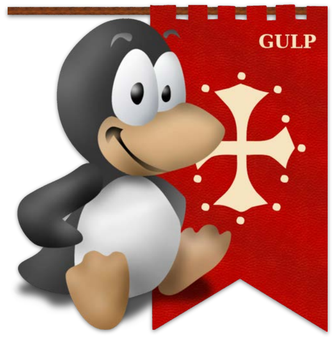


Augiero.it

2013
LINUX
D A Y
I T A L I A

Giuseppe Augiero, *Linux Day Pisa 2013*

L'ARTE DELLA INTERCETTAZIONE 2.0

26 ottobre 2013 - *Scuola Normale Superiore*

AGENDA

DIFENDIAMOCI

Aumentiamo le nostre difese cercando di capire cosa farebbe un attaccante.

ANALIZIAMO UN ATTACCO

Analiziamo un attacco MITM per il traffico SSL.

RENDIAMOLO COMPLESSO

Cerchiamo di rendere l'attaco il più possibile "trasparente" all'utente.

SICUREZZA INFORMATICA

Maggiore sensibilità nei confronti della gestione dei nostri dati personali.

DISCLAIMER

SCOPO DIDATTICO

Il seguente materiale ha scopo unicamente didattico.

REATO PENALE

L'intercettazione è un reato punibile penalmente.

ALTRI SCOPI

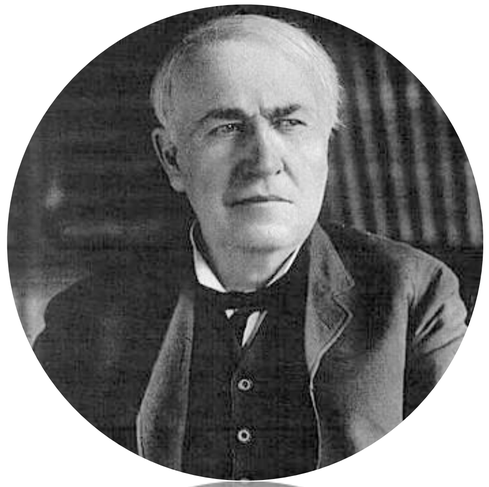
Qualsiasi altro utilizzo delle informazioni riportate in queste slide è vietato.

USI IMPROPRI

L'autore non si assume alcuna responsabilità per usi impropri.

SECURE SOCKETS LAYER

ATTACCHIAMO IL PROTOCOLLO



“*Per inventare hai bisogno di una buona immaginazione e di una pila di cianfrusaglie.*”

THOMAS EDISON

ELEMENTI DELLA COMUNICAZIONE

CLIENT

SERVER

CERTIFICATO SSL

CIFRATURA

MAN IN THE MIDDLE

PRIMA SOLUZIONE

- La comunicazione viene scissa in due.
- L'attaccante genera un falso certificato che invia al client e apre una connessione verso il server.
- Il certificato ssl inviato al client non sarà riconosciuto come attendibile e affidabile.

CATENA DI FIDUCIA

CA CERTIFICATE

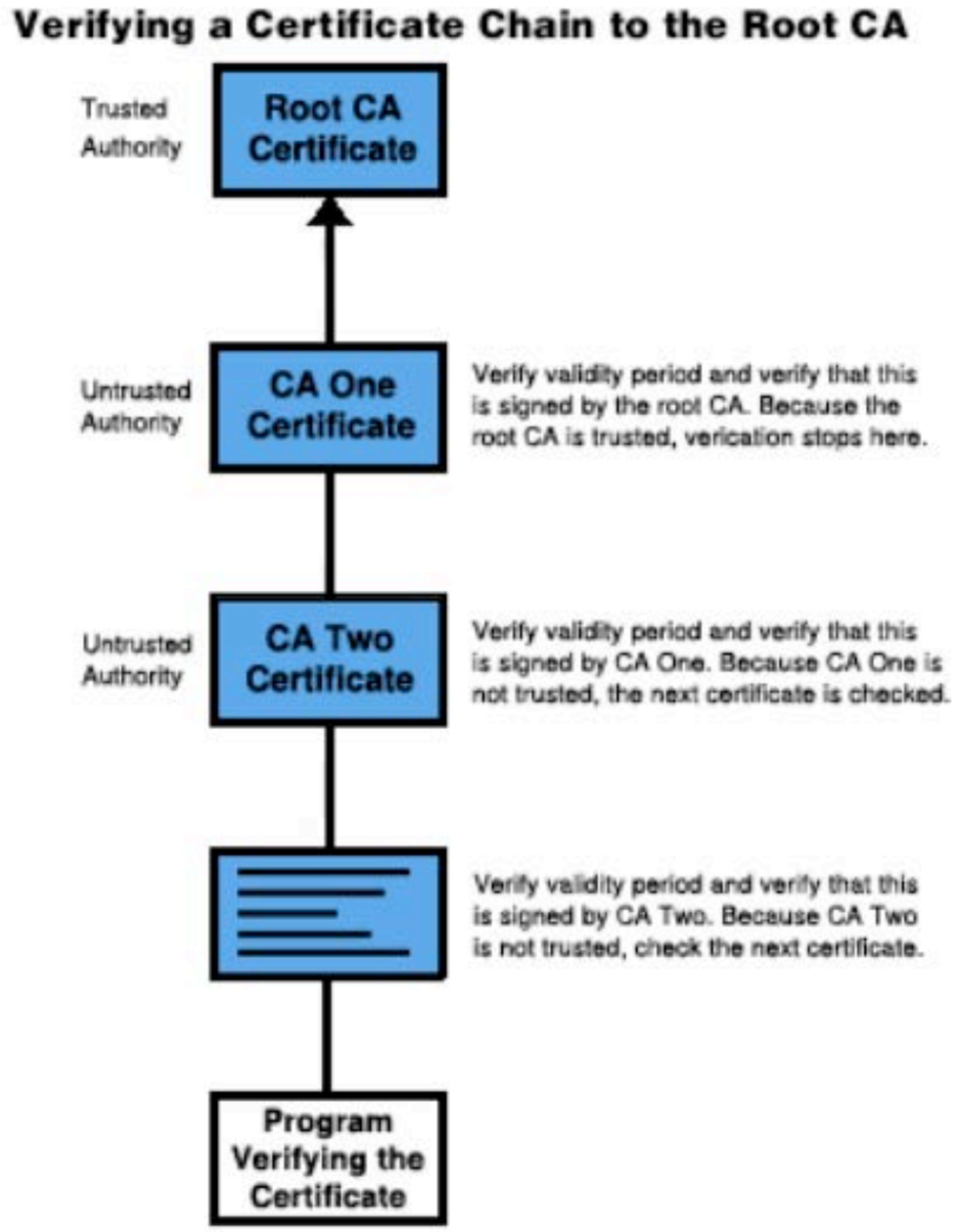
- Integrato nel browser.
- Garantisce l'autenticità del certificato ssl di un sito.

INTERMEDIATE CA

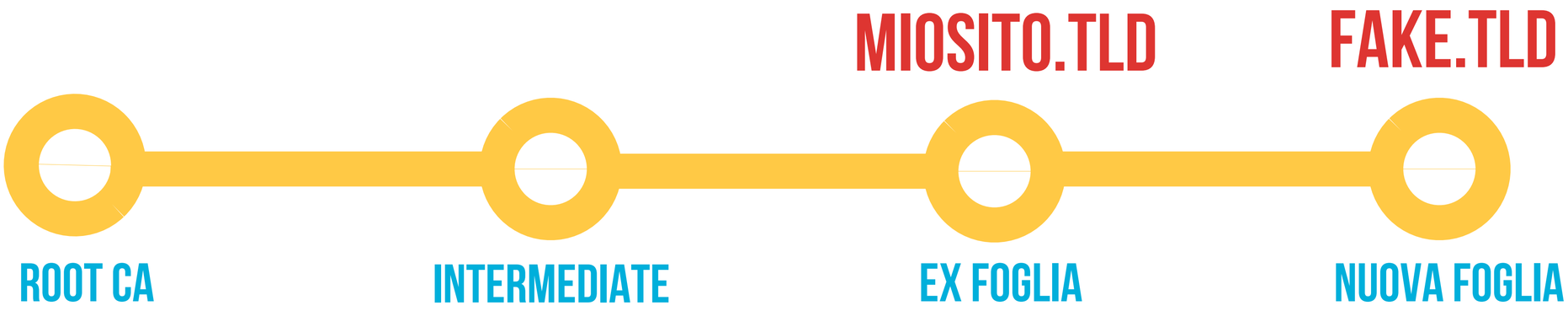
- Non integrato nel browser.
- Garantisce l'autenticità del certificato ssl di un sito.

SITE CERTIFICATE

- Identifica un particolare sito.
- Necessita della verifica della signature.



NUOVO CERTIFICATO



Un certificato è valido se:

- Il nome del certificato coincide con quello del sito.
- Non è scaduto.
- La catena di certificazione è valida.

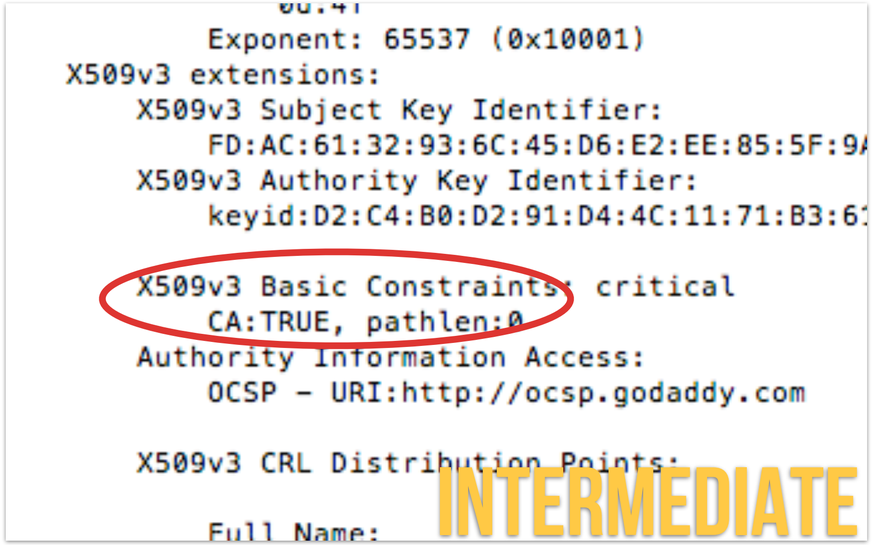
SECONDA SOLUZIONE

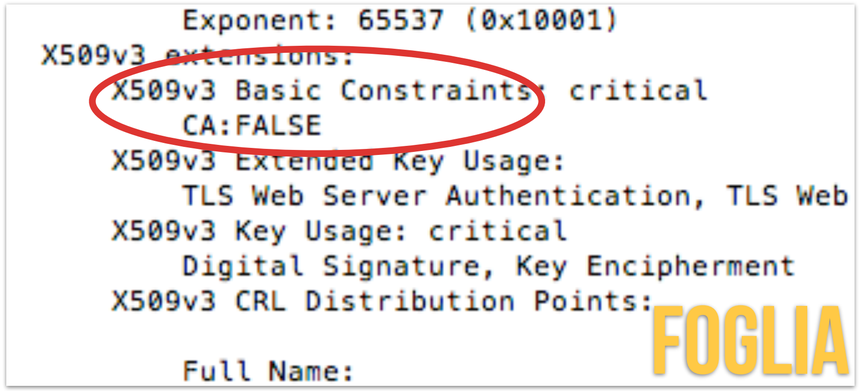
La comunicazione è scissa in due, il certificato ssl inviato dall'attaccante al client "*è riconosciuto*" come valido e affidabile.

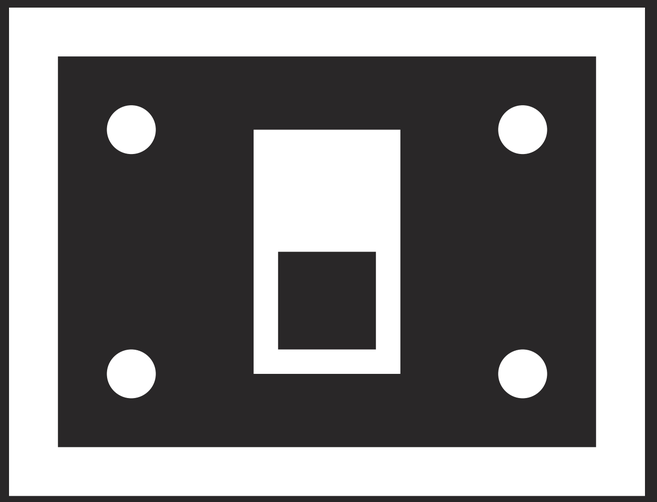
IL DUBBIO

ABBIAMO REALMENTE CREATO UN CERTIFICATO VALIDO?

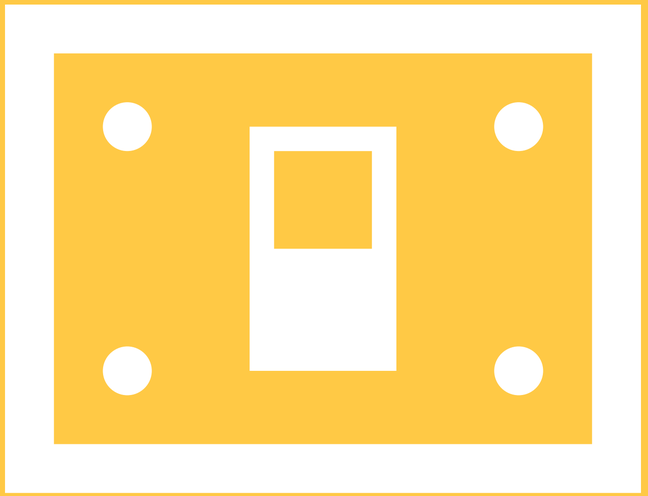
- Vecchia vulnerabilità.
- Alcuni browser non validavano il campo *BasicConstraints* del X509 in cui era settato il bit CA=FALSE rendendo perciò possibile la firma di un altro certificato con un certificato foglia.
- La foglia non era più tale ma diveniva una CA.







OCCORRE CAMBIARE APPROCCIO



NUOVO PUNTO DI VISTA

CONSIDERAZIONI

COME VIENE INVOCATO SSL?

Per aprire le pagine di un sito web:

- Pochi digitano https://...
- Qualcuno scrive http://...
- Molti usano un motore di ricerca.
- Altri credono che sia vera l'equazione *Internet = Facebook.*

LE PERSONE USANO SSL:

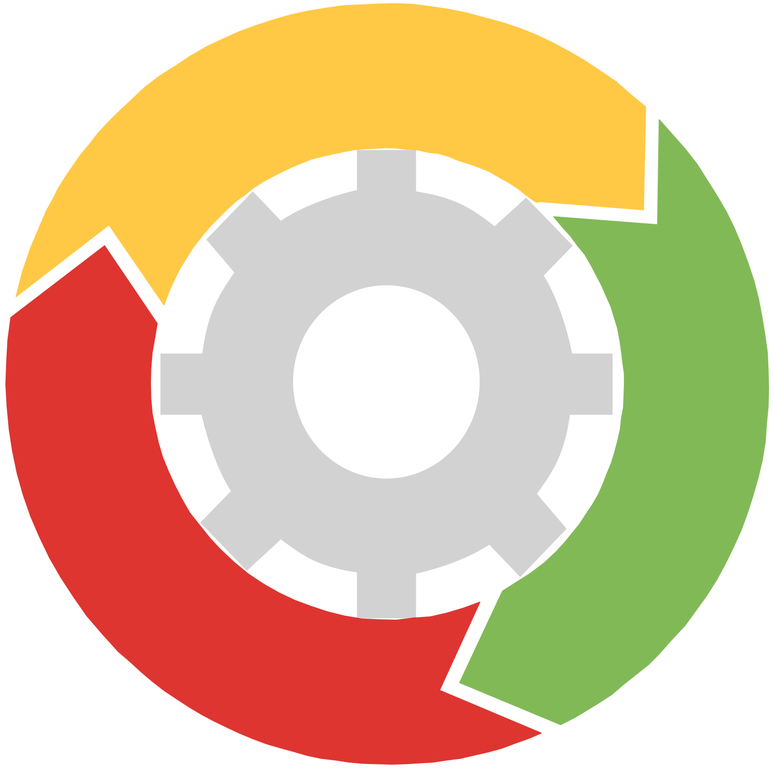
1. CLICCANDO SU UN LINK
2. ATTRAVERSO UN REDIRECT

NUOVO APPROCCIO

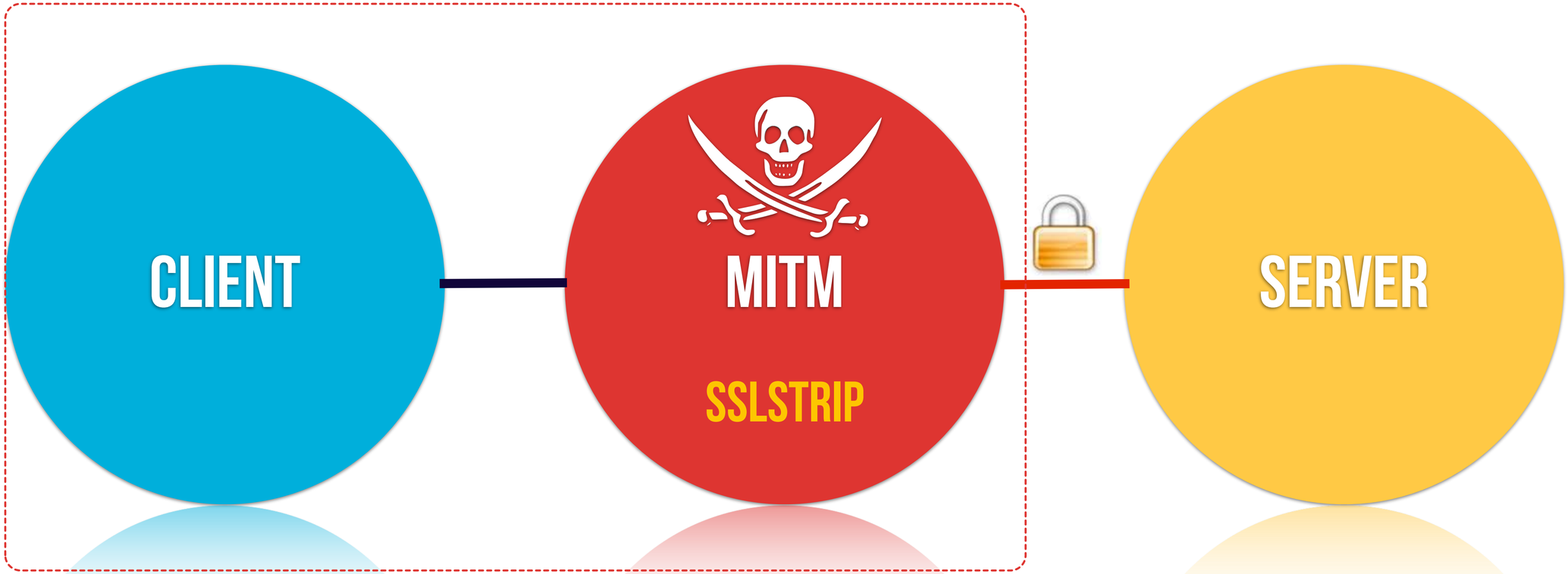
HTTP VS HTTPS

Occorre trovare un nuovo modo di attaccare il protocollo https spogliandolo della cifratura (quindi della s) e gestendo le due casistiche precedenti:

- Https richiamato attraverso un link.
- Redirect da http (**302**).

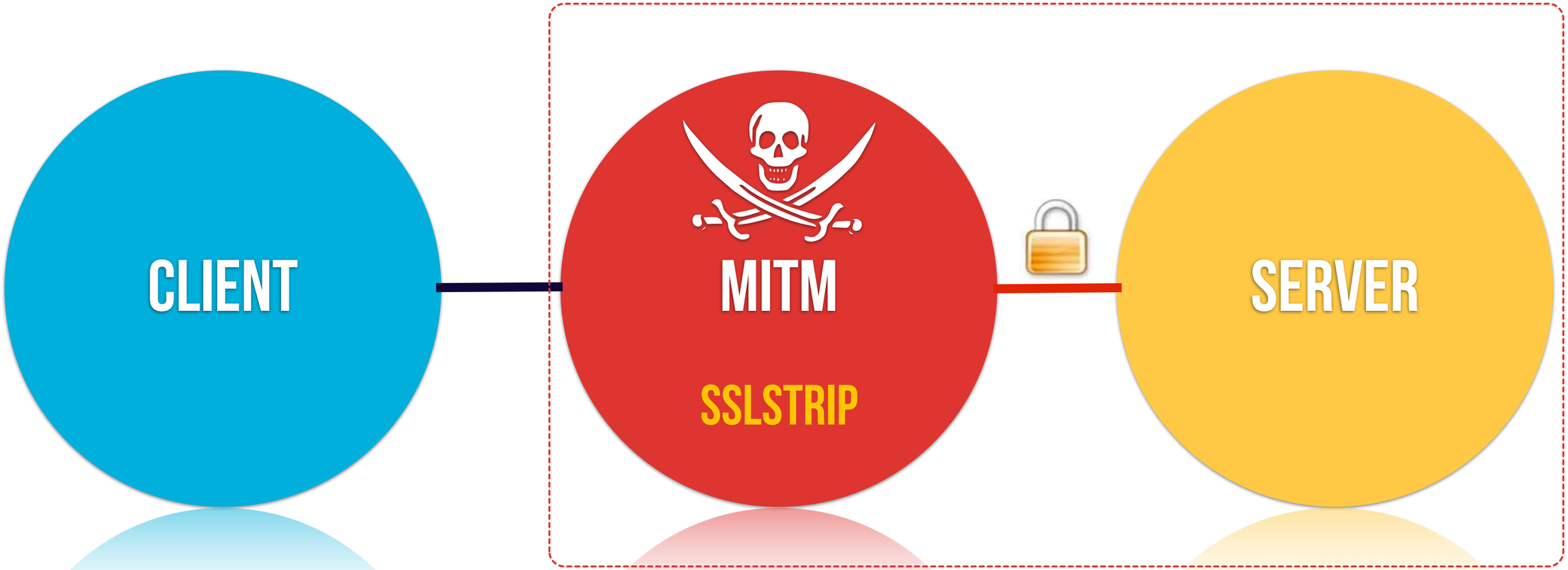


TERZA SOLUZIONE (CLIENT SIDE)



- Il MITM guarda e analizza il traffico http che passa.
- Modifica tutti i link presenti nelle pagine scaricate da https in http e mantiene una mappa.
- Modifica gli indirizzi digitati sostituendo gli https con http e mantiene una mappa.

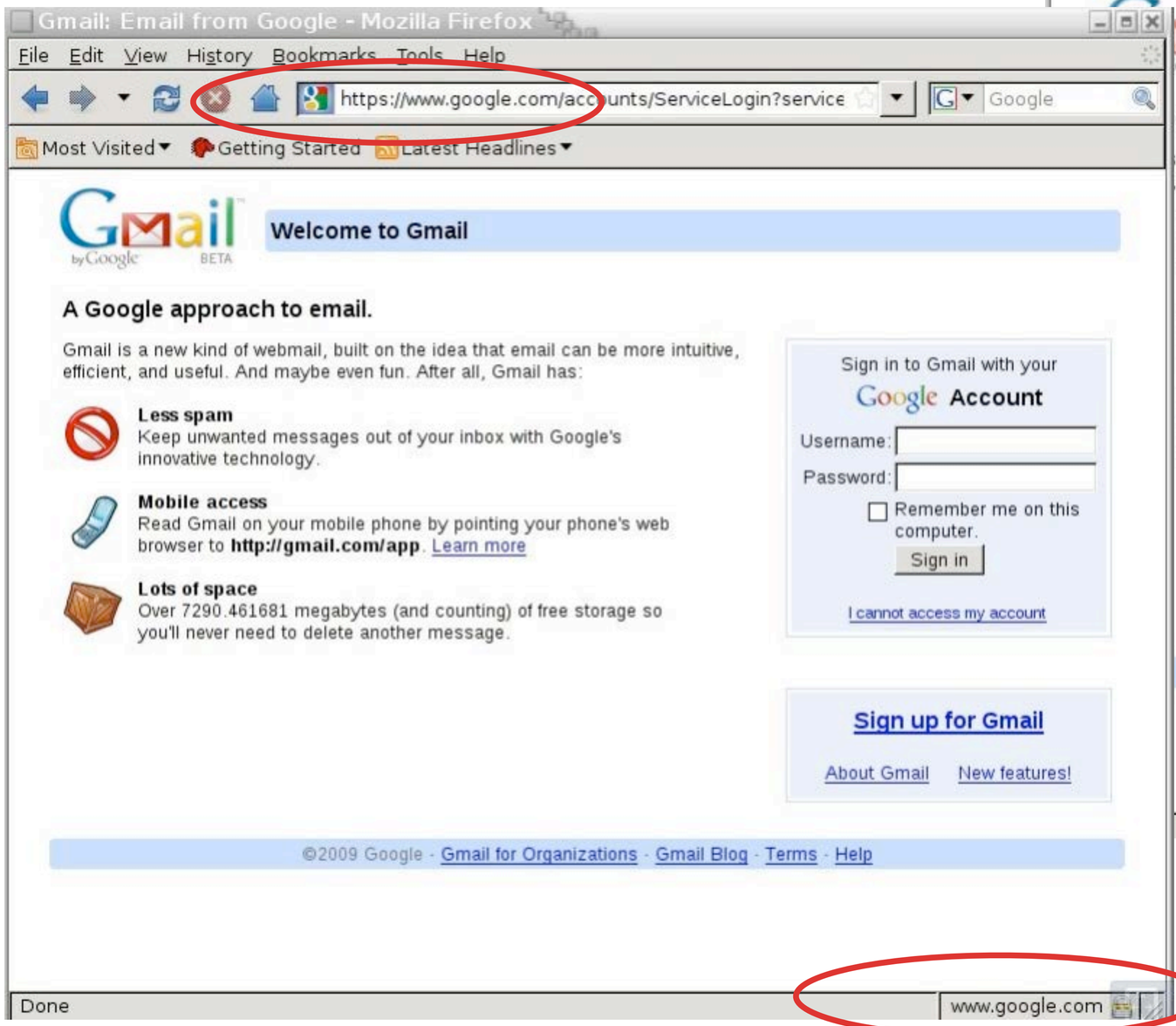
TERZA SOLUZIONE (SERVER SIDE)

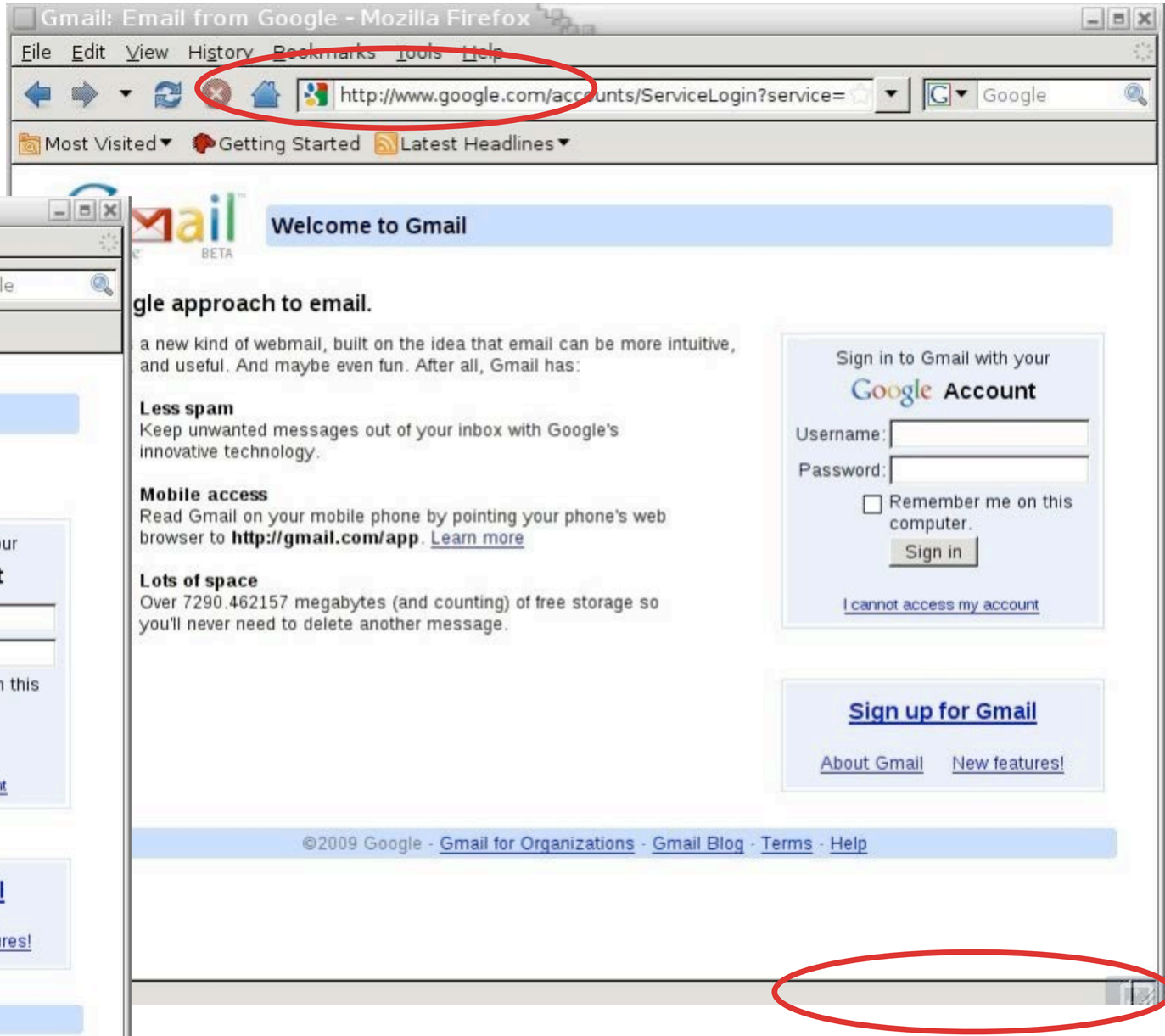


- Il MITM analizza il traffico http che passa.
- Se nota una richiesta http di un url che è stato “spogliato” allora la proxa come https al server
- Analizza il traffico https, effettua un log del traffico e mantiene una mappa dei link.

TERZA SOLUZIONE (RISULTATO)

- Il server non si accorge delle differenze e il client non presenta messaggi di allarme.
- Tutto sembra sicuro.
- L'attaccante vede tutto il traffico in chiaro.


Gmail: Email from Google - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://www.google.com/accounts/ServiceLogin?service
Google
Most Visited
Getting Started
Latest Headlines
Gmail by Google BETA
Welcome to Gmail
A Google approach to email.
Gmail is a new kind of webmail, built on the idea that email can be more intuitive, efficient, and useful. And maybe even fun. After all, Gmail has:
Less spam
Keep unwanted messages out of your inbox with Google's innovative technology.
Mobile access
Read Gmail on your mobile phone by pointing your phone's web browser to http://gmail.com/app. Learn more
Lots of space
Over 7290.461681 megabytes (and counting) of free storage so you'll never need to delete another message.
Sign in to Gmail with your Google Account
Username:
Password:
Remember me on this computer.
Sign in
I cannot access my account
Sign up for Gmail
About Gmail
New features!
©2009 Google - Gmail for Organizations - Gmail Blog - Terms - Help
Done
www.google.com


Gmail: Email from Google - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.google.com/accounts/ServiceLogin?service=
Google
Most Visited
Getting Started
Latest Headlines
Mail BETA
Welcome to Gmail
gle approach to email.
a new kind of webmail, built on the idea that email can be more intuitive, and useful. And maybe even fun. After all, Gmail has:
Less spam
Keep unwanted messages out of your inbox with Google's innovative technology.
Mobile access
Read Gmail on your mobile phone by pointing your phone's web browser to http://gmail.com/app. Learn more
Lots of space
Over 7290.462157 megabytes (and counting) of free storage so you'll never need to delete another message.
Sign in to Gmail with your Google Account
Username:
Password:
Remember me on this computer.
Sign in
I cannot access my account
Sign up for Gmail
About Gmail
New features!
©2009 Google - Gmail for Organizations - Gmail Blog - Terms - Help

POSSIAMO FARE MEGLIO?

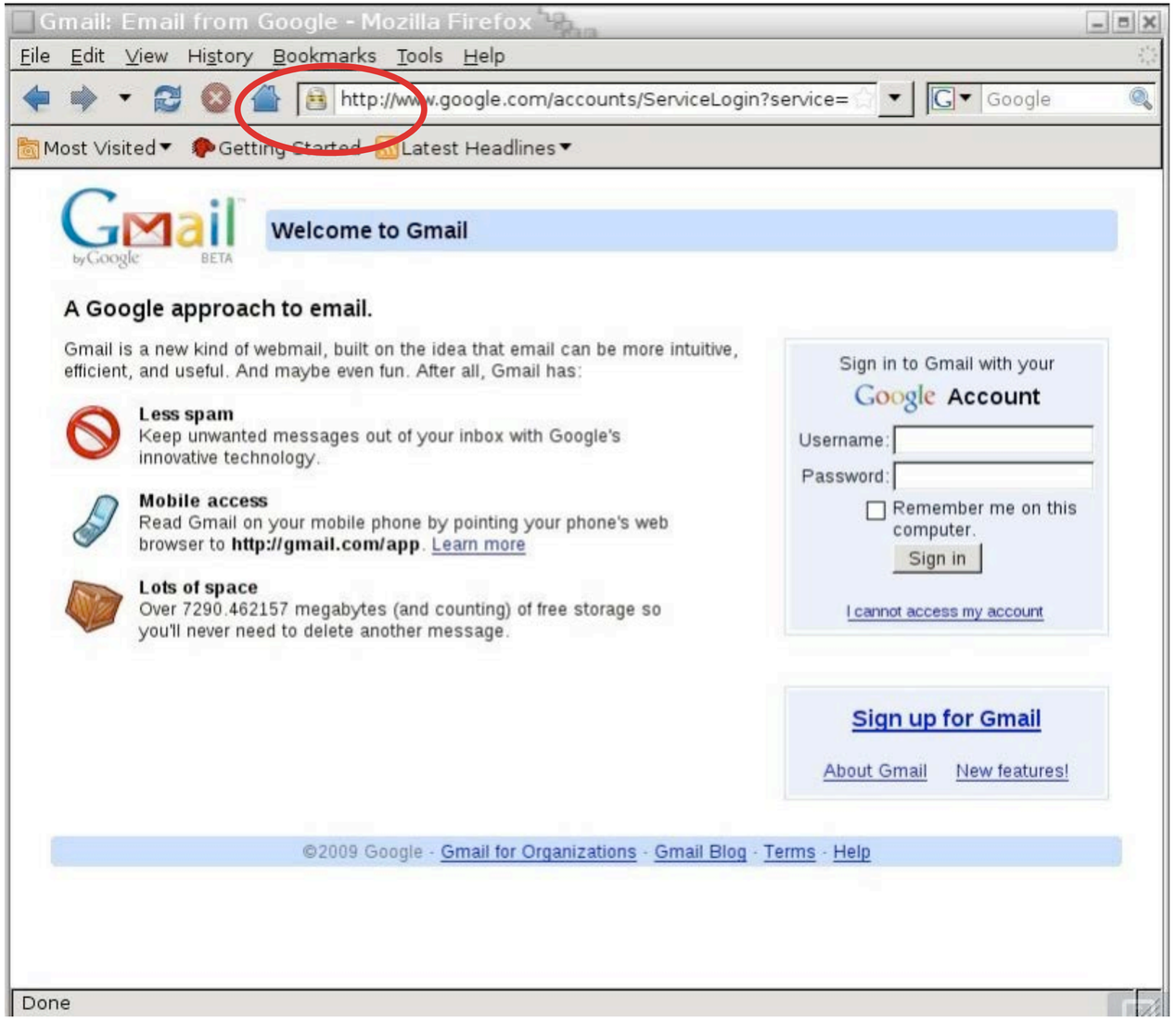
LUCCHETTO

QUARTA SOLUZIONE

Mostrare il simbolo di un lucchetto potrebbe dare una maggiore sensazione di sicurezza.

Il MITM sostituisce, al volo, la vera icona favicon con una creata ad hoc con il simbolo del lucchetto.

Falsa sensazione di sicurezza.



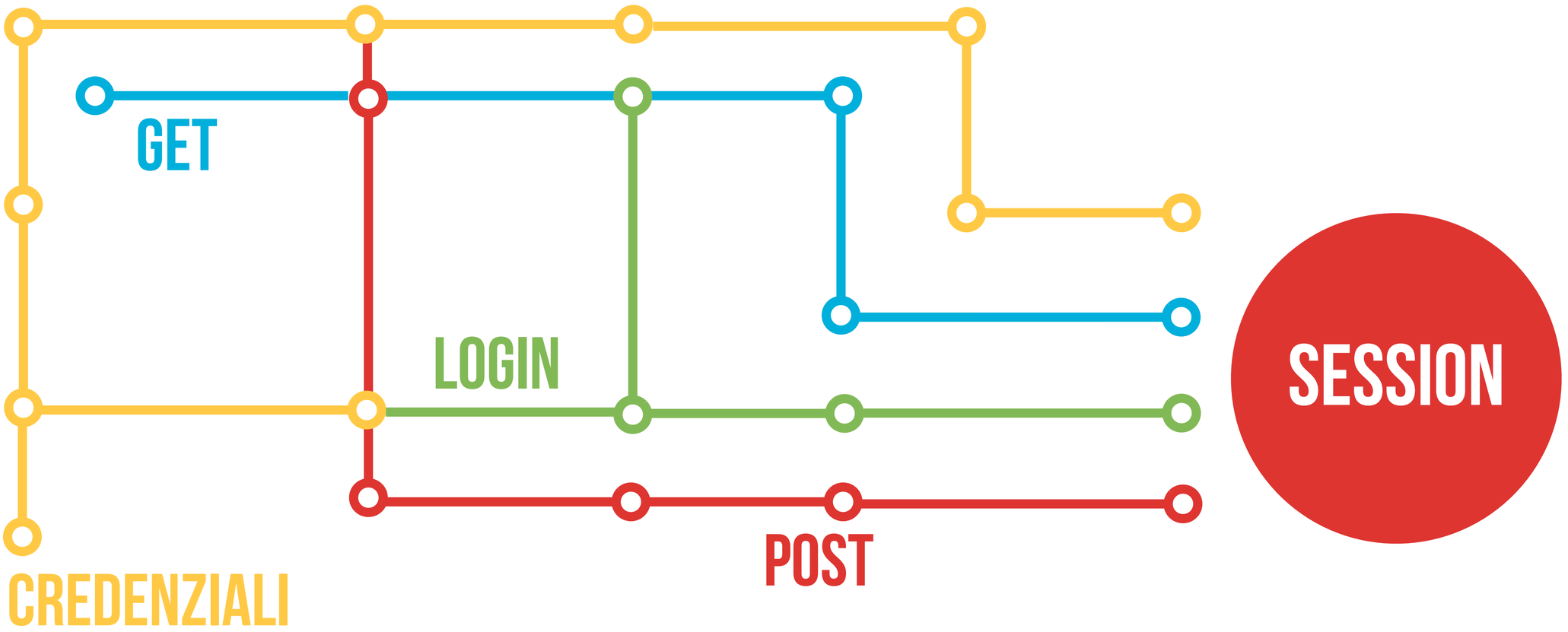
PERFEZIONIAMO

QUINTA SOLUZIONE

Possiamo migliorare ulteriormente la tipologia di attacco andando a lavorare su alcuni aspetti:

1. CONTENT ENCODINGS
2. COOKIES
3. CACHE

SESSIONI



SESTA SOLUZIONE

- E’ possibile far scadere la sessione in un momento successivo prestabilito.
- Dare una maggiore sensazione di naturalità della comunicazione.

SODDISFATTI?

COMPONENTE UMANA

HOMOGRAPH ATTACK

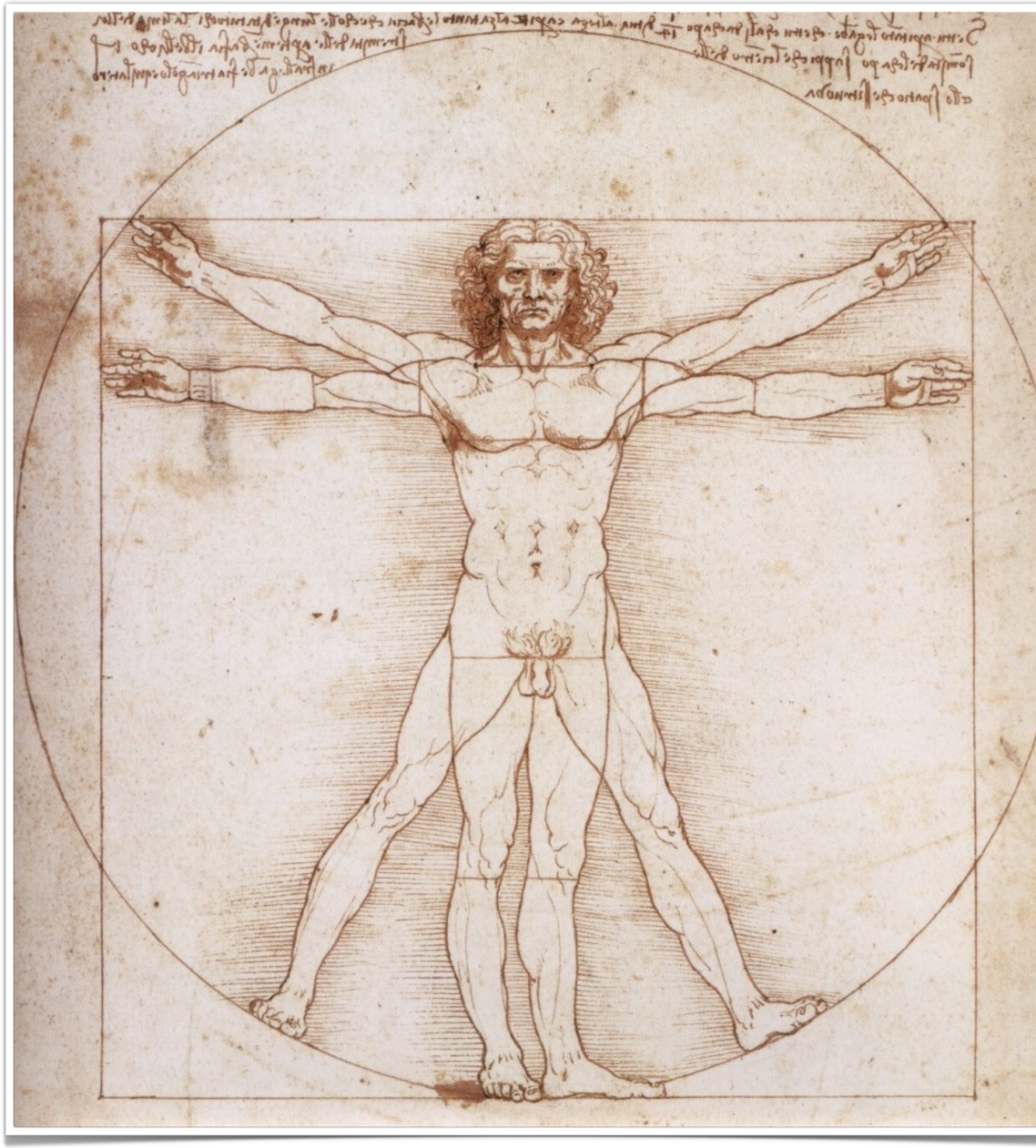
Con le tecniche sino ad ora usate e l'aggiunta di quelle che portano ad errata interpretazione è possibile raffinare ulteriormente l'attacco.

- **IDN**

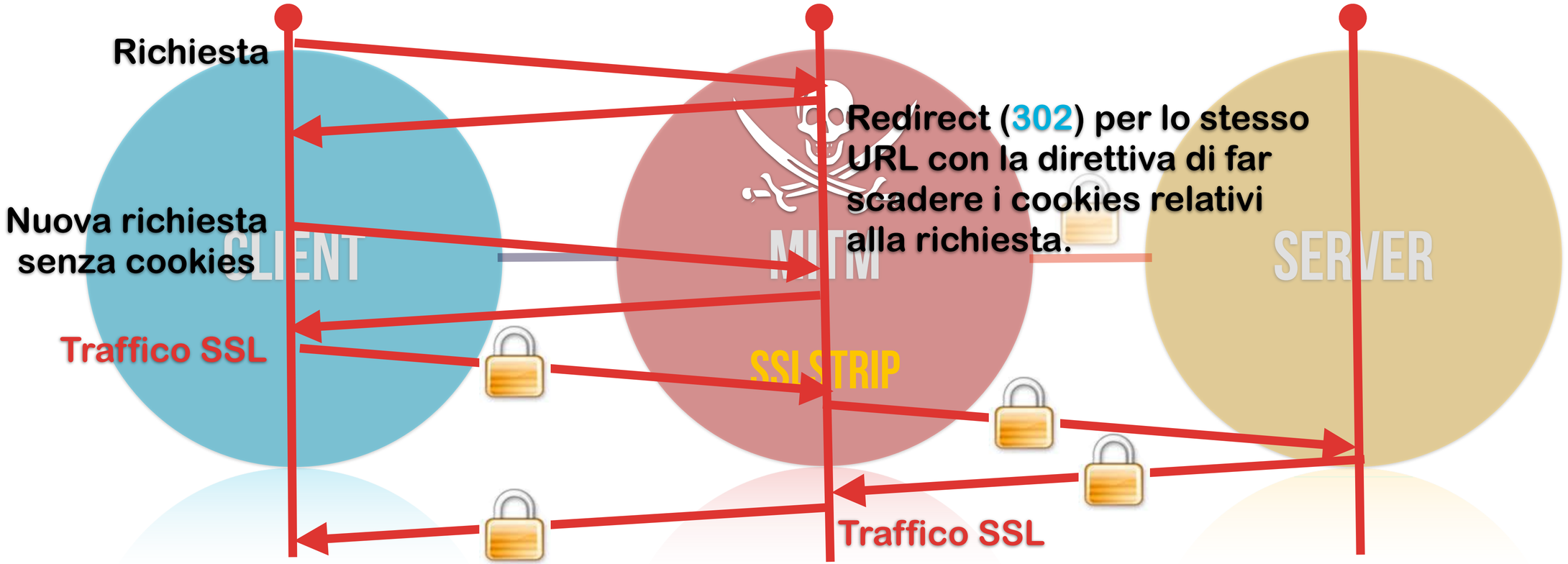
E' possibile usare i simboli:

. ? & /

per costruire un falso url.



SETTIMA SOLUZIONE



Un URL come il seguente: **https://www.miosito.tld/accesso/login**

può diventare: **https://www.miosito.tld/access/login?null.fake.tld**

POTREMMO CONTINUARE...

CONCLUSIONI

La sicurezza di Https può ridursi a causa del protocollo Http

I nostri dati hanno un valore enorme e vanno protetti accuratamente.

Fidarsi è bene.
Non fidarsi è meglio

GRAZIE

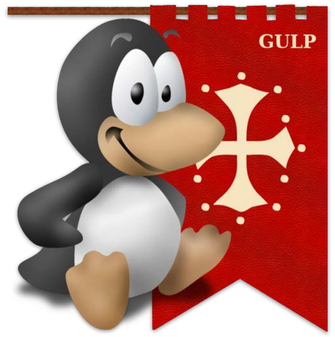
CONTATTI

Potete contattarmi attraverso i seguenti indirizzi:

EMAIL: TALK@AUGIERO.IT

TWITTER: @GIUSEPPEAUGIERO

AUGIERO.IT



Augiero.it

2013
LINUX
D A Y
I T A L I A

Giuseppe Augiero, *Linux Day Pisa 2013*

L'ARTE DELLA INTERCETTAZIONE 2.0

26 ottobre 2013 - *Scuola Normale Superiore*