Manna From Heaven

Improving the state of rogue AP attacks

Turn your wifi off!

Our intention is to demonstrate our research findings, not to cause any damage. We have taken precautions, but some danger is inherent to such live demos. Please turn off your wifi now if you would not like to be involved. If you decide not to, then you do so at your own risk and we take your continued presence as your consent.

SensePost

We

Hack | Build | Train | Scan

Stuff

Ian de Villiers

ian@sensepost.com

@iandvl

Dominic White

dominic@sensepost.com

@singe

Why Wifi

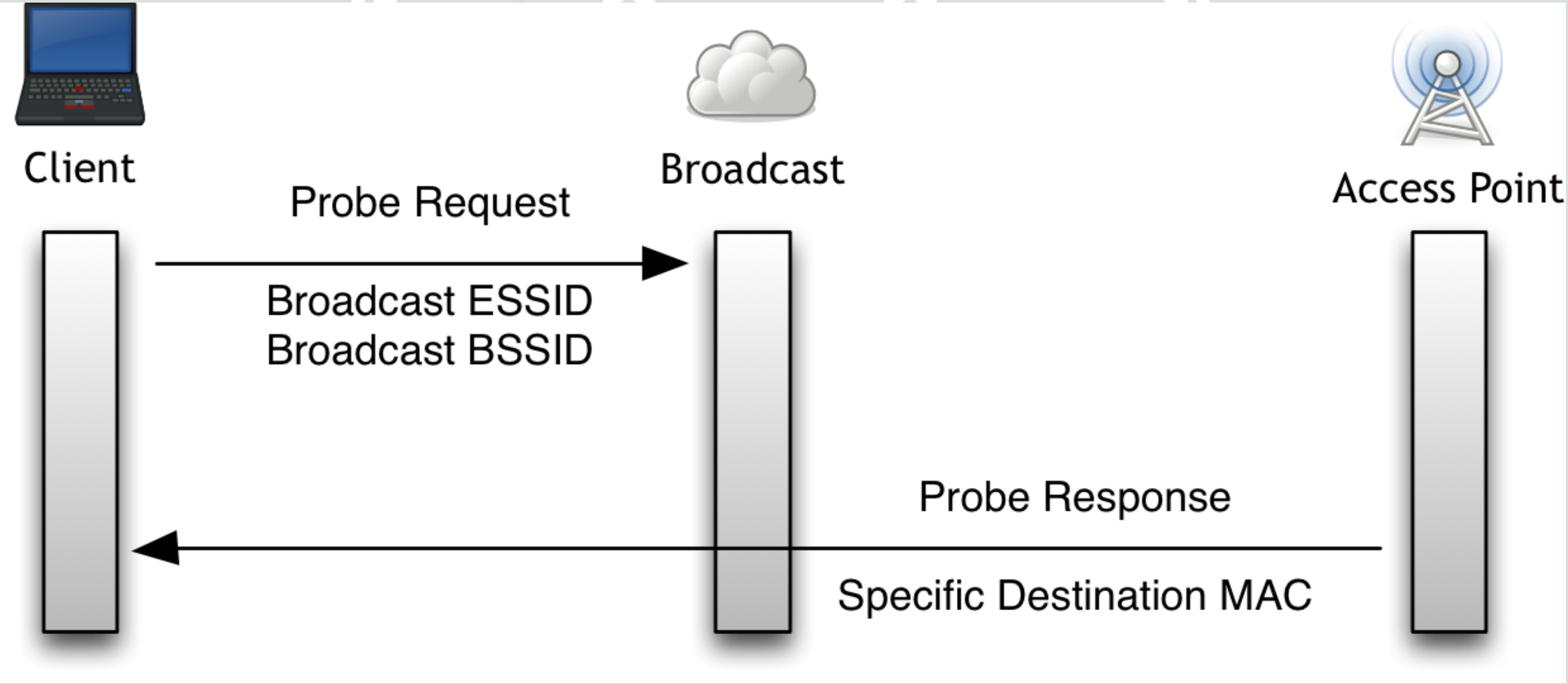
Creds from the Sky

The Current State

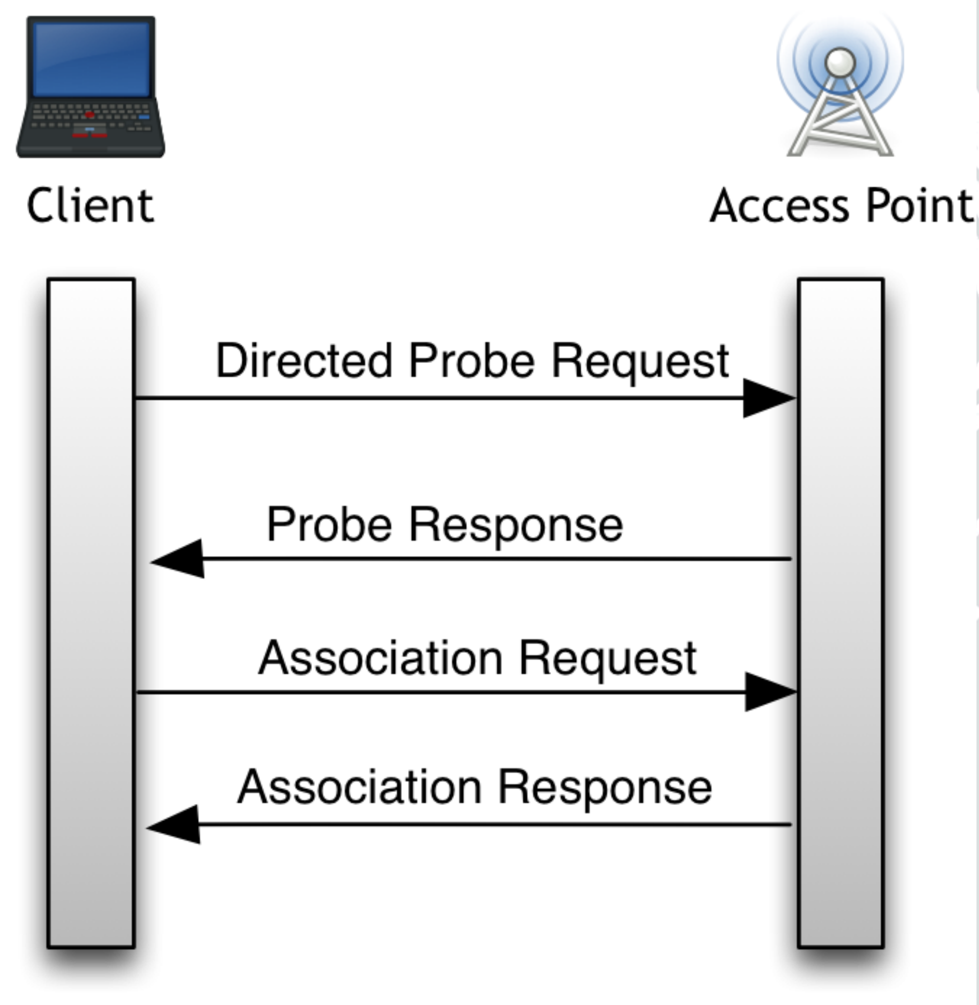
NANA

Targeted Wifi Primer

Finding Networks



Simple Association



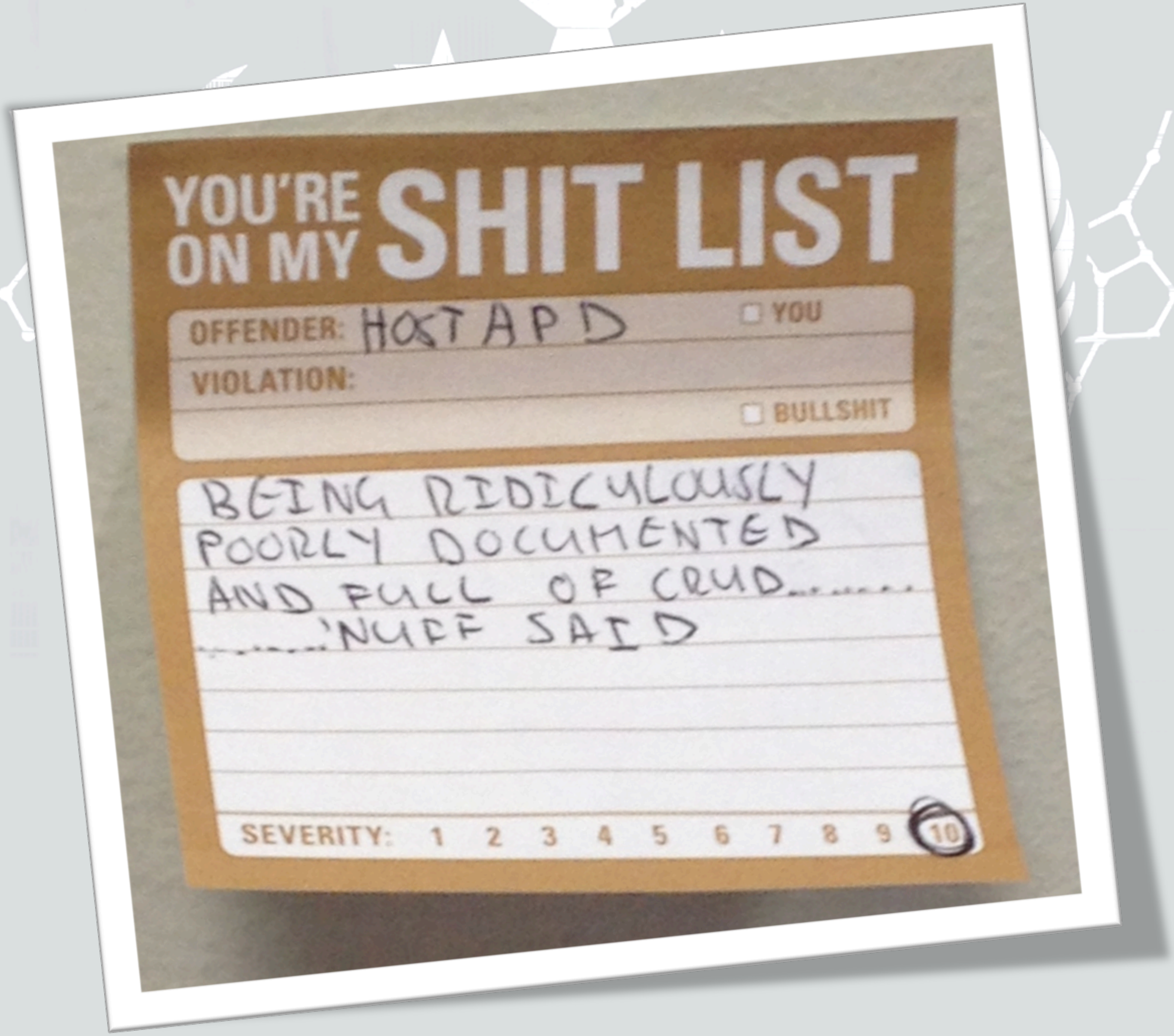
KARMA Attacks

How KARMA Works

Not so well anymore

Build PNL & Respond to Broadcasts

Disclaimer



YOU'RE ON MY SHIT LIST

OFFENDER: HOSTAPD □ YOU

VIOLATION: □ BULLSHIT

BEING RIDICULOUSLY
POORLY DOCUMENTED
AND FULL OF CRUD......
......'NUFF SAID

SEVERITY: 1 2 3 4 5 6 7 8 9 [✓ 10]

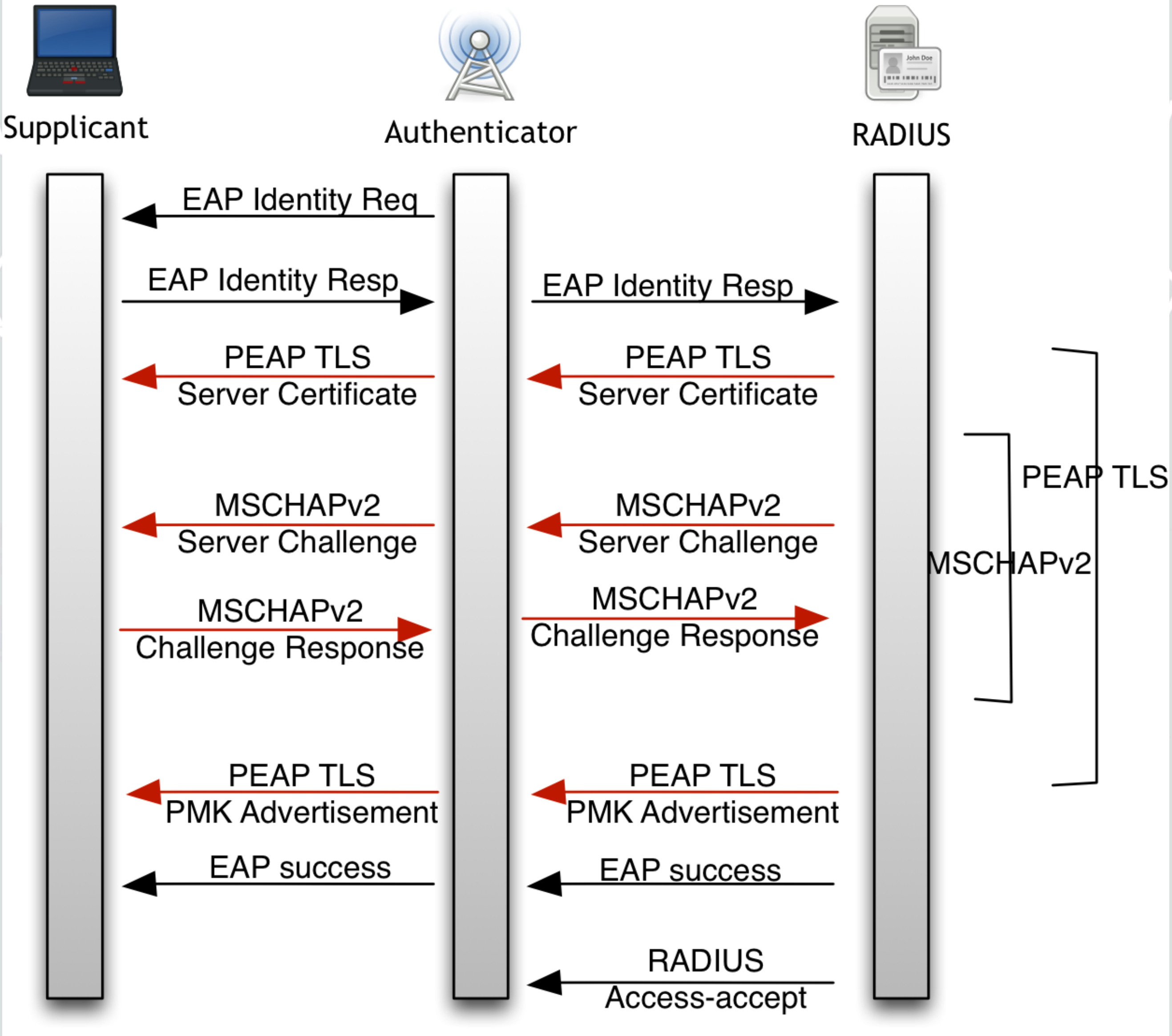
On Probes

Hidden Networks & Loud Mode

Secure Networks

Auto Crack ‘n Add

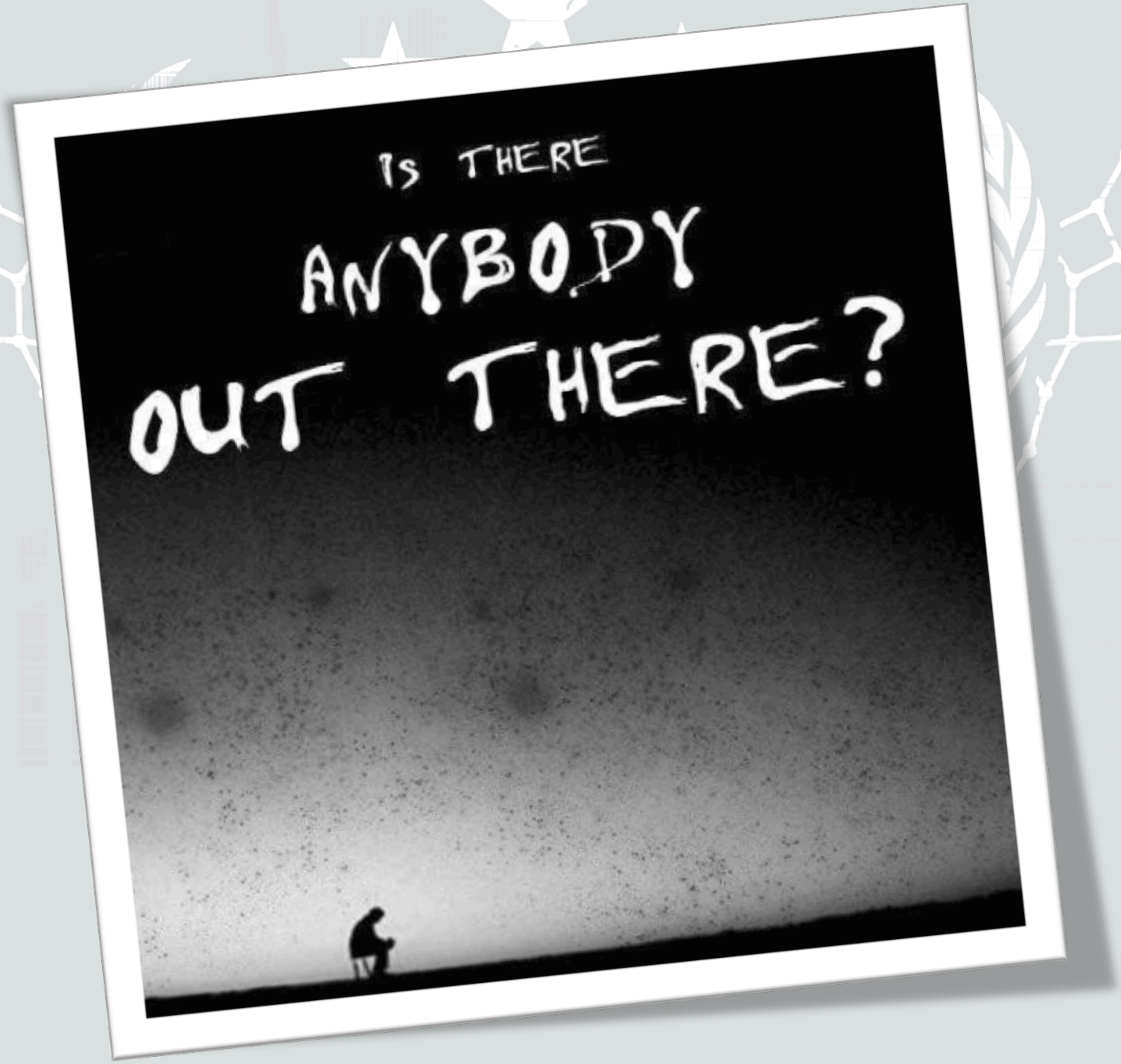
PEAP


Supplicant
Authenticator
RADIUS
EAP Identity Req
EAP Identity Resp
EAP Identity Resp
PEAP TLS
Server Certificate
PEAP TLS
Server Certificate
MSCHAPv2
Server Challenge
MSCHAPv2
Server Challenge
MSCHAPv2
Challenge Response
MSCHAPv2
Challenge Response
PEAP TLS
PMK Advertisement
PEAP TLS
PMK Advertisement
EAP success
EAP success
RADIUS
Access-accept
PEAP TLS
MSCHAPv2

Man In The Middle

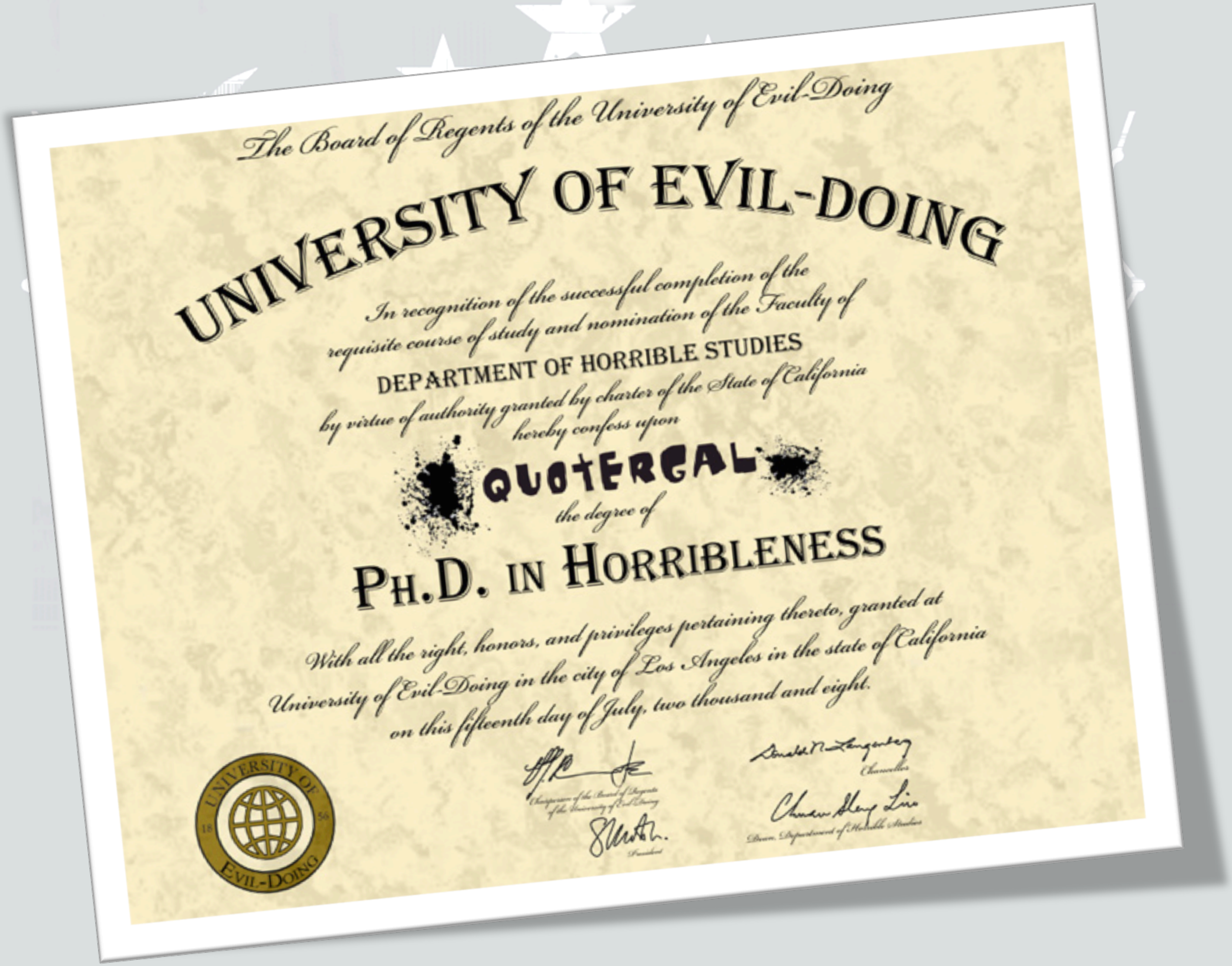
Non-SSL Protocols - SSLSplit

Fake It until you Make It



Captive Portal SE

Side Loading Evil Certs



The Board of Regents of the University of Evil-Doing

UNIVERSITY OF EVIL-DOING

In recognition of the successful completion of the requisite course of study and nomination of the Faculty of

DEPARTMENT OF HORRIBLE STUDIES

by virtue of authority granted by charter of the State of California hereby confess upon

QUOTERGAL

the degree of

PH.D. IN HORRIBLENESS

With all the right, honors, and privileges pertaining thereto, granted at University of Evil-Doing in the city of Los Angeles in the state of California on this fifteenth day of July, two thousand and eight.

Chairperson of the Board of Regents of the University of Evil-Doing

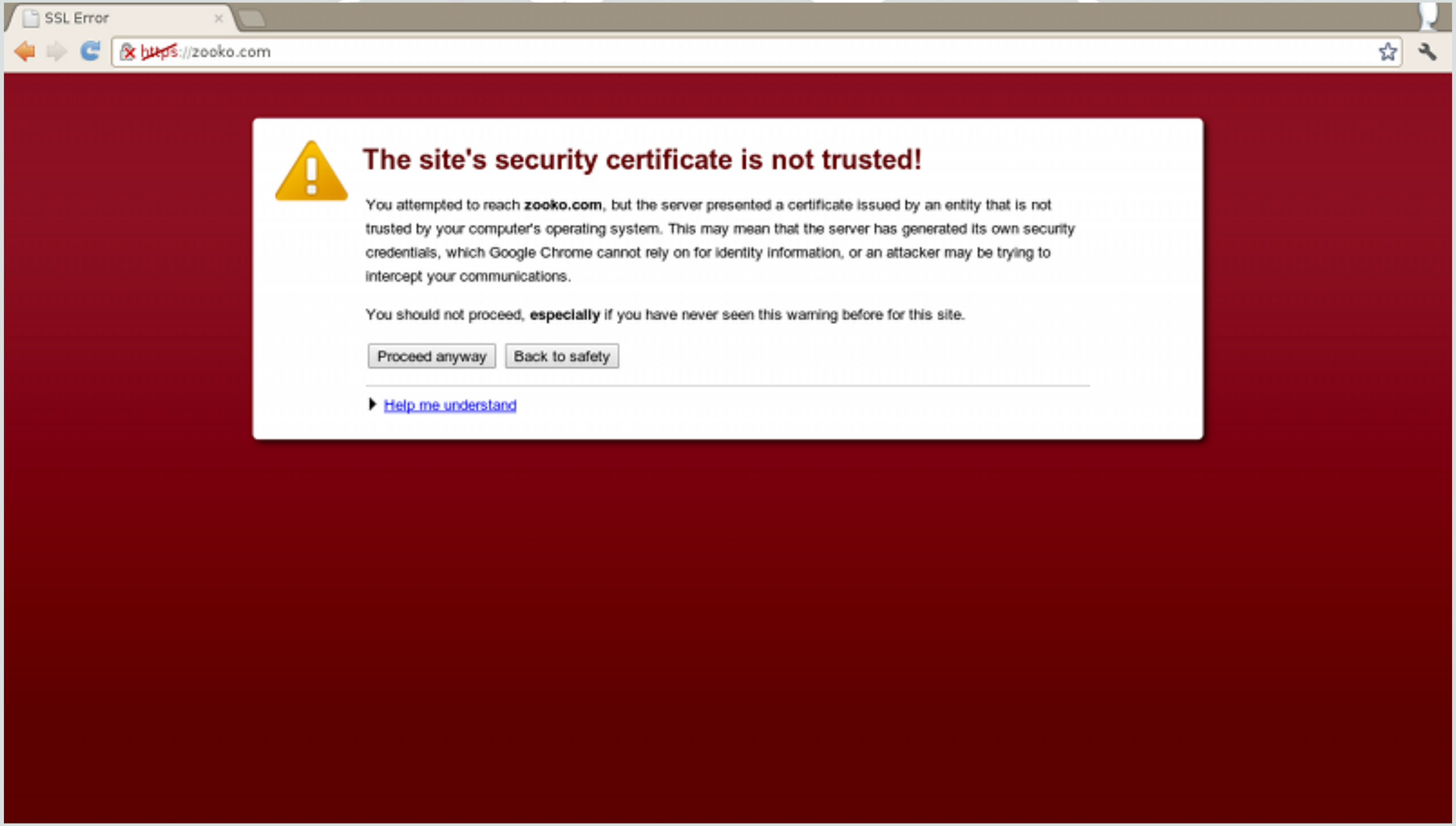
President

Chancellor

Dean, Department of Horrible Studies

UNIVERSITY OF EVIL-DOING 18 56

HSTS Partial Bypass by LeonardoNVE



The site's security certificate is not trusted!

You attempted to reach **zooko.com**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Google Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications.

You should not proceed, **especially** if you have never seen this warning before for this site.

FireSheep ReBorn as FireLamb

Lots of MitM

Online Check Bypass

Creds

Cookies (FireLamb)

Cert Sideloading

HSTS Partial Bypass

Captive Portal SE

Creds from the Sky

More Info

Blog: www.sensepost.com/blog

Tools: github.com/sensepost

- github.com/sensepost/mana
- github.com/sensepost/hostapd-mana
- github.com/sensepost/firelamb
- github.com/sensepost/crackapd
- github.com/sensepost/sslstrip-hsts

SlideShare: slideshare.net/sensepost