mkit | IT & Security Solutions

www.mkit.com.ar

Man-In-The-Middle y robo de información en sesiones protegidas por SSL

Matias Katz

Email: matias@matiaskatz.com

Blog: www.matiaskatz.com

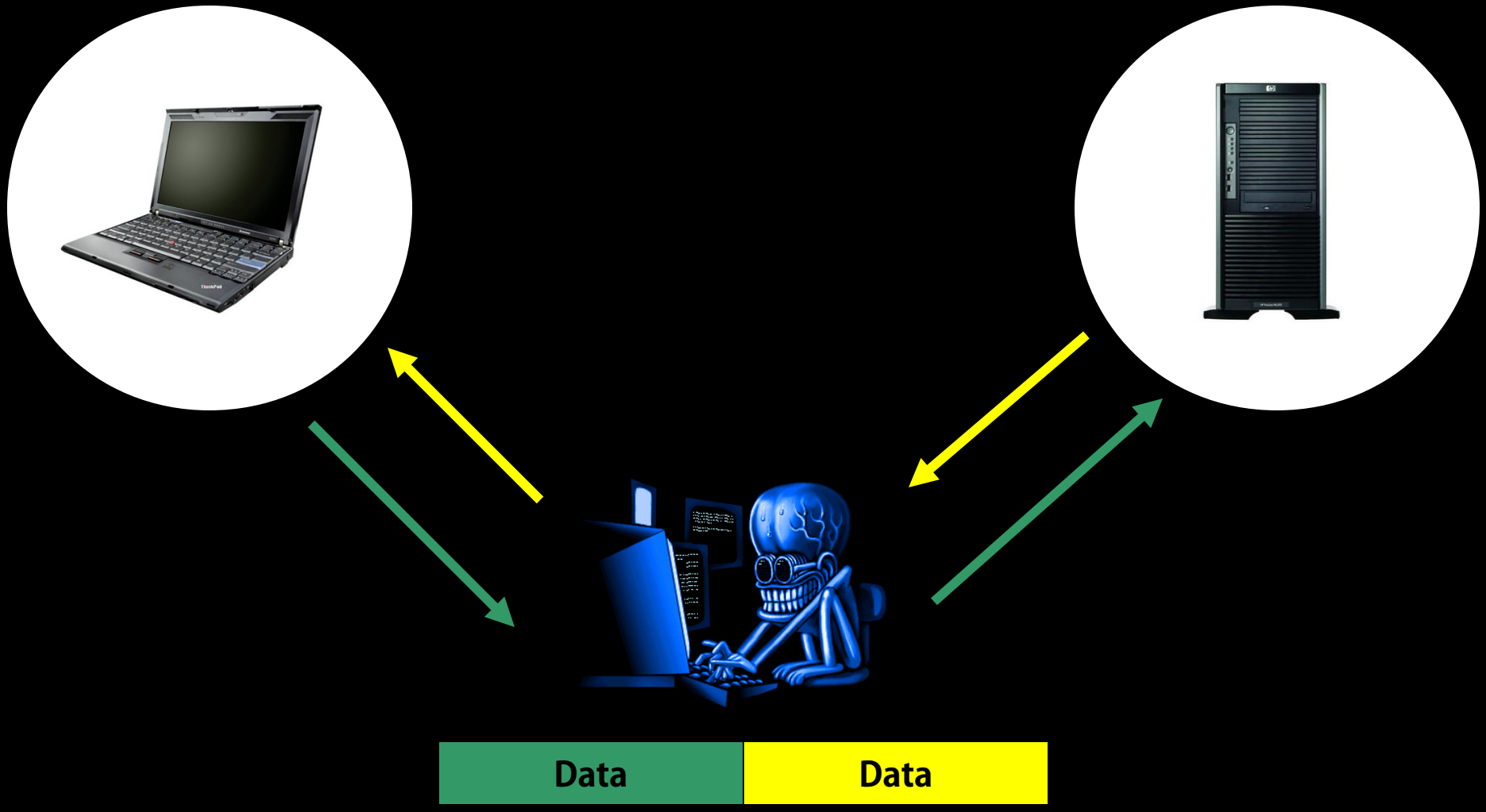
Twitter: @matiaskatz

Analizando un ataque Man-In-The-Middle

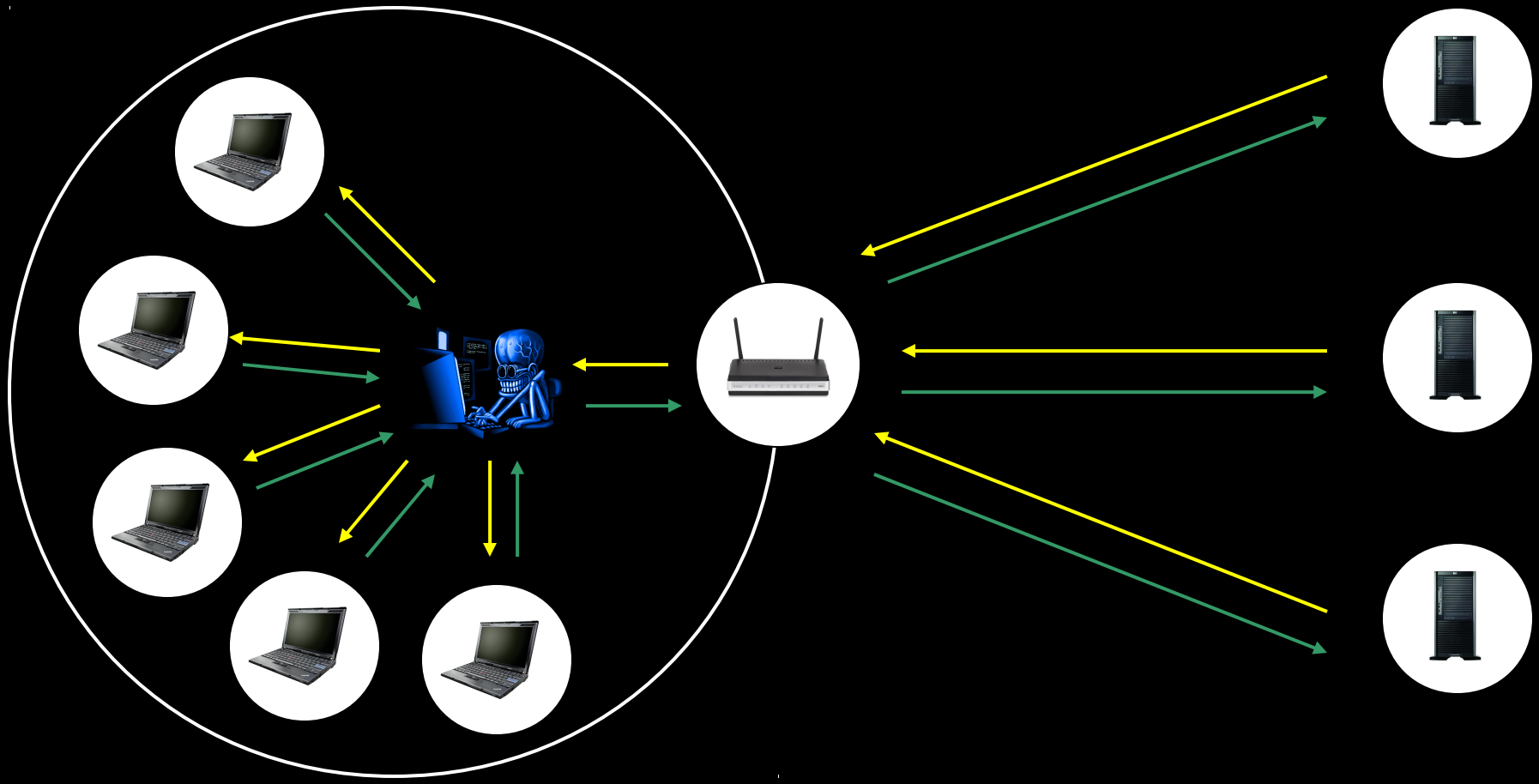
Requests

Replies

Analizando un ataque Man-In-The-Middle (Cont.)



Analizando un ataque Man-In-The-Middle (Cont.)



ARP Cache Poisoning

IP: 10.0.1.1
MAC: AA-AA-AA

IP: 10.0.1.254
MAC: BB-BB-BB

IP: 10.0.1.2
MAC: BB-BB-BB

IP: 10.0.1.1
MAC: BB-BB-BB

IP: 10.0.1.254
MAC: CC-CC-CC

Robo de Información – Protocolos Inseguros

POP3

SMTP

HTTP

FTP

IMAP

TELNET

VNC

SNMP

DEMO

Contramedidas?

Tablas ARP estáticas

IDS / arpwatch

Encriptación

Opciones de encriptación

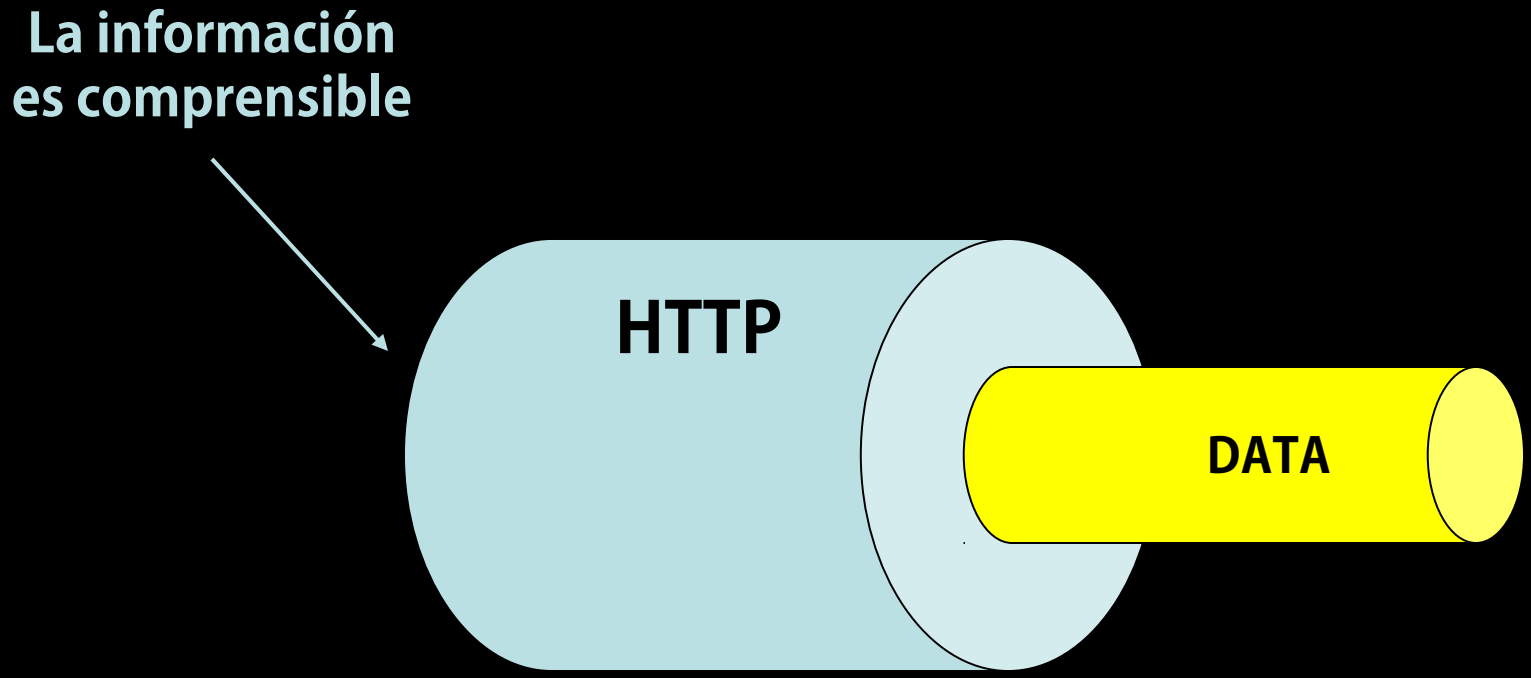
VPN

SSL

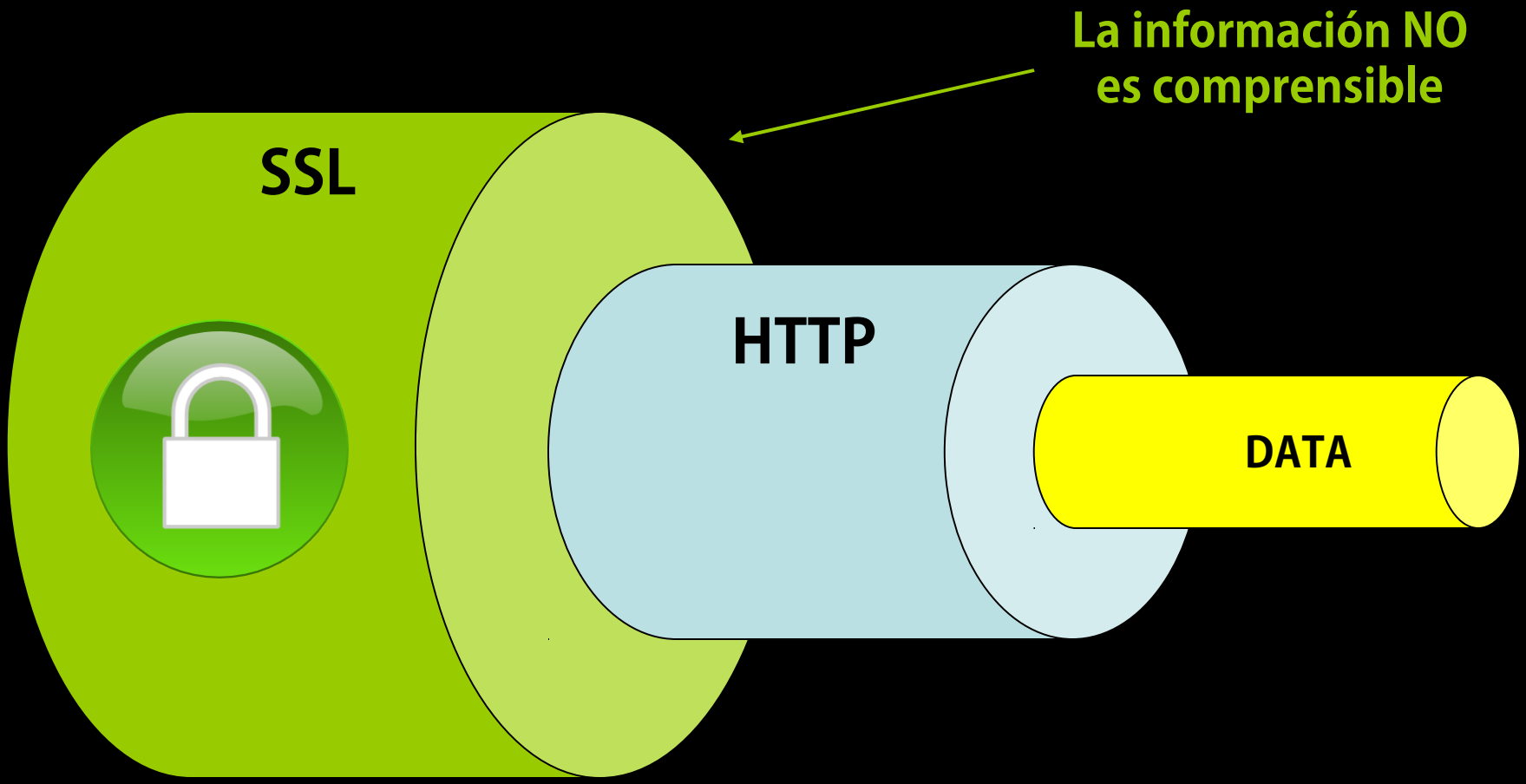
SSH

IPSec

Analizando SSL



Analizando SSL (Cont.)



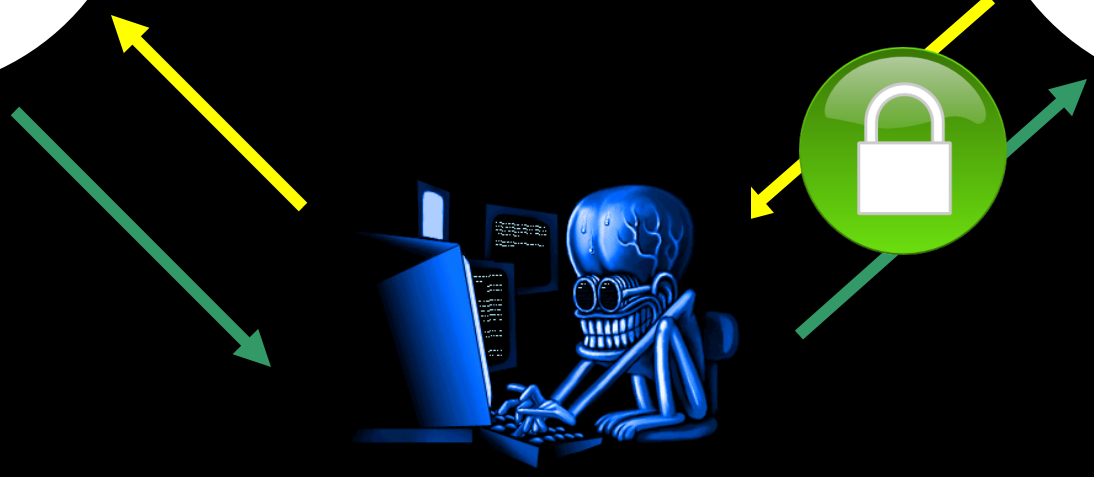
Analizando SSL (Cont.)

La intrusión NO se puede realizar

Evadiendo SSL

sslstrip

Evadiendo SSL (Cont.)



Evadiendo SSL (Cont.)

1. HTTPS Request

2. HTTP Redirect

3. Envío de DATA

6. Reenvío de Respuesta

5. Recepción de Respuesta

4. Reenvío de DATA

DEMO

Contramedidas

Forzar HTTPS

Evitar HTTP 302 (Redirect)

Awareness Training

Links

arpspoof (dsniff):

http://www.monkey.org/~dugsong/dsniff/
apt-get install dsniff

wireshark:

http://www.wireshark.org/
apt-get install wireshark

sslstrip:

http://www.thoughtcrime.org/software/sslstrip/

Mkit | IT & Security Solutions

www.mkit.com.ar

Preguntas?

Matias Katz

Email: matias@matiaskatz.com

Blog: www.matiaskatz.com

Twitter: @matiaskatz