KILL 'EM ALL

DDoS Protecion Total Annihilation!!! 

Network Threats
Information Sharing
and Analysis Center

BLOODSPEAR
LABORATORIES

NEXUSGUARD
DDoS Mitigation Lab

TO SERVE AND TO PROTECT

Network Threats Information Sharing and Analysis Center

BLOODSPEAR LABORATORIES

Industry body formed to foster synergy among stakeholders to promote advancement in DDoS defense knowledge.

NEXUSGUARD

DDoS Mitigation Lab

Independent academic R&D division of Nexusguard building next generation DDoS mitigation knowledge and collaborate with defense community.

BLOODSPEAR LABORATORIES

NEXUSGUARD DDoS Mitigation Lab

AGENDA

- DDoS Relevance, Attack Categories, Detection & Mitigation
- Source Host Verification: Authentication Methods
  - TCP SYN Auth
  - HTTP Redirect Auth
  - HTTP Cookie Auth
  - JavaScript Auth
  - CAPTCHA Auth
- PoC Tool
  - TCP Traffic Model
  - HTTP Traffic Model

BLOODSPEAR LABORATORIES NEXUSGUARD DDoS Mitigation Lab

SHOW ME THE

SIZE:
> 20GBPS

FREQUENCY:
> 2.5MIL
PER YEAR

COMPLEXITY:
APP LEVEL > 30%

COST:
> US$6MIL
PER HOUR

Source: NTT Communications,
"Successfully Combating DDoS Attacks", Aug 2012

BLOODSPEAR LABORATORIES

NEXUSGUARD
DDoS Mitigation Lab

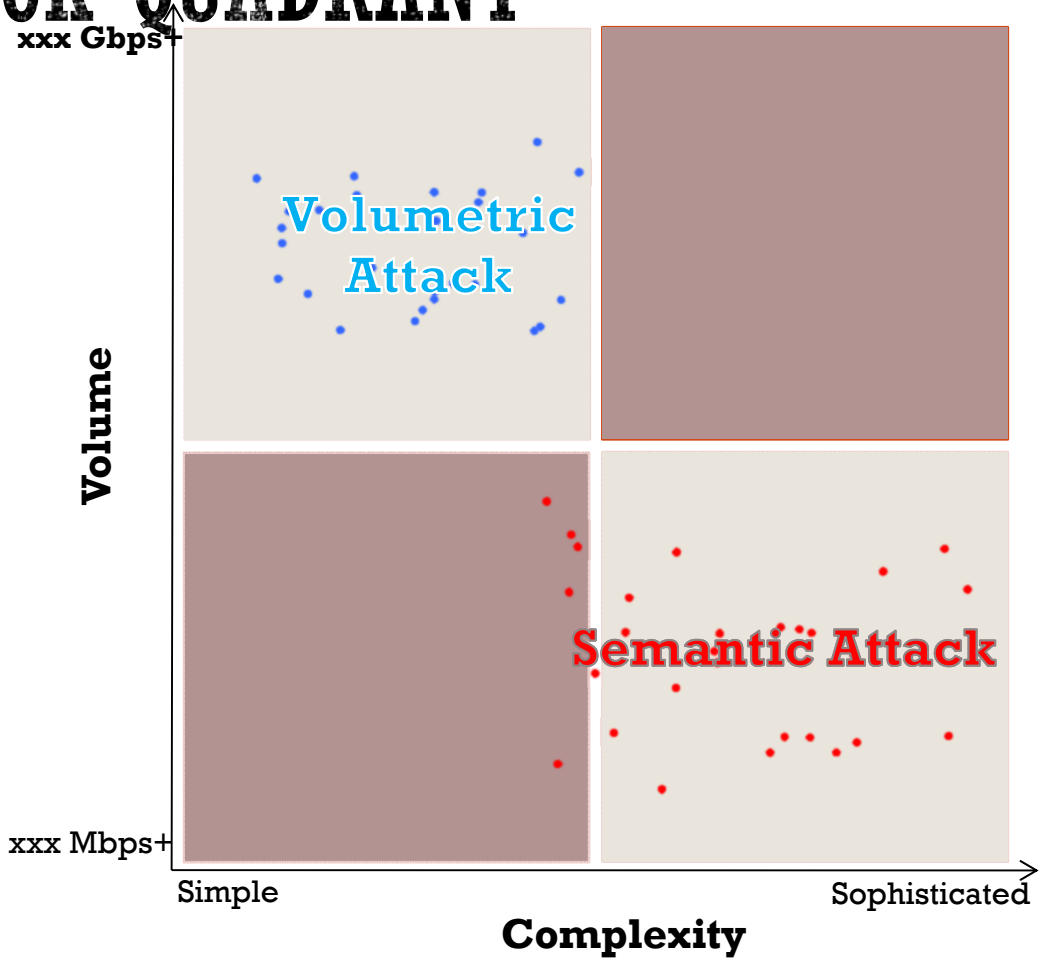
ATTACK CATEGORIES

Volumetric

Semantic

Blended

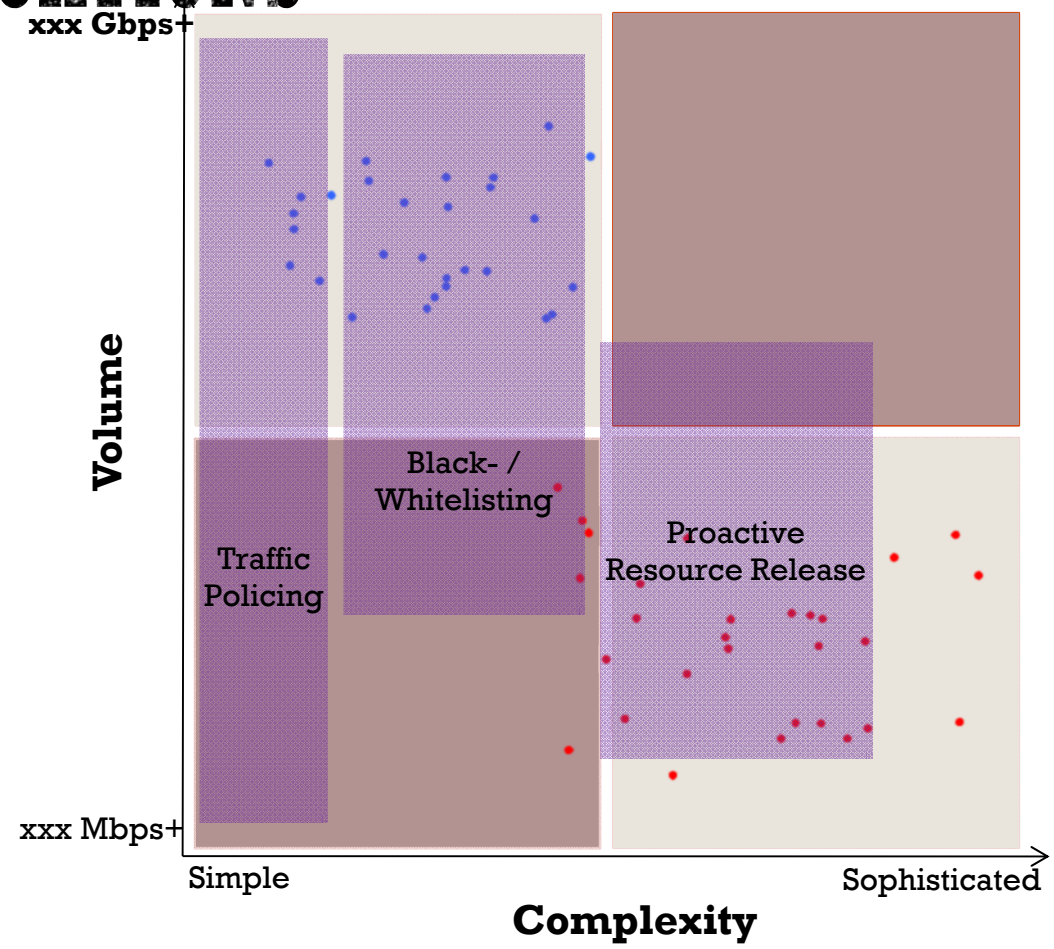
ATTACK QUADRANT



BLOODSPEAR LABORATORIES

NEXUSGUARD
DDoS Mitigation Lab

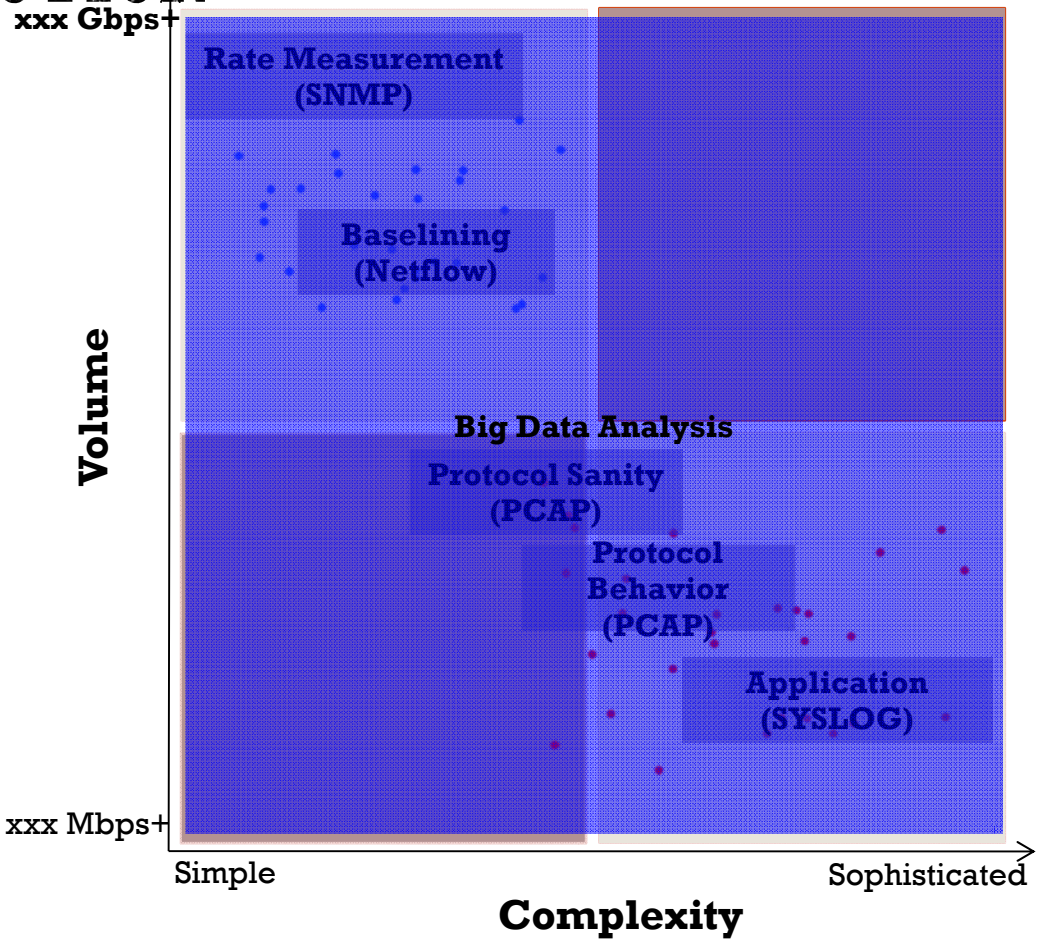
MITIGATIONS



BLOODSPEAR LABORATORIES

NEXUSGUARD
DDoS Mitigation Lab

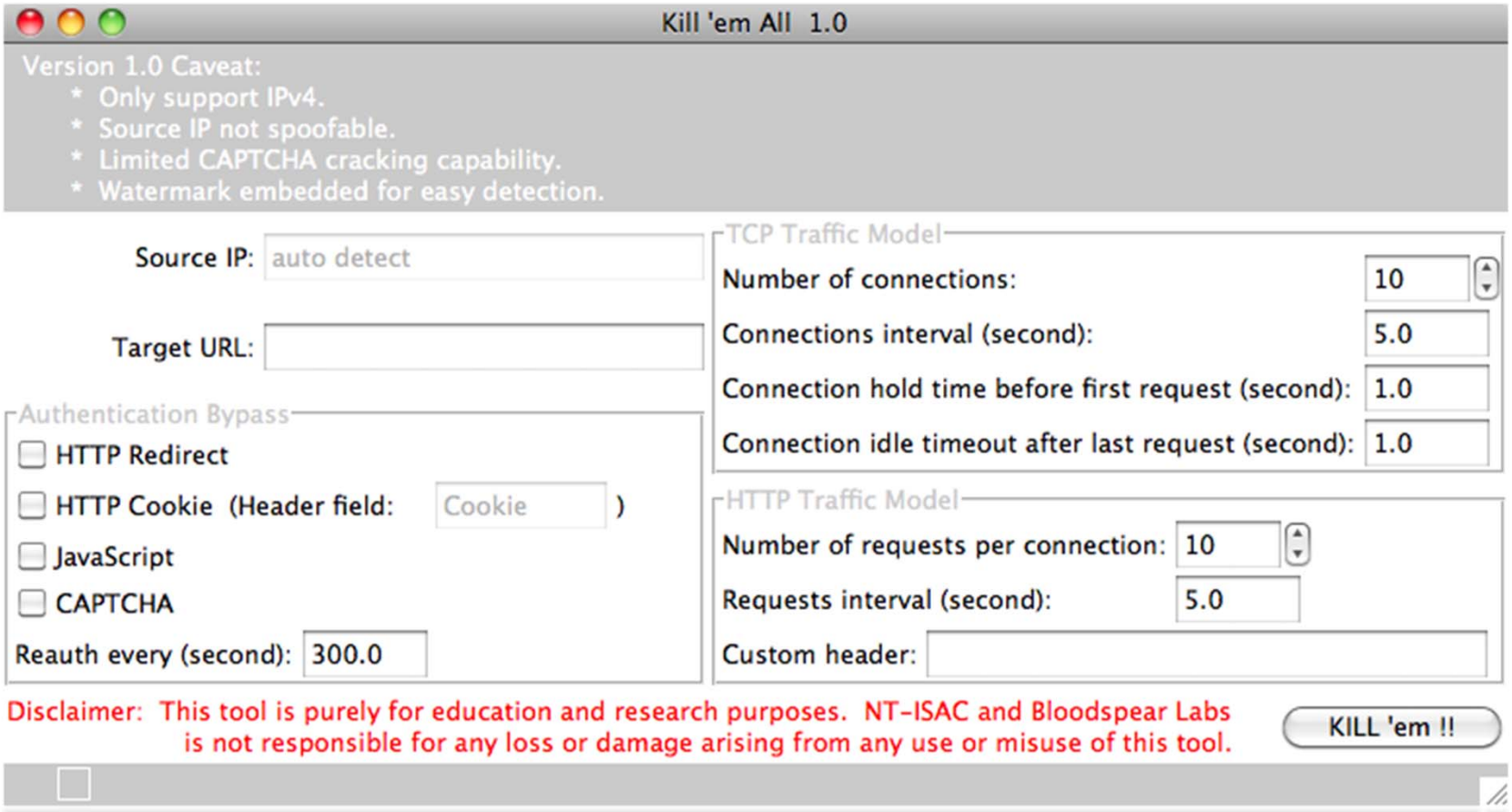
DETECTION



BLOODSPEAR LABORATORIES

NEXUSGUARD
DDoS Mitigation Lab

POC



BLOODSPEAR LABORATORIES

NEXUSGUARD
DDoS Mitigation Lab

WE DO IT AUTOMATICALLY

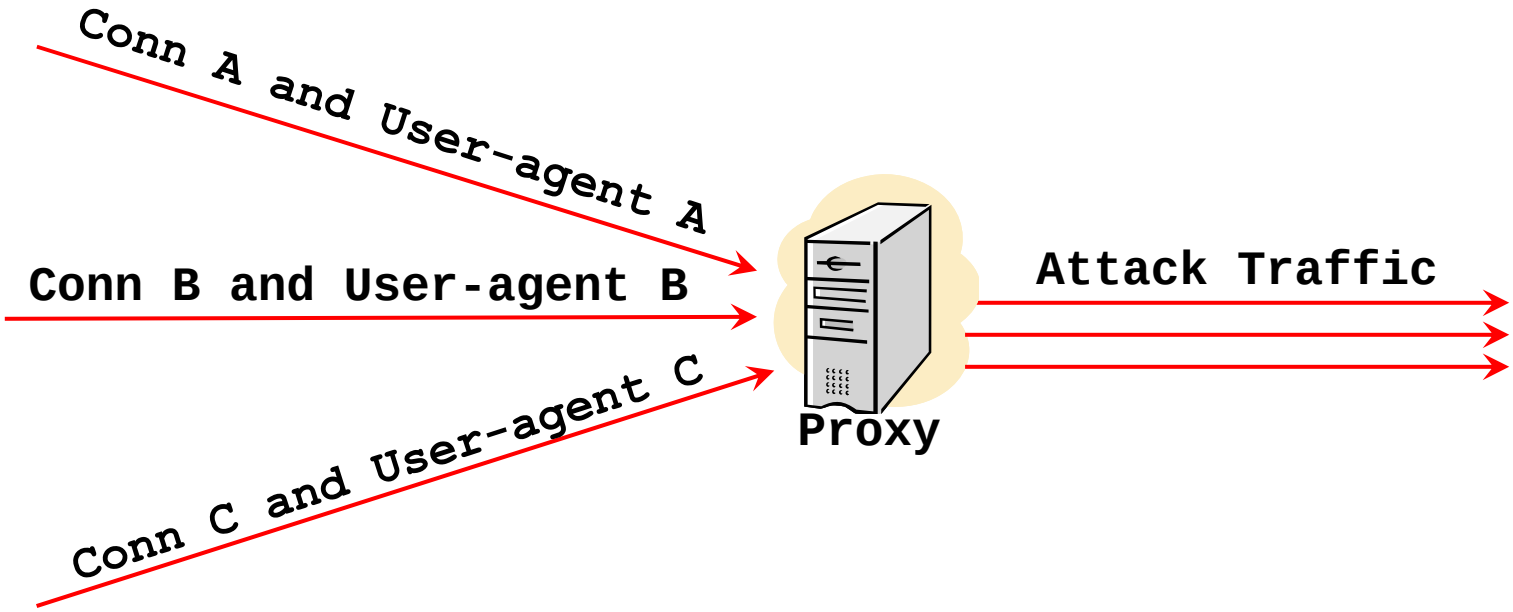
- Traffic Pattern simulation, e.g. Like traffic behind Proxy
- HTTP Header Simulation

Simulate Normal traffic Pattern and Behavior!!!!!

BLOODSPEAR LABORATORIES

NEXUSGUARD
DDoS Mitigation Lab

TRAFFIC PATTERN SIMULATION



HTTP HEADER SIMULATION

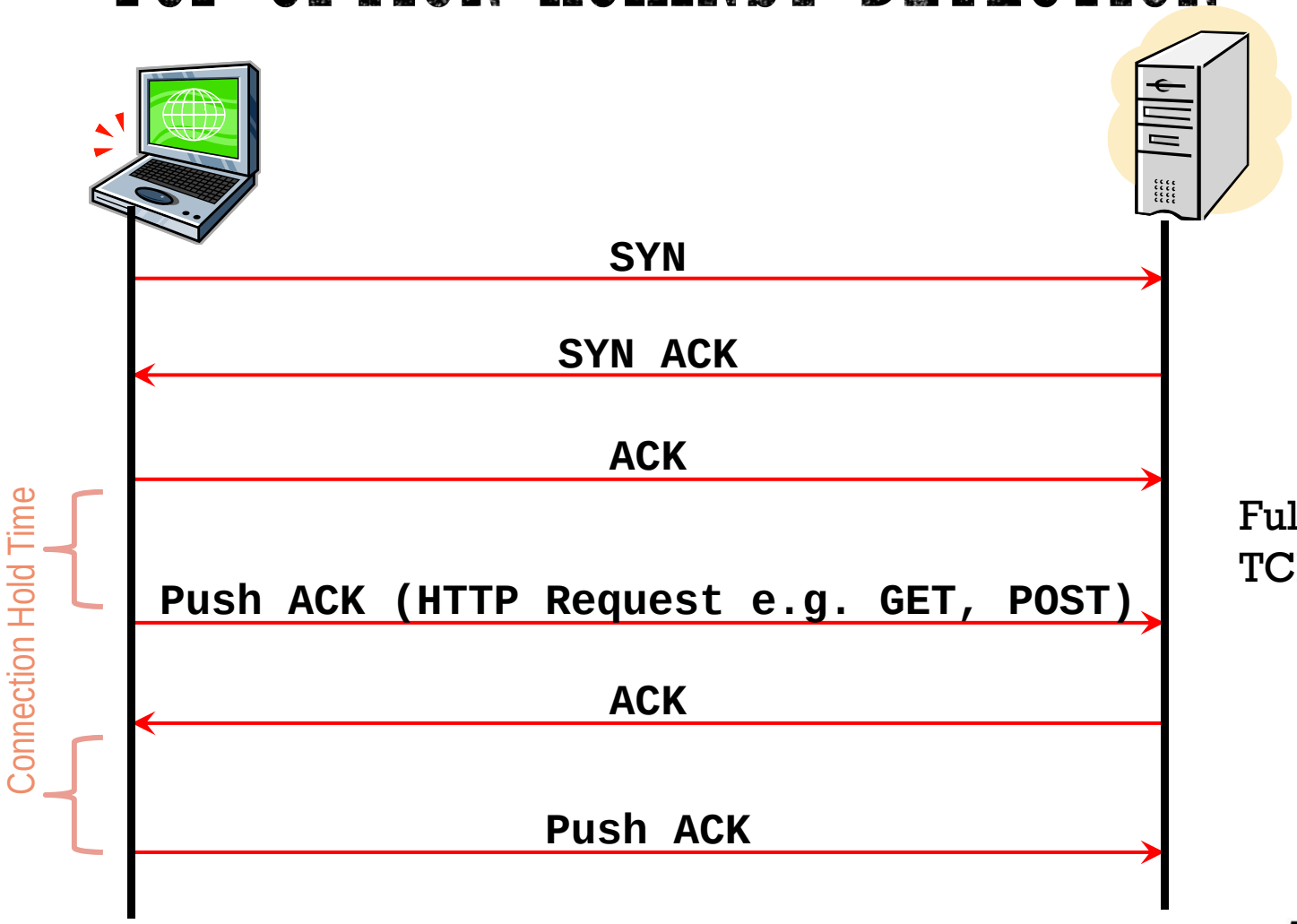
- HTTP header will change during the attack
- For example, first HTTP request for HTTP Header "Accept"

First Request		Second Request
Accept: */*	→	Accept: image/gif, image/jpeg, imag,…..

TCP OPTION EMPOWER

- TCP option against Detection
- Empower attack Power

TCP OPTION AGAINST DETECTION

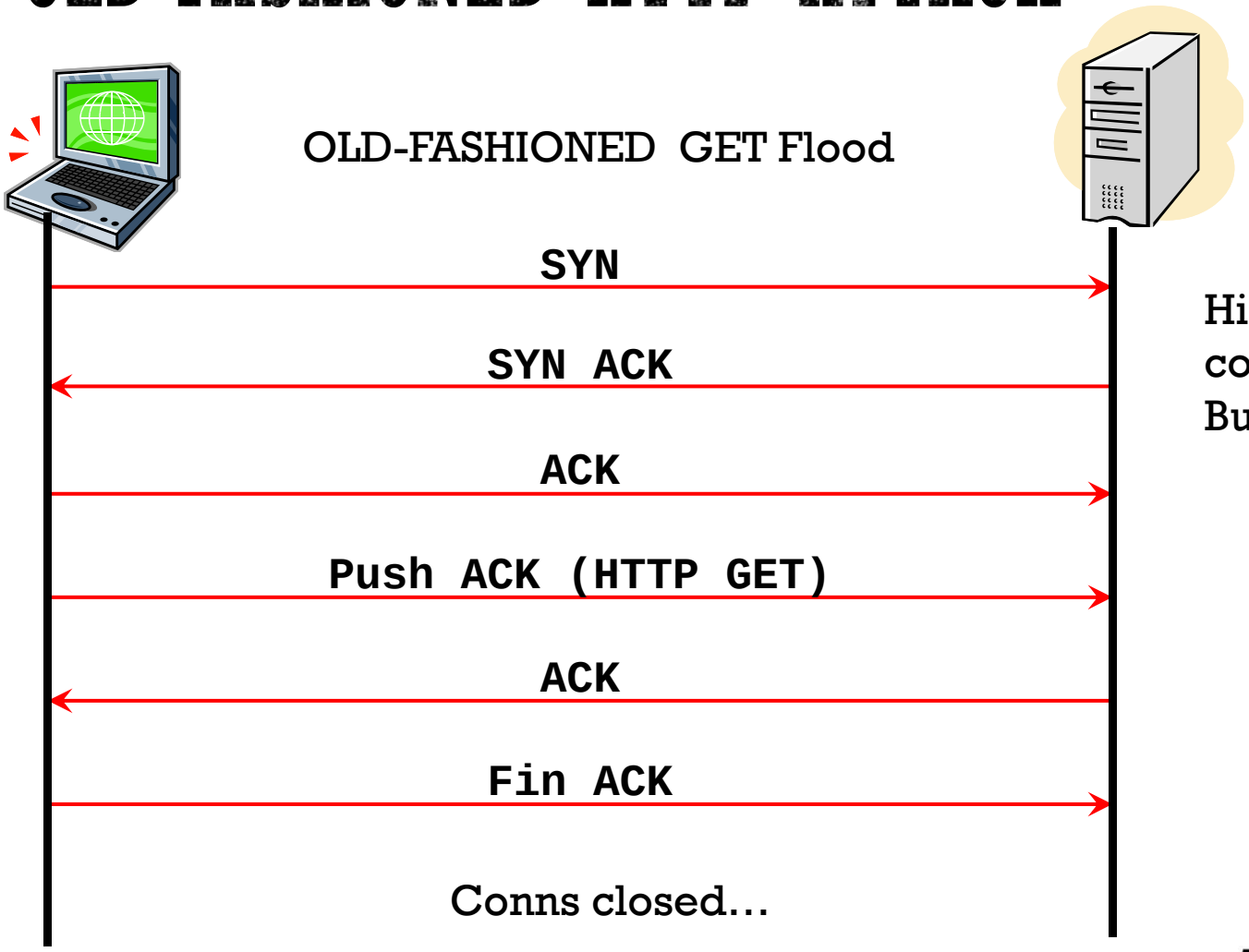


Full Control every TCP State!!!!

BLOODSPEAR LABORATORIES

NEXUSGUARD
DDoS Mitigation Lab

OLD-FASHIONED HTTP ATTACK

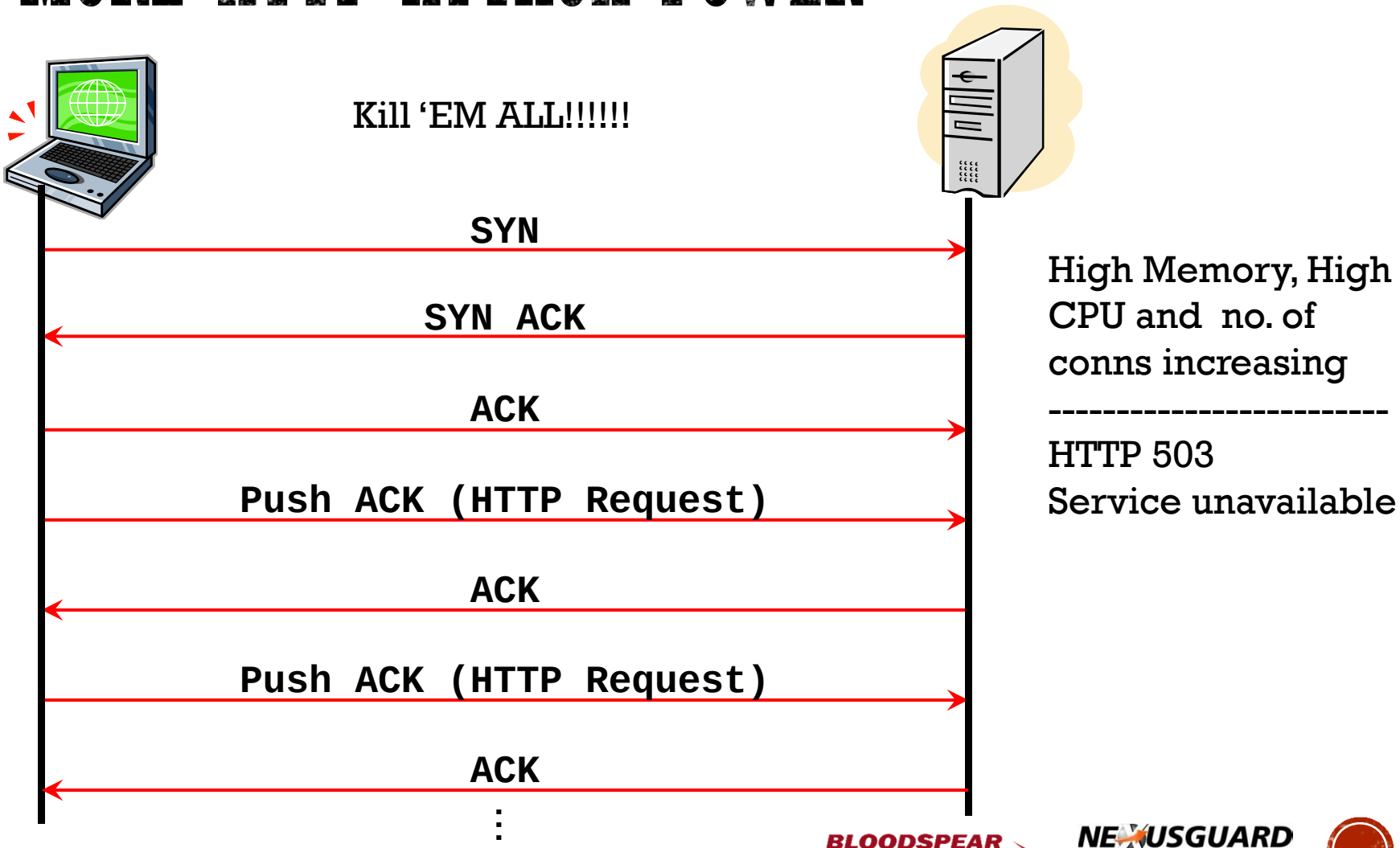


High CPU and constant no. of conns But Still ALIVE!!!

BLOODSPEAR LABORATORIES

NEXUSGUARD DDoS Mitigation Lab

MORE HTTP ATTACK POWER



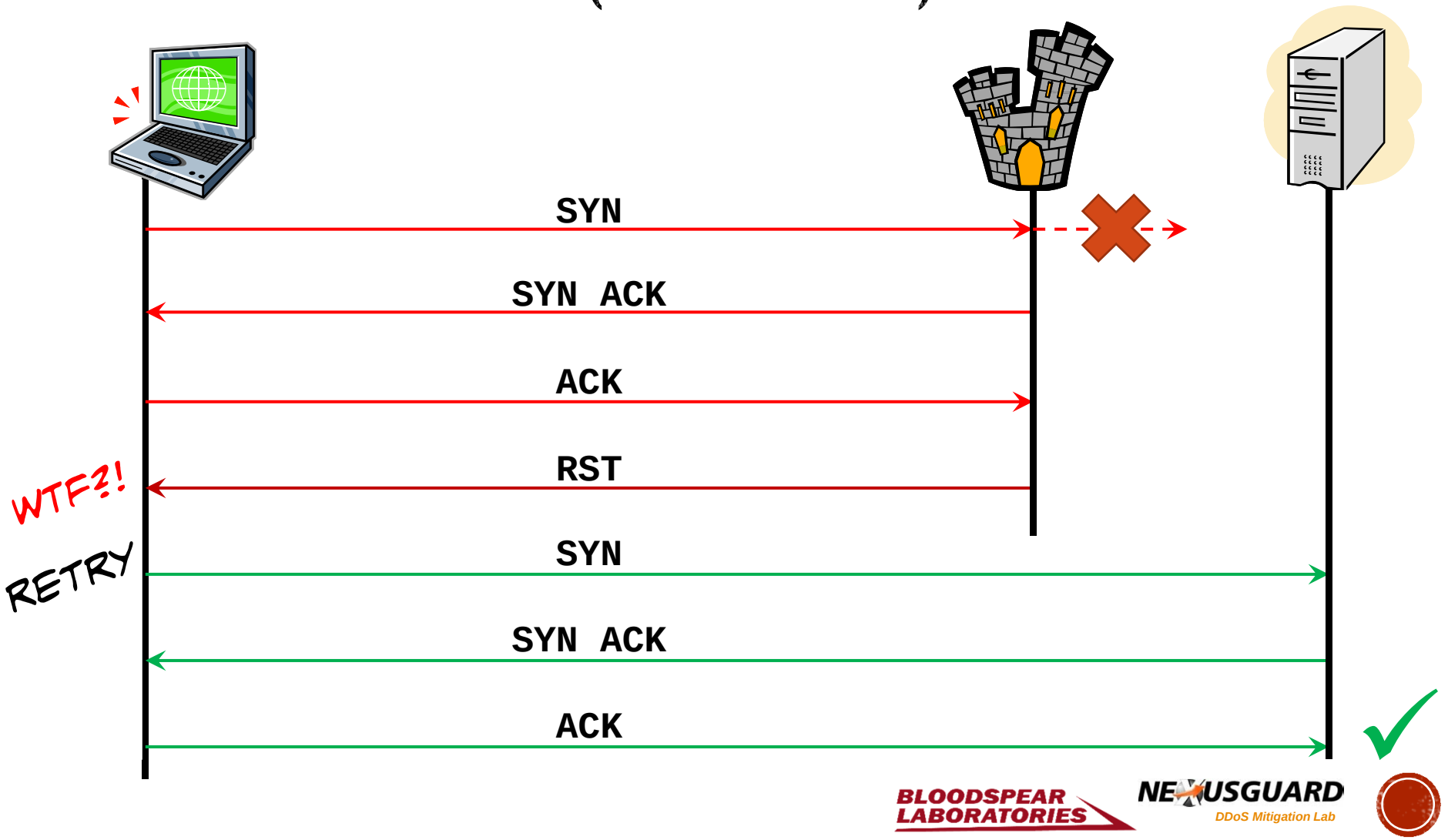
BLOODSPEAR LABORATORIES

NEXUSGUARD DDoS Mitigation Lab

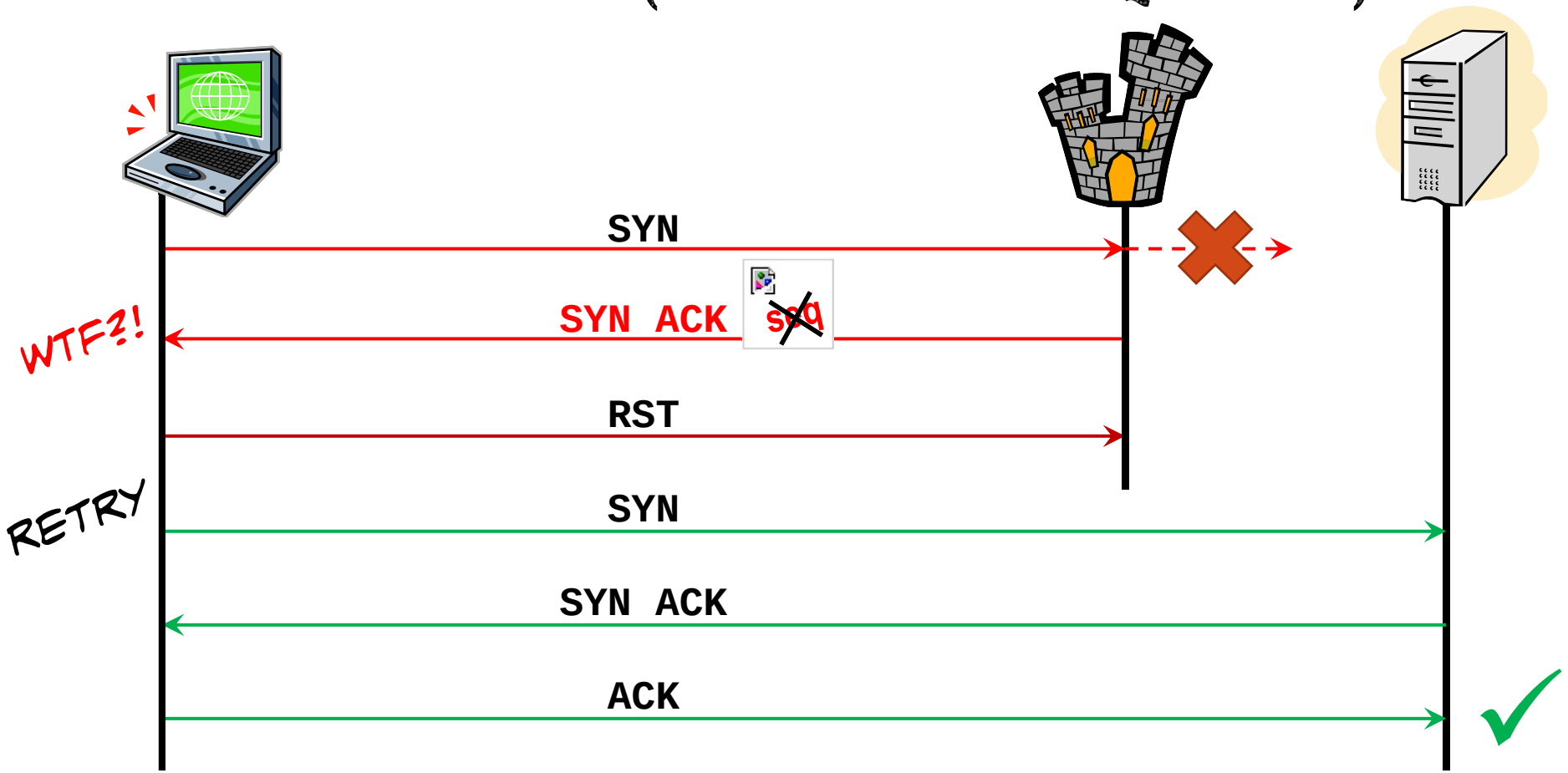
SOURCE HOST VERIFICATION

- TCP SYN Auth
- HTTP Redirect Auth
- HTTP Cookie Auth
- JavaScript Auth
- CAPTCHA Auth

TCP SYN AUTH (TCP RESET)



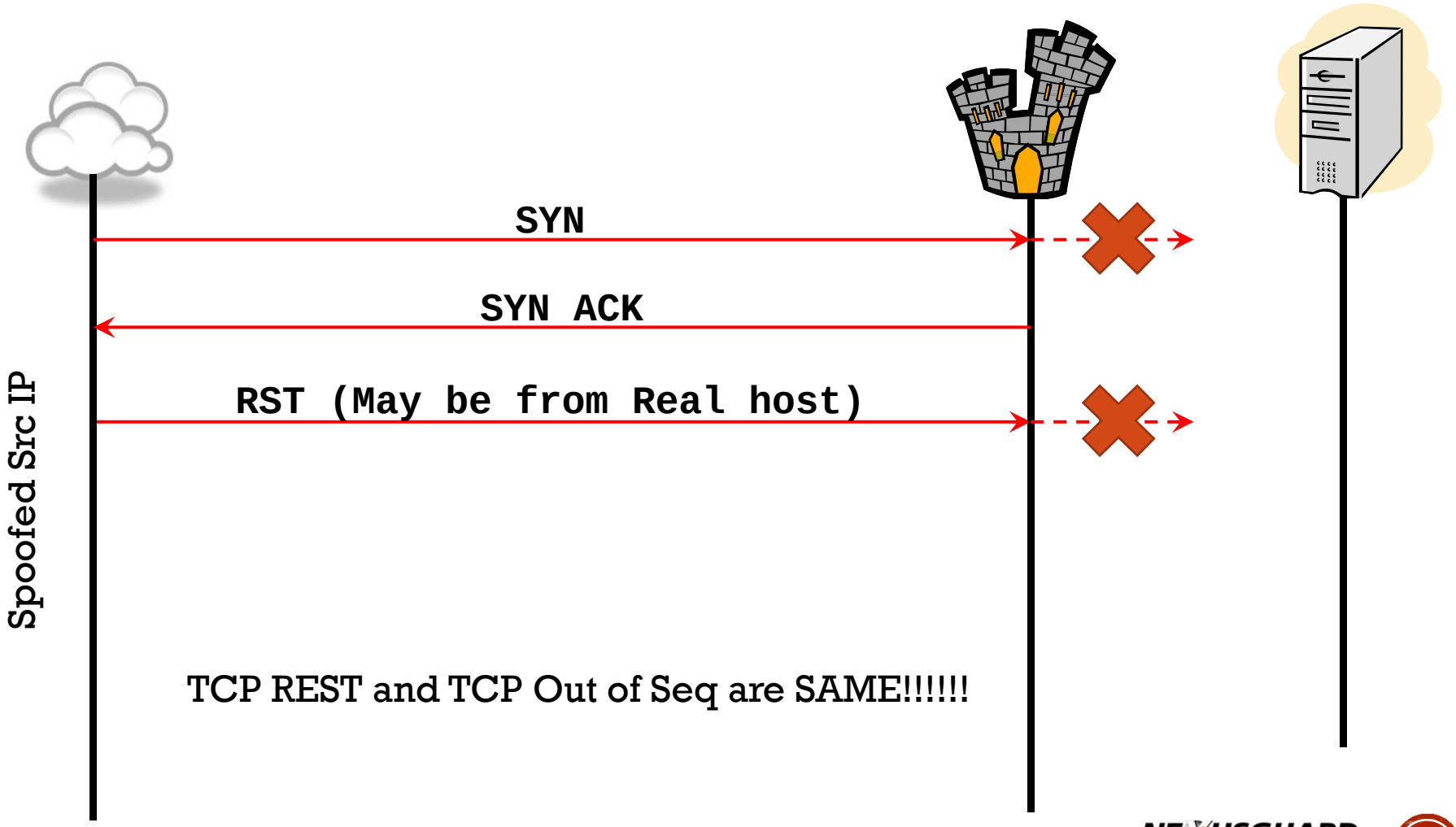
TCP SYN AUTH (TCP OUT-OF-SEQUENCE)



BLOODSPEAR LABORATORIES

NEXUSGUARD
DDoS Mitigation Lab

HANDLE SYN FLOOD ATTACK



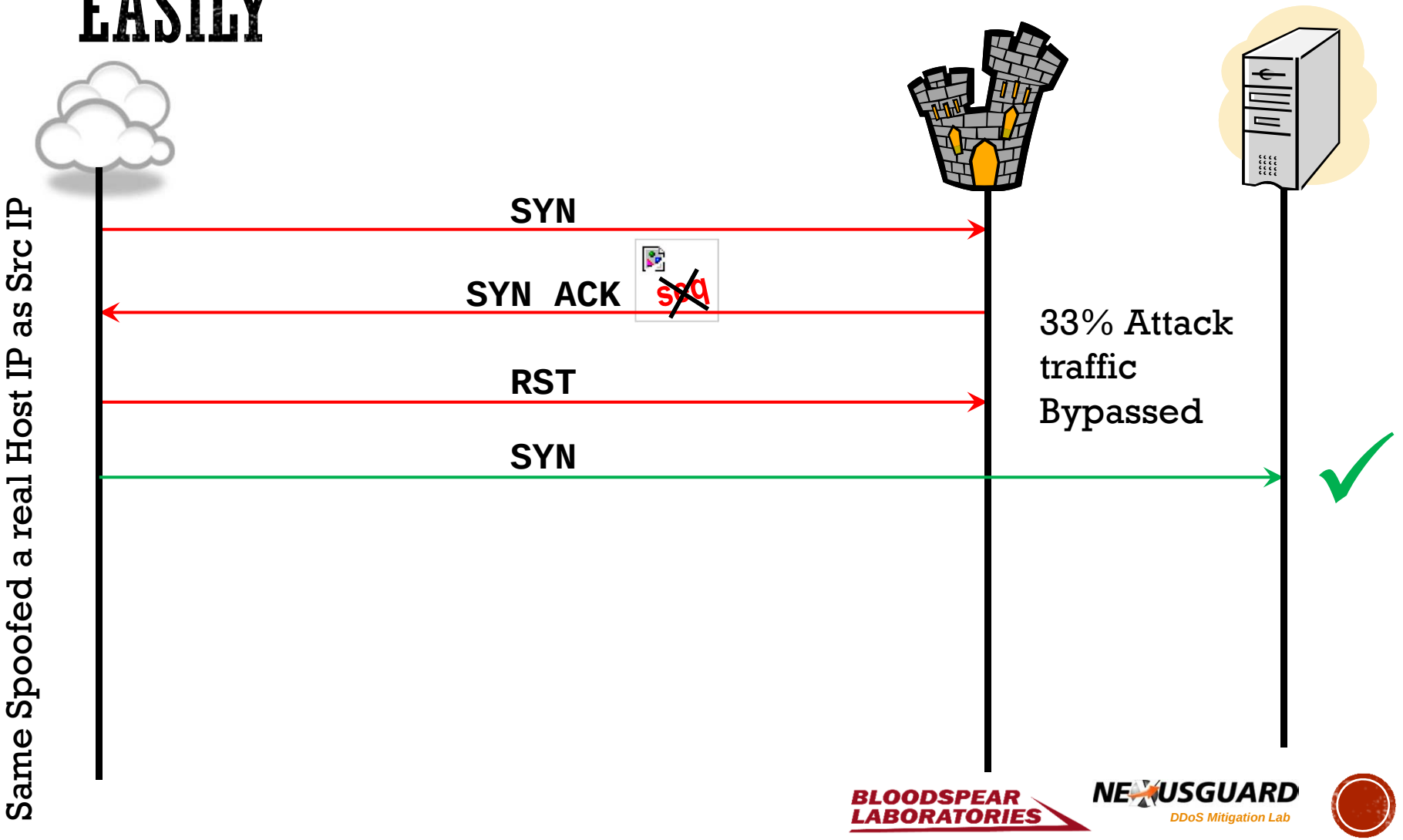
EFFICIENCY HANDLE REAL USER

Handling a Real User access:

TCP REST		TCP out of Seq	
TCP Flag	Total Length	TCP Flag	Total Length
SYN	60	SYN	60
SYN ACK	40	SYN ACK	40
ACK	40	RST	40
RST	40		
Total	180 Bytes	Total	140 Bytes

P.S. TCP SYN Packet size = Header length + Total Length

SYN BYPASS TCP OUT-OF-SEQUENCE EASILY



BLOODSPEAR LABORATORIES

NEXUSGUARD
DDoS Mitigation Lab

REAL POWER OF SYN FLOOD

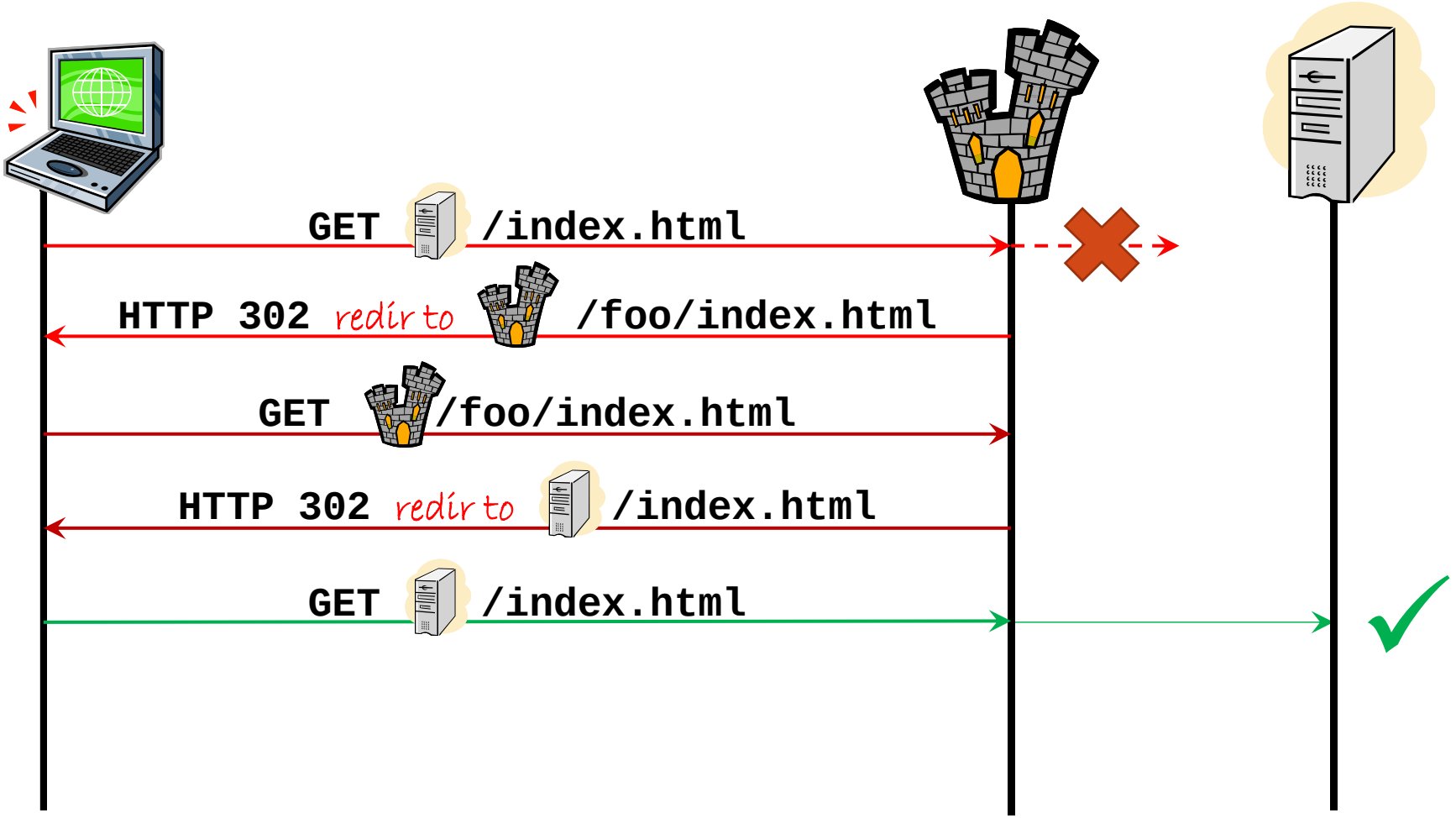
- The traditional SYN Flood is 40 bytes, missing TCP Option

- How to simulate a real SYN traffic:
  - In IP layer: Randomize TTL
  - In TCP layer: Randomize Window size, Correct Option added, e.g. Maximum Segment Size, etc.

48-60 bytes TCP SYN Flood attack is nightmare

BLOODSPEAR LABORATORIES NEXUSGUARD DDoS Mitigation Lab

HTTP REDIRECT AUTH



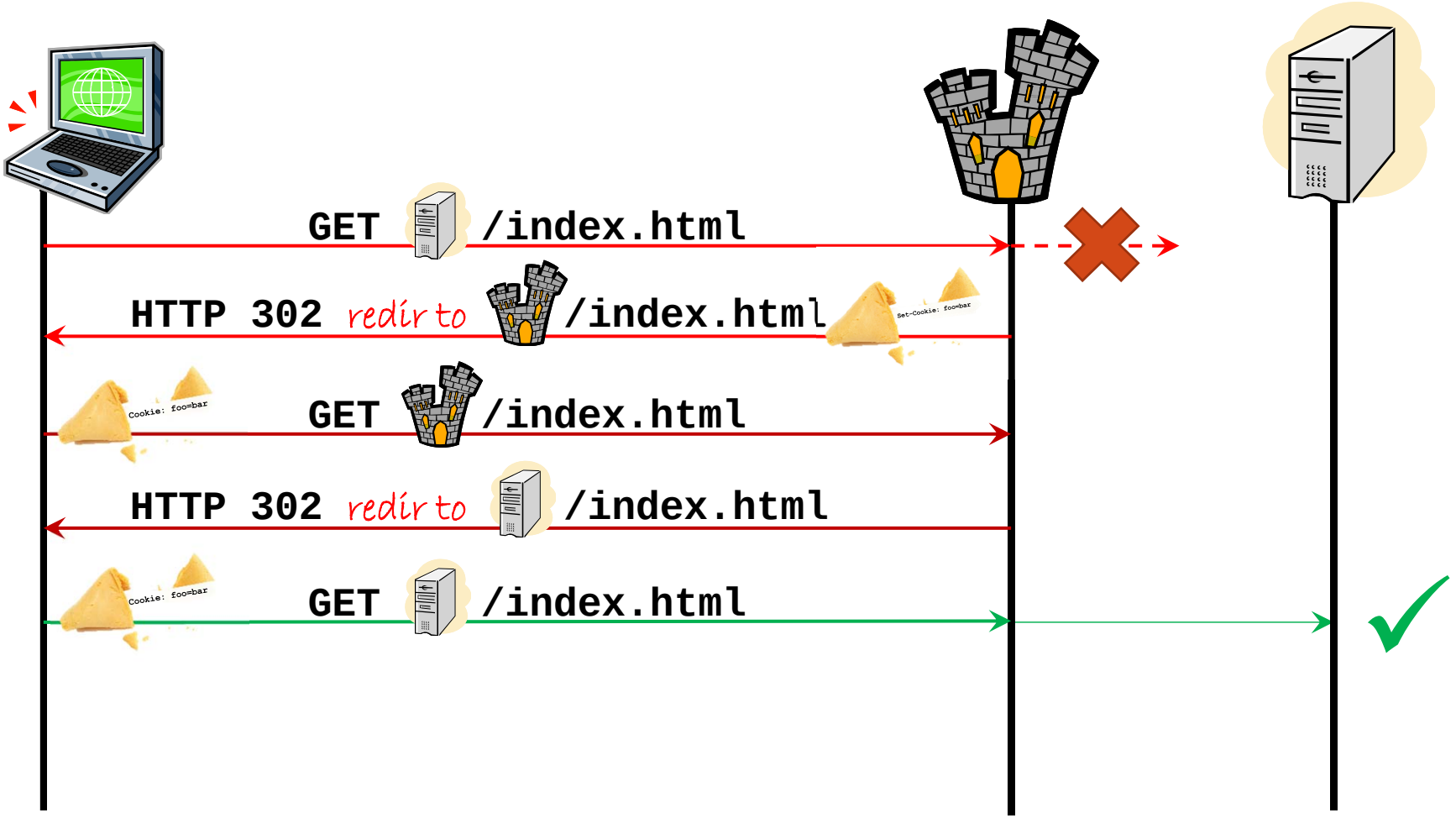
BLOODSPEAR LABORATORIES

NEXUSGUARD DDoS Mitigation Lab

KEY TO BYPASS HTTP REDIRECT

- HTTP / 1.1 302 Found\r\n
- Location: http: a.c.com\r\n
- Loop the script, until "HTTP / 1.1 200 ok"

HTTP COOKIE AUTH



BLOODSPEAR LABORATORIES

NEXUSGUARD
DDoS Mitigation Lab

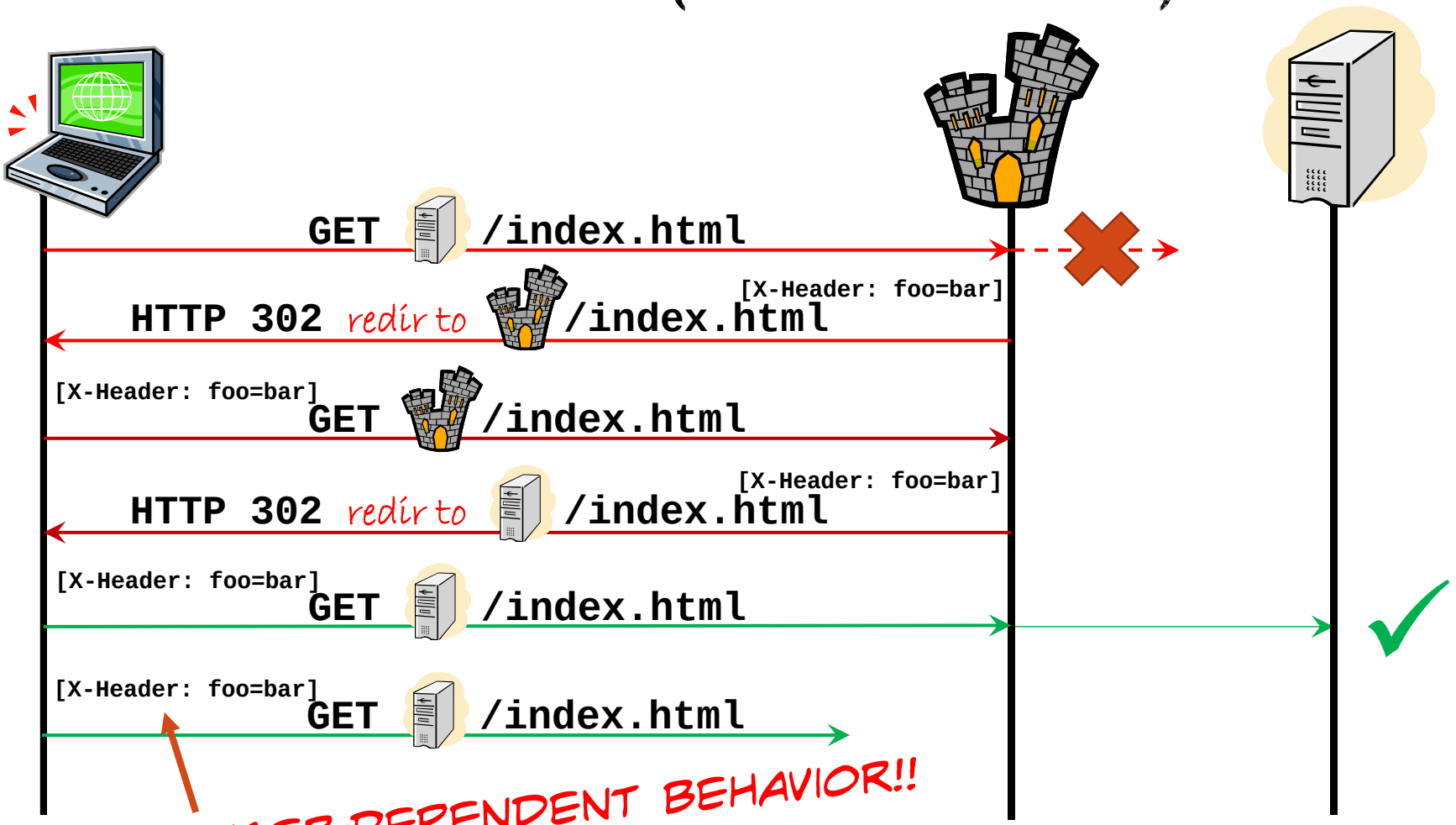
KEY TO BYPASS COOKIE AUTH

- Set-Cookie: AuthCode=d8e; expires=Mon, 23-Dec-2019 23:50:00 GMT; ……., etc
- If Date and time of Expire is between hour or minutes, it is the our REAUTH threshold!!!!!!!!

- If you saw this in third HTTP redirect request

  Set-Cookie:AuthCode=deleted;…….bad luck

HTTP COOKIE AUTH (HEADER TOKEN)



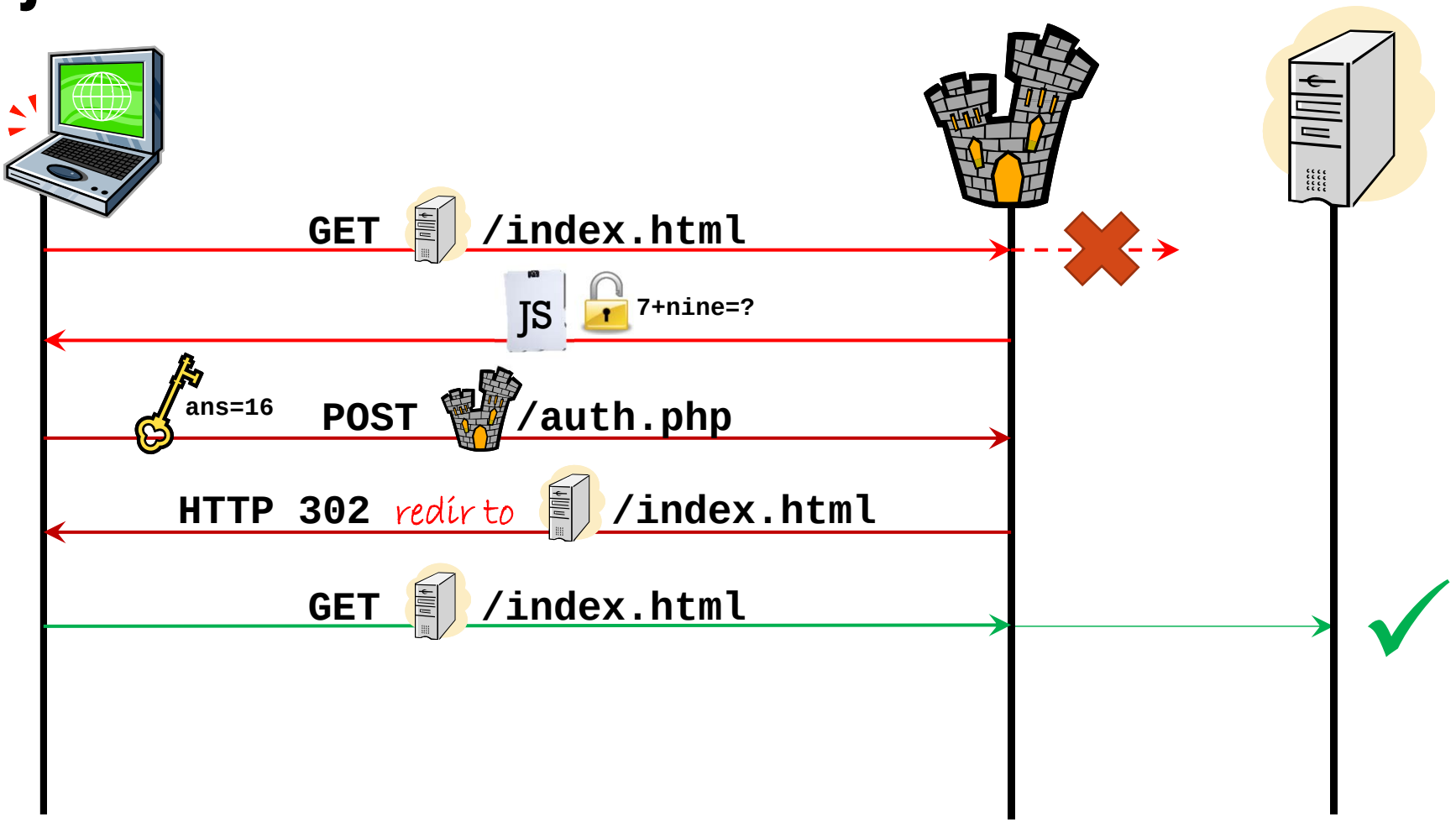
BLOODSPEAR LABORATORIES

NEXUSGUARD
DDoS Mitigation Lab

KEY TO BYPASS HEADER TOKEN AUTH

- API, AJAX or XHR2 is used to deploy header token
- Not all browser compatibility those Techniques
- Existing Mitigation devices can not fully using those Techniques
- Simulation the Traffic Flow BYPASS it!!!!

JAVASCRIPT AUTH



BLOODSPEAR LABORATORIES

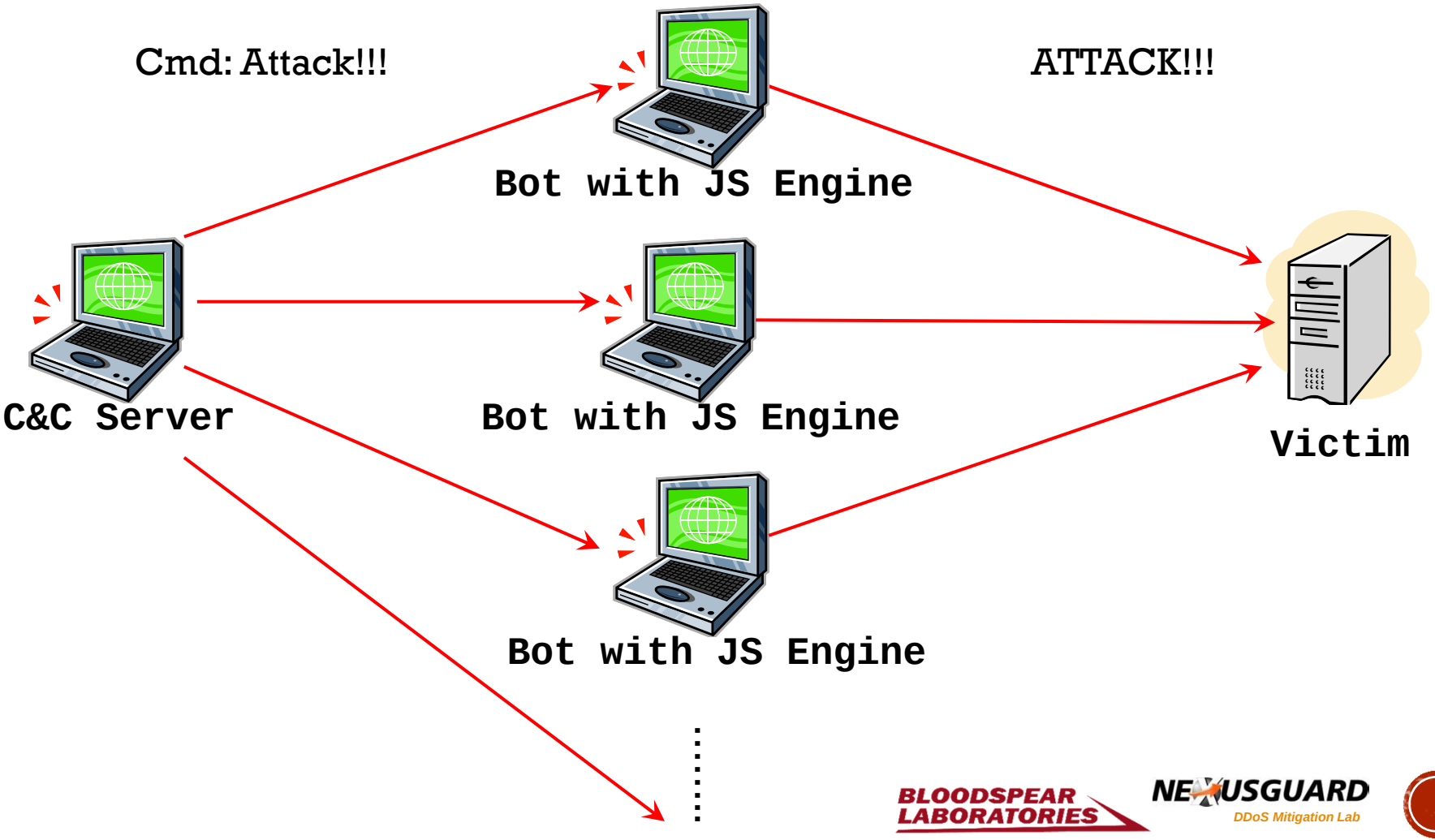
NEXUSGUARD
DDoS Mitigation Lab

KEY TO BYPASS JS AUTH

- JavaScript is client-side-program
- Find the path "http://a.b.com/auth.js", download and analyze it.
- Challenge to embedded JavaScript in Botnet, guys using:
  - Simulate the traffic flow
  - Client Deployment Model
  - Server Deployment Model

- Kill 'Em All is below 1M bytes!!!!!!

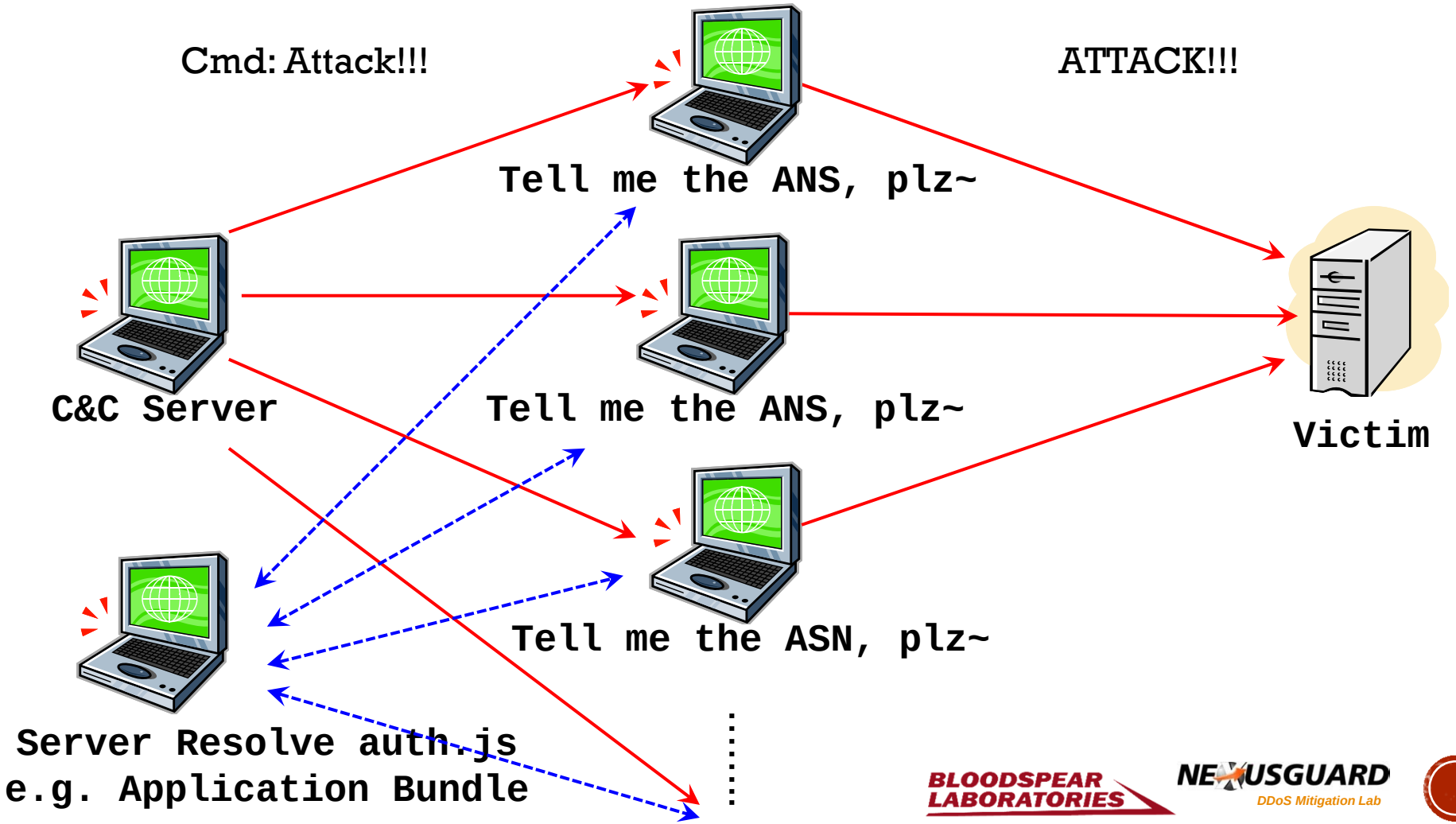
CLIENT DEPLOYMENT MODEL



BLOODSPEAR LABORATORIES

NEXUSGUARD
DDoS Mitigation Lab

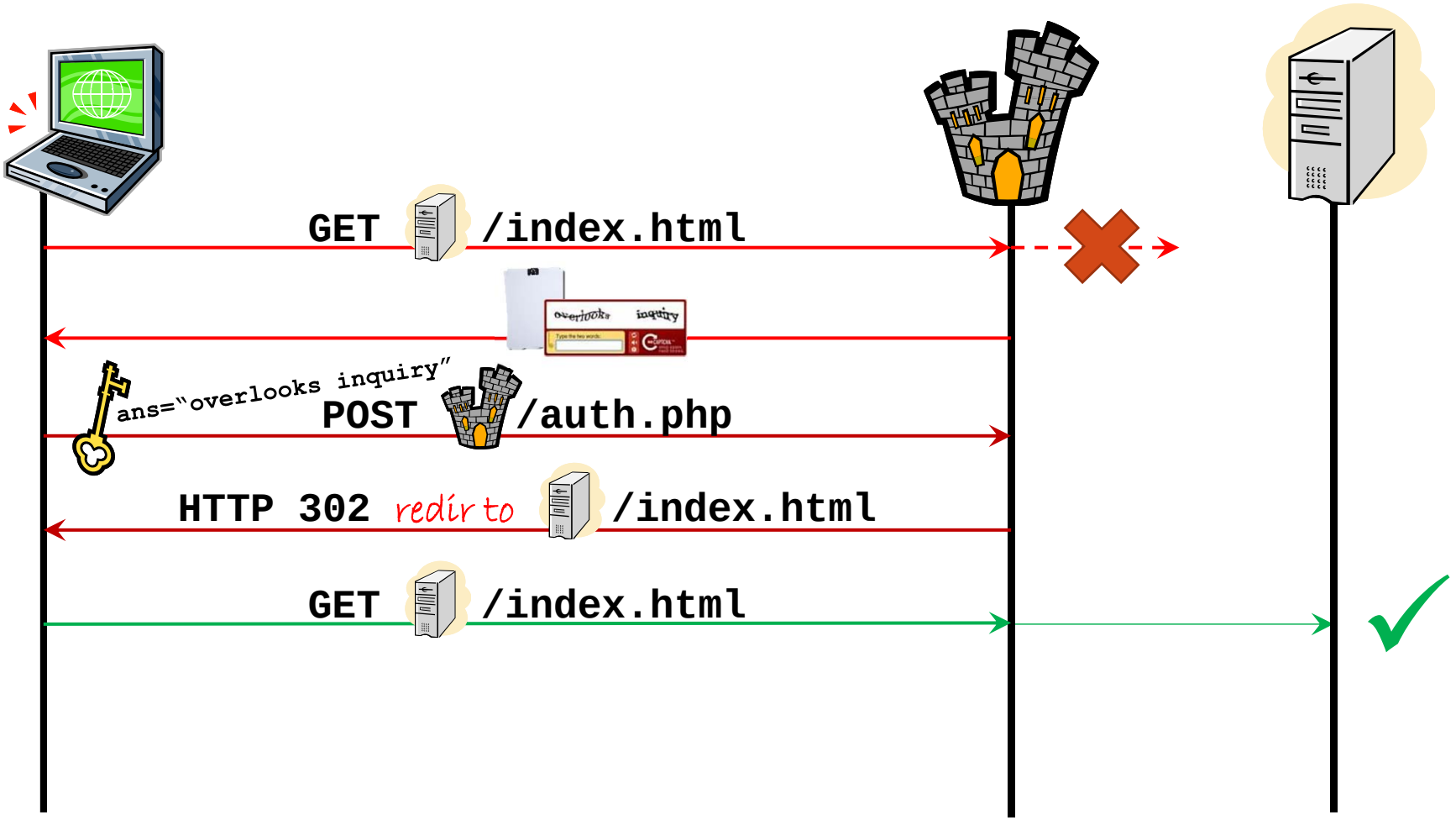
SERVER DEPLOYMENT MODEL



BLOODSPEAR LABORATORIES

NEXUSGUARD
DDoS Mitigation Lab

CAPTCHA AUTH



BLOODSPEAR LABORATORIES

NEXUSGUARD
DDoS Mitigation Lab

KEY TO BYPASS CAPTCHA AUTH

- JavaScript is client-side-program
- Find the path "http://a.b.com/auth.bmp", download and analyze it.
- Challenge to embedded CAPTCHA Engine in Botnet, guys using:
  - Simulate the traffic flow
  - Client Deployment Model
  - Server Deployment Model

DEFCON have FXXKING many CATPCHA engine!!!!

BLOODSPEAR LABORATORIES

NEXUSGUARD DDoS Mitigation Lab

SOURCE HOST VERIFICATION

Verifies	TCP SYN	HTTP Redirect	HTTP Cookie	JavaScript	CAPTCHA
Non-Spoofed Source IP	✓	✓	✓	✓	✓
HTTP Compliant Application		✓	✓	✓	✓
Real Browser				✓	✓
Real Human					✓

BYPASS TO GAIN WHITELIST PASS THEN FIRE AWAY FREELY!!

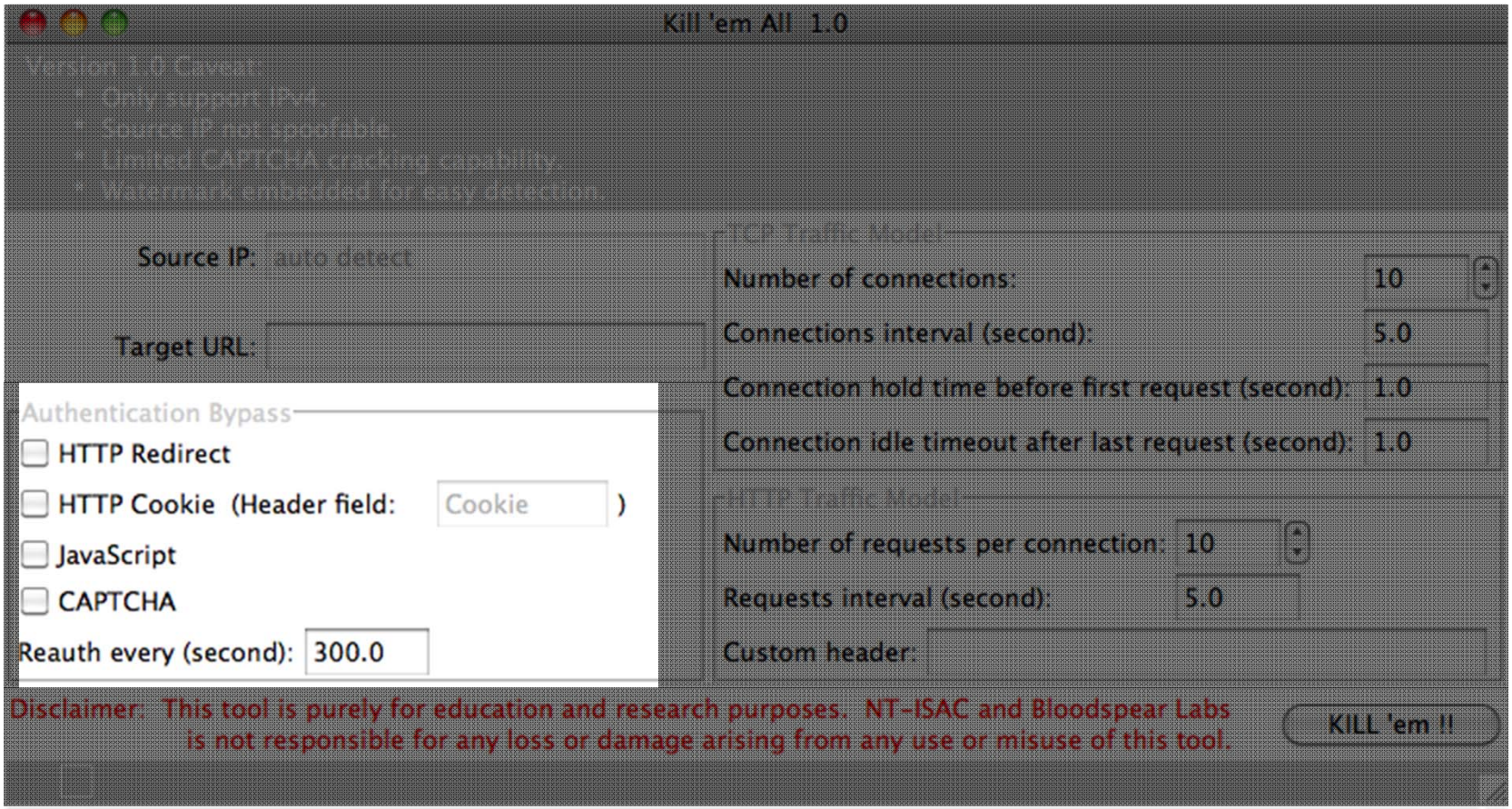
BLOODSPEAR LABORATORIES

NEXUSGUARD
DDoS Mitigation Lab

POC TOOL DESIGN

- 3 tries per authentication attempt (in practice more likely to success)
- True TCP/IP behavior thru use of OS TCP/IP stack
- Auth cookies persist during subsequent dialogues
- JavaScript execution using embedded JS engine (lack of complete DOM an obstacle to full emulation)

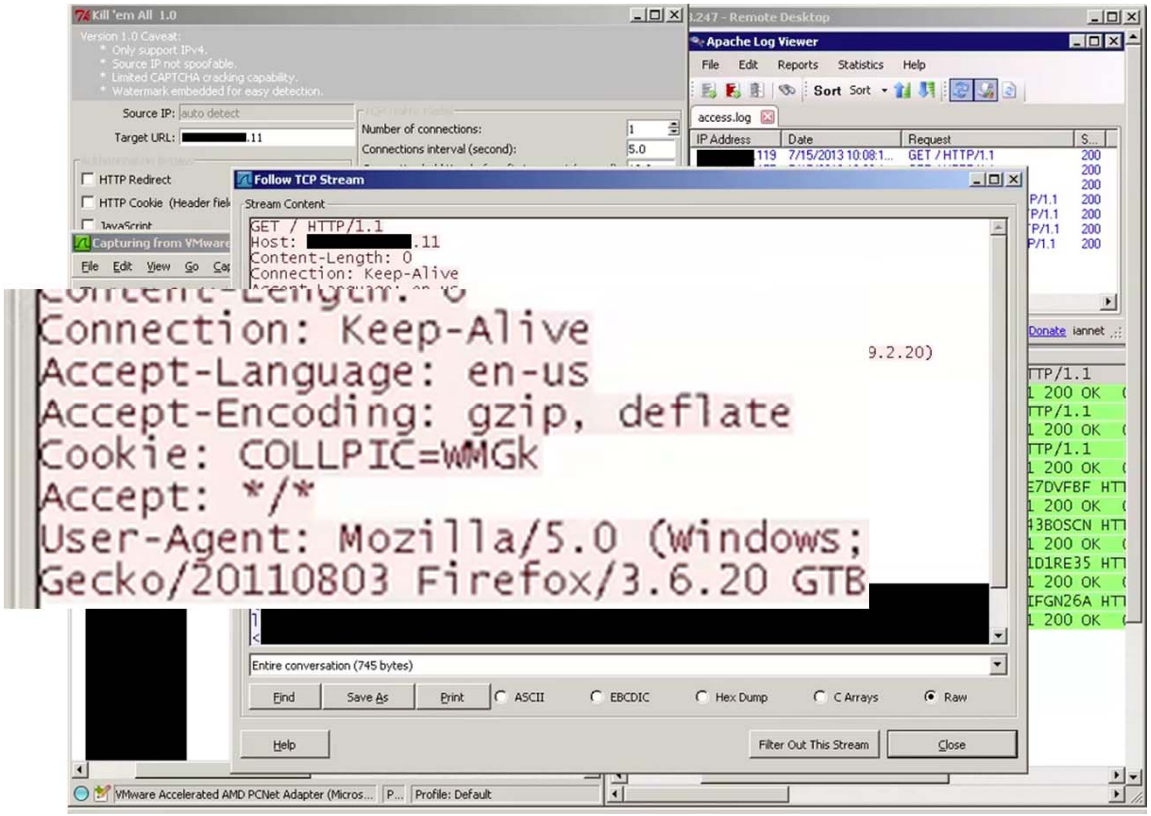
POC



BLOODSPEAR LABORATORIES

NEXUSGUARD
DDoS Mitigation Lab

CAPTCHA PWNAGE

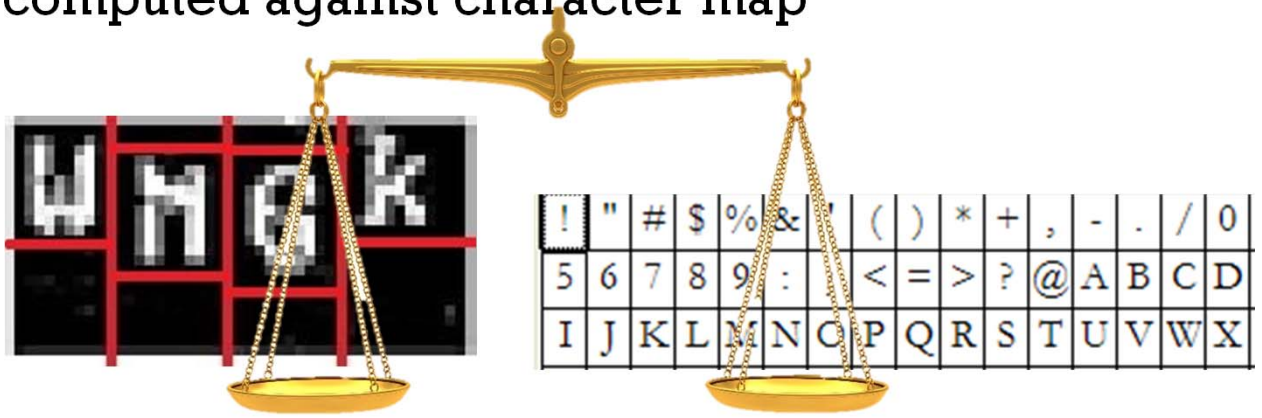


BLOODSPEAR LABORATORIES

NEXUSGUARD
DDoS Mitigation Lab

CAPTCHA BYPASS DESIGN

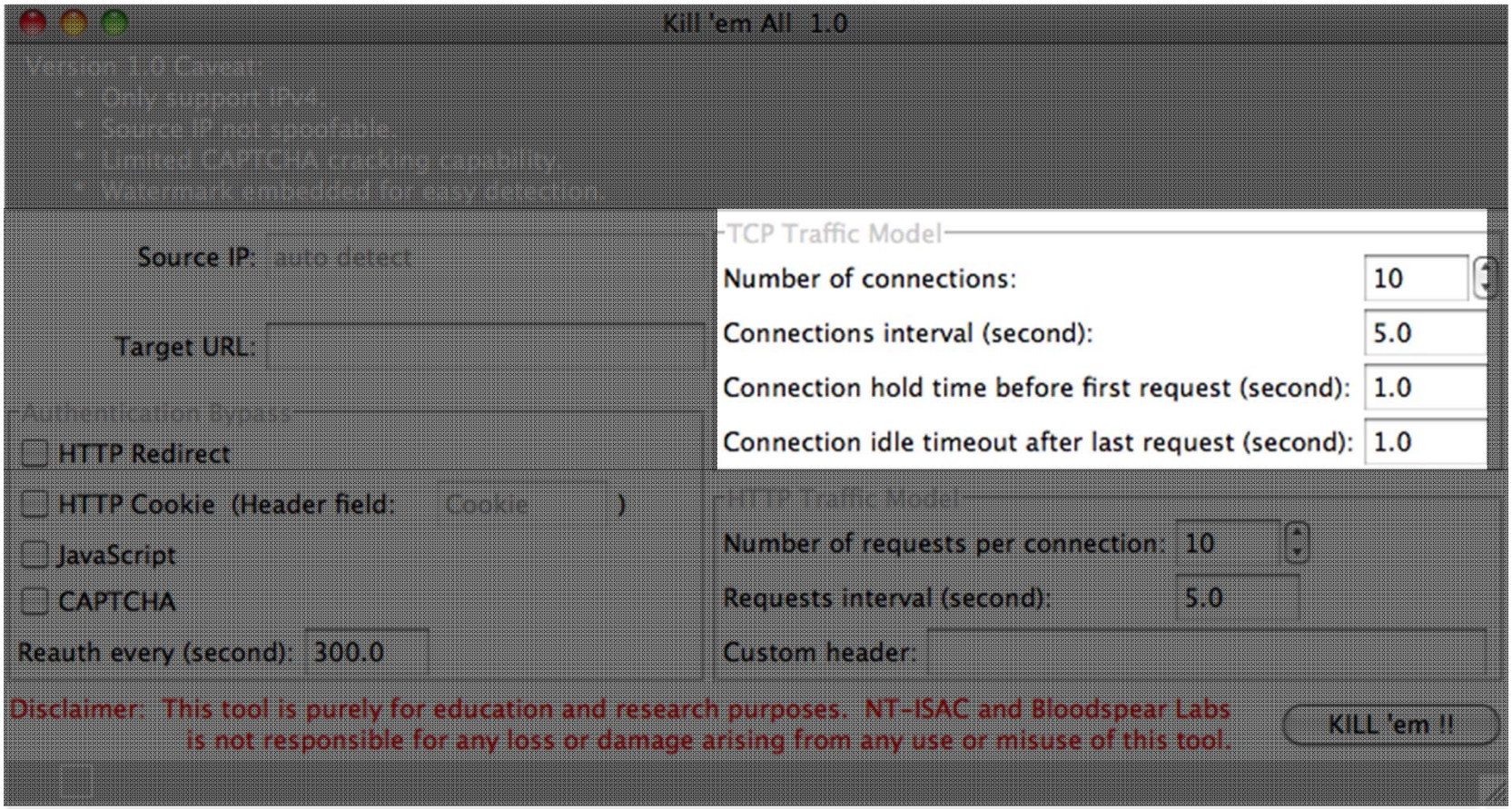
1. Converted to black-and-white for max contrast
2. 3x3 median filter applied for denoising
3. Word segmentation
4. Boundary recognition
5. Pixel difference computed against character map



BLOODSPEAR LABORATORIES

NEXUSGUARD
DDoS Mitigation Lab

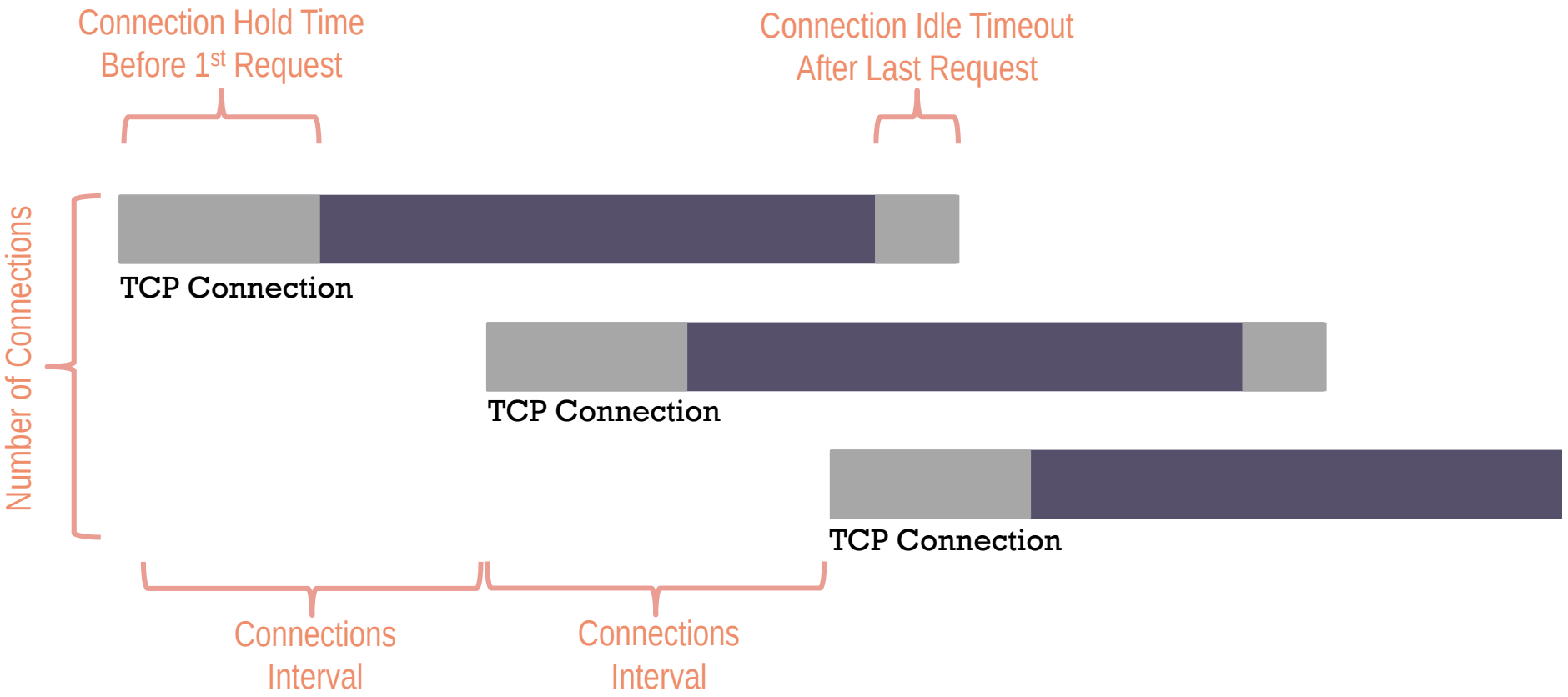
POC



BLOODSPEAR LABORATORIES

NEXUSGUARD DDoS Mitigation Lab

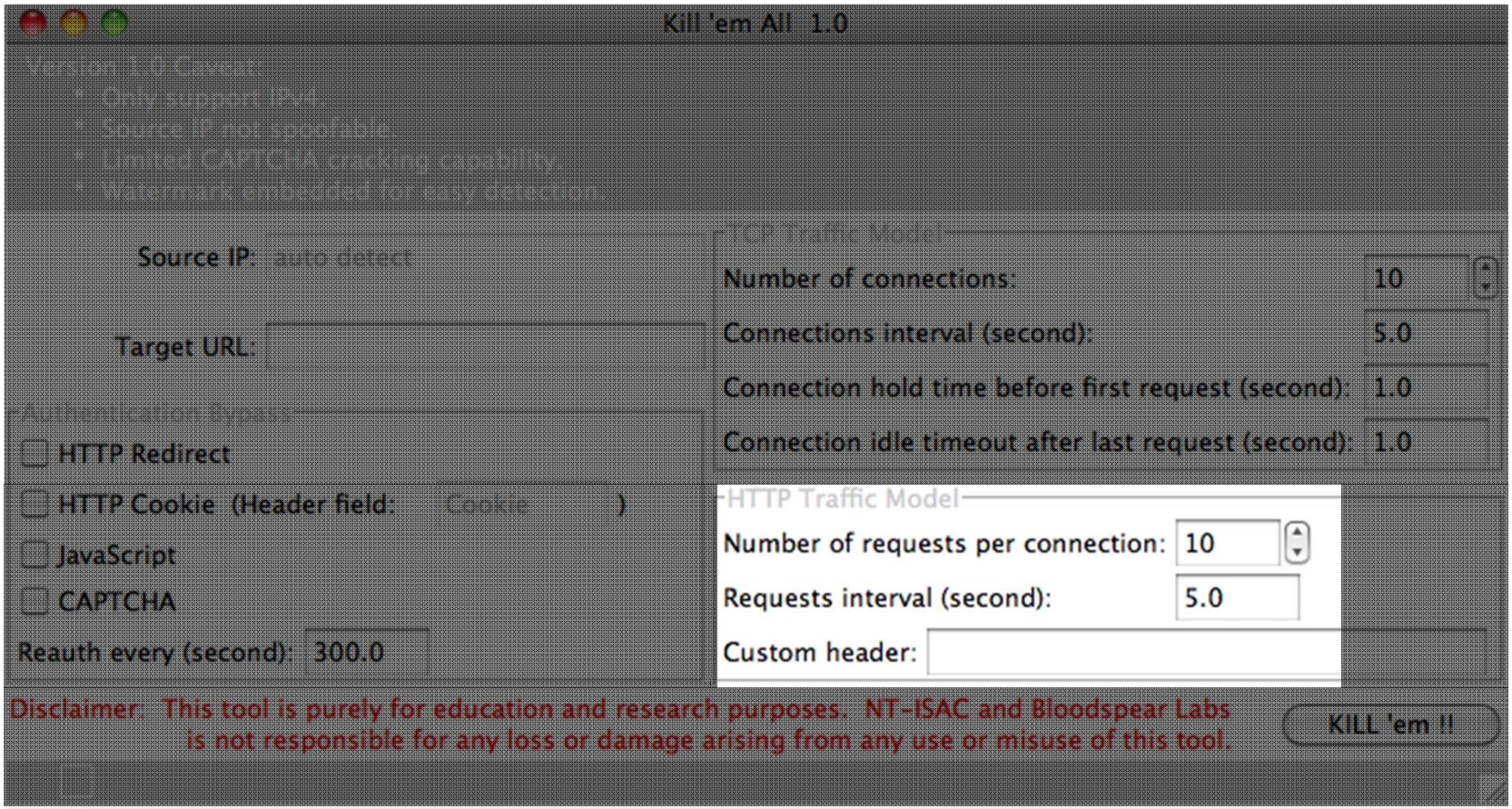
TCP TRAFFIC MODEL



BLOODSPEAR LABORATORIES

NEXUSGUARD
DDoS Mitigation Lab

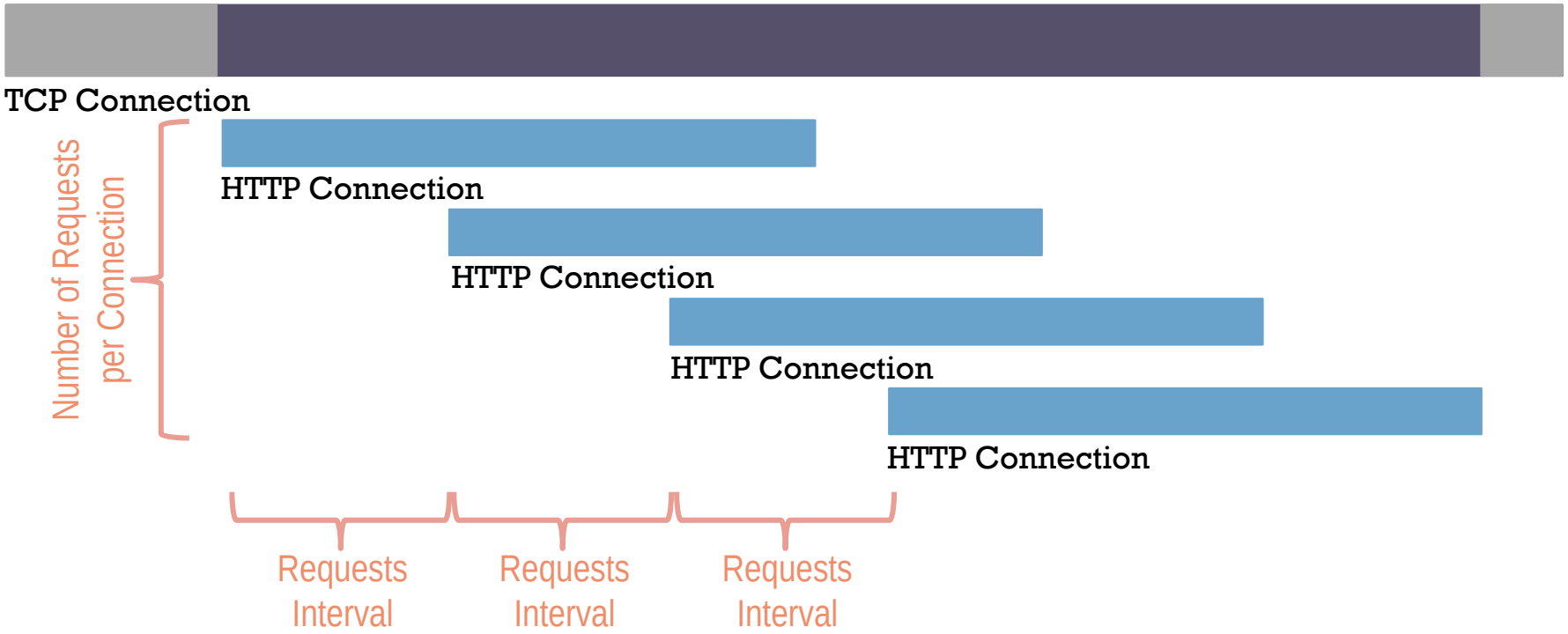
POC



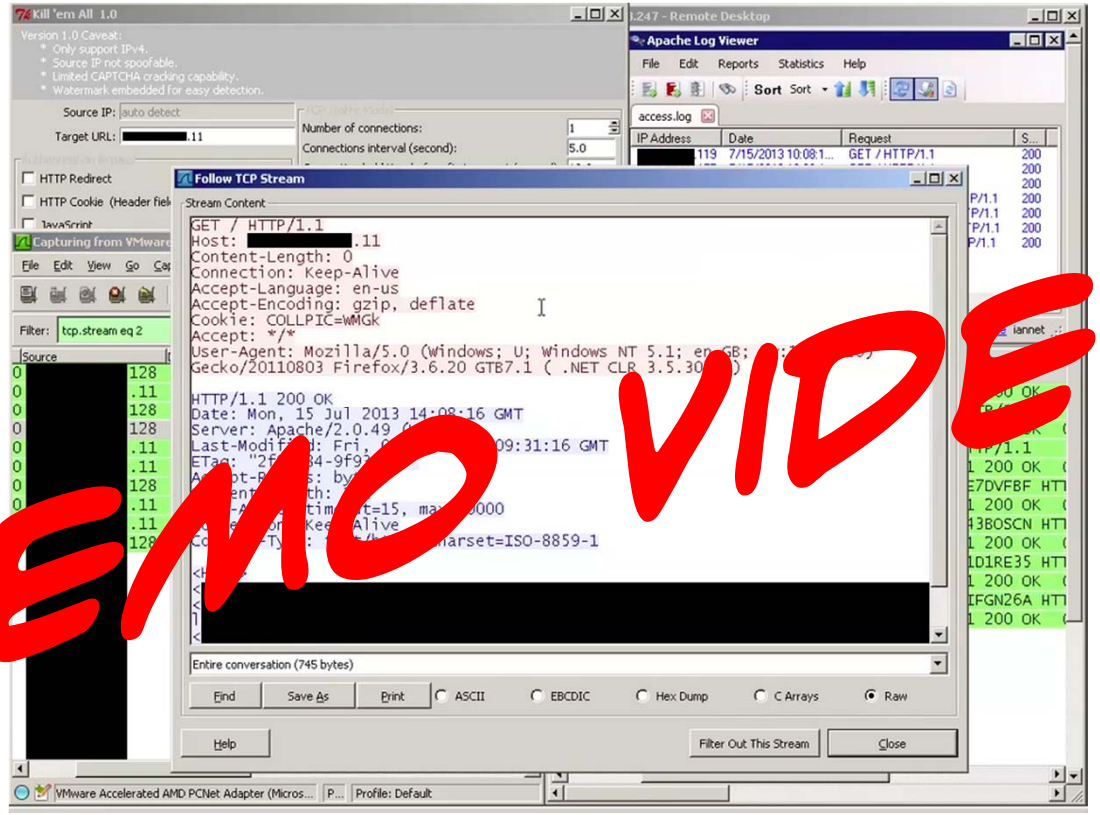
BLOODSPEAR LABORATORIES

NEXUSGUARD
DDoS Mitigation Lab

HTTP TRAFFIC MODEL



SHOW TIME



DEMO VIDEO

BLOODSPEAR LABORATORIES

NEXUSGUARD
DDoS Mitigation Lab

POC TOOL STRENGTHS

- True TCP/IP behavior (RST, resend, etc.) thru use of true OS TCP/IP stack
- Believable HTTP headers (User-Agent strings, etc.)
- Embedded JavaScript engine
- CAPTCHA solving capability
- Randomized payload
- Tunable post-authentication traffic model

TO THE BACKEND

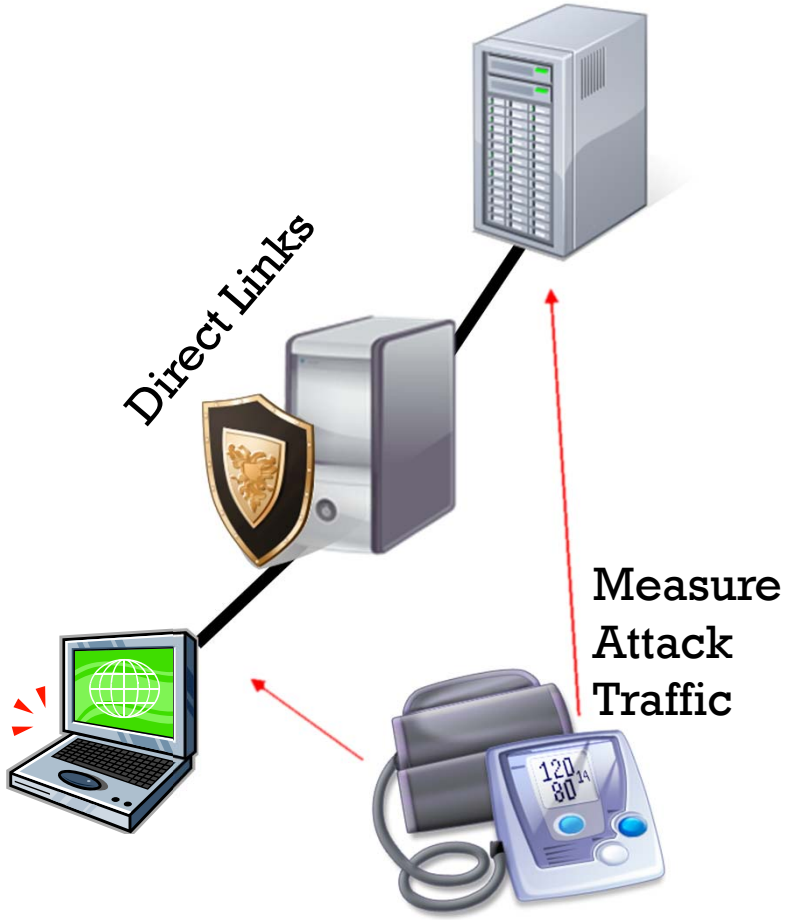
- 44 Page views

BLOODSPEAR LABORATORIES

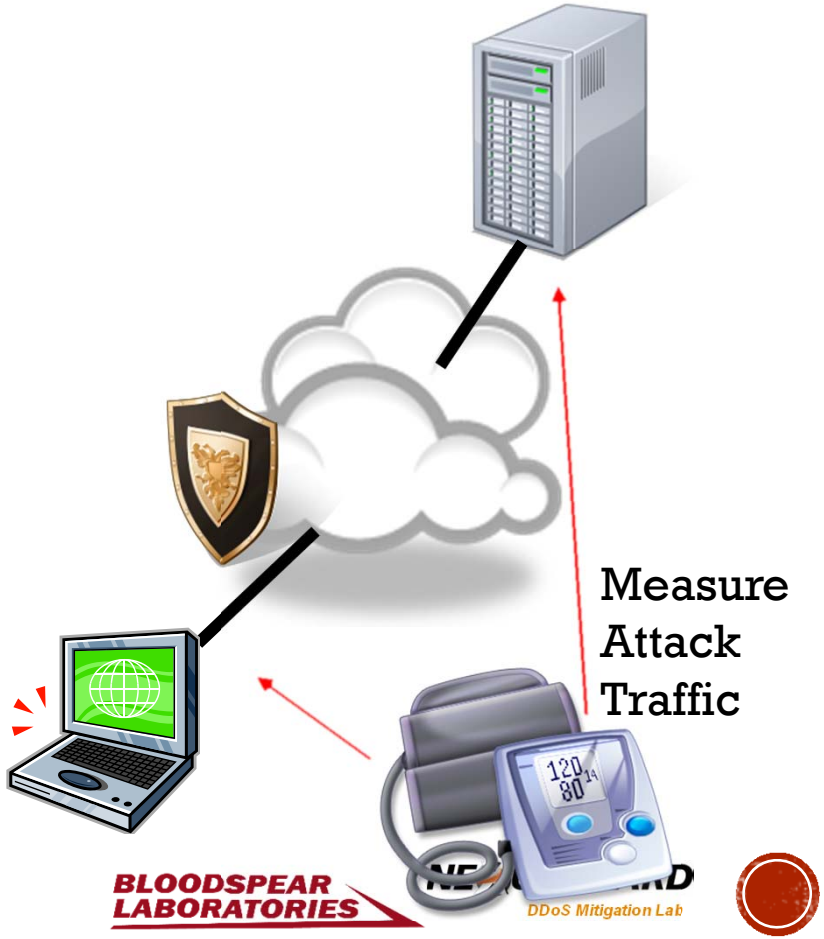
NEXUSGUARD
DDoS Mitigation Lab

TESTING ENVIRONMENT

- Against Devices



- Against Services



MITIGATION BYPASS

Auth Bypass

Detection Techniques	Arbor Peakflow SP TMS	NSFocus ADS
Source Host Verification		
TCP SYN Authentication	PWNED!	PWNED!
HTTP Redirect Authentication	PWNED!	PWNED!
HTTP Cookie Authentication	PWNED!	PWNED!
JavaScript Authentication	— (Not implemented in TMS)	PWNED!
CAPTCHA Authentication	— (Not implemented in TMS)	PWNED!

Testing results under specific conditions, valid as of Jul 13, 2013

Post-Auth

Detection Techniques	Arbor Peakflow SP TMS	NSFocus ADS
Rate Measurement / Baseline Enforcement	PWNED! (Zombie Removal, Baseline Enforcement, Traffic Shaping, Rate Limiting)	PWNED!
Protocol Sanity & Behavior Checking	PWNED! (TCP Connection Reset)	PWNED!
Proactive Resource Release	PWNED! (TCP Connection Reset)	PWNED!
Big Data Analysis	PWNED! (GeoIP Policing)	(Not implemented in ADS)
Malicious Source Intelligence	PWNED! (Black White List, IP Address Filter List, Global Exception List, GeoIP Filter List)	— (Not implemented in ADS)
Protocol Pattern Matching	PWNED! (URL/DNS Filter List, Payload Regex)	PWNED!

BLOODSPEAR LABORATORIES

NEXUSGUARD DDoS Mitigation Lab

MITIGATION BYPASS (PROTECTION SERVICES)

Auth Bypass

Detection Techniques	Cloudflare	Akamai
Source Host Verification		
TCP SYN Authentication	N/A	N/A
HTTP Redirect Authentication		N/A
HTTP Cookie Authentication		N/A
JavaScript Authentication		N/A
CAPTCHA Authentication	✘	N/A

Testing results under specific conditions, valid as of Jul 13, 2013

Post-Auth

Detection Techniques	Cloudflare	Akamai
Rate Measurement / Baseline Enforce-ment	N/A	N/A
Protocol Sanity & Behavior Checking	N/A	N/A
Proactive Resource Release	N/A	N/A
Big Data Analysis	N/A	N/A
Malicious Source Intelligence	N/A	N/A
Protocol Pattern Matching	N/A	N/A

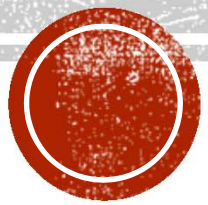
BLOODSPEAR LABORATORIES

NEXUSGUARD DDoS Mitigation Lab

HASTA LA VISTA, BABY.

tony.miu@nexusguard.com

leng@bloodspear.org



http://www.bloodspear.org

CHECK OUT NEW VERSION HERE!!