

12 years and a Baker's Dozen

Lessons and learnings from
my Infosec journey

#NullCON 2014,
Goa

Saumil Shah

CEO Net Square





Welcome



To



Nullcon



Happy



5th



Birthday!

भाषा अनेक लक्ष्य एक



@therealsaumil



saumilshah



डेड हैकर Hacker

I.

The Evolution of Targets

How Have Targets Shifted?

Servers

Applications

Desktops

Browsers

Identities

The Game Changers

Perimeter
Security

Web Apps

Broadband
Networks

WiFi

Social
Networks

Cellular
Data

Target Top Spot – Retail, Manufacturing, IT
Shifted away from financial organizations to its users.

Myth: Insiders cause the maximum damage.
Attributed to external attackers: 92% (5 yr avg: >70%)

2008: Servers 94%, Users 17%
2012: Servers: 54%, Users 71%

Shift in attacker profile.
Organized crime, state sponsored "threat actors".

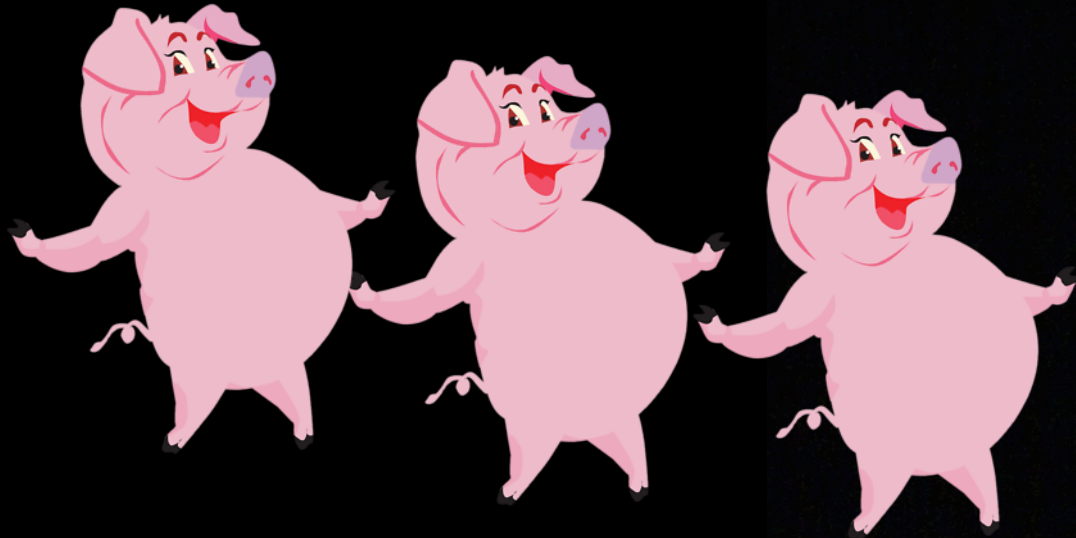
Effectiveness of breach detection
IT Audits, Fraud detection, IDS, Logs, MSS < 1%

An aerial photograph of the Great Wall of China. The wall is a long, grey stone structure with crenellations, winding along the ridges of steep, green mountains. A large, square watchtower with multiple windows and a crenellated roof stands out in the center. Two small figures of people are visible on the wall near the tower. The background shows more green mountains and a small waterfall on a distant peak.

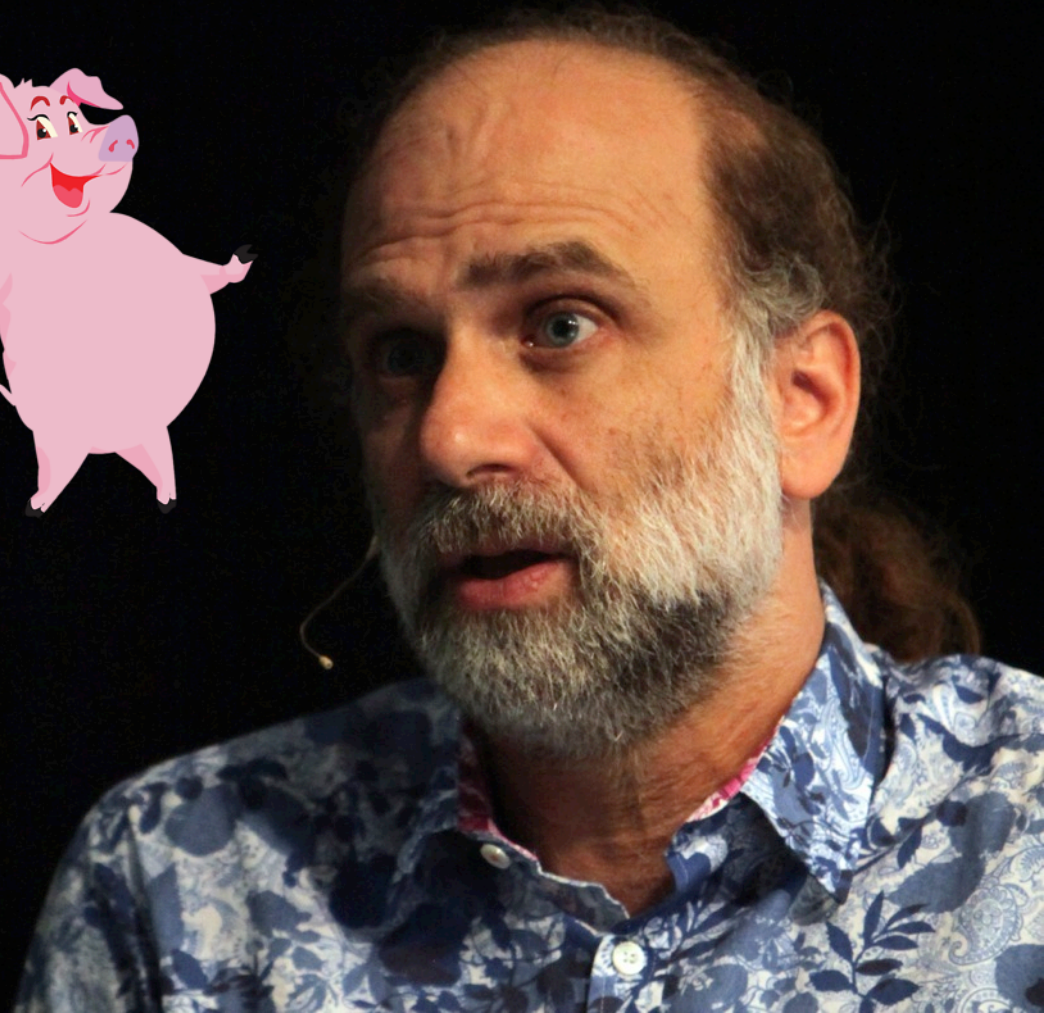
"A wall is only as good as those who
defend it"

Genghis Khan

The user's going to pick dancing pigs over security every time.



Bruce Schneier



Intelligence Driven Defence



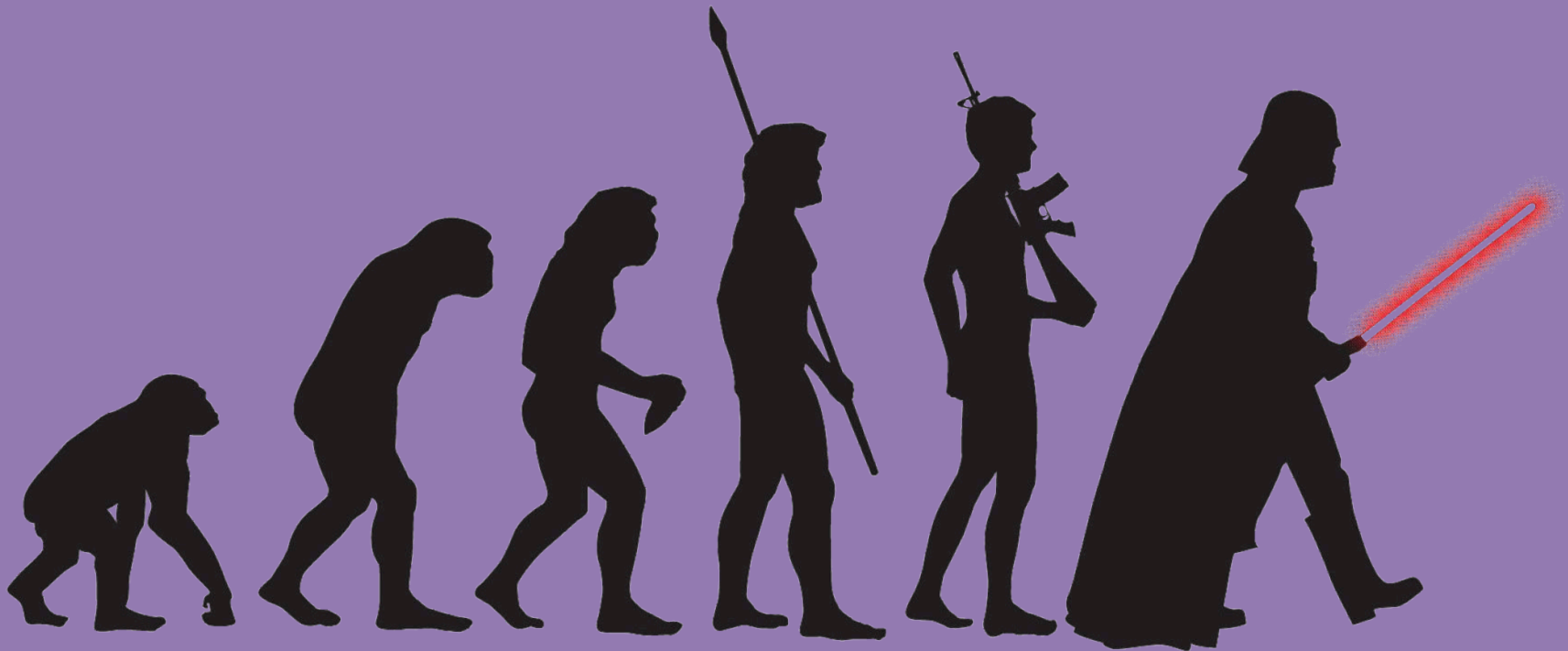
From reactive to proactive

2.

The Evolution of Exploits



The Advance of Exploits



It was different 12 years ago!


- Individual effort.
- 1 week dev time.
- 3-6 months shelf life.
- Hundreds of public domain exploits.
- "We did it for the fame. lols."



Today...



- Team effort
- 2-12 month dev time
- 24h to 10d shelf life
- Public domain exploits nearly zero
- Cost,value of exploits has significantly risen
- WEAPONIZATION.



"For a few hundred K,
could you put together
a team that would
break-in just about
anywhere?"

Haroon Meer

CCDCOE Conference on
Cyber Conflict - 2010

NullCON '14 

(4) Some Ugly Facts

“For a few hundred K (USD), could you put together a team that would break-in just about anywhere?”

haroon meer	YES
Saumil Shah	YES
Ivan Arce	YES
Felix (fx) Lindner	YES



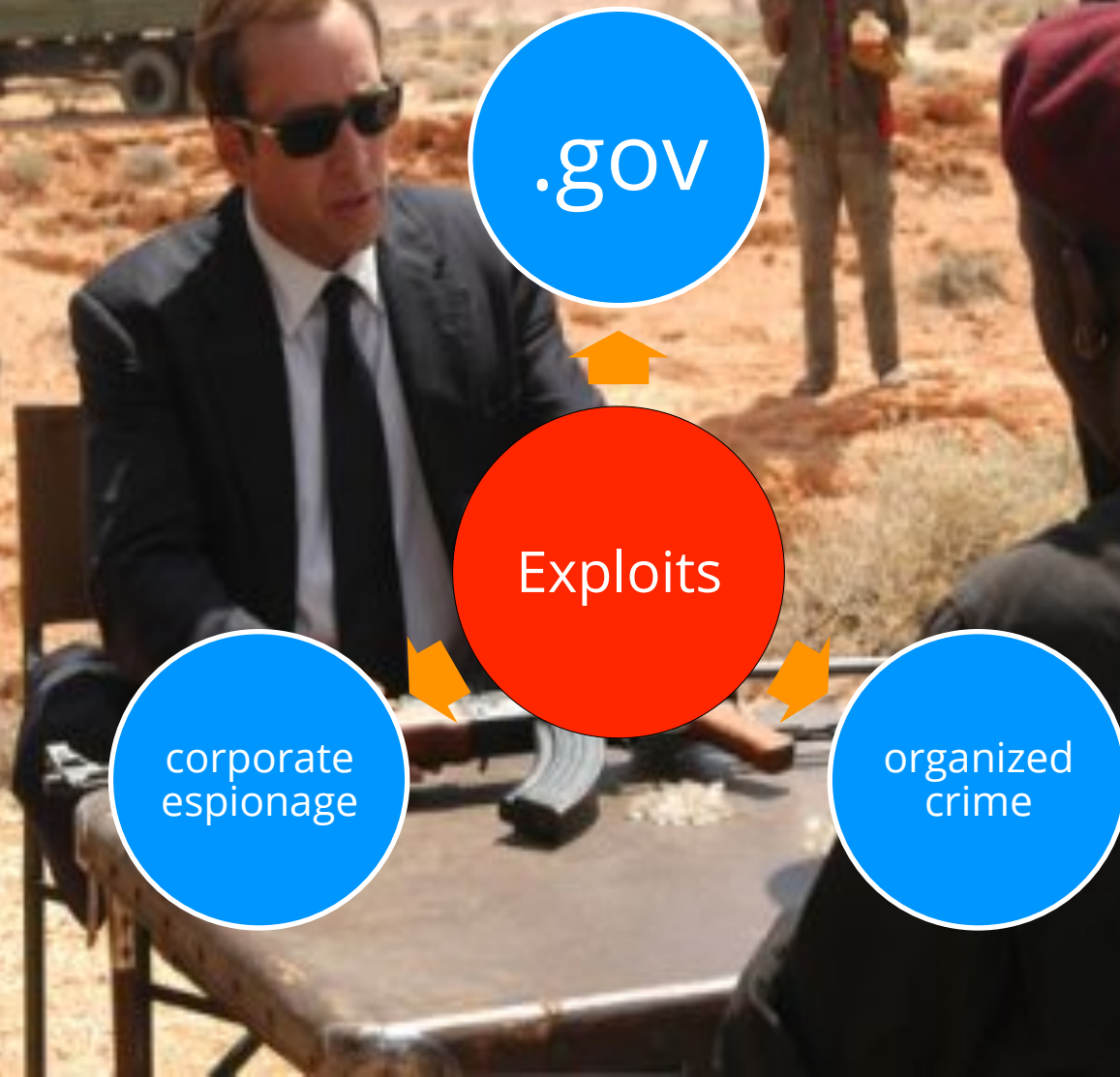
\$100k – 500k

Attacking is (much) cheaper
than defence.

Attacker toolchains
are far more complex
than the public
demonstrations
we have seen so far.



Exploit Buyers



Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits

4 comments, 2 called-out + [Comment now](#)

This story accompanies a [profile of the French exploit-selling firm Vupen](#) in the April 9th issue of [Forbes](#) magazine.

A clever hacker today has to make tough choices. Find a previously unknown method for dismantling the defenses of a device like an iPhone or iPad, for instance, and you can report it to Apple and present it at a security conference to win fame and lucrative consulting gigs. Share it with HP's Zero Day Initiative instead and earn as much as \$10,000 for helping the firm shore up its security gear. Both options also allow Apple to fix its bugs and make the hundreds of millions of iPhone and iPad users more secure.



Meet The Hackers Who Sell Spies The Tools To

But any hacker who happens to know one Bangkok-based security researcher who goes by the handle "the Grugq"—or someone like him—has a third option: arrange a deal through the pseudonymous exploit broker to hand the exploit information over to a government agency, don't ask too many questions, and get paid a quarter of a million dollars—minus the Grugq's 15% commission.

Vulnerability	\$	Source
Some exploits"	250,000	Govt. official referring to what "some people" pay.
A "real good" exploit	> 100,000	SNOsoft Research Team
Chrome	60,000	Google
Vista	50,000	Raimund Genes, Trend Micro
Weaponized exploit	30,000	David Maynor, Secureworks
iDefense purchases	10,000	David Maynor, Secureworks
WMF	4,000	Alexander Gostev, Kaspersky
Google	3,133.7	Google
Mozilla	3,000	Mozilla
Excel	1,200	Ebay auction site

credit: Forbes 23.3.2012 Shopping for Zero Days
Charlie Miller, the 0-day market

Attack Sophistication



3.

What Secure
means to me

Confidentiality
Integrity
Availability

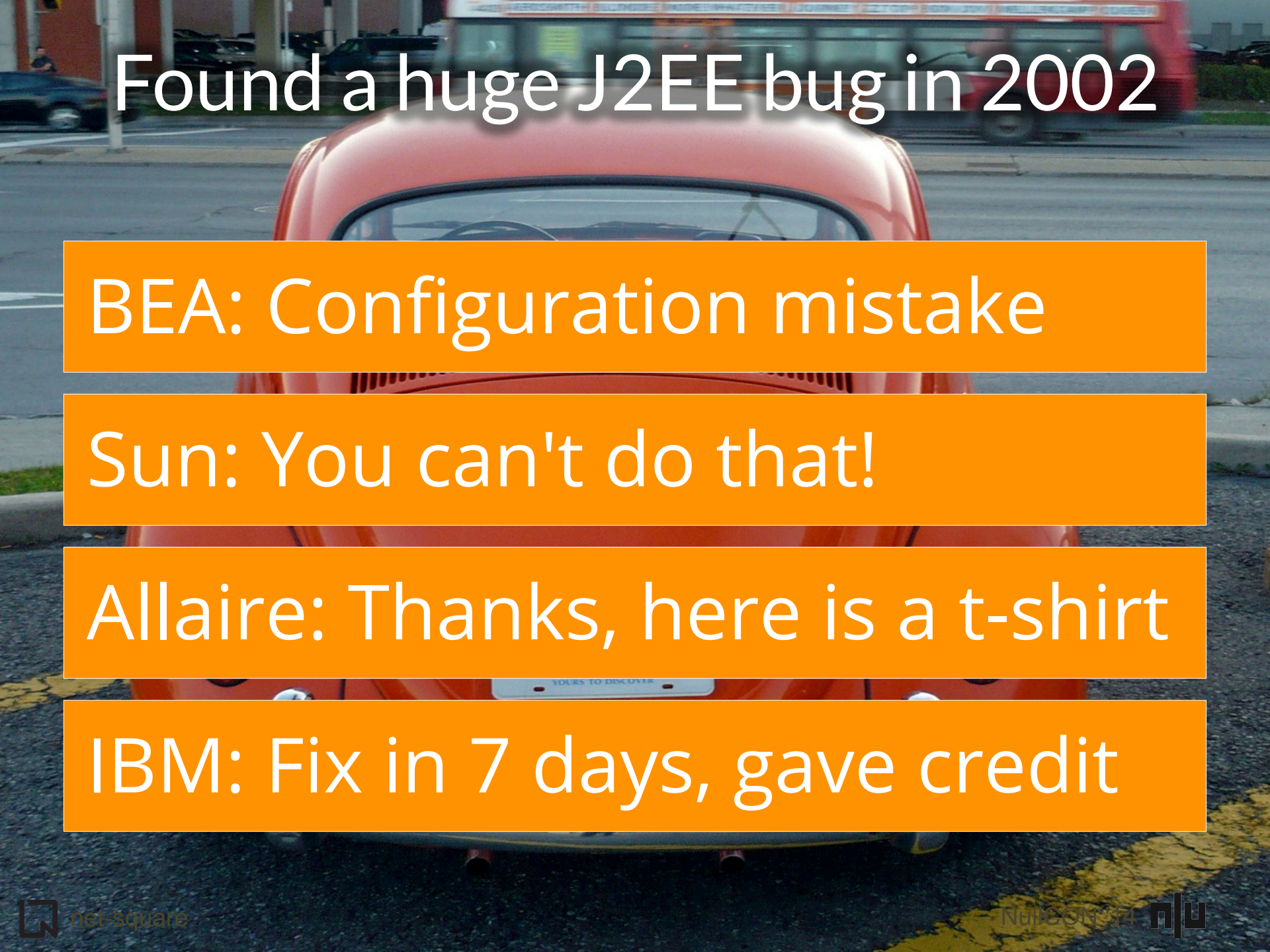
Invulnerable

Up-to-date

Accountable

Found a huge J2EE bug in 2002





Found a huge J2EE bug in 2002

BEA: Configuration mistake

Sun: You can't do that!

Allaire: Thanks, here is a t-shirt

IBM: Fix in 7 days, gave credit

What defenders are up to



- HIGH EXPOSURE
- Rigorous Internal Testing
- Proactive Exploit Mitigation Technology
- Quick Turnaround Times (24 hours)
- Mature Bug Bounties

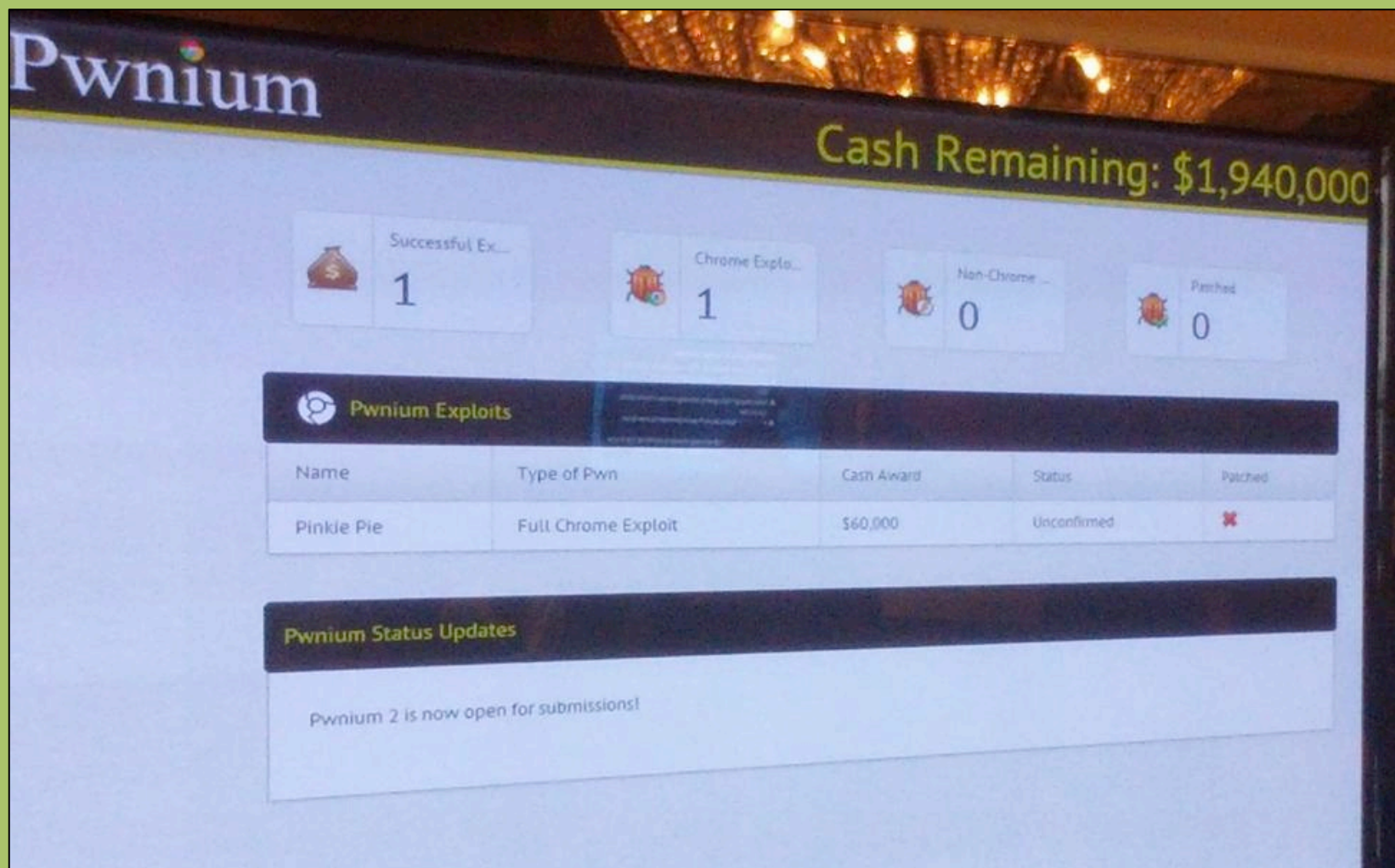


ORACLE®



- HIGH EXPOSURE
- Good Efforts
- Don't have resources / focus
- Slow Turnaround Times (1 month)
- Learning the hard way

Bug Bounties: high stakes game



The screenshot shows the Pwnium bug bounty program dashboard. At the top, the 'Pwnium' logo is on the left, and 'Cash Remaining: \$1,940,000' is on the right. Below the logo, there are four boxes showing exploit counts: 'Successful Ex...' with 1, 'Chrome Explo...' with 1, 'Non-Chrome...' with 0, and 'Patched' with 0. Each box has a corresponding icon (money bag, bug, bug, and bug). Below these boxes is a section titled 'Pwnium Exploits' which contains a table of exploits. The table has columns for Name, Type of Pwn, Cash Award, Status, and Patched. One exploit is listed: 'Pinkle Pie' with a 'Full Chrome Exploit' type, a '\$60,000' cash award, and an 'Unconfirmed' status. The 'Patched' column for this exploit shows a red 'X' icon. Below the table is a section titled 'Pwnium Status Updates' which contains the text 'Pwnium 2 is now open for submissions!'.

Pwnium

Cash Remaining: \$1,940,000

Successful Ex... 1

Chrome Explo... 1

Non-Chrome... 0

Patched 0

Pwnium Exploits

Name	Type of Pwn	Cash Award	Status	Patched
Pinkle Pie	Full Chrome Exploit	\$60,000	Unconfirmed	✗

Pwnium Status Updates

Pwnium 2 is now open for submissions!

The Lure of Bug Bounties

Take up a QA job
instead, or better yet,
build the goose that
lays the golden eggs

What "SECURE" means to me

Resilience

Fitness

Max time to fix: 72 hrs

4.

On Standards & Compliance

Feeling Secure?



Compliance != Security



Saumil Shah

@therealsaumil

+ Follow

@weldpond @nopsec I've always maintained the maxim that "Compliance != Security". Be careful what you want, 'cause that's what you will get

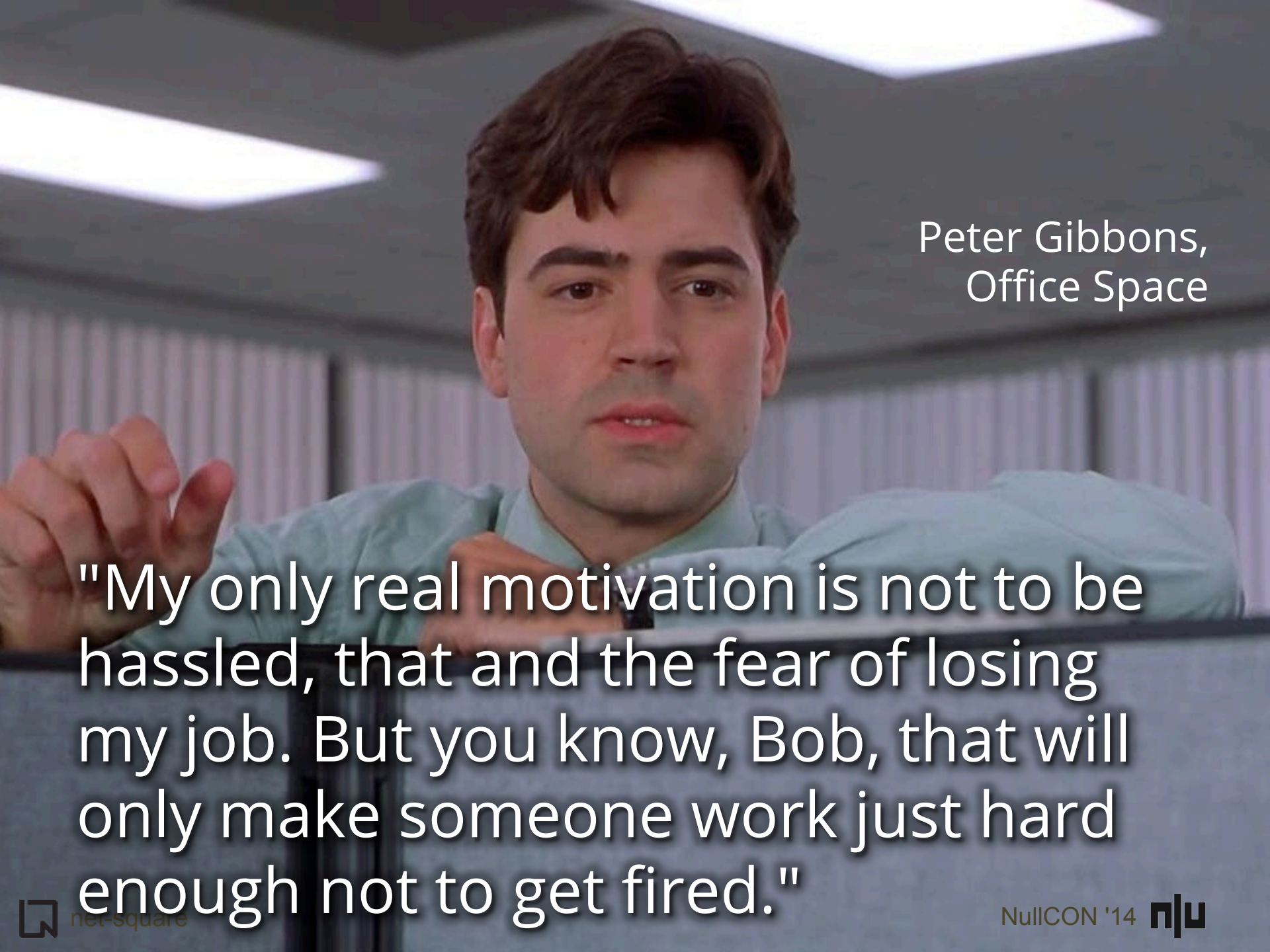
↩ Reply ↻ Retweet ★ Favorite ⋮ More

FAVORITE

1





A medium shot of Peter Gibbons, played by Mike Myers, in an office setting. He is wearing a light blue button-down shirt and has a weary, slightly annoyed expression. His hands are resting on a desk in front of him, with his fingers slightly curled. The background shows office cubicles and fluorescent lighting.

Peter Gibbons,
Office Space

"My only real motivation is not to be hassled, that and the fear of losing my job. But you know, Bob, that will only make someone work just hard enough not to get fired."

REGULATORS,
CAN YOU
PREVENT
THIS?



NICK LEESON

\$1.31B



KWEKU ADOBOLI

\$2B



JEROME KERVIEL

\$7.22B



BERNIE MADOFF

\$50B

Who are you more scared of?



A close-up photograph of a black cat's face. The cat has large, round, yellow-green eyes with black pupils, looking directly at the camera. Its fur is black with some white markings on its chest and face. The background is a plain, light-colored wall.

Who are you more scared of?

A collage of two images. The left image shows a close-up of a man with dark hair and round glasses, looking slightly to the side. The right image shows the lower half of three people standing in a row, wearing dark suits and holding briefcases, set against a light blue background.

Attackers or Auditors?

5.

Necessity is
the Mother of
Invention

Firewalls

IDS/IPS

Antivirus

WAF

Endpoint Security

ASLR, DEP

Sandbox

One-way Hacking

Packet Fragmentation

Obfuscation

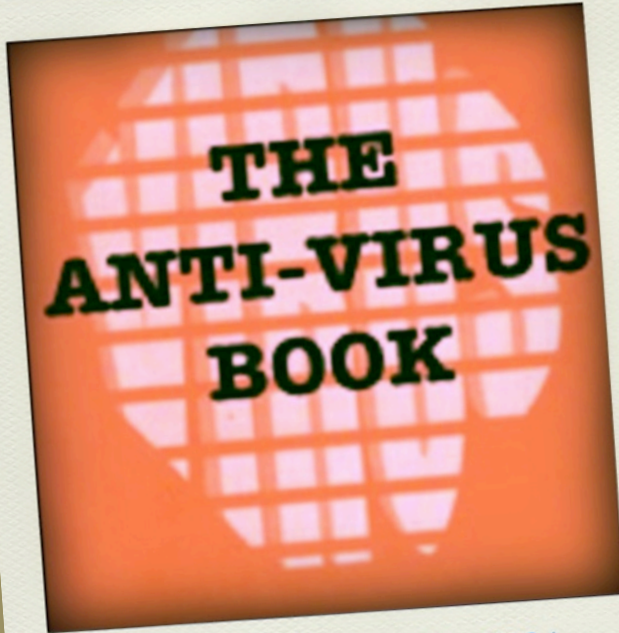
Character Encoding

DNS Exfiltration

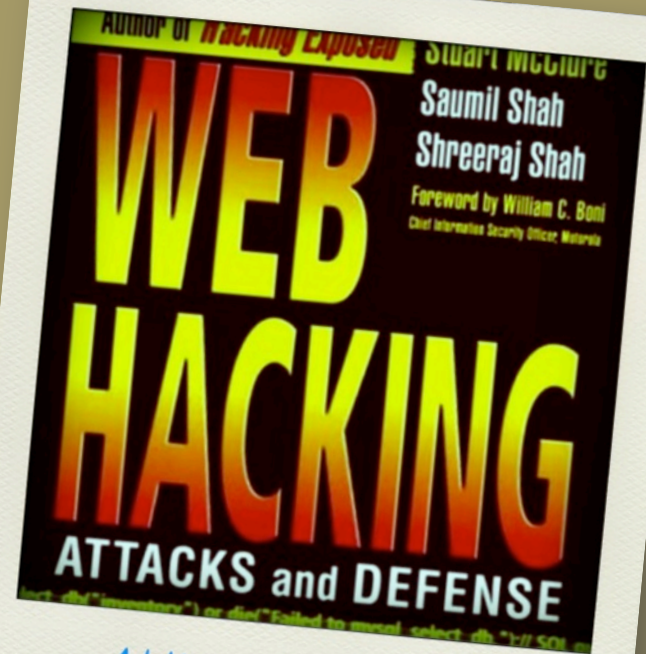
Return Oriented
Programming

Jailbreak

My attempts at writing books



Tata McGraw-Hill, 1996



Addison Wesley, 2002

Inside Out Attacks - 1999

Inside-Out Attacks

An old concept with a new threat

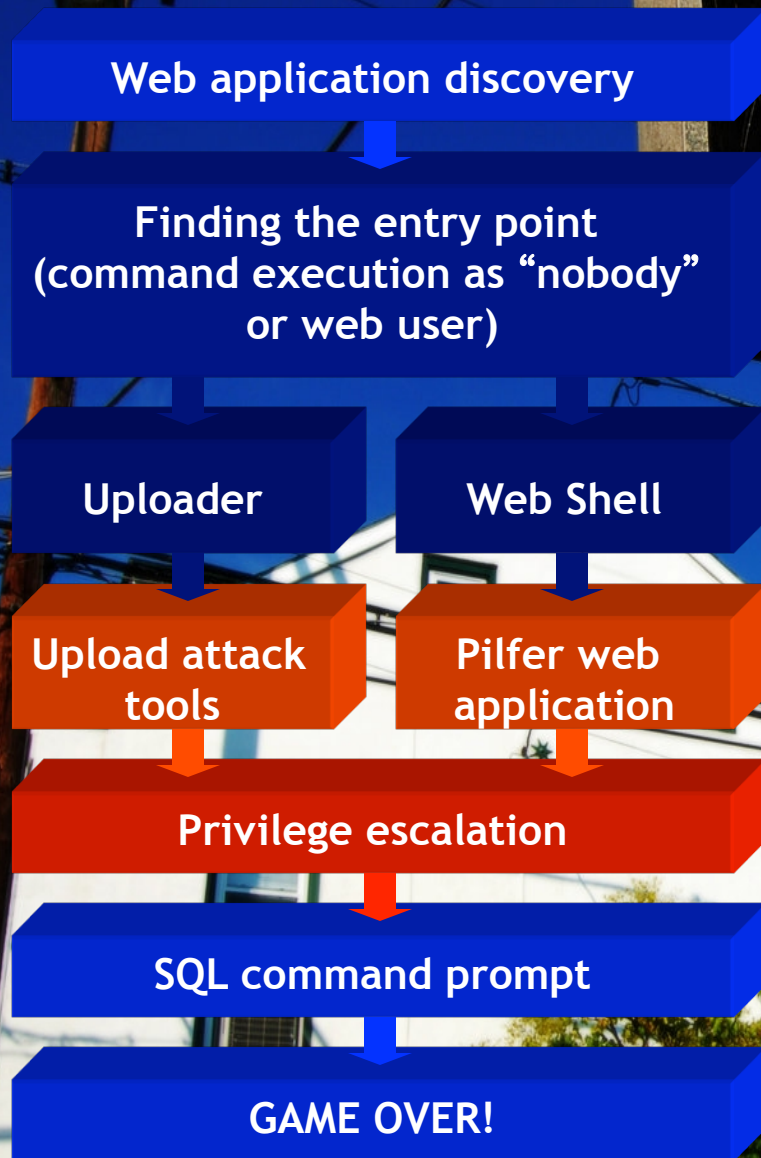
Patrick Heim and Saumil Shah

Saturday, July 10, 1999

Management of security in the Internet age has been focused on border defenses such as firewalls consisting of packet filters and proxy hosts. These protect from outside-in attacks. These are attacks that are initiated by an attacker from the outside wishing to establish a session or send data to a system within the perimeter of the corporate network. The objective can be varied, but in all cases, the job of the firewall is to protect internal resources by restricting external connections to specific resources either directly (packet filter) or indirectly (proxy).

The often-overlooked problem is that this only protects the company from attacks that originate from the outside. Many times, firewall rules allow broad access for outbound

One Way Attacks - 2001














HTTP Page Signatures - 2002

200:A302E6F1DC10112A5AF8624E5EA11B367F93DD04

Accurately identify HTTP responses
Minimize false positives in error detection
Content Independent
Computation time: $O(n)$
Comparison time: $O(k)$

HTTP Fingerprinting - 2003

		web server fingerprinting report				
host	port	ssl	banner reported	banner deduced	icon	confidence
www.walmart.com	80		Microsoft-IIS/5.0	Apache/2.0.x		
www.foundstone.com	80		WebSTAR	Apache/2.0.x		
www.port80software.com	80		Yes we are using ServerMask	Microsoft-IIS/5.1, Microsoft-IIS/5.0 ASP.NET, Microsoft-IIS/4.0		
www.ubizen.com	80		web server	Apache/2.0.x		
www.datek.com	80		Ameritrade Web Server	Netscape-Enterprise/4.1		
 httprint © 2003 net-square						

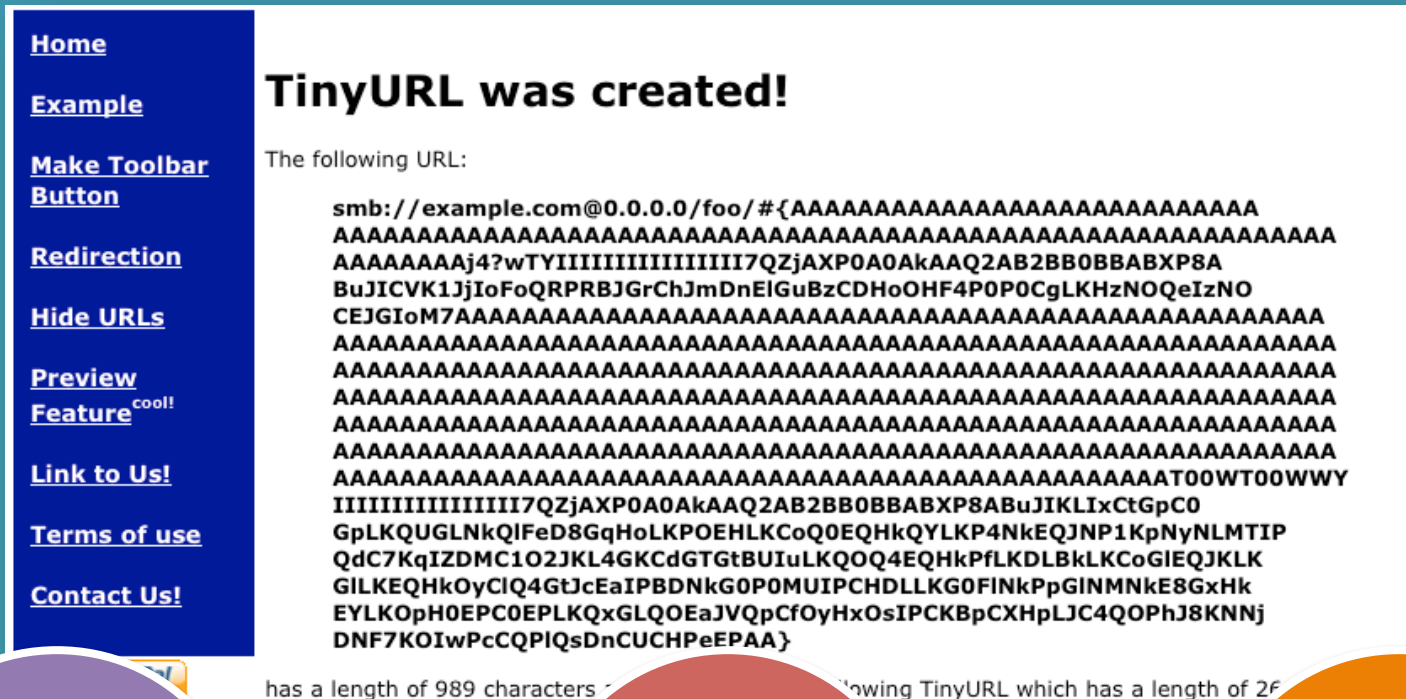
Teflon - 2008

My humble attempt
at browser security.

"Anti-stick for your
browser's attack surface".

FAILED RESEARCH.

Abusing URL Shorteners - 2010



The screenshot shows the TinyURL website. On the left is a blue sidebar with links: Home, Example, Make Toolbar Button, Redirection, Hide URLs, Preview Feature^{cool!}, Link to Us!, Terms of use, and Contact Us!. The main content area has the heading "TinyURL was created!" and the text "The following URL:". Below this is a very long URL starting with "smb://example.com@0.0.0.0/foo/{". The URL is truncated in the middle of the screenshot. Below the URL, it says "has a length of 989 characters" and "The following TinyURL which has a length of 26".

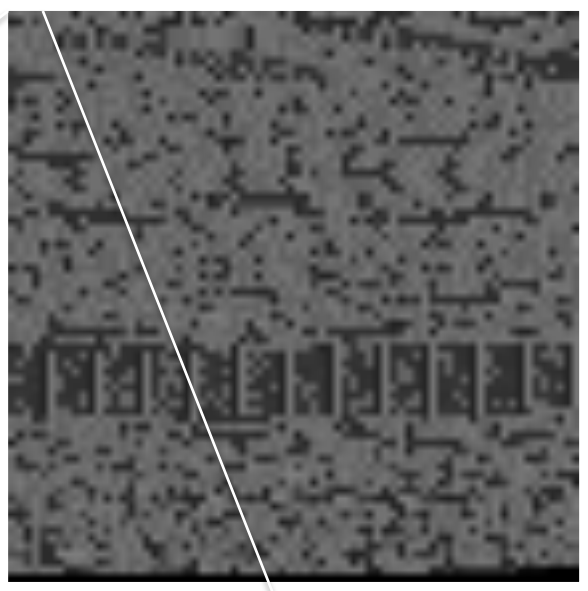
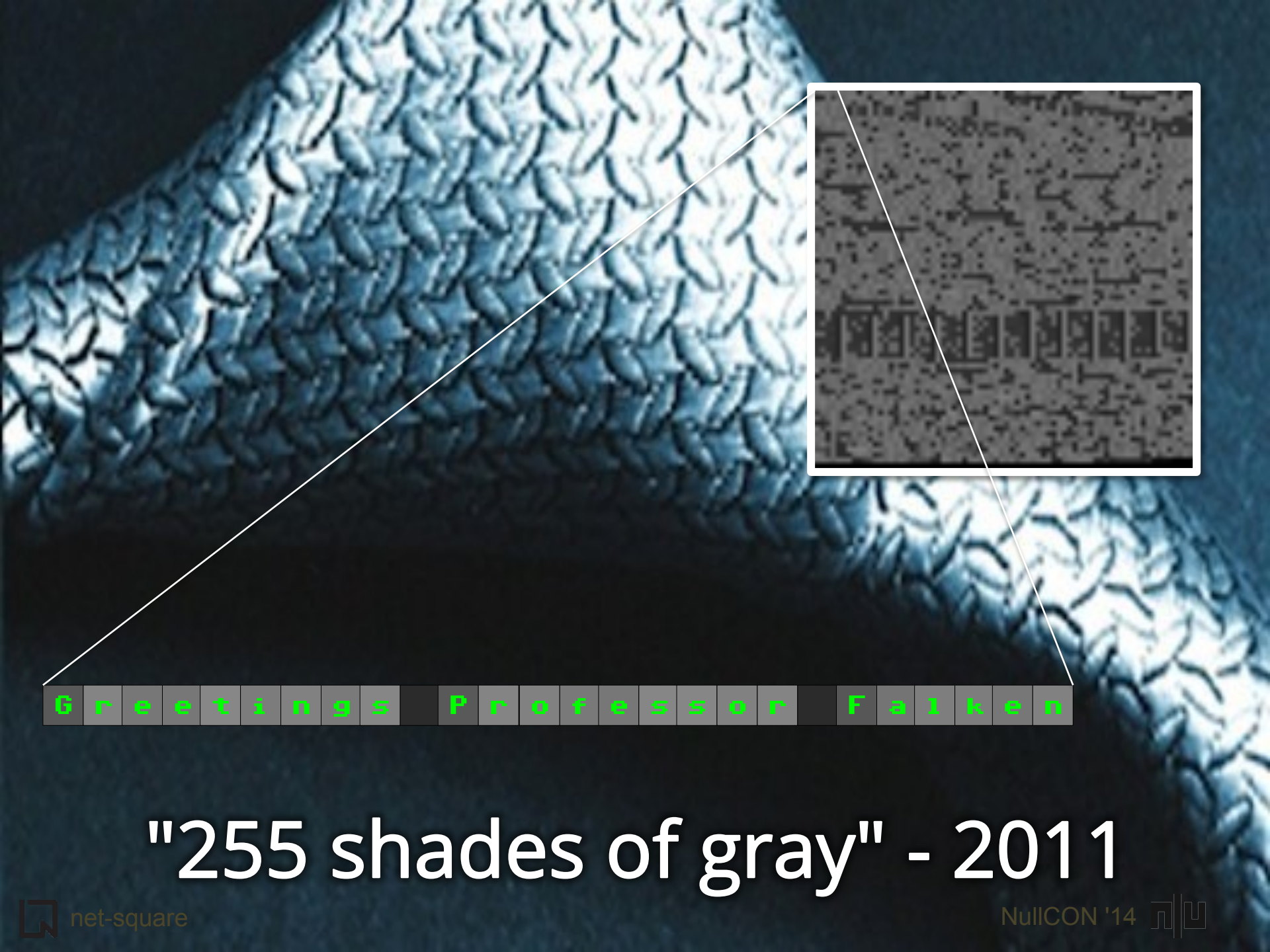
Alpha
Encoded
Exploit



Tiny
URL



ZOMFG



GREETINGS PROFESSOR FALKEN

"255 shades of gray" - 2011


Mozilla Firefox

http://192.168.128.129/png/data2png.php

```
function packv(n){var s=new Number(n).toString(16);while(s.length<8)s="0"+s;
return(unescape("%u"+s.substring(4,8)+"%u"+s.substring(0,4)))}var addressof=new
Array();addressof["ropnop"]=0x6d81bdf0;addressof["xchg_eax_esp_ret"]=0x6d81bdef;
addressof["pop_eax_ret"]=0x6d906744;addressof["pop_ecx_ret"]=0x6d81cd57;
addressof["mov_peax_ecx_ret"]=0x6d979720;
addressof["mov_eax_pecx_ret"]=0x6d8d7be0;
addressof["mov_pecx_eax_ret"]=0x6d8eee01;addressof["inc_eax_ret"]=0x6d838f54;
addressof["add_eax_4_ret"]=0x00000000;addressof["call_peax_ret"]=0x6d8aec31;
addressof["add_esp_24_ret"]=0x00000000;addressof["popad_ret"]=0x6d82a8a1;
addressof["call_peax"]=0x6d802597;function
```

Convert

data length 5108
dimension 72



Done

192.168.128.129 Tor Disabled

I'm an evil Javascript

I'm an innocent image

Cross Container Scripting - 2012



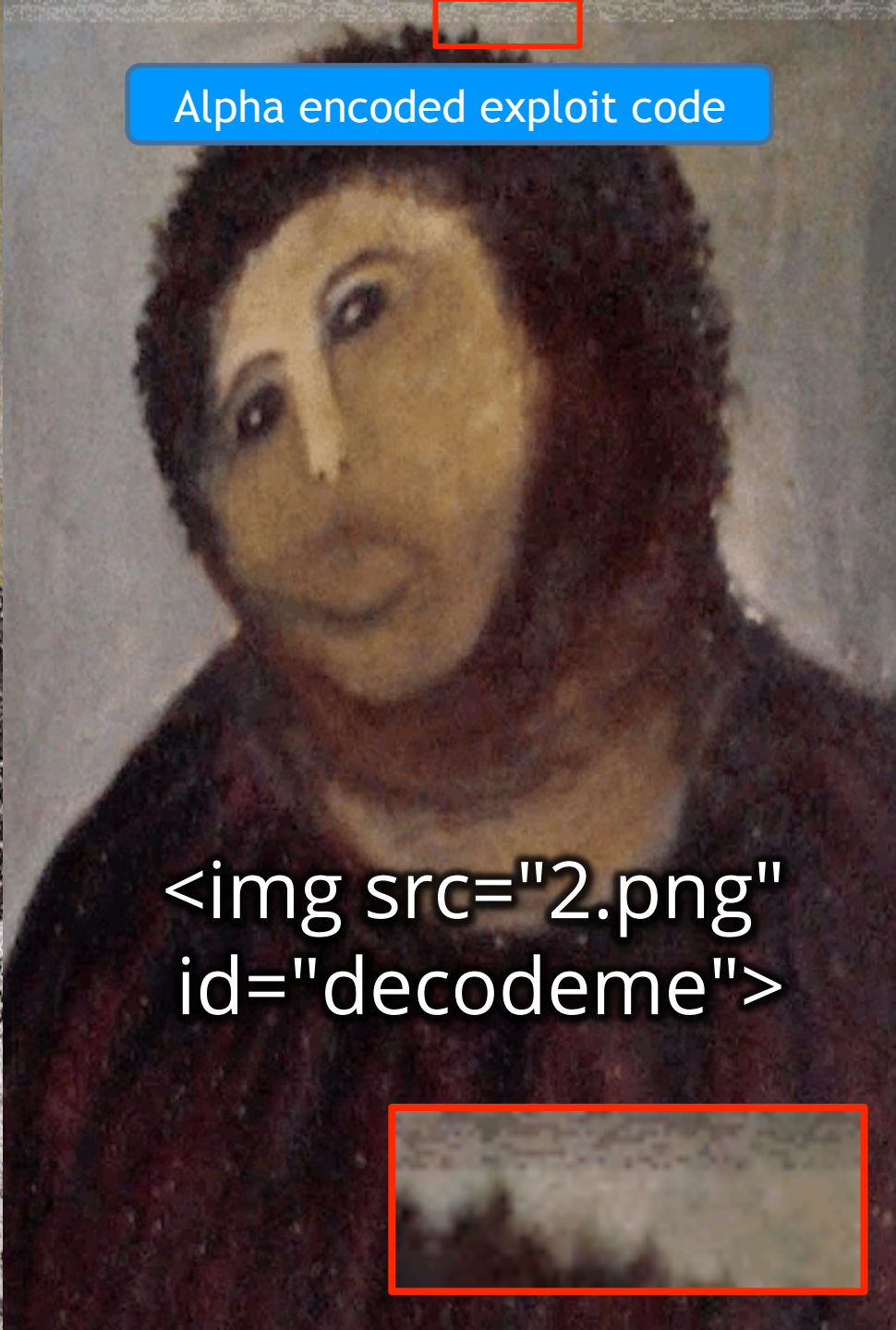
XCS

```
  
<script src="itsatrap.gif">  
</script>
```




```
<script src="1.gif">  
</script>
```

IMAJ5 CANVAS "loader" script



Alpha encoded exploit code

```

```



Theory Becomes Practice - 2014



Saumil Shah
@therealsaumil

Theory becomes practice. Malware in the wild uses my "255 shades of grey" technique.

blog.sucuri.net/2014/02/new-if...

Talk: slideshare.net/saumilshah/dea...

04/02/14 1:31 PM

35
RETWEETS

28
FAVORITES



Hiding In Plain Sight

6.

Infosec

Conferences

1999: Blackhat and Defcon
Blackhat – 15 years in a row
RSA 2002 – the only commercial con

HITB, Cansecwest, HackLU, NullCON,
Hackcon, ITWeb, IT Underground, IT
Defense, DeepSec, NoSuchCon,
REcon, SeacureIT, 44CON, SyScan...



1 conference every 3 days...



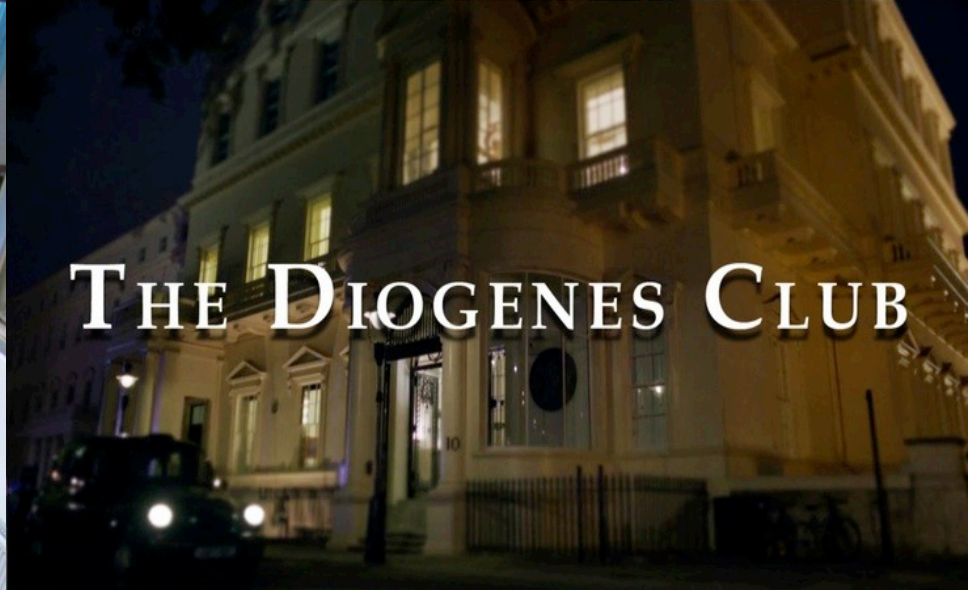
...and 5000 talks for 2013!



Hacker Cons

Where else will
you find a more
diverse, open,
global, talented
and energetic
crowd?

Hackerspaces



THE DIOGENES CLUB



Hackerspaces

"There are many men in London, who, some from shyness, some from misanthropy, have no wish for the company of their fellows.

Yet they are not averse to comfortable chairs and the latest periodicals."



My type of hacker cons

Smaller events
Single/Dual track
Meet the speakers
Meet the audience
Learn something new!

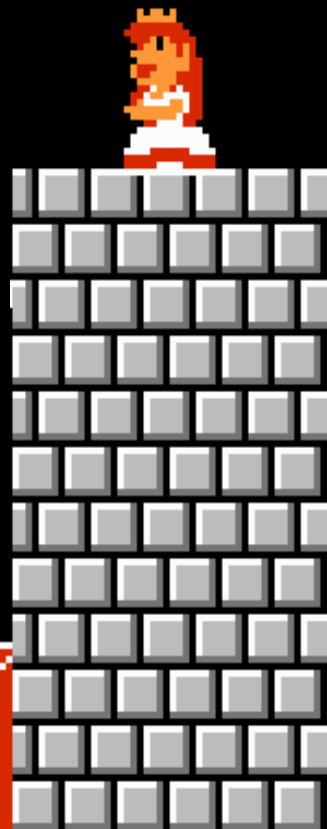
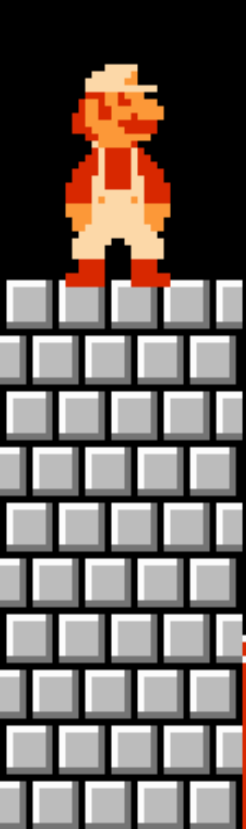


Researchers

Industry

Mr. Right

Wants
"Mr. Right Now"



Mind the Researcher/Industry Gap

7.

Hackers :
who are we?

WE ARE HACKERS

**WE PUSH THE
ENVELOPE**

**WE THRIVE ON
FACTS AND LOGIC..**

**..AND LATERAL
THINKING**

**WE QUESTION AND
CHALLENGE AND**

**WORK ON LIMITED
RESOURCES**



My Hacker Hero



Heretics?
Blasphemers?
Anarchists?
Free-thinkers?
Rebels?



"The time to think of your ethical boundaries is BEFORE you are put in a difficult situation."

Alex Stamos

The White Hat's Dilemma
Defcon 21



You find a critical remote exploit in a very widespread product. Do you:

- A) Publicly announce the flaw immediately
- B) Build a whole Black Hat talk around it
- C) Perform responsible disclosure with deadlines
- D) Use it to sell “consulting” to the vendor
- E) Weaponize and sell directly to your government
- F) Weaponize and sell to a trader
- G) Use it yourself for fun and/or profit

READ HIS TALK AND ANSWER ALL HIS QUESTIONS!

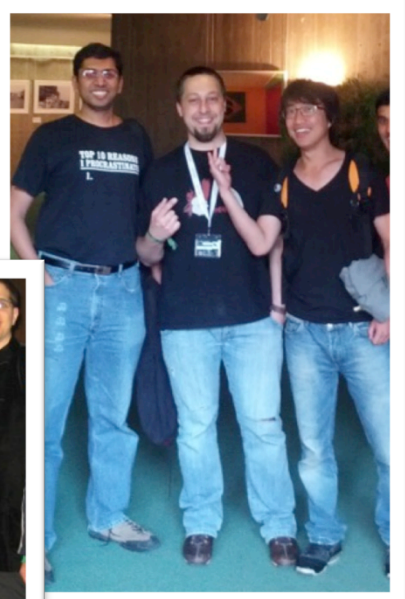
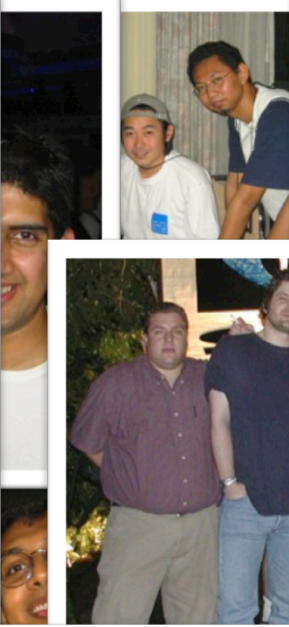
8.

And
who am I ?

```
saumil  ttys001  Feb 15 14:35  
saumil@gayatri:~$ _
```



I stood on the
shoulders of giants



Stranger Than Fiction

Big Fish (2003)

9.

On building Products

My Product building journey

Web app scanners

Network scanner

Windows Desktop Scanner

Share Inspector

Accounts Inspector

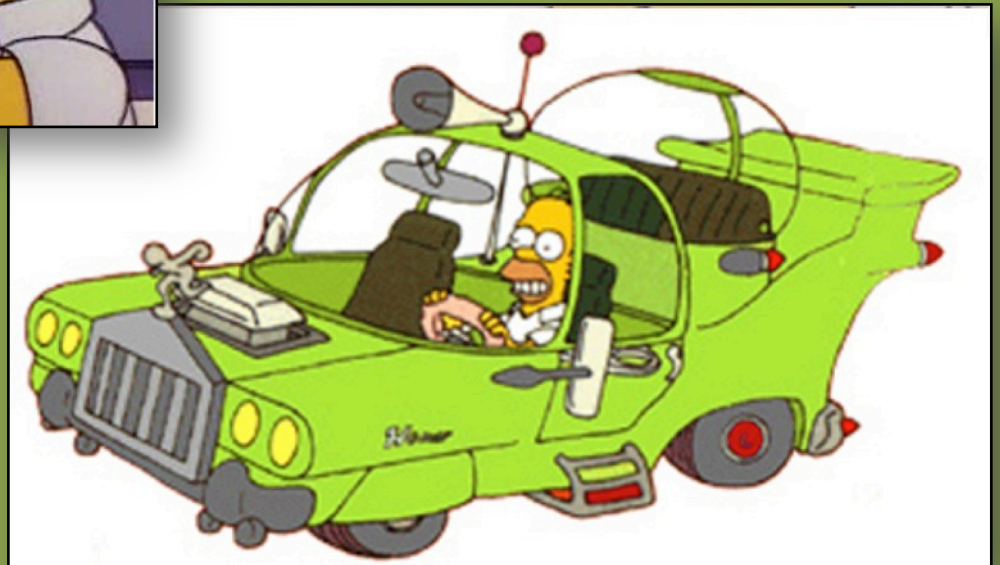
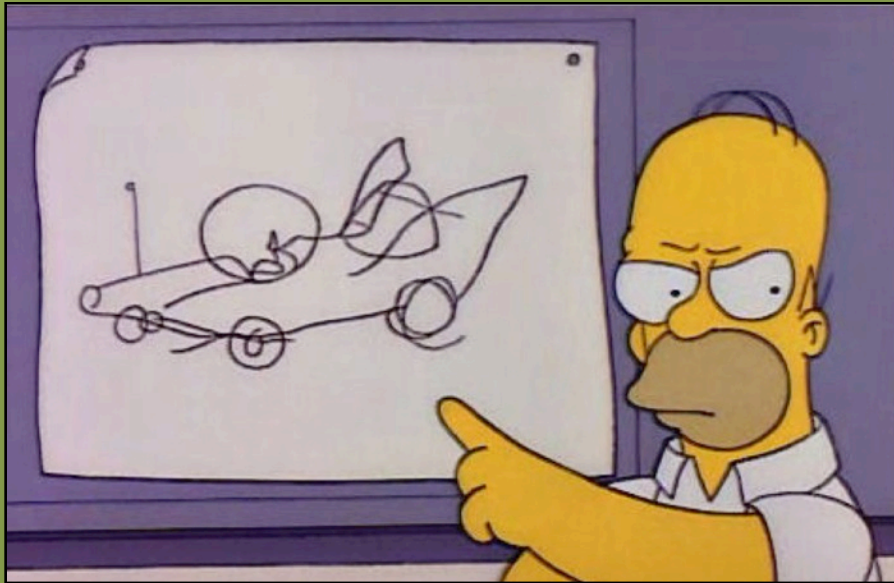
Browser plug-in for app testing

ServerDefender

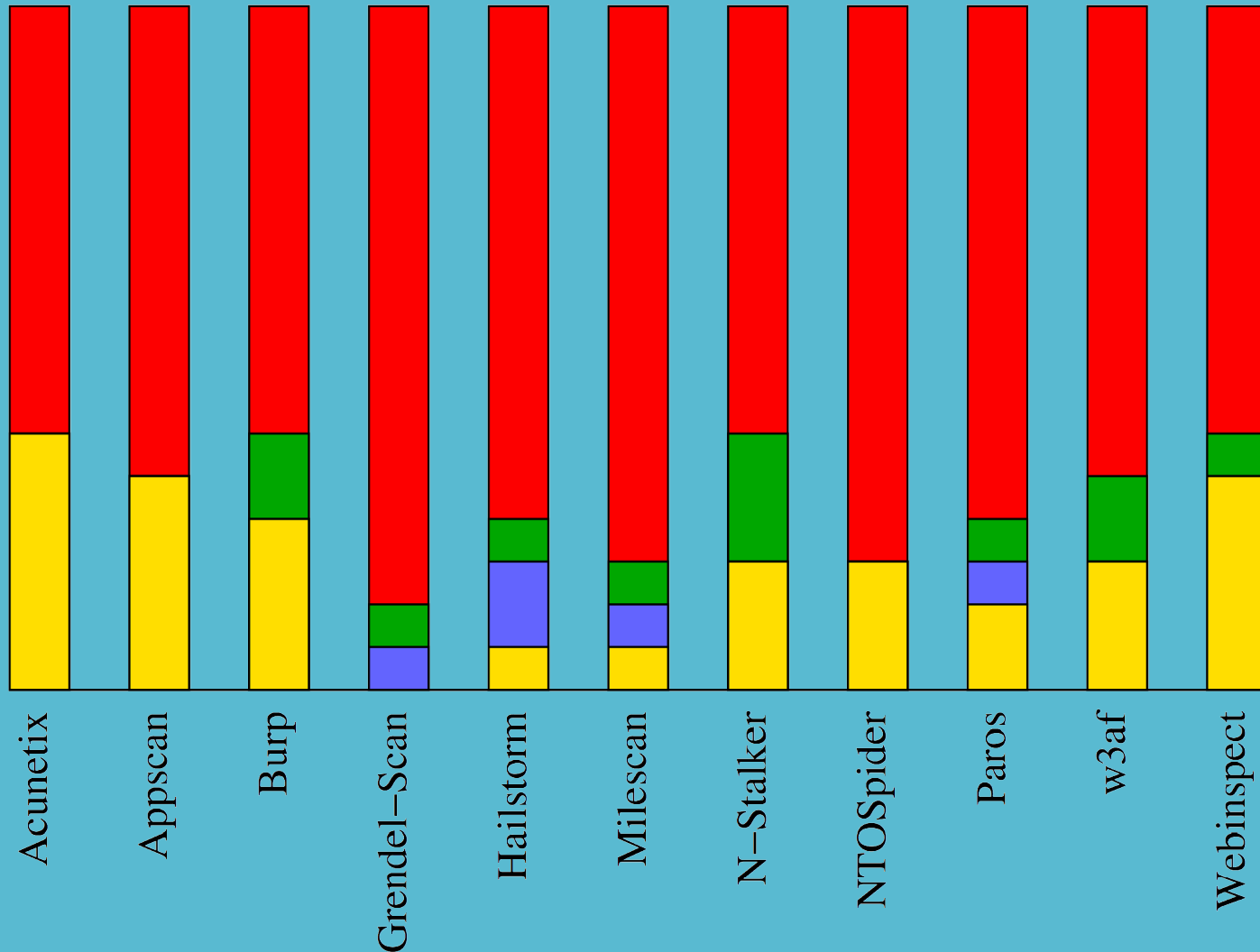
Hardened Browser from Chromium code base



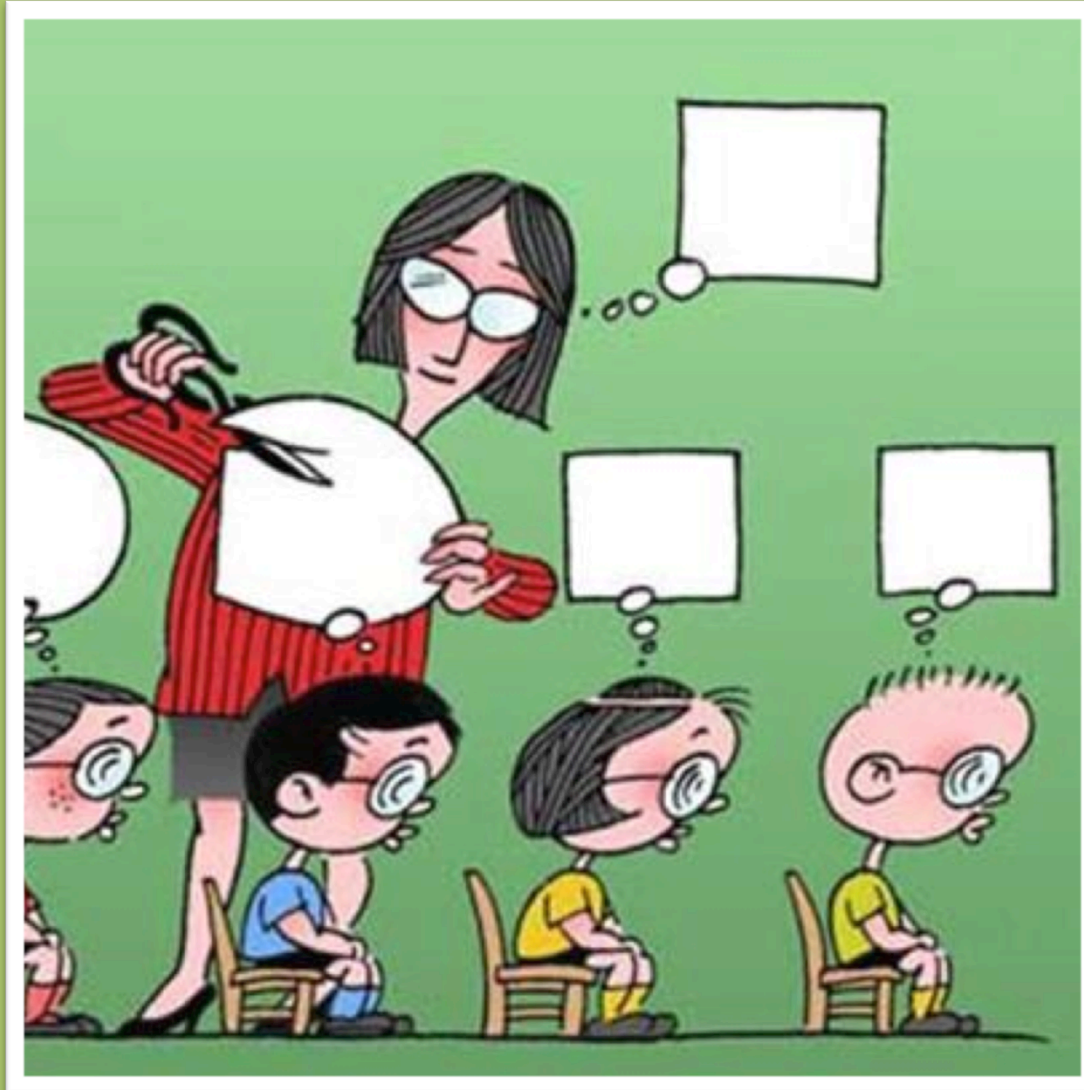
Don't build the "Homer Car"



Why Johnny Can't Pentest



Schools Shaping Our Thoughts



10.

When the
going gets
tough

Stolen Ideas Stolen Content

I'm Flattered ☺



Stolen Ideas Stolen Content

Saumil,

None of my business, but I would just let it be. Karma and all. He's digging a deep grave with that last post. Just let it be.

RT



KEEP
CALM
AND
KARMA
ON

...fool me twice
shame on me.

II.


On Stunts and Sensationalism

"If you can bear to hear
the truth you've spoken
Twisted by knaves
to make a trap for fools"



Rudyard
Kipling

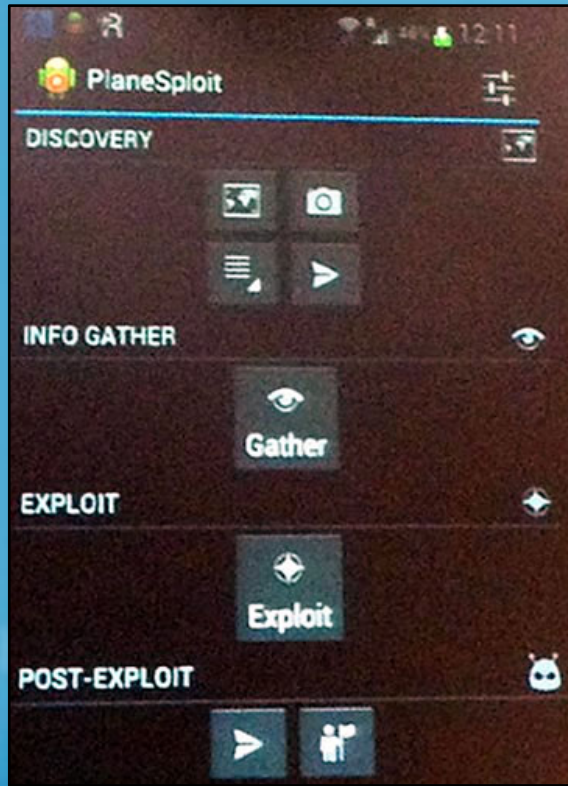
Media training is an OPSEC skill



Vet your journo.
"Off the record".
Answer in writing.
Putting words in
your mouth.
Stay on target.
Watch your mouth.

The Grugq
grugq.tumblr.com

HACKING A PLANE?



THERE'S AN APP FOR THAT!



INTERNATIONAL NEWS

SMARTPHONE APP CAN HIJACK PLANE GERMAN MAN DEMONSTRATED ON VIRTUAL PLANE

FORECASTS

FORT PIERCE

8AM

71°

PARTLY CLOUDY

5:09



"Preventing Security Theatre is OUR responsibility"

Andrea Barisani

No Such Con #1
Keynote

IT Security community
loses reputation

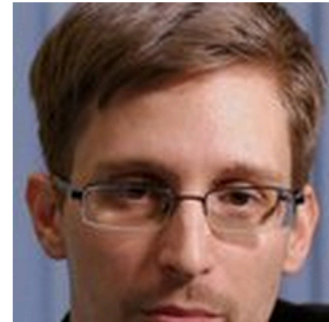
Remediation NOT given
to original researchers



The New York Times

Snowden Used Low-Cost Tool to Best N.S.A.

Intelligence officials say Edward J. Snowden used inexpensive and widely available software to “scrape” the N.S.A.’s networks, even though they were protected to withstand more sophisticated cyberat...



Marc Andreessen ✓

@pmarca

+ Follow

The gardener used a "lawn mower" to "mow" the lawn.

↩ Reply ↻ Retweet ★ Favorite ⋮ More



12.

On India and Cybersecurity



CAN
SEC
WEST

DARPA CFT

New way of working with people in a change-resistant organization.

Fresh thought, fresh talent.

Low overhead and investment.

Crowdsource. Catalyse.

Did not LOCK IN participants.



Mudge

Indigenous Cryptography

Military
Grade

Commercial
Grade

Trusted OS Initiative



The "Theo de Raadt" approach to OpenBSD.

Open Source.

Maintained, verified, updated and distributed.

13.

The Future

2010

DEP
bypassing
ROP code

Man in the
Browser

Political
Cyber
warfare

© CG4TV.com

A man with long, dark, wavy hair and a light beard is looking directly at the camera. He is holding a large, glowing crystal ball in his right hand. The crystal ball is illuminated from within, showing a bright orange and yellow light. The background is dark and out of focus, with some blurred lights visible.

2011

Browser Attacks

PDF Attacks

Web App Attacks

Social Engineering

A man with long, dark, wavy hair and a light beard is looking directly at the camera. He is holding a large, glowing, orange and red sphere in his hands. The background is dark and out of focus, with some bokeh lights.

2012

Full ASLR by 2014
Mobile Attacks
Real Time Analytics
Blurred boundaries
IPv6

2013

HTML5 Video
SVG
WebGL
Mobile Browsers



THE FUTURE
IS ALREADY HERE





REALTIME

Written and Directed by
ROELOF_TEMMINGH

Today: Realtime
acquisition, storage,
analysis and correlation
of ALL data.

Tomorrow: Predictions

I AM
BIG DATA!



RELAX-
I ONLY DETECT
PATTERNS.



AND IF YOU HAVE
NOTHING TO HIDE,
YOU HAVE NO
REASON TO WORRY.



DISC. BY TRISTYNE MEDIA SERVICES

www.bostonglobe.com/wasserman

BUT I DO LIKE
MY PRIVACY.



SO YOU WORRY
ABOUT IT?

YES

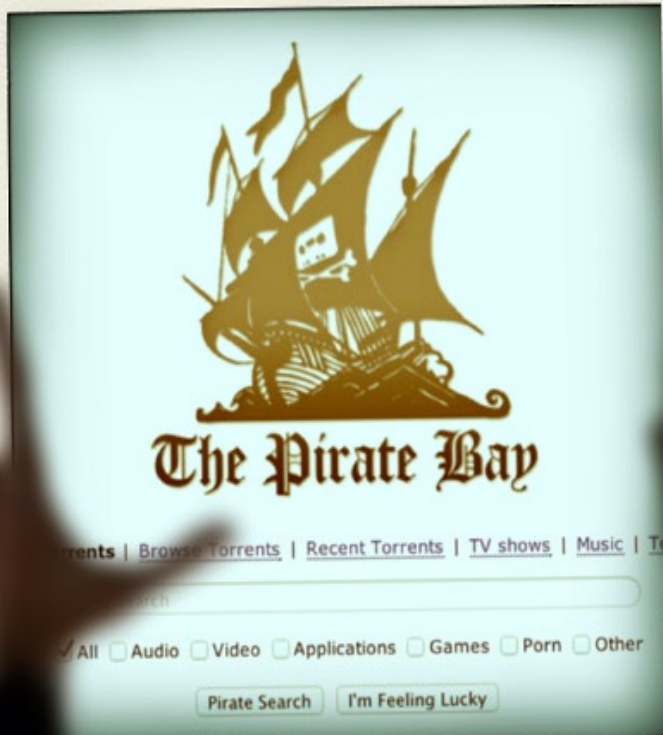


WASSERMAN © 6-13

I AM DETECTING
A PATTERN.



Will the Internet
remain a level
playing field?



Special Thanks

Haroon Meer & Marco Slaviero

Andrea Barisani

Roelof Temmingh

Alex Stamos

The Grugq

NULL & our fantastic community!

Further Reading

Con Collector

<http://cc.thinkst.com/>

The White Hat's Dilemma

<http://tinyurl.com/whitehatdilemma>

Realtime

<http://www.realtime-film.com/>

Media training – OPSEC for hackers

<http://tinyurl.com/opsecmedia1>

<http://tinyurl.com/opsecmedia2>

#NullCON 2014,
Goo

Thank You...
Questions?

saumil@net-square.com

@therealsaumil

