  
.....3M0,..t./L...]......i..KA.d...Q.....!  
E...S...o1...m.g.....un...y.....Q..W...vIY.....M.....'S.t:Ng.{l  
(3y#..<&.."Y.L.....z...%i.....z#\'.|.?<.....3.>e..  
(=.4...c.CF2...R.  
..|x...D?.9i.2.g.a.d...3t..&6..#...Nu.n#...(...U..My,GaLZS.....<|. [...z9.#  
D6n..0.C:r}.....q...g{  
F4p66.f....^'....|...U.K.!. [.d[m  
.....*.....#.  
.gi...B.....;...T..v[.....A.V.&.K8..  
gyL.....+.@.....}.....B;&..3uj....'FF*2.[.zk....4.@w./m..%E-...#.7.A4...L..yv|  
n.R.C.....n2j..tS.kP.<8}N..._[H1HR.o.l.s..@.In...~  
...]P.....f.S&NEWQ.y.....j.....
```

Entire conversation (17211 bytes)

Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw

Help Filter Out This Stream Close

0000 b8 8d 12
0010 05 ac 7e
0020 01 67 01
0030 02 9e fa
0040 60 fd 17
0050 22 1a c0
0060 b8 c3 f0
0070 7c 3b 49
0080 af c1 05 96 85 bf fd f0 36 ad 61 91 4b d2 45 d8 6.a.K.E.
0090 c0 d0 30 af c0 44 7d 33 bf 65 5d 76 ad 5a 0a dd 0 n13 a1u 7

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

Brand	Device Model	Supported Functionality						Attacks found				Tk	
		s	as	cobj	chan	w	ws	wd	rs	ru	su		
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



The code for devices like RSA Security's SecurID 800 constantly changes, but computer scientists have found weaknesses.

Scientists Make Short Work Of Breaking Security Keys

By SOMINI SENGUPTA

For years private companies and government agencies have given their employees a card or token that produces a constantly changing set of numbers. Those devices became the preferred method of securing confidential communications online. No one could have access to the data without a secret key generated by the device.

Computer scientists say they have now figured out how to extract that key from a widely used RSA electronic token in as little as 13 minutes.

The scientists, who call themselves Team Prosecco, said their experiment can pry open one model of the RSA dongle — the SecurID 800 — as well as similar tools produced by other companies. They published their findings in a research paper to be presented at a cryptography conference in August; the findings were first reported Monday morning by Ars Technica, a technology news site.

encryption tools were antiquated and susceptible to attack.

"It would be nice if manufacturers paid more heed to what they might see only as theoretical attacks and were more cautious," said Chris Peikert, a theoretical cryptographer who teaches computer science at the Georgia Institute of Technology. "In an ideal world this problematic standard would have been transitioned away from years ago."

One of the reasons this standard has persisted, Mr. Peikert said, is that until now, researchers and manufacturers reckoned that it would take a long time to

Cracking the codes on devices used to safeguard confidential data.

crack the key — and would there-

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**

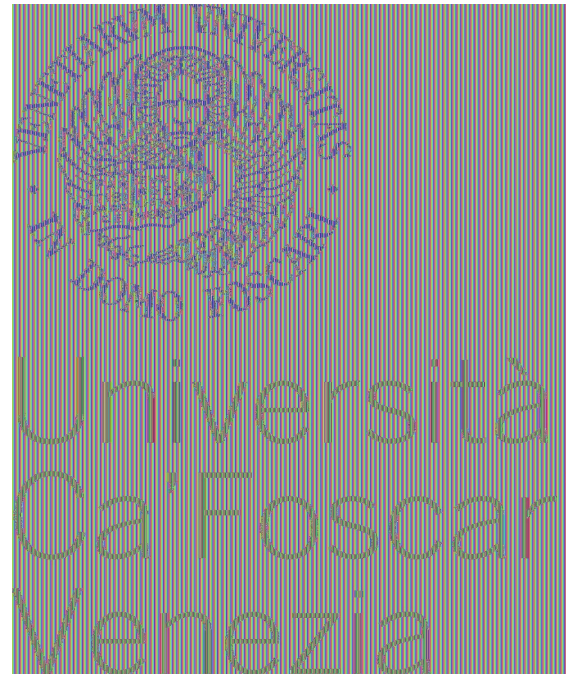


Cattivo utilizzo di cifrari sicuri

Un cifrario sicuro usato in modo errato può essere facilmente attaccabile



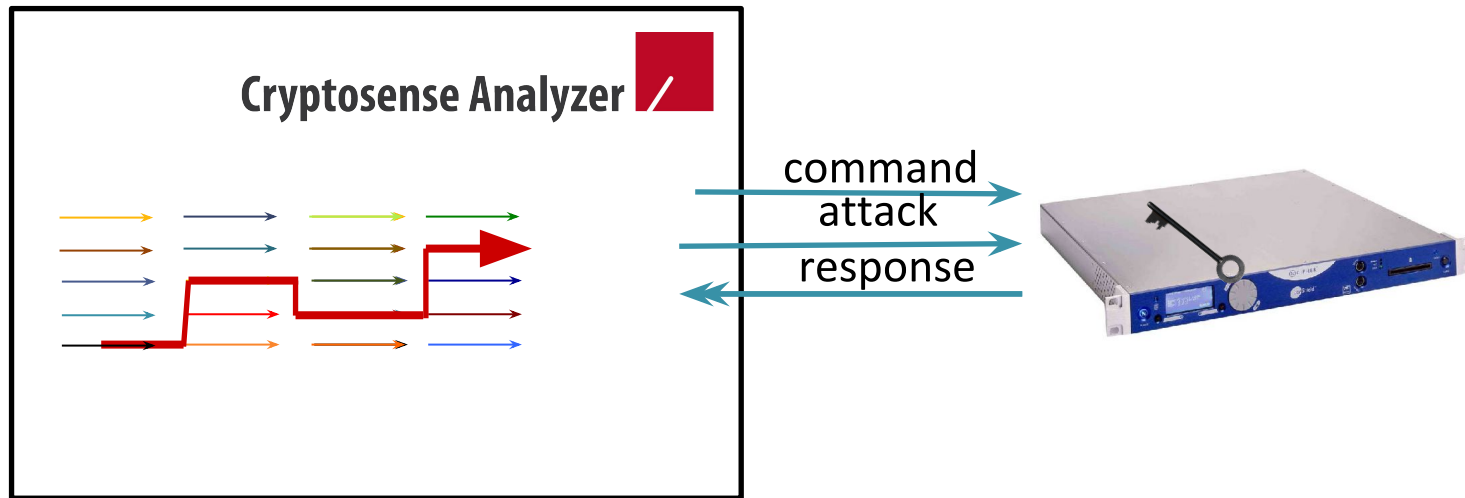
Università
Ca' Foscari
Venezia



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