Network Visibility

Taking Back Control of Your Network

To detect compromise and prevent Data Loss

By

Gideon J. Lenkey CISSP

The Gold Standard in Network Security

RaSecurity.com

About Me

- Volunteer Fireman AND Amateur Tattoo Artist
- Who nearly stood up to the vicious Chicken of Bristol
- Who had personally wet himself at the Battle of Badon Hill

The Gold Standard in Network Security

RaSecurity.com

Seriously Though

- Sporadic Author
- See me in a movie: Code 2600
- Hire me to Hack your company
- I can provide Managed Security Services to your company

The Gold Standard in Network Security

RaSecurity.com

What We'll Cover

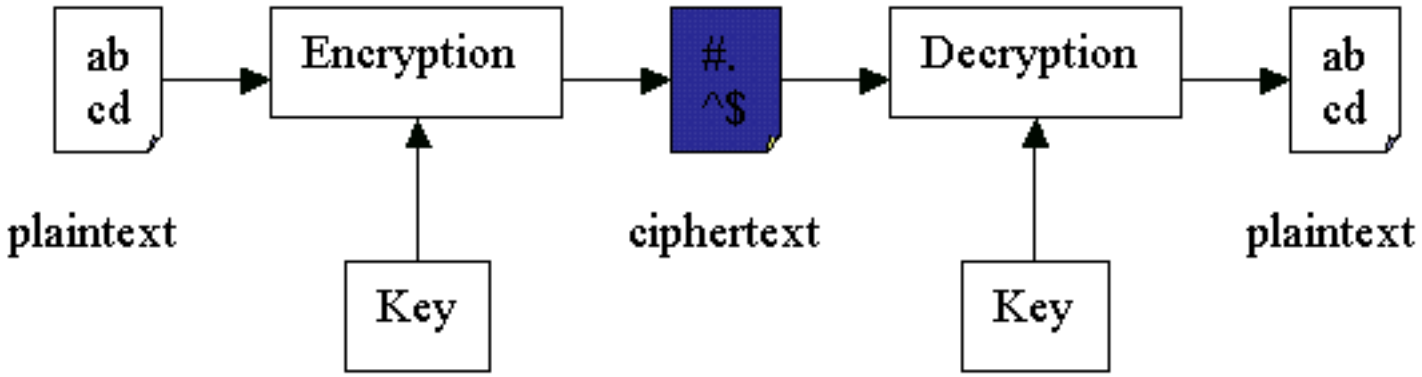
- Encryption Primer
- How SSL Works
- Why the bad guys are winning
- How we can take the advantage back

The Gold Standard in Network Security

RaSecurity.com

Simple Encryption

Symmetrical

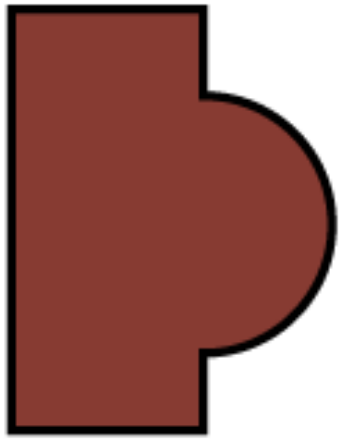


The Gold Standard in Network Security

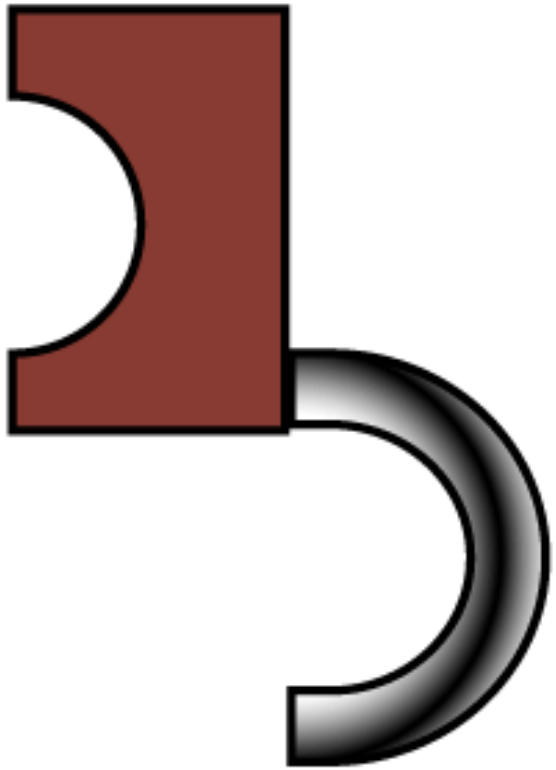
RaSecurity.com

Public Key Encryption

Private key



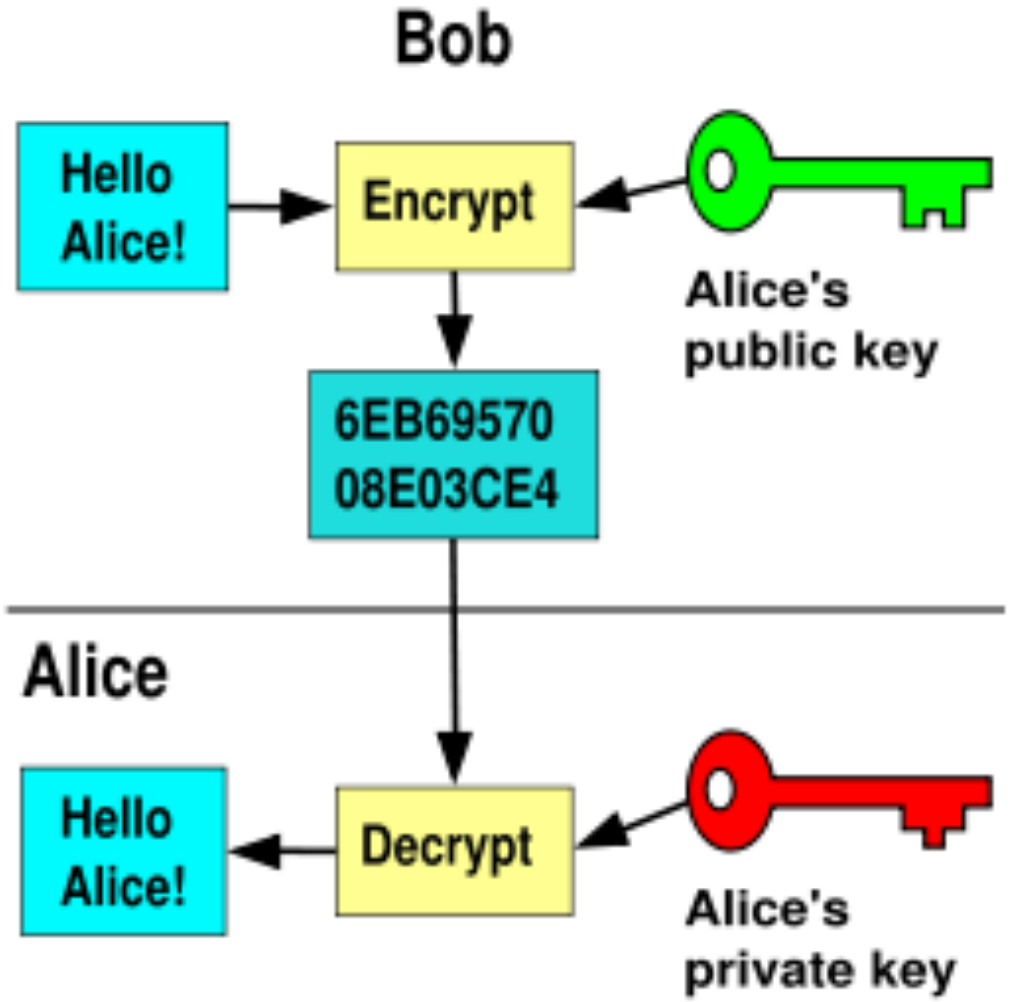
Public key



The Gold Standard in Network Security

RaSecurity.com

Public Key Encryption



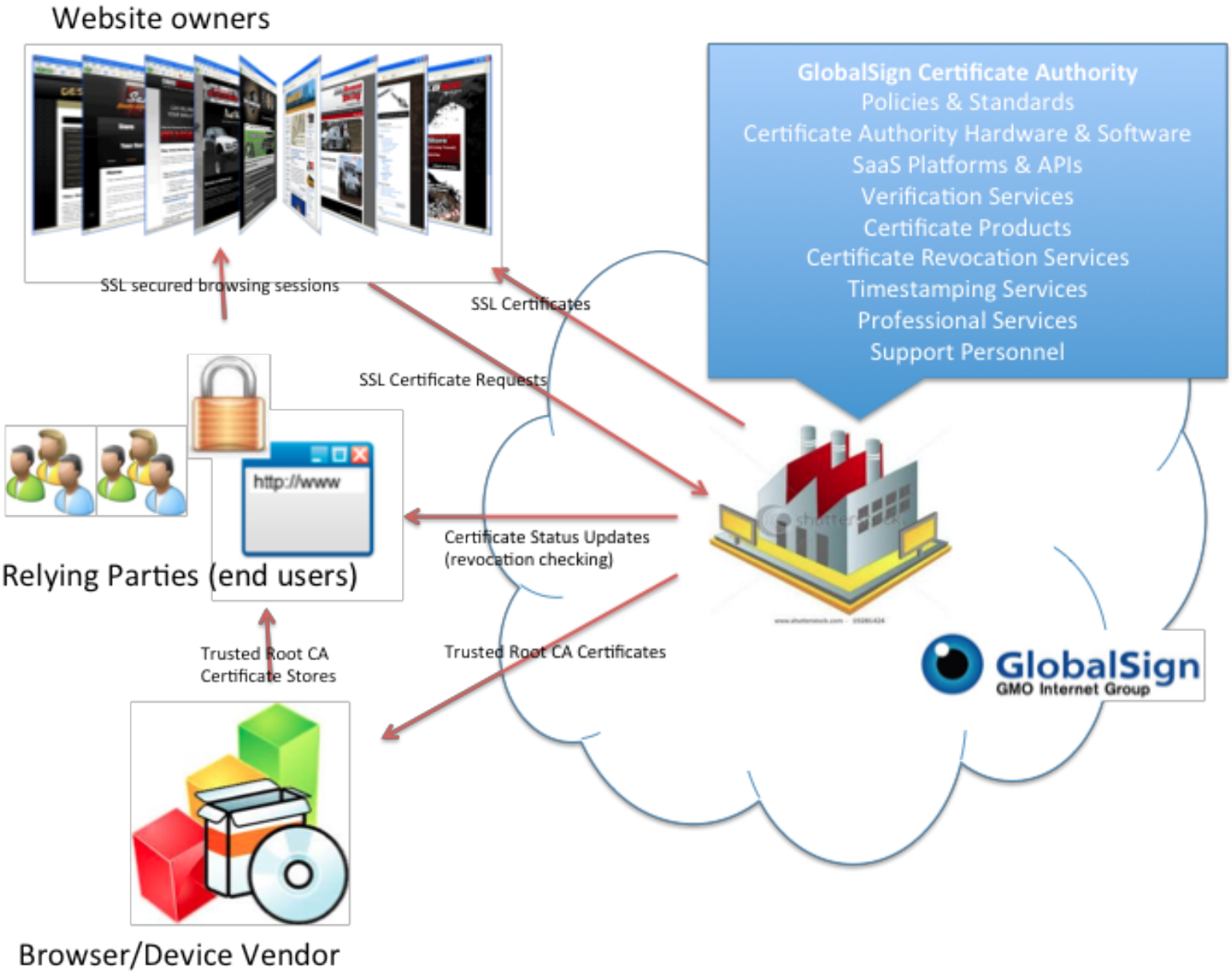
The Gold Standard in Network Security

RaSecurity.com

Advantages / Disadvantages

- Zero Trust (no shared secrets)
- Information Integrity
- Non-repudiation
- Slower than Symmetrical
- More Complex in general
- Doesn't handle first time one to many relationships well

Certificate Authority



The Gold Standard in Network Security

RaSecurity.com

HTTPS / SSL Flow

How does HTTPS work: SSL explained

This presumes that SSL has already been issued by SSL issuing authority.

3. Website Records found.
Going to the Host Web Server.

4. Requesting Secure SSL connection from Website Host.

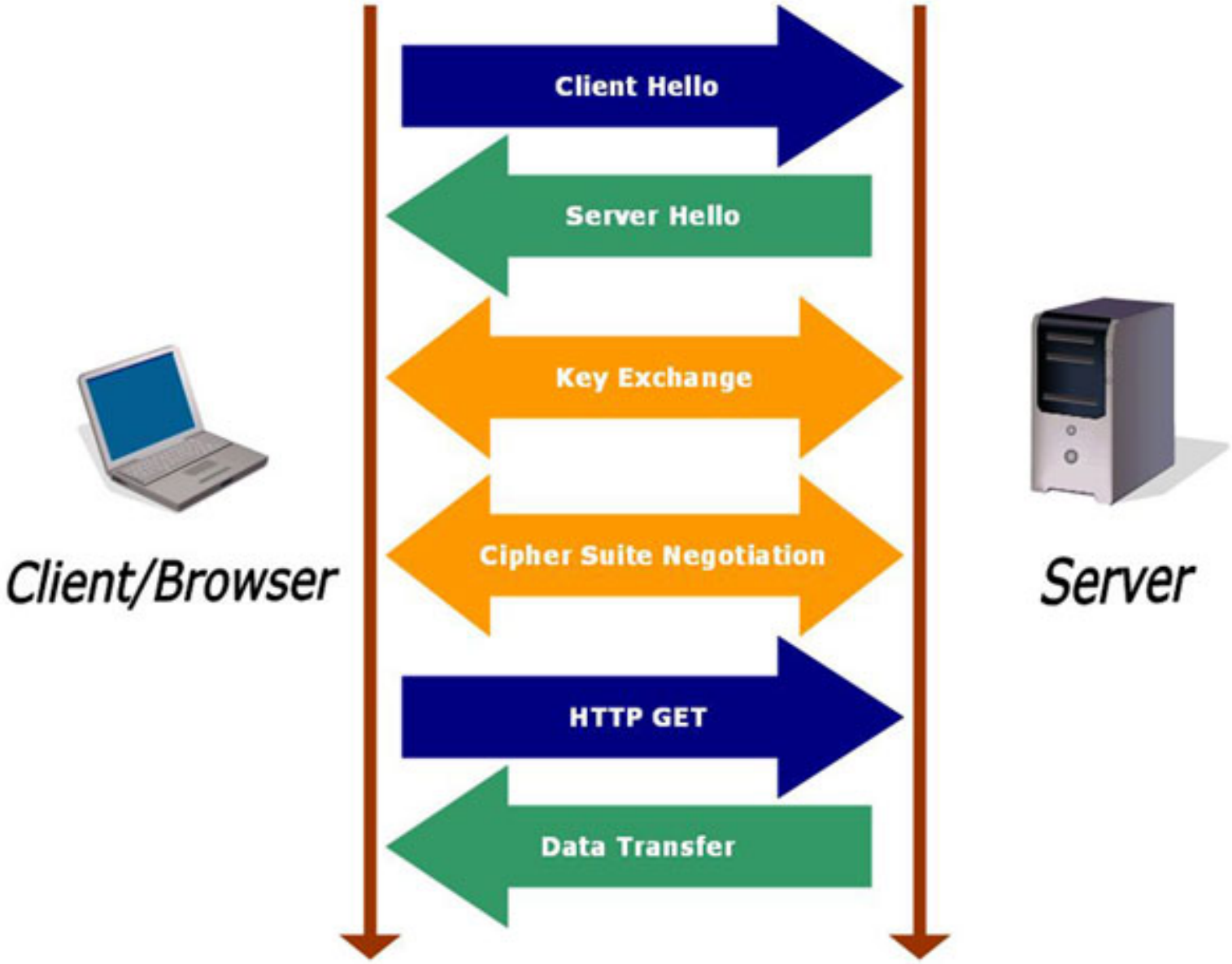
2. Check DNS records for IP address to find website host.

5. Host responds with valid SSL certificate.

1. User accessing secure site.

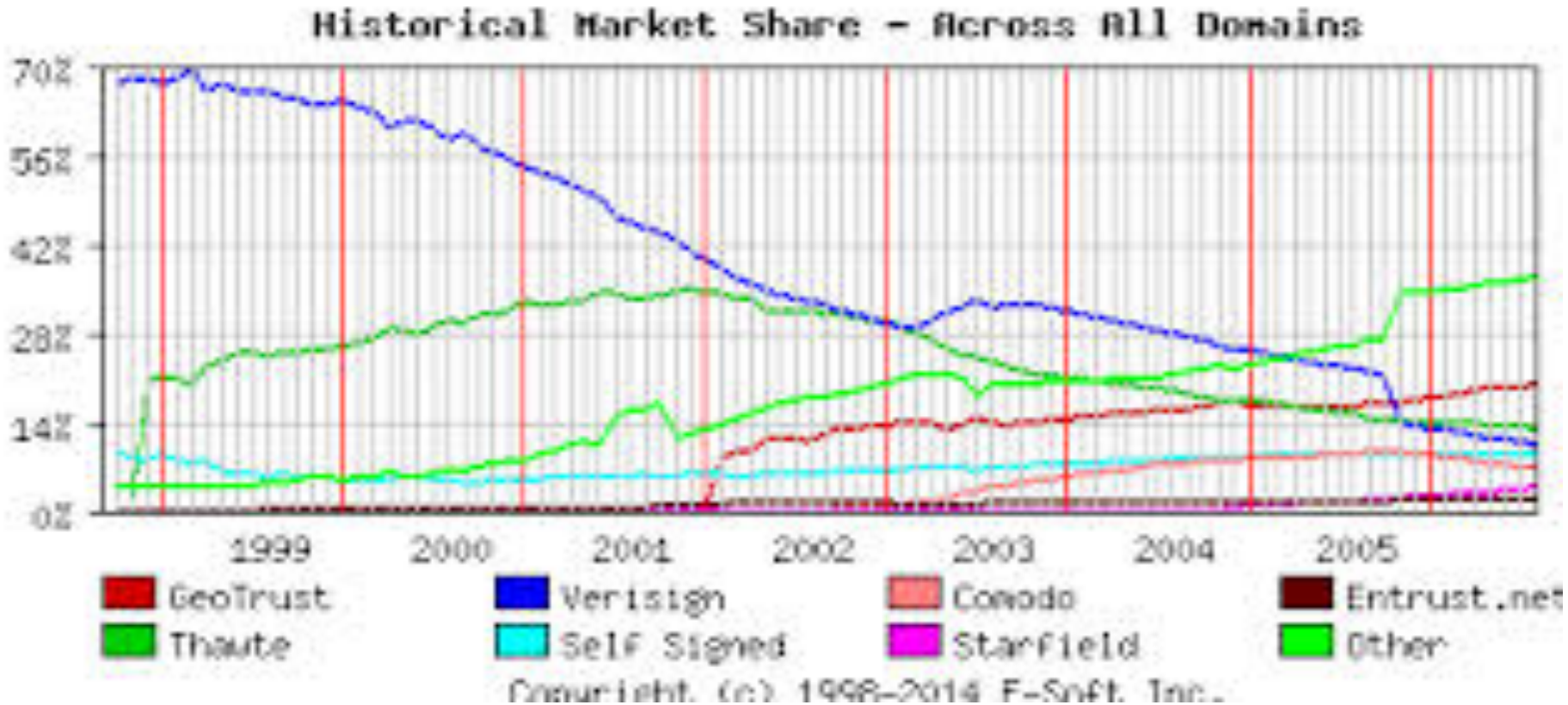
6. Secure connection is now established.
Transferred data is encrypted.

HTTPS / SSL Flow

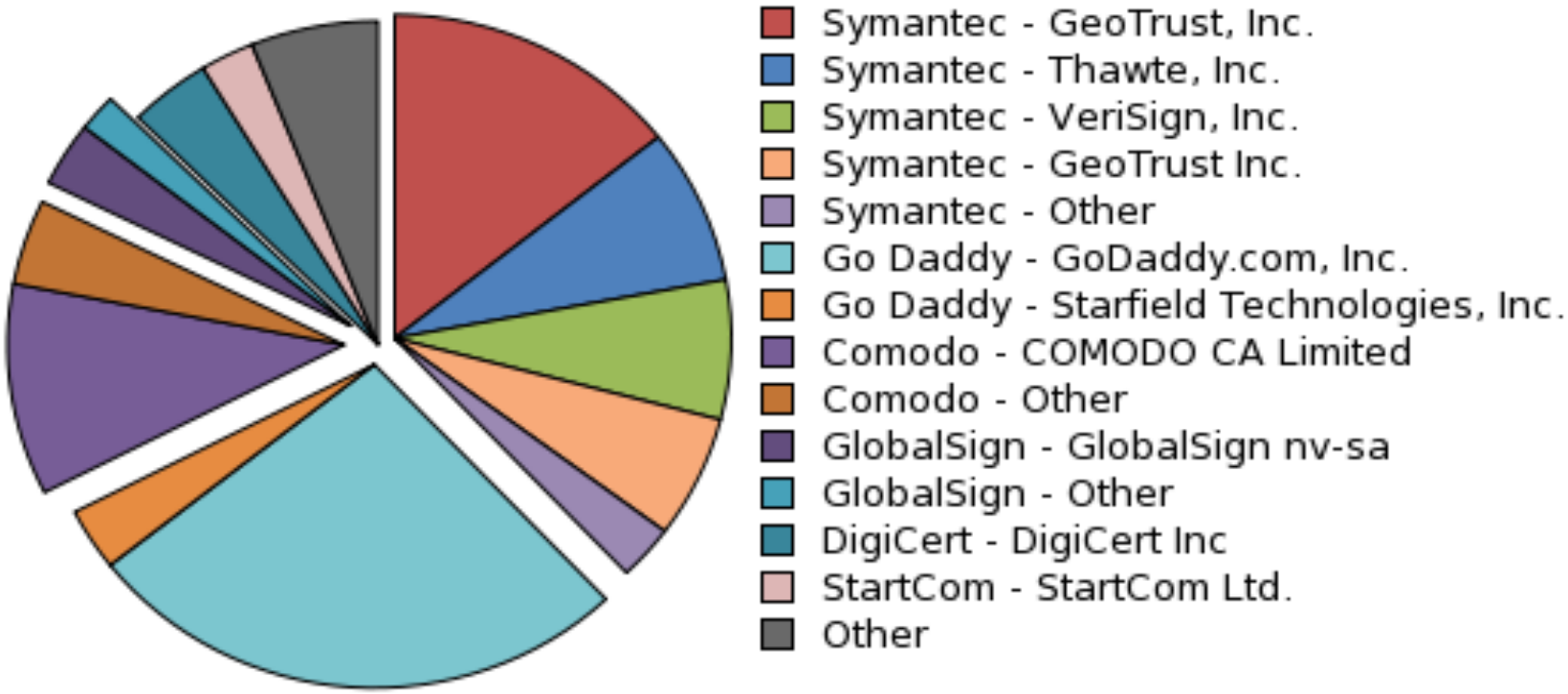


The Gold Standard in Network Security

RaSecurity.com


Historical Market Share - Across All Domains
70%
56%
42%
28%
14%
0%
1999
2000
2001
2002
2003
2004
2005
GeoTrust
Verisign
Comodo
Entrust.net
Thawte
Self Signed
Starfield
Other
Copyright (c) 1998-2014 E-Soft, Inc.

CA Market Share 2013



Sounds Good So Far: But

- Most internal network traffic is now SSL
- Almost all will be in the near future
- Traditional network based security controls can't see inside SSL
- The bad guys are using SSL to hide communication and exfiltration

The Gold Standard in Network Security

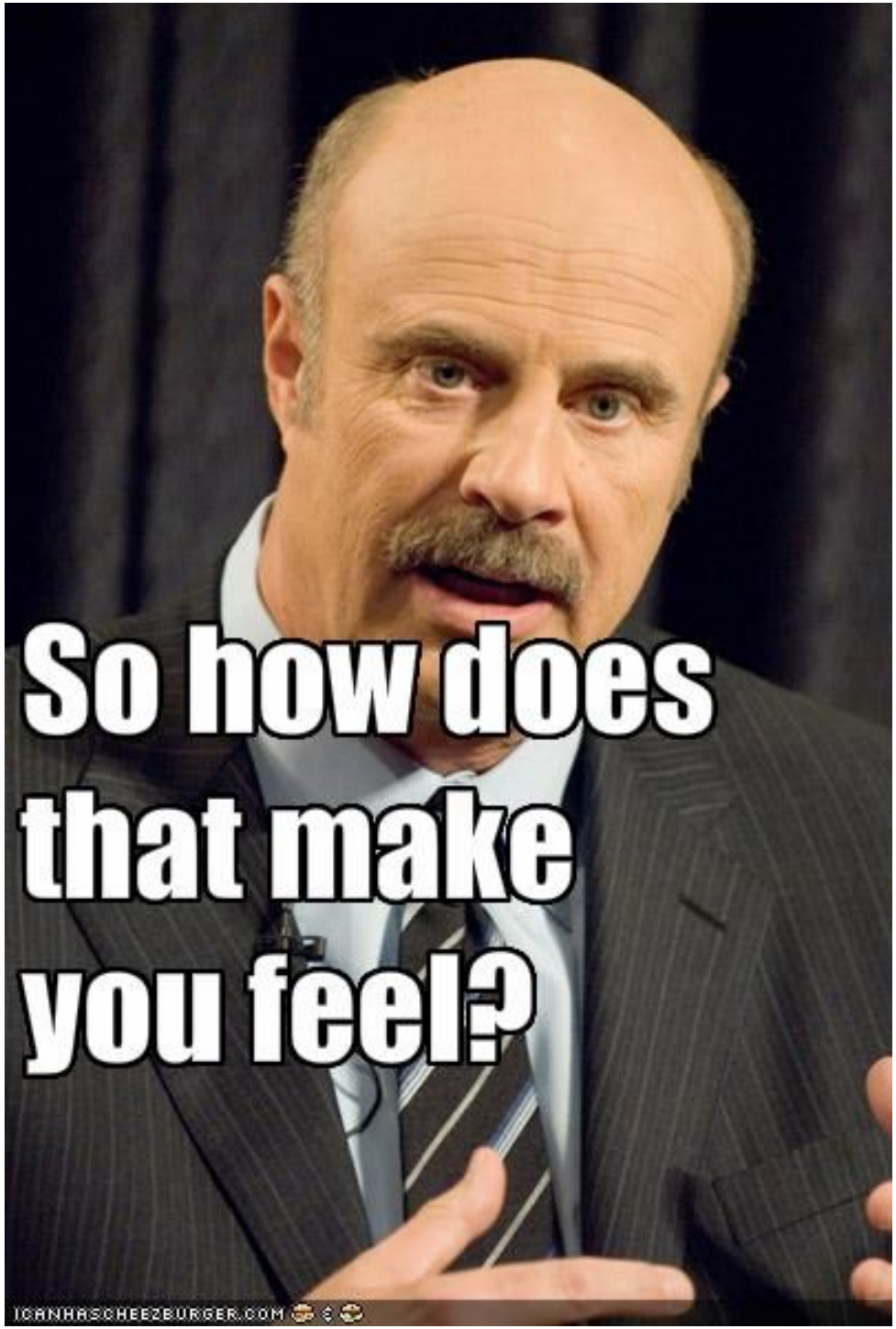
RaSecurity.com

Binaries			
payload 1	D=N, S=Y	D=N, S=Y	D=N, S=Y
payload 2	D=N, S=N	D=N, S=N	D=N, S=Y
payload 3	D=Y (cleaned)	D=Y (cleaned)	D=N, S=Y
payload 4	D=Y (cleaned)	D=Y (cleaned)	D=N, S=Y
payload 5	D=N, S=Y	D=N, S=Y (limited)	D=N, S=Y
payload 6	D=N, S=Y	D=N, S=Y	D=N, S=Y
payload 7	D=N, S=Y	D=N, S=Y	D=N, S=Y
payload 16	D=N, S=Y	D=N, S=Y	D=N, S=Y
payload 17	D=N, S=Y	D=N, S=Y	D=N, S=Y
payload 18	D=N, S=Y	D=N, S=Y	D=N, S=Y
payload 19	D=N, S=Y	D=N, S=Y	D=N, S=Y
payload 20	D=N, S=Y	D=N, S=Y	D=N, S=Y
payload 21	D=N, S=Y	D=N, S=Y	D=N, S=Y
payload 22	D=N, S=Y	D=N, S=Y	D=N, S=Y
Powershell			
payload 11	D=N, S=N (proxy)	D=N, S=N (proxy)	D=N, S=N (proxy)
payload 13	D=N, S=Y	D=N, S=Y	D=N, S=Y

File			
Document	D=Y (cleaned)	D=Y (cleaned)	D=Y (option to clean)
PDF	D=Y	D=Y	D=Y (cleaned)
zip/document	D=Y	D=Y	D=Y
browser Java	D=N, S=Y	D=N, S=Y	D=N, S=Y
Trojan exe			
psexec	D=Y (cleaned)	D=Y (cleaned)	D=N S=Y
putty	D=Y (cleaned)	D=Y (cleaned)	D=Y (cleaned)
Domain Login			
psexec	D=Y	D=Y	D=Y
psexec_com	D=N, S=Y	D=N, S=Y	D=N, S=Y

Key:

AV Protected	D = Detected
AV Failed	S = Payload Sucessful
Partial Protection	


So how does that make you feel?
ICANHASCHEEZBURGER.COM

How do we take the initiative?
How do we take the fight back to the enemy?

The Gold Standard in Network Security

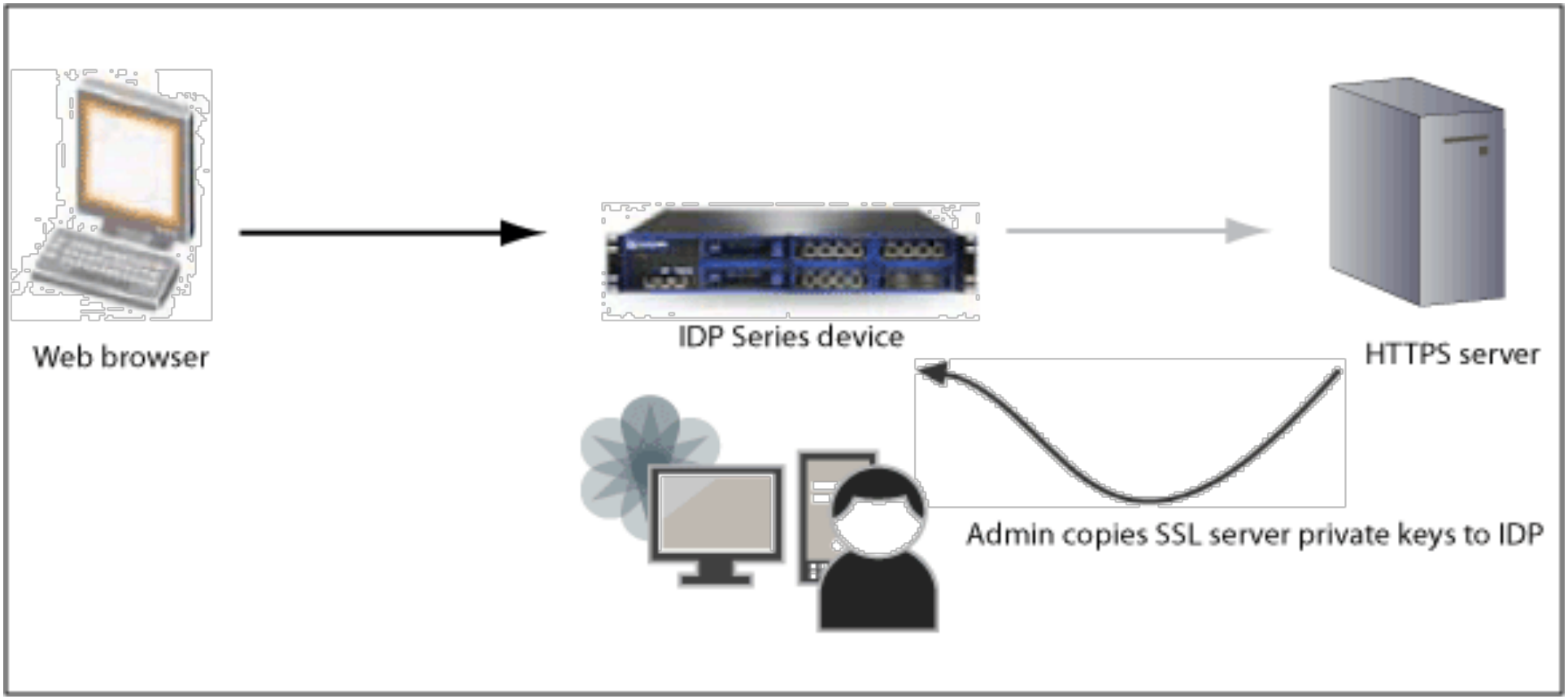
RaSecurity.com

We Proxy SSL

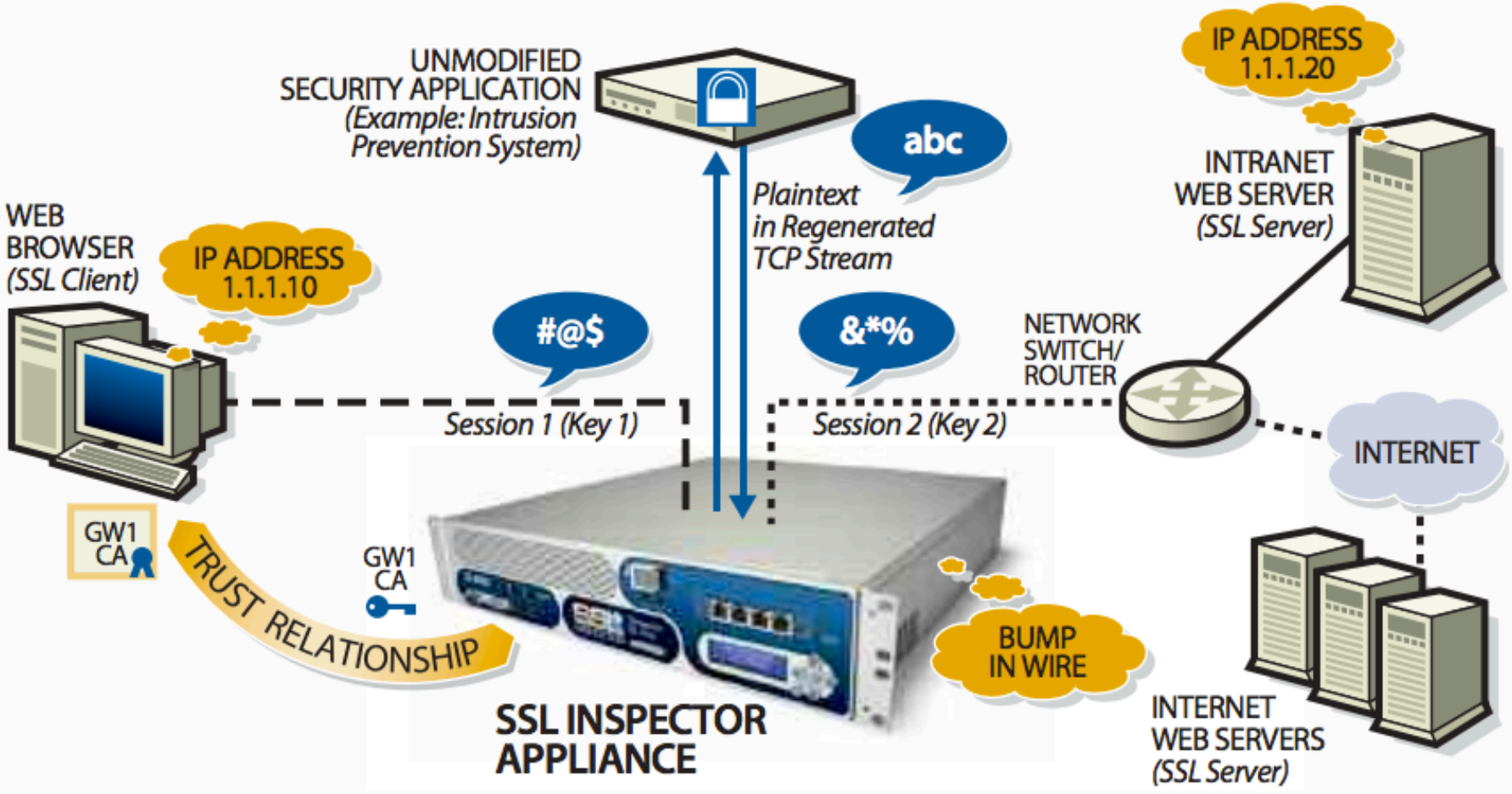
The Gold Standard in Network Security

RaSecurity.com

SSL Proxy to a server is fairly Easy



Transparently Decrypting SSL for Existing Applications (In-line Mode)



With This we Can

- Monitor all the clear text in the SSL tunnel
- Control which certificates are excepted by policy
- Detect protocols tunneled within other protocols
- Terminate suspicious connections

The Gold Standard in Network Security

RaSecurity.com

Performance & Function



	SV1800	SV2800	SV3800
Total Throughput	4 Gbps	20 Gbps	40 Gbps
SSL Inspection Throughput	1.5 Gbps	2 Gbps	4 Gbps
Cut-through Latency	<40µs	<40µs	<40µs
Concurrent SSL Flow States	100,000	200,000	400,000
SSL Flow Setups/Teardowns	6,500 per second	9,500 per second	11,500 per second
SSL Session Log Entries	50,000,0000	50,000,0000	50,000,0000
Easy-to-Use Web-based Management	Yes	Yes	Yes
Policy-based Categorization of SSL Traffic	Yes (subscription-based license)	Yes (subscription-based license)	Yes (subscription-based license)

Advantages

- Restores ability to detect IOCs
- Control subversion can be detected
- Reduces reliance on protective controls
- Enhances deep packet protective controls such as application proxies
- Enhances efficiency of all network based control
- Relatively low cost, $5-7K for most

The Gold Standard in Network Security

RaSecurity.com

The Gold Standard in Network Security

RaSecurity.com

How the NSA, and your boss, can intercept and break SSL

Summary: *Most people believe that SSL is the gold-standard of Internet security. It is good, but SSL communications can be intercepted and broken. Here's how.*

By Steven J. Vaughan-Nichols for Networking | June 8, 2013 -- 22:44 GMT (15:44 PDT)

Follow @sjvn

Is the National Security Agency (NSA) really "wiretapping" the Internet? Accused accomplices Microsoft and Google deny that they have any part in it and the core evidence isn't holding up that well under closer examination.

Some, however, doubt that the NSA could actually intercept and break Secure-Socket Layer (SSL) protected Internet communications.

Ah, actually the NSA can.

And, you can too and it doesn't require "Mission Impossible" commandos, hackers or supercomputers. All you need is a credit-card number.

There are many ways to attack SSL, but you don't need fake SSL certificates, a rogue Certification Authority (CA), or variations on security expert Moxie Marlinspike's man-in-the-middle SSL attacks. Why go to all that trouble when you can just buy a SSL interception proxy, such as Blue Coat Systems' ProxySG or their recently acquired Netronome SSL appliance to do the job for you?

Blue Coat, the biggest name in the SSL interception business, is far from the only one offering SSL interception and breaking in a box. Until recently, for example, Microsoft would sell you a program, Forefront Threat Management Gateway 2010, which could do the job for you as well.

In Conclusion

- This is a rare opportunity to get ahead
- This will hopefully be the status quo
- Please consider protecting your network this way (we have a lot to lose)

The Gold Standard in Network Security

RaSecurity.com

Thanks For Your Time!

Gideon J. Lenkey, CISSP

glenkey@rasecurity.com

(908) 246-0634

The Gold Standard in Network Security

RaSecurity.com