SSL e cyberwar

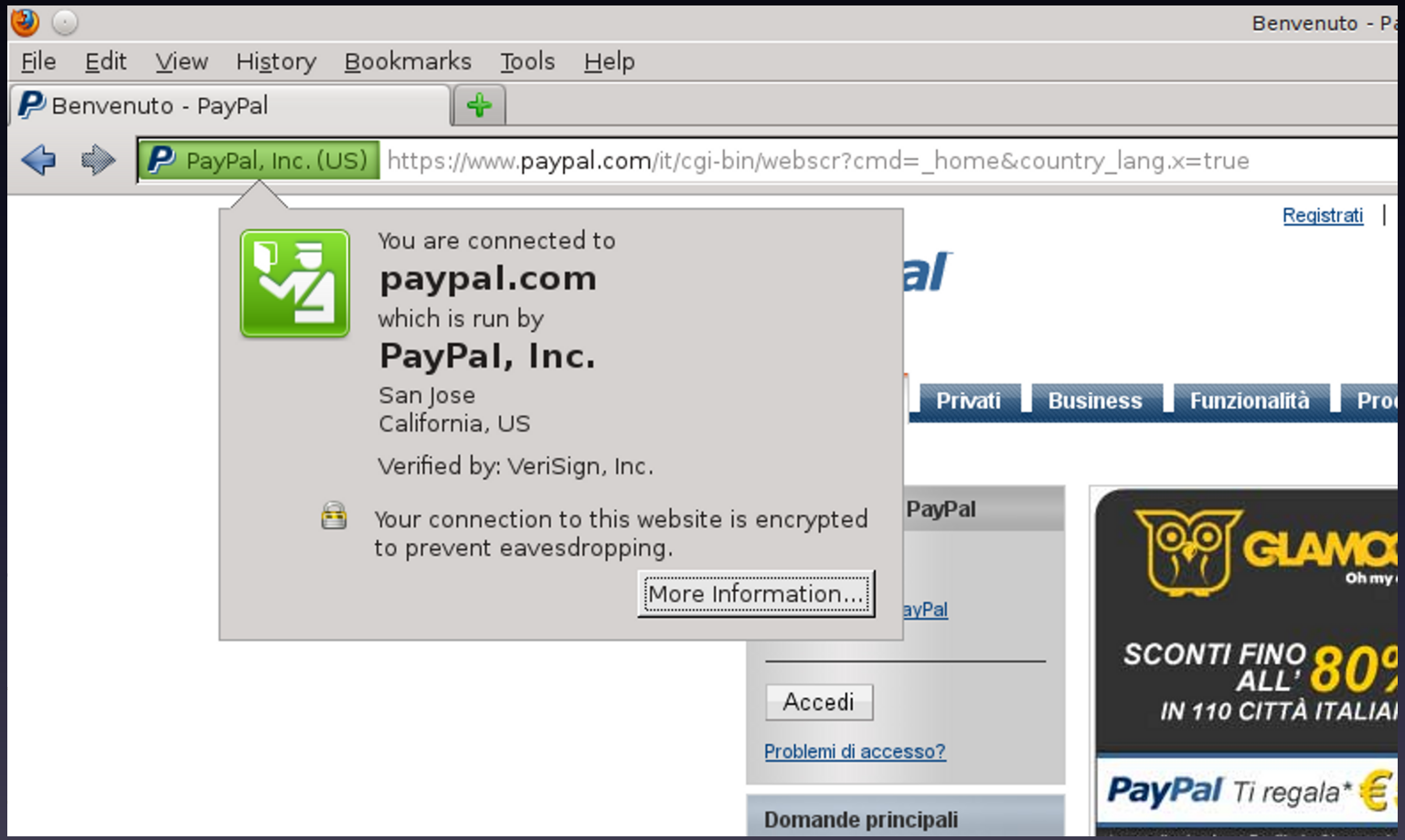
Di chi ci fidiamo?

Politecnico Open unix Labs

Sicurezza Informatica: Privacy “Virtuale”

Indice

Di cosa parleremo



A cosa serve?

- SSL garantisce:
  - segretezza: solo il destinatario sa quel che gli ho scritto
  - integrità: quel che ricevo non è stato manomesso
  - autenticazione: sto parlando effettivamente con chi penso

A cosa serve?

- SSL garantisce:
  - segretezza: solo il destinatario sa quel che gli ho scritto
  - integrità: quel che ricevo non è stato manomesso
  - autenticazione: sto parlando effettivamente con chi penso

A cosa serve?

- SSL garantisce:
  - segretezza: solo il destinatario sa quel che gli ho scritto
  - integrità: quel che ricevo non è stato manomesso
  - autenticazione: sto parlando effettivamente con chi penso

Oggi si parla di autenticazione

Demo

Fuor di metafora

- Alice: l'utente
- Bob: il server
- Trudy: un attacker
- Chi timbra i lucchetti: la Certification Authority
- Il lucchetto: il certificato del server
- Timbrare il lucchetto: firmare il certificato

Indice

Abbiamo capito che

Le CA sono un punto critico

Conosciamole!

- VeriSign (Facebook, Twitter, Live.com, PayPal, Amazon, Mozilla...)
- DigiCert (Wikipedia, github, torproject.org...)
- Thawte (kernel.org, Google, ...)
- Equifax (Yahoo!...)
- StartCom (certificati gratuiti, EFF...)
- GlobalSign (Skype...)
- GoDaddy
- Google
- Comodo
- Diginotar
- GeoTrust
- RSA Security

Indice

Comodo

Firma da $\frac{1}{5}$ a $\frac{1}{4}$ dei certificati[1]

[1] https://www.eff.org/observatory

Quando un brutto giorno...[3]

- Il rivenditore italiano di Comodo viene attaccato[2]
- Vengono firmati 9 certificati abusivamente:
  - mail.google.com
  - www.google.com
  - login.yahoo.com ($\times 3$)
  - login.skype.com
  - addons.mozilla.org
  - login.live.com
  - global trustee

[2] InstantSSL.it
[3] Il 15 marzo 2011

Quando un brutto giorno...[3]

- Il rivenditore italiano di Comodo viene attaccato[2]
- Vengono firmati 9 certificati abusivamente:
  - mail.google.com
  - www.google.com
  - login.yahoo.com ($\times 3$)
  - login.skype.com
  - addons.mozilla.org
  - login.live.com
  - global trustee

[2] InstantSSL.it

[3] Il 15 marzo 2011

Il punto di vista di Comodo

- Comodo rilascia una dichiarazione:[4]

  “L’attacco era estremamente sofisticato ed è stato eseguito con estrema precisione... era molto ben orchestrato e l’attacker sapeva cosa doveva fare e quanto rapidamente.”

  Melih Abdulhayoğlu, Comodo Founder

[4] http://www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html

Iran

- Comodo rilascia dettagli sull'attacco
- Compreso un indirizzo IP:

IP Address Location	
IP Address	212.95.136.18
City	Tehran
State or region	Tehran
Country	Iran
ISP	Pishgaman TOSE Ertebatat Tehran Network
Latitude & Longitude	35.696111 51.423056

Le conclusioni di Comodo

- The perpetrator can only make use of these certificates if it had control of the DNS infrastructure.[5]
- The perpetrator has executed its attacks with clinical accuracy.
- The Iranian government has recently attacked other encrypted methods of communication.
- All of the above leads us to one conclusion only: that this was likely to be a **state-driven attack**.

[5] Non è vero

Questo non è un attacco informatico...

Cyberwar

Questa è guerra!

Indice

L’attacker

- L’autore di sslsniff [6] cerca tra i log dei download l’IP
- E lo trova!

[6] Moxie Marlinspike

L’attacker

- L’autore di sslsniff [6] cerca tra i log dei download l’IP
- E lo trova!

[6] Moxie Marlinspike

Lo user-agent

212.95.136.18 [16/Mar/2011:09:56:03 +0000]
“GET http:// www.thoughtcrime.org/software/sslsniff/index.html HTTP/1.1” 200
“Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.13 Gecko/20101203 Firefox/3.6.13 (.NET CLR 3.5.30729; .NET4.0E)”

- Usa Windows
- Usa Windows XP
- Usa un Firefox vecchio di 4 mesi
- Usa la lingua inglese

Lo user-agent

212.95.136.18 [16/Mar/2011:09:56:03 +0000]
“GET http:// www.thoughtcrime.org/software/sslsniff/index.html HTTP/1.1” 200
“Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.13 Gecko/20101203 Firefox/3.6.13 (.NET CLR 3.5.30729; .NET4.0E)”

- Usa Windows
- Usa Windows XP
- Usa un Firefox vecchio di 4 mesi
- Usa la lingua inglese

Lo user-agent

212.95.136.18 [16/Mar/2011:09:56:03 +0000]
“GET http:// www.thoughtcrime.org/software/sslsniff/index.html HTTP/1.1” 200
“Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.13 Gecko/20101203 Firefox/3.6.13 (.NET CLR 3.5.30729; .NET4.0E)”

- Usa Windows
- Usa Windows XP
- Usa un Firefox vecchio di 4 mesi
- Usa la lingua inglese

Lo user-agent

212.95.136.18 [16/Mar/2011:09:56:03 +0000]
“GET http:// www.thoughtcrime.org/software/sslsniff/index.html HTTP/1.1” 200
“Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.13 Gecko/20101203 Firefox/3.6.13 (.NET CLR 3.5.30729; .NET4.0E)”

- Usa Windows
- Usa Windows XP
- Usa un Firefox vecchio di 4 mesi
- Usa la lingua inglese

Lo user-agent

212.95.136.18 [16/Mar/2011:09:56:03 +0000]
“GET http:// www.thoughtcrime.org/software/sslsniff/index.html HTTP/1.1” 200
“Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.13 Gecko/20101203 Firefox/3.6.13 (.NET CLR 3.5.30729; .NET4.0E)”

- Usa Windows
- Usa Windows XP
- Usa un Firefox vecchio di 4 mesi
- Usa la lingua inglese

E il referrer?

Il referrer[7]

[7] http://hak5.org/episodes/episode-610

L’hacker parla[8]

- I’m not a group, I’m single hacker with experience of 1000 hacker
- At first I decided to hack RSA algorithm, tried to find an algorithm for factoring integer, for now I was not able to do so, at least not yet, but I know it’s not impossible and I’ll prove it

[8] http://pastebin.com/u/ComodoHacker

L'hacker parla[8]

- I'm not a group, I'm single hacker with experience of 1000 hacker
- At first I decided to hack RSA algorithm, tried to find an algorithm for factoring integer, for now I was not able to do so, at least not yet, but I know it's not impossible and I'll prove it

[8] http://pastebin.com/u/ComodoHacker

L’hacker parla

- I know you are really shocked about my knowledge, my skill, my speed, my expertise, that’s all OK, all of it was so easy for me, I did more important things I can’t talk about, so if you have to worry, you can worry...
- My Rules as I rule to internet, you should know it already...
- Rule#6: I’m a GHOST

L’hacker parla

- I know you are really shocked about my knowledge, my skill, my speed, my expertise, that’s all OK, all of it was so easy for me, I did more important things I can’t talk about, so if you have to worry, you can worry...
- My Rules as I rule to internet, you should know it already...
- Rule#6: I’m a GHOST

L’hacker parla

- I know you are really shocked about my knowledge, my skill, my speed, my expertise, that’s all OK, all of it was so easy for me, I did more important things I can’t talk about, so if you have to worry, you can worry...
- My Rules as I rule to internet, you should know it already...
- Rule#6: I’m a GHOST

Non finisce qui

- Comodo viene attacca in totale 4 volte in pochi mesi

Conseguenze?

Nessuna

Anzi

- Il fondatore di Comodo viene premiato da RSA:

Enterpreneur of the year

Indice

Diginotar

- 17 giugno 2011
- 500 certificati firmati
- Almeno 300’000 persone colpite[9]
- Stesso attacker, noto come ichsun

[9] Dai log OSCP

Chi ha usato i certificati?

- I 300’000 IP corrispondono tutti a 6 ISP iraniani
- Tutto il traffico passa per il Data Communications of Iran (DCI)

Alcuni domini colpiti

- *.*.com
- *.*.org
- *.android.com
- *.aol.com
- *.comodo.com
- *.digicert.com
- *.globalsign.com
- *.google.com
- *.microsoft.com
- *.mossad.gov.il
- *.mozilla.org
- *.skype.com
- *.startssl.com
- *.thawte.com
- *.torproject.org
- *.windowsupdate.com
- *.wordpress.com

Altri attacchi da “ichsun”

- Ichsun sostiene di aver avuto accesso ad altre 4 CA
- Tra cui GlobalSign e StartCom

Indice

Il caso di Thawte

- Mike Zusman ha ottenuto un certificato per login.live.com
- Thawte verificava la proprietà di un dominio tramite e-mail
- SSLCertificates@dominio
- Mike ha registrato SSLCertificates@live.com

Il caso di Thawte

- Mike Zusman ha ottenuto un certificato per login.live.com
- Thawte verificava la proprietà di un dominio tramite e-mail
- SSLCertificates@dominio

- Mike ha registrato SSLCertificates@live.com

StartCom

- Eddy Nigg ha ottenuto una firma per mozilla.com
- Non ha dovuto effettuare nessuna validazione

VeriSign

- Pare abbia rilasciato un certificato code-signing
- A nome di “Microsoft Corporation”
- Sono anche nel business delle intercettazioni

VeriSign

- Pare abbia rilasciato un certificato code-signing
- A nome di “Microsoft Corporation”
- Sono anche nel business delle intercettazioni

VeriSign

- Pare abbia rilasciato un certificato code-signing
- A nome di “Microsoft Corporation”
- Sono anche nel business delle intercettazioni

Altri

- sslinabox.com: login in account altrui a random
- certigna.fr: la chiave privata è stata pubblica per anni
- GeoRoot: pagando si può diventare CA intermedia

Altri

- sslinabox.com: login in account altrui a random
- certigna.fr: la chiave privata è stata pubblica per anni
- GeoRoot: pagando si può diventare CA intermedia

Altri

- sslinabox.com: login in account altrui a random
- certigna.fr: la chiave privata è stata pubblica per anni
- GeoRoot: pagando si può diventare CA intermedia

Mappa

Mappa

- Sono oltre 650[10]
- Anche le isole Bermuda possono firmare certificati

[10] https://www.eff.org/observatory

Mappa

- Sono oltre 650[10]
- Anche le isole Bermuda possono firmare certificati

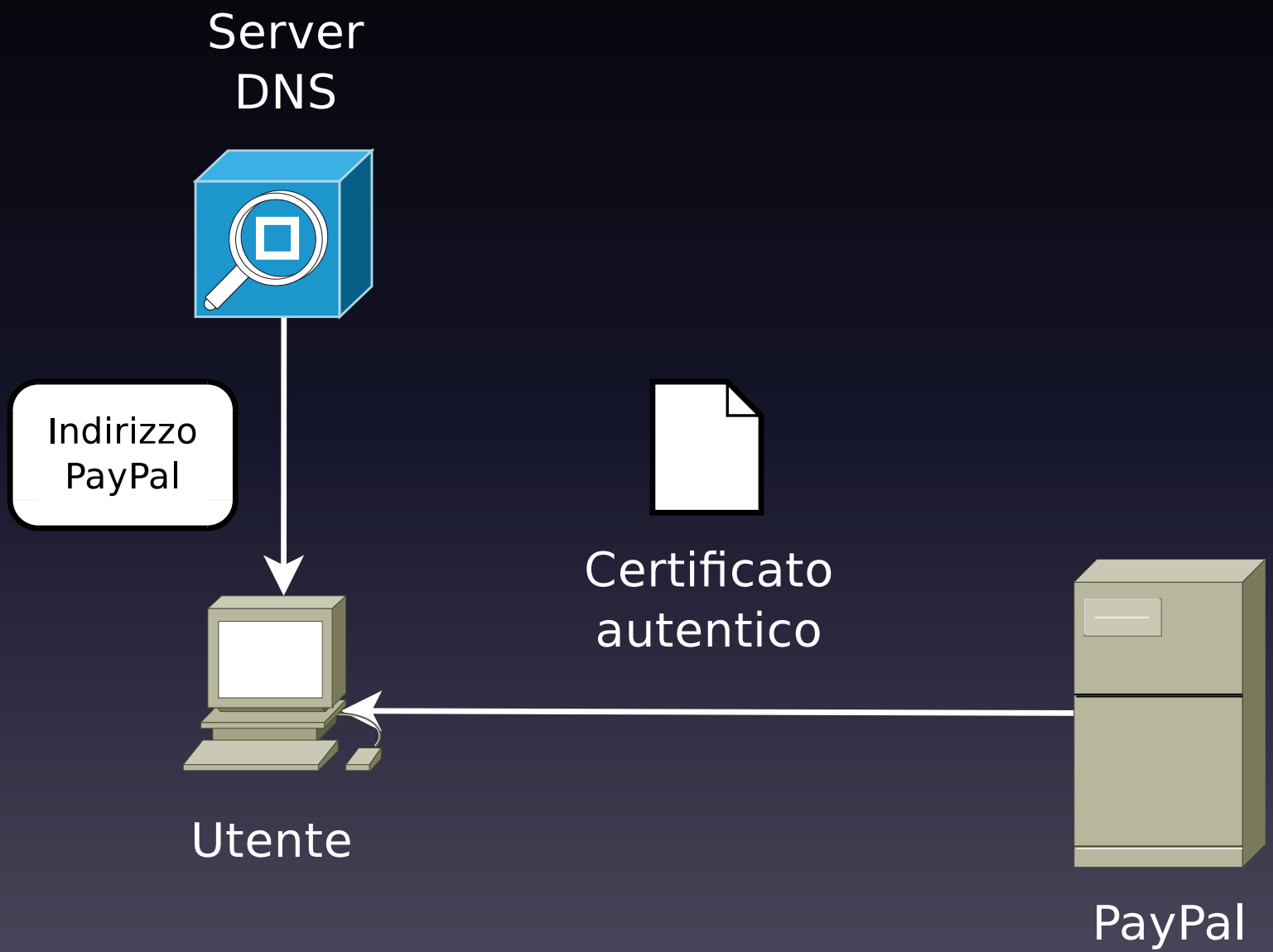
[10] https://www.eff.org/observatory

Di chi ci stiamo fidando?

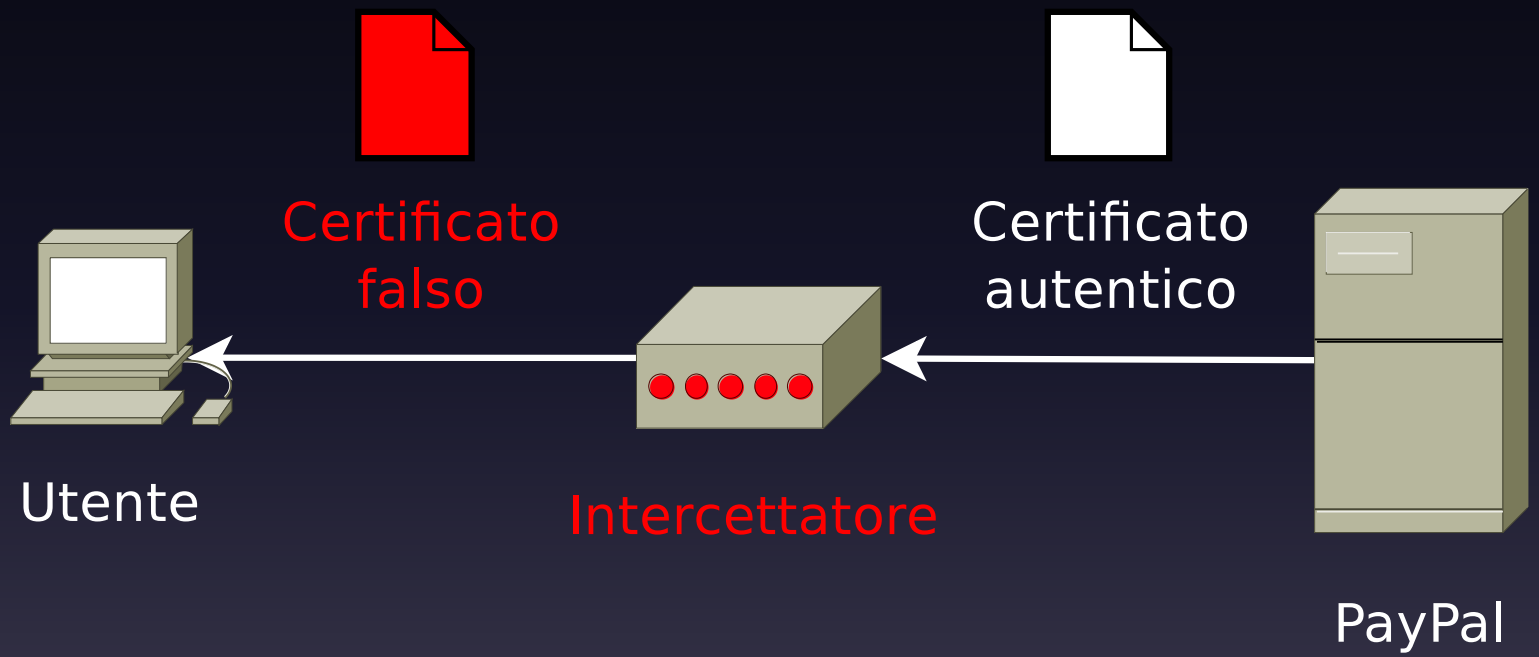
Indice

Indice

Normalmente



Transparent proxy



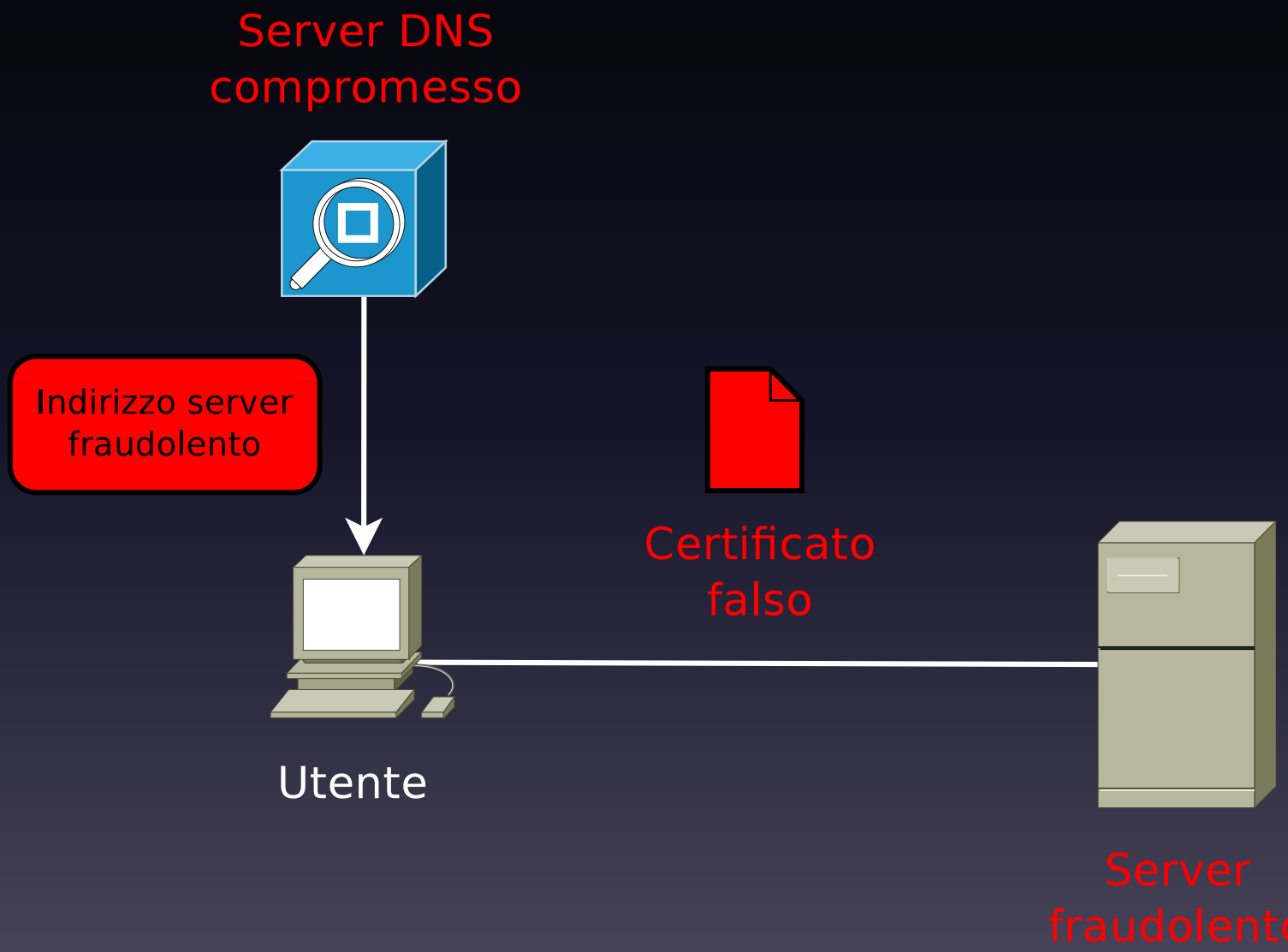
Transparent proxy

- Il traffico passa attraverso una macchina malevola
- Agisce come un proxy:
  - Manda al client il certificato fraudolento
  - Il client si fida e inizia la comunicazione
  - Il proxy redirige il traffico al server reale
- Il tutto è trasparente all'utente

Come?

- L’ISP, se complice, può farlo sempre
- Un router sul percorso può farlo
  - ARP spoofing
  - Rogue DHCP server

DNS


Server DNS
compromesso
Indirizzo server
fraudolento
Certificato
falso
Utente
Server
fraudolento

DNS

- Quando ci si collega ad un sito
  - www.google.com
- Questo viene tradotto in un IP tramite il DNS
  - 173.194.35.49
- Se un DNS è compromesso, può restituire un IP malevolo
- L'attacker cattura le credenziali simulando il servizio

Come?

- Il server DNS, se complice, può farlo sempre[11]
- Il server DNS può essere impostato ad arte
  - Rouge DHCP
- Le voci del server DNS possono essere manomesse
  - DNS cache poisoning

[11] Come è provato sia successo in Iran con Diginotar

DNS cache poisoning

- Sostituzione dell'IP associato ad un dominio in un DNS
- I server DNS sono gerarchici e hanno una cache
- È possibile spacciarsi per un server di livellio superiore
- E quindi è possibile cambiare l'associazione IP-dominio

Rogue DHCP server

- Alla connessione ad una rete si chiede:
  - un indirizzo IP
  - verso chi mandare il traffico (tipicamente il router)
  - quale server DNS usare
- È il server DHCP che risponde a queste richieste
- Se ci si spaccia per esso si possono manomettere quei dati
- Funziona solo se si è nella rete locale della vittima

ARP spoofing

- Si continua ad annunciare sulla rete di essere il router
- Tutto il traffico passerà così per la macchina malevola
- Funziona solo se si è nella rete locale della vittima

La situazione iraniana

- In Iran serviti 300’000 certificati Diginotar fasulli
- Probabilmente DNS cache poisoning di alcuni server

Indice

Isolare le CA per paese/aree

- Impedirebbe alle isole Bermuda di firmare per tutti
- Ma se non ci si fida del proprio stato?
  - USA (SOPA e PROTECT-IP)
  - Cina (Great Firewall of China, Skype...)
  - Iran
- Non si potrebbe neppure accedere a servizi stranieri

Rimuovere CA inaffidabili

- Non tutte si comportano male
- Si potrebbero rimuovere le inaffidabili
- Ammettiamo di rimuovere Comodo

  Si perderebbe un quarto dei certificati!

Rimuovere CA inaffidabili

- Non tutte si comportano male
- Si potrebbero rimuovere le inaffidabili
- Ammettiamo di rimuovere Comodo

Si perderebbe un quarto dei certificati!

Rimuovere CA inaffidabili

- Non tutte si comportano male
- Si potrebbero rimuovere le inaffidabili
- Ammettiamo di rimuovere Comodo
- Si perderebbe un quarto dei certificati!

Una volta che ti fidi di qualcuno

Devi fidarti per sempre

DNSSEC

- Con DNSSEC una copia del certificato è nei DNS
- I DNS sono distribuiti, a prima vista

In realtà...

- I DNS sono distribuiti ma gerarchici
- Quindi bisogna fidarsi di:
  - server DNS
  - registrar del dominio
  - TLD (e.g. .com, .org, .net...) oppure ccTLD (e.g. .it, .fr...)
  - root (ICANN)

DNS: di chi fideremmo?

- I registrar non sono nati per avere un ruolo simile
- Il TLD .com è gestito da VeriSign
- I ccTLD sono gestiti dai vari paesi
- Solo pochi paesi hanno una Certification Authority
- Con DNSSEC bisognerebbe fidarsi di tutti gli stati
- L'ICANN è sottoposta alla legislazione americana

Indice

La situazione odierna

- Un certificato viene firmato abusivamente
- Cosa succede oggi?

Certificate Revocation List

- Immediatamente la CA emette una revoca
- La revoca finisce in una CRL pubblica
- I browser e gli OS la inseriscono negli aggiornamenti

Problema

- Bisogna aspettare che lo sviluppatore rilasci l'aggiornamento
- L'utente medio aggiorna il software raramente

Risultato

Ampio periodo di vulnerabilità

Online Certificate Status Protocol

- Ad ogni connessione SSL si contatta la CA in questione
- I dati sulle revoche dei certificati vengono aggiornati
- OCSP è supportato da tutti i browser moderni

Problemi

- Privacy: le CA sanno quali siti vengono visitati e quando
- Carico: le CA devono rispondere a innumerevoli richieste
- Si perde uno dei vantaggi per cui le CA sono nate:
  - Offrire certificati auto-certificanti

Indice

Due problemi

1. Non è l'utente a decidere di chi fidarsi
2. Non è possibile cambiare idea

Convergence

L’idea: cambiare prospettiva

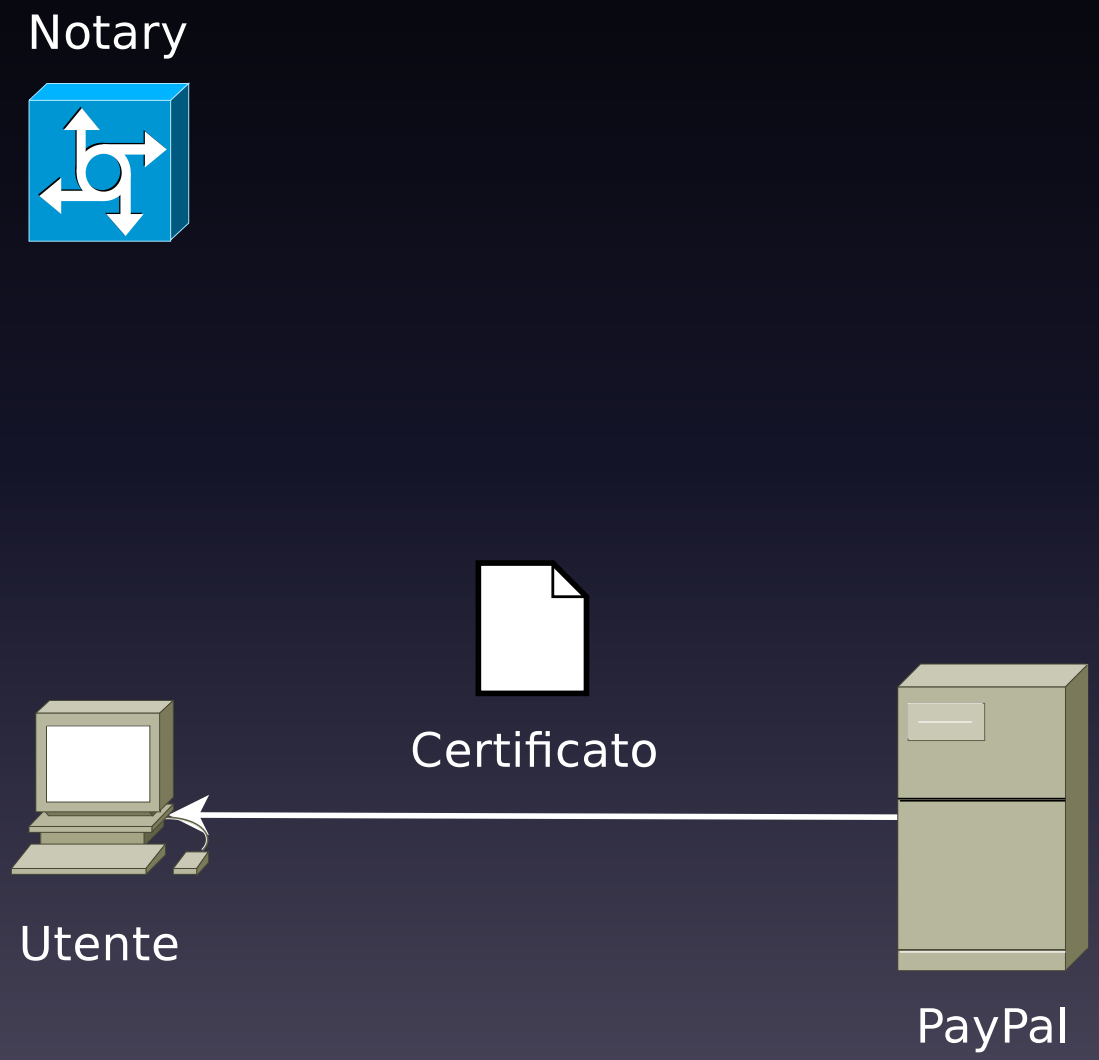
- Cambiare prospettiva nel guardare il certificato
- Un altra entità lo richiede da un altro punto della rete
- Confrontiamo se corrispondono

I notary

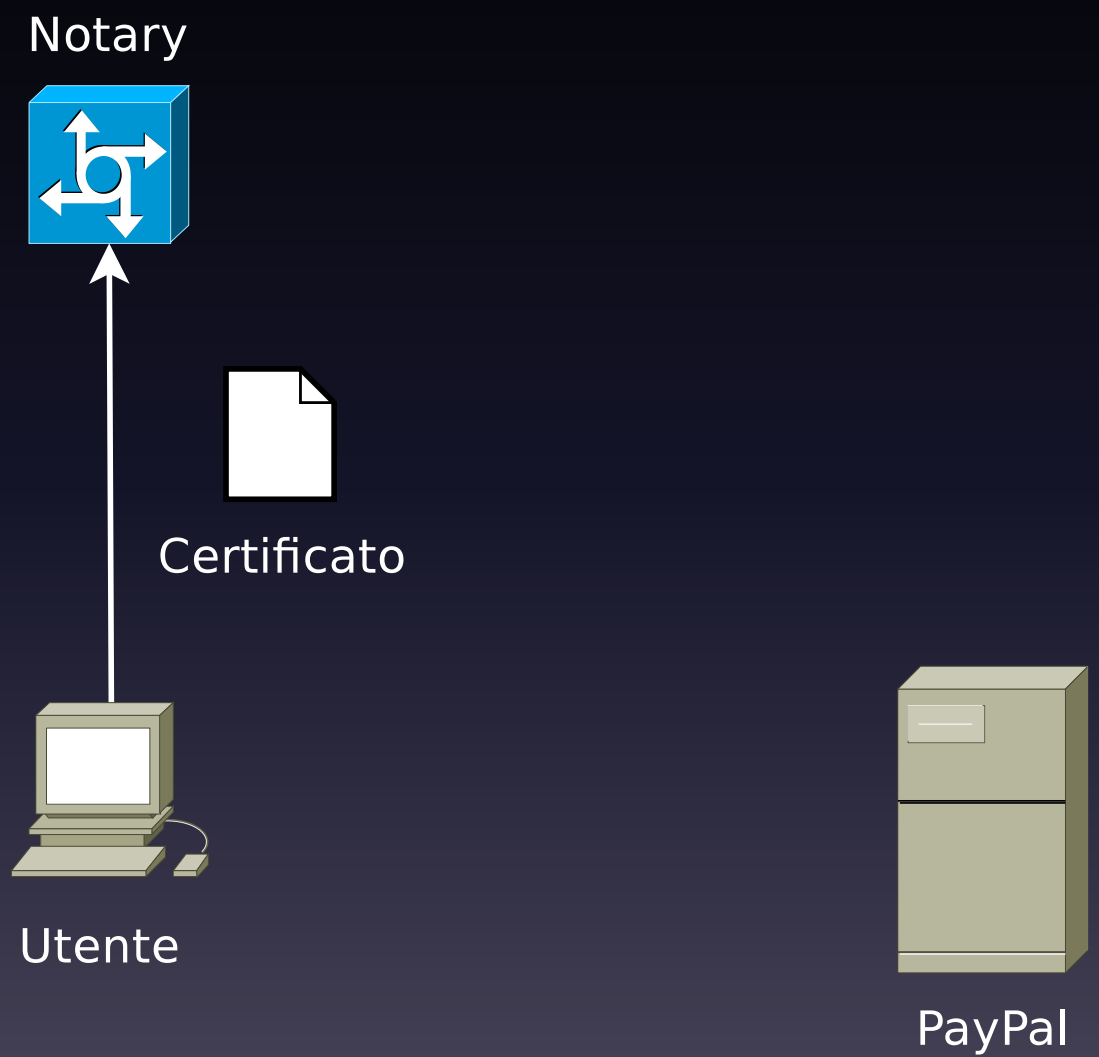
- Rimuoviamo il concetto di CA
- Inseriamo il concetto di notary
- I notary sono server che tengono una cache dei certificati

Come funziona?

L’utente richiede il certificato al server

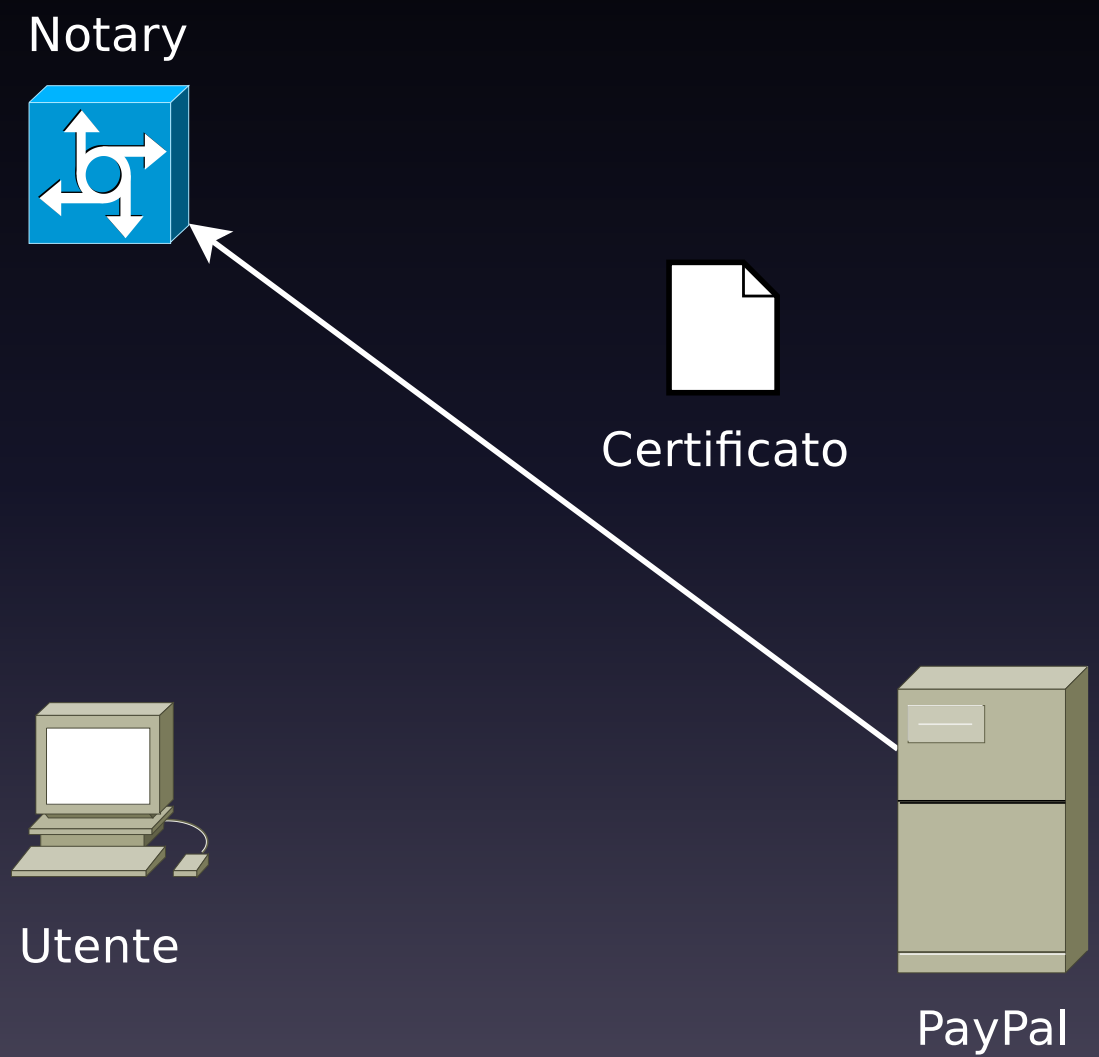


L'utente invia il certificato al notary[12]



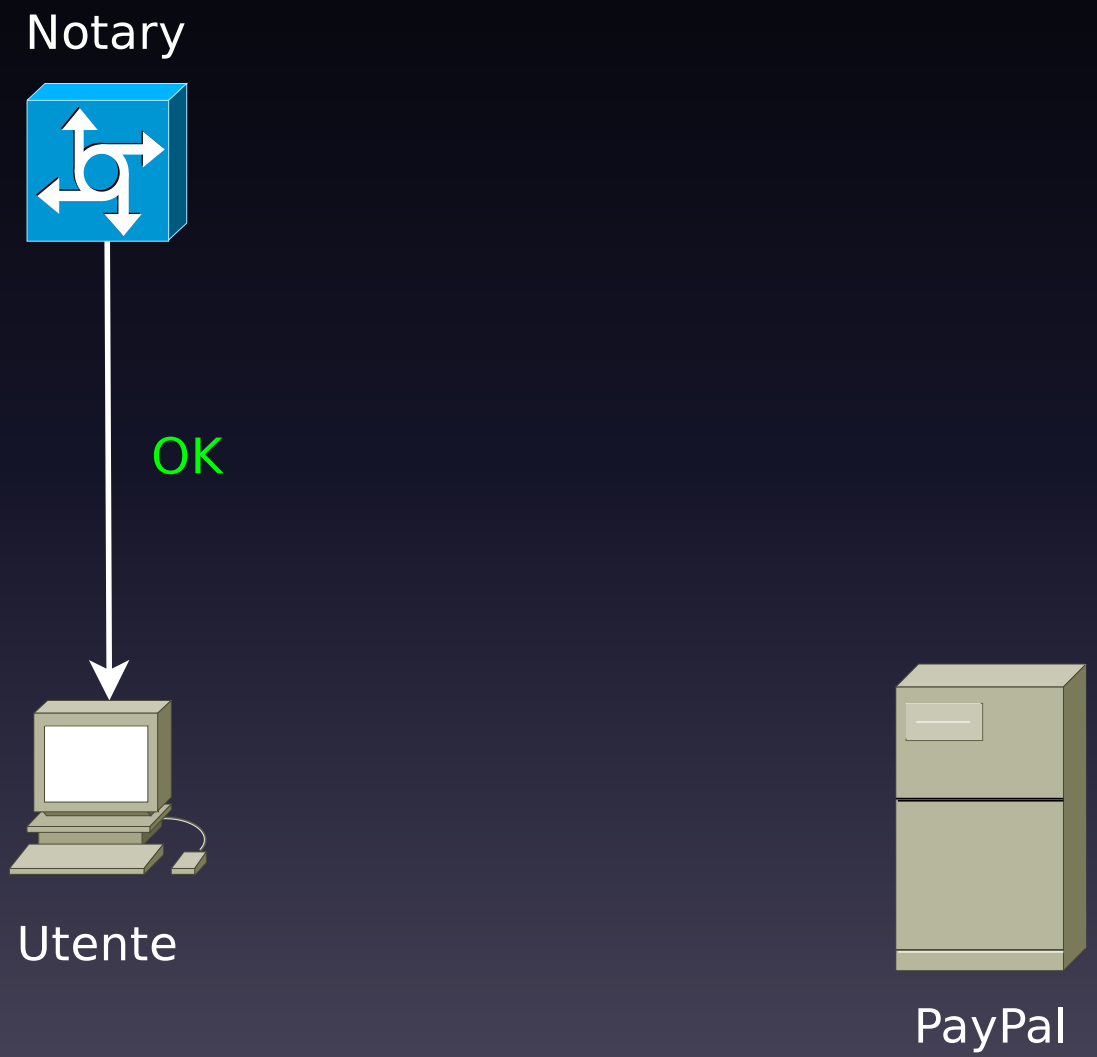
[12] A meno che non lo abbia già fatto in passato

Il notary chiede il certificato[13]



[13] A meno che non lo abbia già in cache

Il notary risponde all'utente



Ricapitoliamo

1. Richiedo al server il certificato
2. Lo invio al notary
3. Il notary lo confronta con la sua copia
4. Se non corrisponde o non è nella sua cache
   - Lo richiede al server
5. Se anche la nuova versione non corrisponde
   - Il certificato non è valido
6. Se valido, lo salvo in una cache locale

Dov’è il vantaggio?

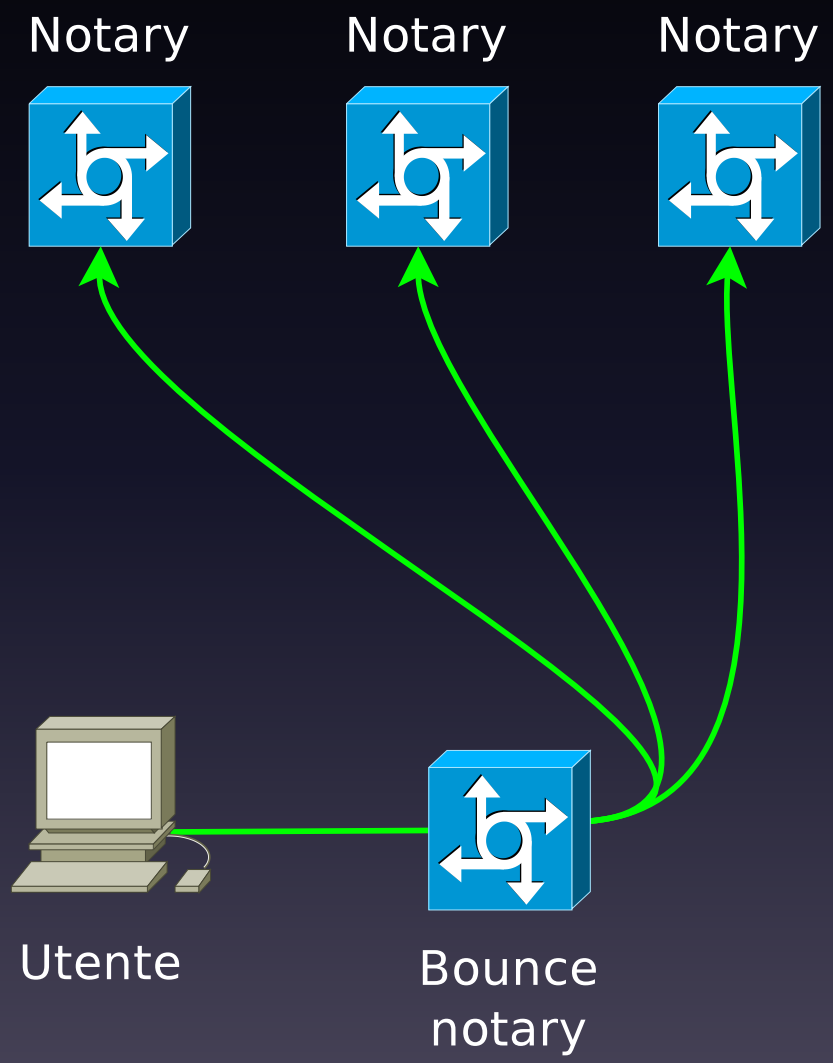
1. Si possono interrogare più notary diversi
2. Più prospettive si hanno, più è difficile ingannare l’utente!
3. I notary possono anche servirsi delle CA o usare DNSSEC
4. Si combinano i metodi per avere consenso o maggioranza
5. L’utente sceglie i notary e può cambiarli senza rischi

E la privacy?

- È garantita in maniera simile a Tor[14]
- Si elegge un notary come “Bounce”:
  - Viene usato come tunnel per collegarsi ad altri notary
  - Non conosce il contenuto della richiesta
  - I notary non vedono l’IP del client ma del bounce
- La privacy è garantita
- A meno che si abbia controllo sia sul bounce che sul notary

[14] Qualcuno ha letto il mio articolo sul Giornalinux?

Bounce notary



Convergence

- Esiste *hinc et nunc* come plugin per Firefox
- È liberamente scaricabile da http://convergence.io/
- È disponibile anche il codice per i notary

Demo