

RSAC Conference 2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: SPO3-W04

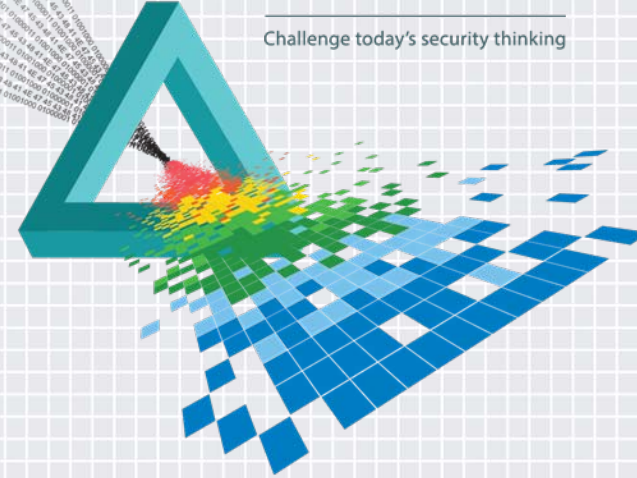
Secure Apache Web Server with HMTL5 and HTTP 2.0

Brandy Mauff

Chief Technology Evangelist
HOB Inc.

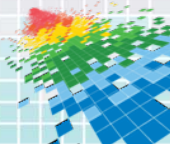
CHANGE

Challenge today's security thinking



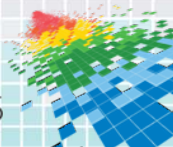
“The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards...”

- Eugene Spafford

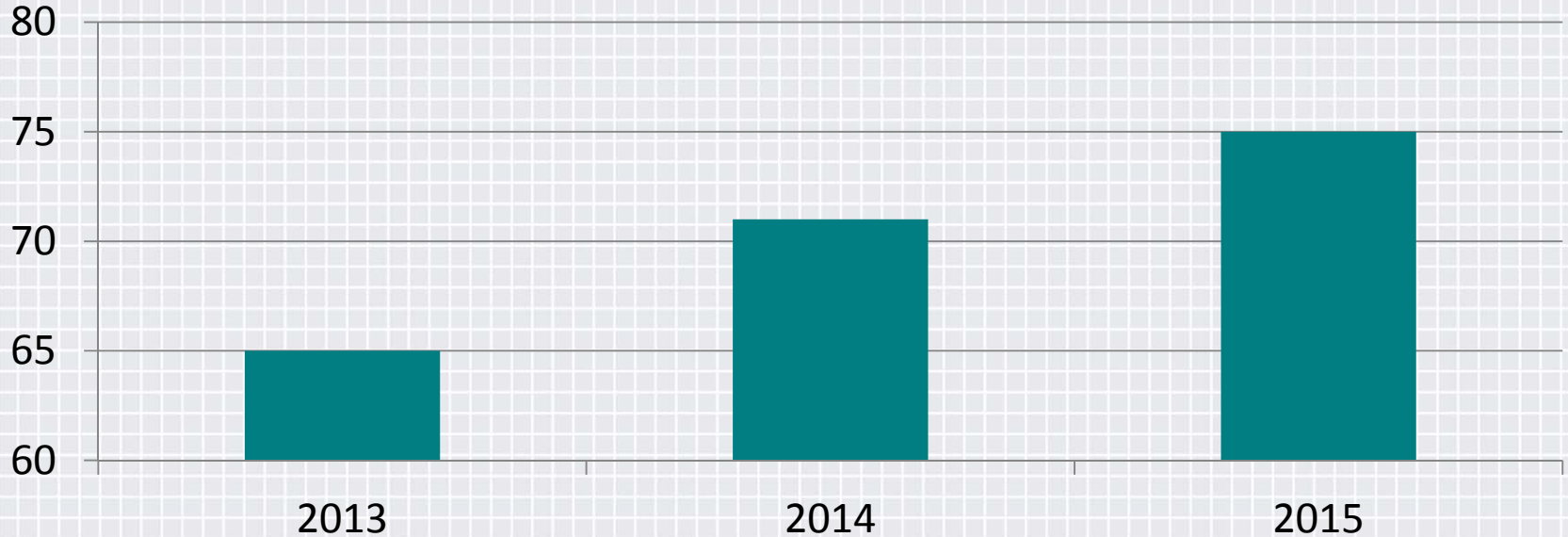


The Importance of Security

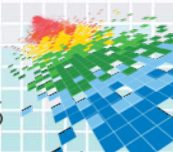
- ◆ Sensitive data
- ◆ Critical infrastructure
- ◆ Cyber attacks
- ◆ Mobile devices/apps



Information Security Spending Worldwide (in \$)



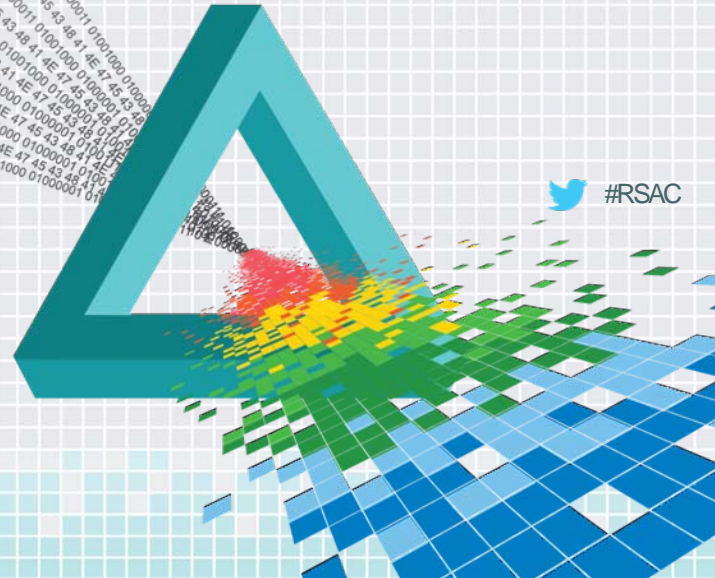
<http://www.gartner.com/newsroom/id/2828722>



RSAC®Conference2015

San Francisco | April 20-24 | Moscone Center

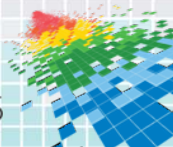
Apache Web Server



 #RSAC

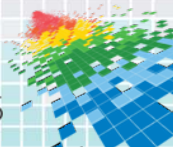
What is Apache Web Server?

- ◆ Originally designed for Unix environments in 1995
- ◆ Large public library of add-ons
- ◆ Most widely used Web server
- ◆ Open source



Key features of Apache Web Server

- ◆ Highly adaptable
- ◆ Configurable
- ◆ Content negotiation
- ◆ TLS support



Apache Web Server Hardening



Information leakage

Hide version, disable directory listing



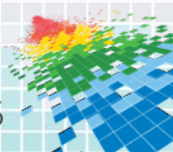
Unnecessary modules

Disable modules, update regularly



Lack of authorization

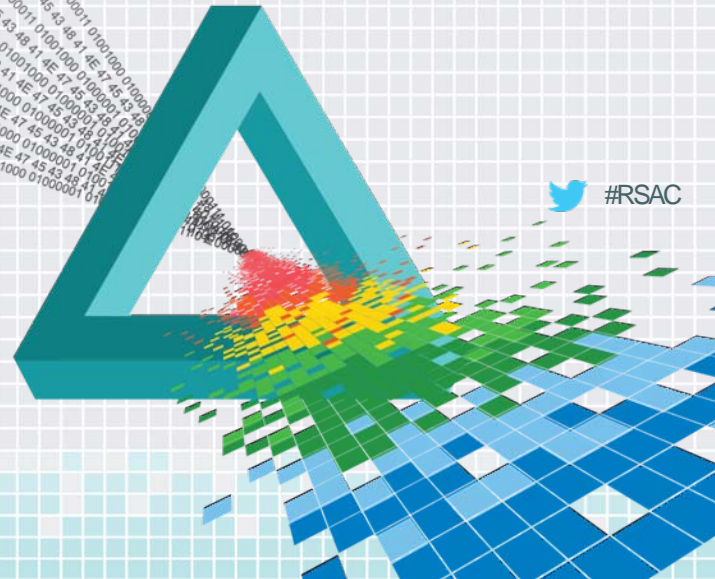
Separate user/group, restrict access



RSA[®]Conference2015

San Francisco | April 20-24 | Moscone Center

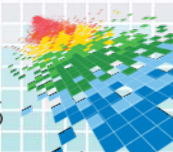
Apache Web Server and HTML5



 #RSAC

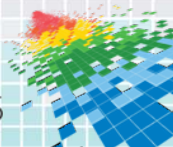
What is HTML5?

- ◆ Markup language
- ◆ Living standard (2014)
- ◆ Structuring and presenting content
- ◆ Support for latest multimedia types

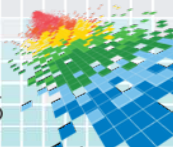
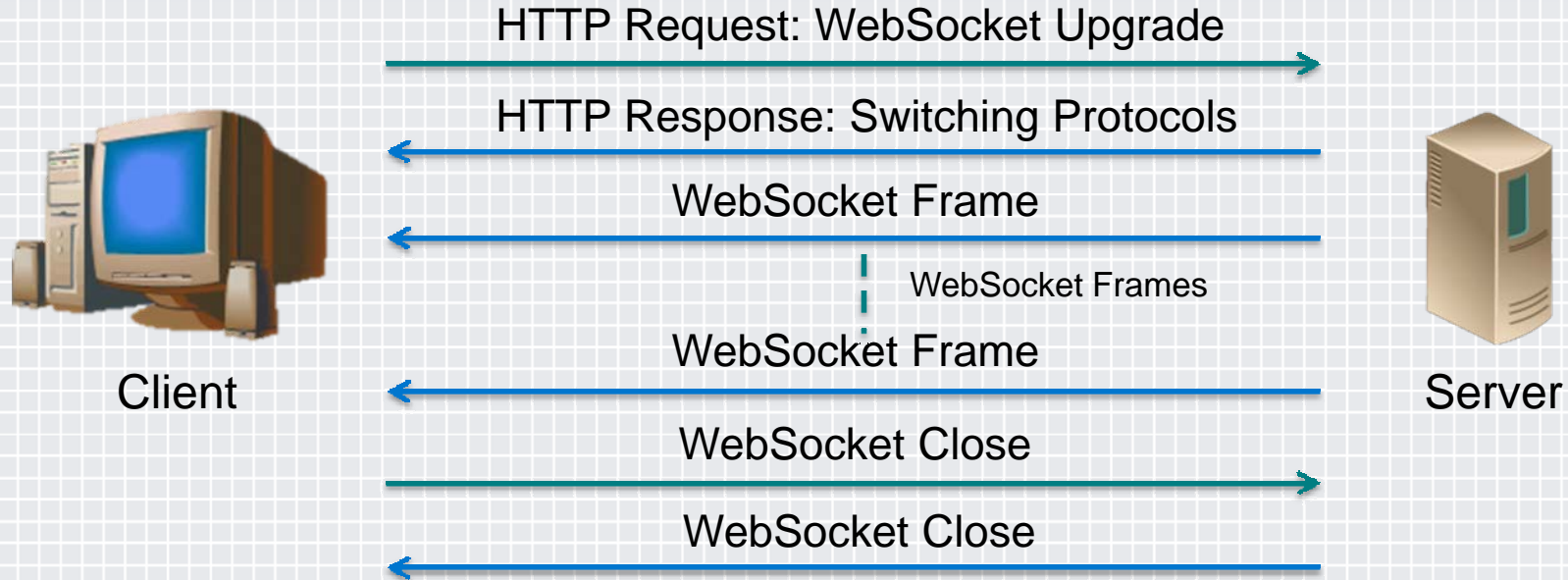


Features of HTML5

- ◆ Audio/video support
- ◆ Content editable
- ◆ Placeholders
- ◆ localStorage and sessionStorage



WebSockets

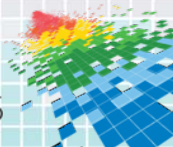


WebStorage

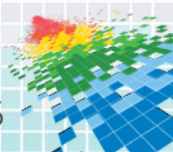
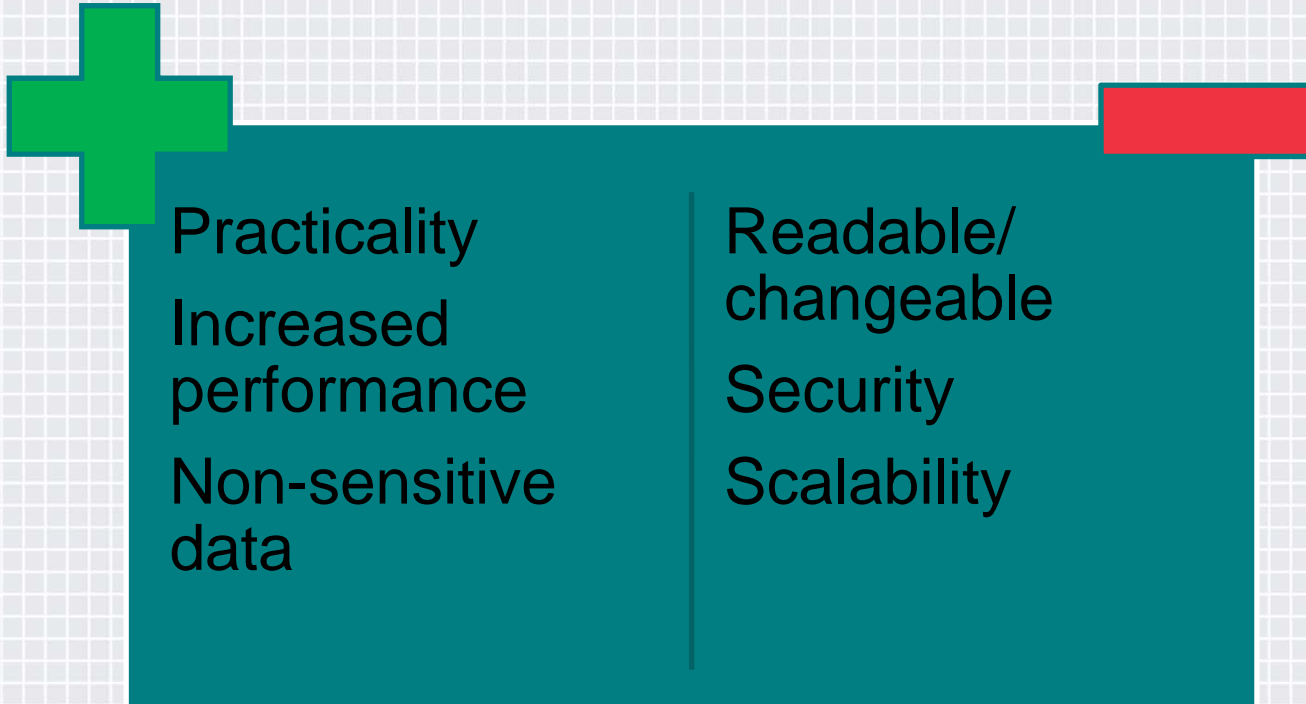


localStorage (no expiration date)

sessionStorage (only one session)



WebStorage – good or bad?



HTML5 Hardening



Cross-origin resource sharing

Validate URLs, discard requests



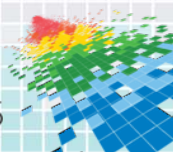
Offline Web application

Clear UA cache, only trusted sites



Web messaging

State origin, assign data value properly



RSA[®]Conference2015

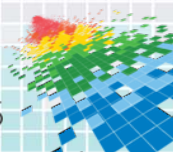
San Francisco | April 20-24 | Moscone Center

Apache Web Server and HTTP/2



What is HTTP/2?

- ◆ Exchanging/transferring hypertext
- ◆ Foundation of data communication for the World Wide Web
- ◆ Based on SPDY
- ◆ To become standard 2015



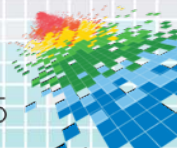
HTTP/2 – Key Improvements

server push

header
compression

multiplexing

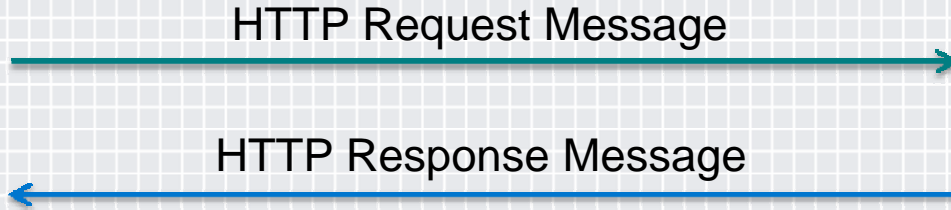
TLS support



How does HTTP/2 work?

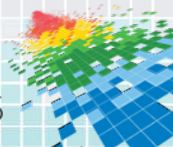


HTTP Client
(Web Browser)



HTTP Server
(Web Server)

HTTP over TCP/IP



HTTP/2 Hardening



POODLE

Disable SSL 2.0 and SSL 3.0



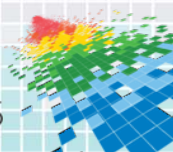
CRIME

Disable TLS 1.0



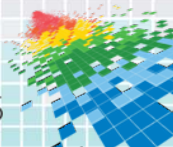
Heartbleed

Upgrade OpenSSL, disable TLS Heartbeat

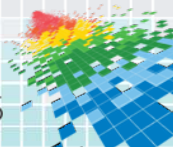
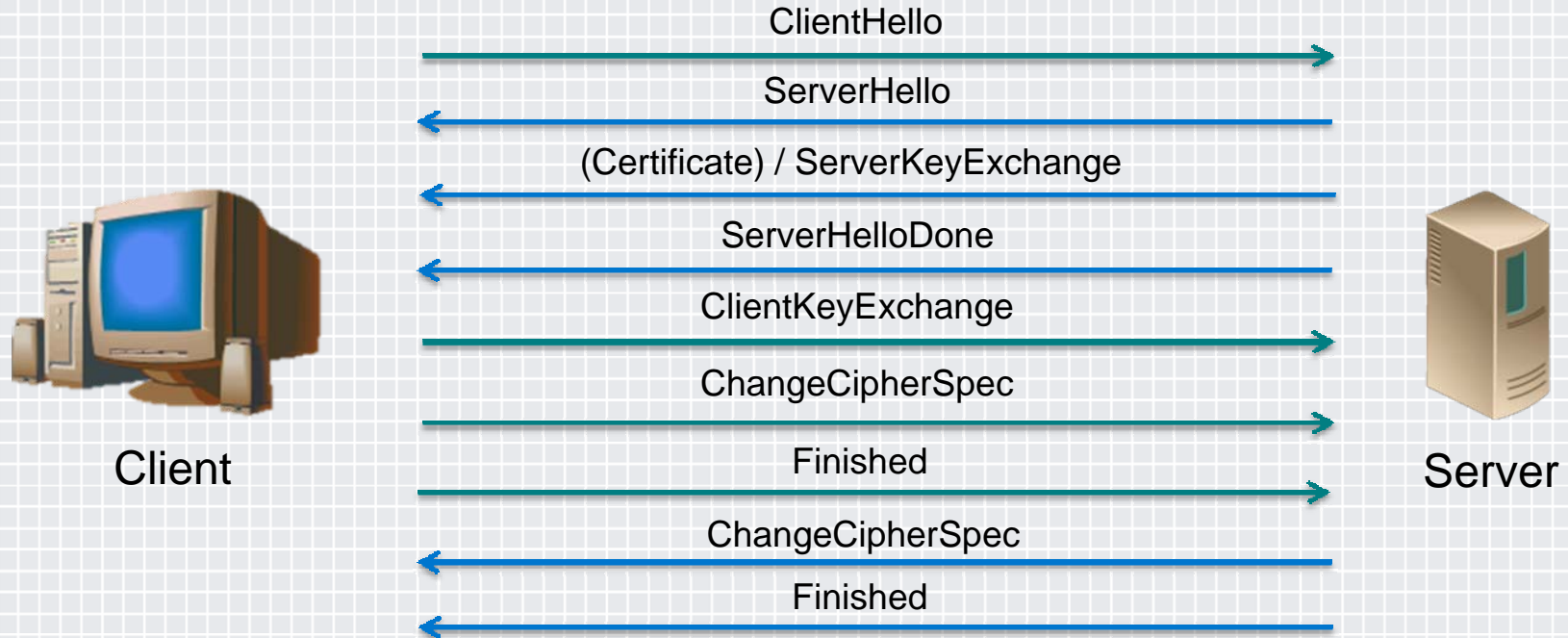


What is TLS?

- ◆ Cryptographic protocol designed to provide communication security and data integrity between client/server applications communicating over a computer network
- ◆ Supported by all major web browsers
- ◆ Made up of two layers

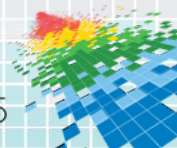


Basic TLS Handshake



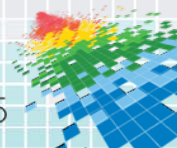
Advantages of TLS

- + Strong authentication
- + Algorithm flexibility
- + Interoperability
- + Easy to deploy
- + Easy to use



Disadvantages - the cost of TLS

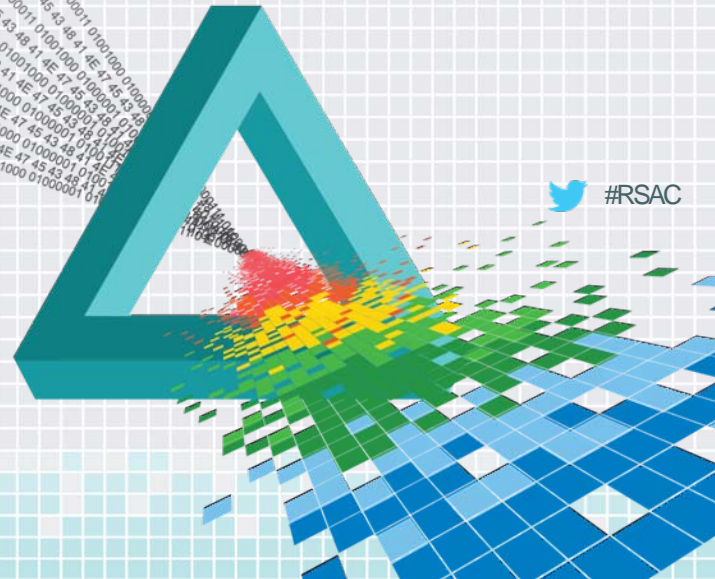
- Computational
- PKI
- Operational



RSA[®]Conference2015

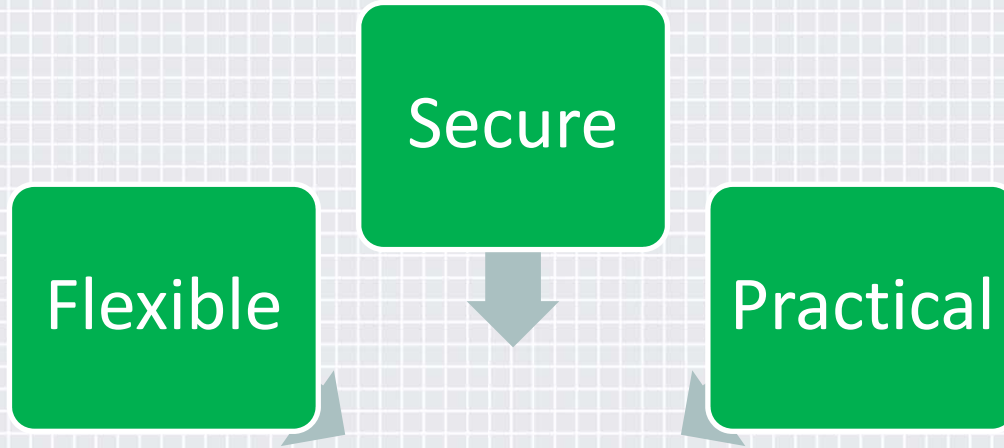
San Francisco | April 20-24 | Moscone Center

Apache Web Server
+ HTML5
+ HTTP/2
= ?



 #RSAC

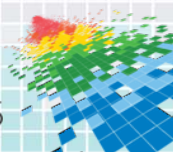
Apache Web Server + HTML5 + HTTP/2 = ?



Secure Apache Web Server with HTML5 and HTTP/2

What now?

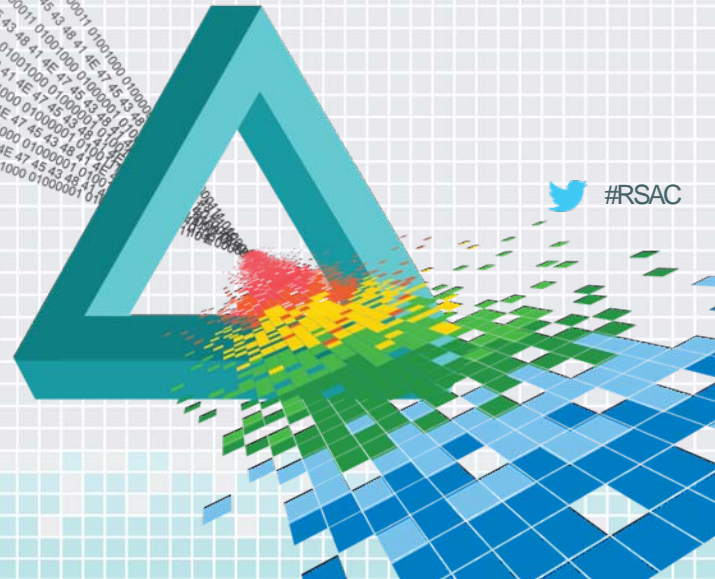
- ◆ Threat assessment – test, test, test!
- ◆ Solution feasibility
- ◆ Invest



RSA[®]Conference2015

San Francisco | April 20-24 | Moscone Center

Questions?



 #RSAC