About: Me

@haroonmeer
haroon@thinkst.com

http://cc.thinkst.com/speaker/Meer/Haroon/timeline/
http://cc.thinkst.com/speaker/Meer/Haroon/timeline/
### Speaker: Dan Kaminsky [Speaker-Timeline] [Speaker-Links]

**Submit Patch For Speaker**

<table>
<thead>
<tr>
<th>Conference</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>CanSecWest-2011 - Canada- Vancouver</td>
<td>Showing How Security Has (And Hasn'T) Improved, After Ten Years Of Trying</td>
</tr>
<tr>
<td>Berlinsides-2010 - Berlin</td>
<td>Dankam : Augmented Reality For Color Blindness</td>
</tr>
<tr>
<td>Berlinsides-2010 - Berlin</td>
<td>Towards The Domain Key Infrastructure</td>
</tr>
<tr>
<td>Berlinsides-2010 - Berlin</td>
<td>Hacker Speed Debates</td>
</tr>
<tr>
<td>BlueHat-2010 - USA</td>
<td>The Unified Theory Of Dns Security</td>
</tr>
<tr>
<td>Blackhat-10 - USA</td>
<td>Black Ops Of Fundamental Defense: Web Edition</td>
</tr>
<tr>
<td>SANS Pen Test Summit-2010 - Baltimore-Usa</td>
<td>Keynote: Penetration Testing By Targeting The Soft Underbelly Of Infrastructure</td>
</tr>
<tr>
<td>SANS Pen Test Summit-2010 - Baltimore-Usa</td>
<td>Speaker Panel: Most Effective New Technique You Ve Applied In The Past 12 Months</td>
</tr>
<tr>
<td>QuahogCon-2010 - USA</td>
<td>Keynote - New Research Tba</td>
</tr>
<tr>
<td>Source Boston-2010 - USA</td>
<td>The Fine Art Of Hari Kari (J's), And Other Approaches For The Strange Reality Of Web Defense</td>
</tr>
<tr>
<td>Chaos Communication Congress-26 - Berlin</td>
<td>Black Ops Of Pki</td>
</tr>
<tr>
<td>Defcon-17 - USA</td>
<td>Something About Network Security</td>
</tr>
<tr>
<td>Defcon-17 - USA</td>
<td>Hello, My Name Is /Hostname/</td>
</tr>
<tr>
<td>Blackhat-09 - USA</td>
<td>Something About Network Security</td>
</tr>
<tr>
<td>Source Boston-2009 - USA</td>
<td>The Partial Disclosure Dilemma</td>
</tr>
<tr>
<td>Source Boston-2009 - USA</td>
<td>Lessons Learned: Limited, Targeted, Collaborative Disclosure And Multi-Organizational Cooperation</td>
</tr>
<tr>
<td>Chaos Communication Congress-25 - Berlin</td>
<td>Why Were We So Vulnerable To The Dns Vulnerability?</td>
</tr>
<tr>
<td>BlueHat-2008 - Microsoft corporate headquarters</td>
<td>Black Ops 2008 Â It's The End Of The Cache As We Know It</td>
</tr>
<tr>
<td>Defcon-16 - USA</td>
<td>Dns Goodness</td>
</tr>
<tr>
<td>Blackhat-08 - USA</td>
<td>Black Ops 2008 -- It's The End Of The Cache As We Know It</td>
</tr>
<tr>
<td>Chaos Communication Congress-24 - Berlin</td>
<td>Dns Rebinding And More Packet Tricks</td>
</tr>
<tr>
<td>Sector-2007 - Canada</td>
<td>Black Ops 2007: Dns Rebinding Attacks</td>
</tr>
<tr>
<td>BlueHat-2007 - Microsoft corporate headquarters</td>
<td>Black Ops 2007: Dns Rebinding Attacks</td>
</tr>
<tr>
<td>Blackhat-07 - USA</td>
<td>Black Ops 2007: Design Reviewing The Web</td>
</tr>
<tr>
<td>Shmoocon-2007 - Washington</td>
<td>Weaponizing Noam Chomsky, Or Hacking With Pattern Languages</td>
</tr>
<tr>
<td>Chaos Communication Congress-23 - Berlin</td>
<td>Black Ops 2006 Viv Edition</td>
</tr>
<tr>
<td>Defcon-16 - USA</td>
<td>Black Ops 2006</td>
</tr>
</tbody>
</table>

About: Dan

http://cc.thinkst.com/speaker/Kaminsky/Dan/timeline/
About: Me

@haroonmeer
http://blog.thinkst.com

http://cc.thinkst.com/speaker/Meer/Haroon/timeline/
About: You!

& Your Research
For || Against ?

Setec Astronomy
Setec Confer Moan (yo!)

Number of Industry Related InfoSec conferences in 1997 vs. Number of Industry Related Infosec conferences in 2010

The Established Conferences keep getting bigger...

At Least one InfoSec Conference is going on in any given month (with 19 in October alone!)

That means an infosec conference is taking place for 205/365 days of the year

http://blog.thinkst.com
For || Against?

YES!

http://blog.thinkst.com
For Good Research
What’s that?
Stuff we did the past year.
<past year>
Memory Corruption Bugs as a Percentage of Total Reported Bugs

http://cc.thinkst.com/folklore/
>
past year
</past year>
i’m obviously poorly qualified
Richard Hamming
``You and Your Research''

Transcription of the
Bell Communications Research Colloquium Seminar
7 March 1986

http://www.cs.virginia.edu/~robins/YouAndYourResearch.html
“I'm not talking about ordinary run-of-the-mill research; I'm talking about great research.”

... 

“I mean those kinds of things which we perceive are significant things.”
Now, how did I come to do this study?

... I saw I was a stooge.
I saw Feynman up close.
I saw Fermi and Teller.
I saw Oppenheimer.
I saw Hans Bethe.
I became very interested in the difference between those who do and those who might have done.
2 Paragraphs in...
ὁ δὲ ἀνεξέταστος βίος οὐ βιωτὸς ἀνθρώπῳ

- Socrates
I became very interested in the difference between those who do and those who might have done.
I continued examining the questions, “Why?” and “What is the difference?”
Wait.
Wasn’t he a mathematician?
I will talk mainly about science because that is what I have studied. But much of what I say applies to many fields. Outstanding work is characterized very much the same way in most fields,
I have to get you to drop modesty and say to yourself, “Yes, I would like to do first-class work.”
I find that the major objection is that people think great science is done by luck.
Well, consider Einstein. Note how many different things he did that were good. Was it all luck? Wasn't it a little too repetitive?
You see again and again, that it is more than one thing from a good person.
The Flaw at the Heart of the Internet

DAN KAMINSKY DISCOVERED A FUNDAMENTAL SECURITY PROBLEM IN THE INTERNET... AND NOT PEOPLe TO CARE IN TIME TO FIX IT. IT'S A DRAMATIC STORY WITH A HAPPY ENDING... BUT WE WERE LUCKY THIS TIME.

BY ERICA NAIGLE

D as Kaminsky, a characteristic, was not looking for a bug earlier this year when he happened upon a flaw at the core of the Internet. The security researcher, who has been instrumental in breaking down the Internet's defenses, was on the lookout for vulnerabilities. His expertise is in the Internet's domain name system (DNS), the protocol responsible for translating website addresses into human-readable URLs. Kaminsky was able to identify weaknesses in DNS, which can be exploited by malicious actors.

Kaminsky's expertise is in the Internet's domain name system (DNS), the protocol responsible for translating website addresses into human-readable URLs. This allows him to identify weaknesses in DNS, which can be exploited by malicious actors.

Normally, DNS is reliable but not immune. When a computer contact's a website, it sends a request to a DNS server to translate the website's address into an IP address, which is required to access the website. If the DNS server is compromised, it can be used to redirect users to malicious websites.

Kaminsky discovered a flaw in the way that DNS requests are handled. He found that if a DNS server receives a request for a domain name that it doesn't know how to resolve, it can be tricked into sending the request to another server. This is known as a DNS cache poisoning attack.

The flaw Kaminsky discovered is particularly dangerous because it allows an attacker to redirect users to websites that they wouldn't normally visit. For example, an attacker could use this flaw to redirect users to websites that are known to be malicious.

Kaminsky's discovery is significant because it highlights the importance of securing DNS. If DNS is not secure, attackers can use it to gain control of websites and steal sensitive information.

In the future, Kaminsky hopes that the Internet community will take his findings seriously and work to secure DNS. He believes that this is a critical step in protecting the Internet from further attacks.
“Luck favors the prepared mind”

The prepared mind sooner or later finds something important and does it.

So yes, it is luck. The particular thing you do is luck, but that you do something is not.
So what’s a key characteristic?
independent thoughts
+
the courage to pursue
them
Lot’s of Brains?

Great work is something else more than brains..
Bill Pfann & Clogston!
Once you get your courage up and believe that you can do important problems, then you can
Once you get your courage up and believe that you can do important problems, then you can
Once you get your courage up and believe that you can do important problems, then you can
Once you get your courage up and believe that you can do important problems, then you can
Once you get your courage up and believe that you can do important problems, then you can

You found that on Google?

Gaining awareness about “Google Hackers”
Johnny Long
johnny@ihackstuff.com
Once you get your courage up and believe that you can do important problems, then you can
Once you get your courage up and believe that you can do important problems, then you can
Age
Einstein did things very early, and all the quantum mechanic fellows were disgustingly young when they did their best work.
Wait? Are we too old?

**Lifetime Achievement Award**

Most hackers have the personality of a supermodel who does discrete mathematics for fun. Like mathematicians, hackers get off on solving very obscure and difficult to even explain problems. Like models, hackers wear a lot of black, think they are more famous than they are, and their career effectively ends at age 30. Either way, upon entering one's fourth decade, it is time to put down the disassembler and consider a relaxing job in management.

This award is to honor the previous achievements of those who have moved on to bigger and better things such as management or owning (in the traditional sense) a coffee shop.
On the other hand, in music, politics and literature, often what we consider their best work was done late. I don't know how whatever field you are in fits this scale, but age has some effect.
When you are famous it is hard to work on small problems. This is what did Shannon in. After information theory, what do you do for an encore?
PKCS #10 Certificate Signing Request

CertificateRequest
- Version
- Subject
- PublicKey
- Attributes

www.paypal.com\0 thoughtcrime.org

WHOIS Lookup

And contact... me!

Moxie Marlinspike
Institute For Disruptive Studies

Firstly, congrats on the new internship, it sounds like a wonderful opportunity for you and I'm sure you'll love working with Apple.

I have a few question for you if wouldn't mind answering them. Firstly, why did you choose to get involved in specifically the iPhone jailbreaking scene, what was it attracted you to the iPhone? Secondly, did you always set out to be a hacker or was it just something that interested you and found you had a knack for? Finally, in regards to the PDF bug used for the JailbreakMe.com jailbreak, where on earth did you get the brilliant idea for it?

Thanks for doing this AMA!

[comex]: comex
[-] Colonel_Ham_Sandwich 16 points 18 days ago

Firstly, why did you choose to get involved in specifically the iPhone jailbreaking scene, what was it attracted you to the iPhone?

I had one... and it was a device that (a) had a lot of functionality, (b) had a nice and flexible UNIX OS, (c) already had an active homebrew community, and (d) was really cool. :p

Secondly, did you always set out to be a hacker or was it just something that interested you and found you had a knack for?

I never wanted to be a black hat hacker, but I did enjoy hacking (originally SQL injection and crap) as a natural extension of programming.

Finally, in regards to the PDF bug used for the JailbreakMe.com jailbreak, where on earth did you get the brilliant idea for it?

FreeType was one of the less studied open source components of iOS.
So you need lot’s of free time!
This brings up the subject .. of working conditions. What most people think are the best working conditions, are not.
So what you need is..
Now for the matter of drive. You observe that most great scientists have tremendous drive.
Newton said:
“If others would think as hard as I did, then they would get similar results.”
thegruggq
tell them that drinking that much takes effort and dedication, you can't just start out as the life of the party, you have to work at it! :D
8 hours ago Delete
How can anybody my age know as much as John Tukey does?
“You would be surprised Hamming, how much you would know if you worked as hard as he did that many years”
Knowledge and productivity are like compound interest.
Knowledge and productivity are like compound interest.

The more you know, the more you learn; the more you learn, the more you can do; the more you can do, the more the opportunity
Given two people of approximately the same ability and one person who works ten percent more than the other, the latter will more than twice outproduce the former.
If you have found a bug, chances are that someone else has also. And chances also are that the person is @taviso.
taviso Tavis Ormandy
This crackme was really hard work...fun though.
http://www.crackmes.de/users/crp/trace_q/
13 Apr 10  Favorite  Retweet  Reply
So it’s a little bit hard?
Genius is 99% perspiration and 1% inspiration
Karate Kid Ruined Us!

It’s a lot hard!
It comes down to an emotional commitment. Most great scientists are completely committed to their problem. Those who don't become committed seldom produce outstanding, first-class work.
Everybody who has studied creativity is driven finally to saying:
“creativity comes out of your subconscious.”
Everybody who has studied creativity is driven finally to saying: “creativity comes out of your subconscious.”

http://www.youtube.com/watch?v=zGt3-fxOvug
Everybody who has studied creativity is driven finally to saying: “creativity comes out of your subconscious.”
Didn’t he ever rest?
Lunch with the Chemists..
What are the important problems of your field?
What important problems are you working on?
The average scientist, so far as I can make out, spends almost all his time working on problems which he believes will not be important and he also doesn't believe that they will lead to important problems.
Good & Bad Procrastination

http://www.paulgraham.com/procrastination.html
Great Thoughts Time.
When we win it's with small things, and the triumph itself makes us small.

What is extraordinary and eternal does not want to be bent by us.
Be Prepared..
Most great scientists know many important problems. They have something between 10 and 20 important problems for which they are looking for an attack. And when they see a new idea come up, one hears them say “Well that bears on this problem.”

They drop all the other things and get after it.
“a horror story”

“they came in second!”
What if I have to work on little problems?
I want to talk on another topic. It is based on the song which I think many of you know:

“It ain't what you do, it's the way that you do it.”
<table>
<thead>
<tr>
<th>Exploit Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>apache_chunked_win32</td>
<td>Apache Win32 Chunked Encoding</td>
</tr>
<tr>
<td>blackice_pam_icq</td>
<td>Blackice/RealSecure/Other ISS ICQ Parser Buffer Overflow</td>
</tr>
<tr>
<td>exchange2000_xexch50</td>
<td>Exchange 2000 MS03-46 Heap Overflow</td>
</tr>
<tr>
<td>frontpage_fp30reg_chunked</td>
<td>Frontpage fp30reg.d11 Chunked Encoding</td>
</tr>
<tr>
<td>ia_webmail</td>
<td>IA WebMail 3.x Buffer Overflow</td>
</tr>
<tr>
<td>iis50_nsisislog_post</td>
<td>IIS 5.0 nsisislog.dll POST Overflow</td>
</tr>
<tr>
<td>iis50_printer_overflow</td>
<td>IIS 5.0 Printer Buffer Overflow</td>
</tr>
<tr>
<td>iis50_webdav_ntdll</td>
<td>IIS 5.0 WebDav ntdll.dll Overflow</td>
</tr>
<tr>
<td>imail_lap</td>
<td>IMail LDAP Service Buffer Overflow</td>
</tr>
<tr>
<td>msrpc_dcom_ms03_026</td>
<td>Microsoft RPC DCOM MS03-026</td>
</tr>
<tr>
<td>mssql2000_resolution</td>
<td>MSSQL 2000 Resolution Overflow</td>
</tr>
<tr>
<td>pop3top_negative_read</td>
<td>PoPTop Negative Read Overflow</td>
</tr>
<tr>
<td>realserver_describe_linux</td>
<td>RealServer Describe Buffer Overflow</td>
</tr>
<tr>
<td>samba_trans2open</td>
<td>Samba trans2open Overflow</td>
</tr>
<tr>
<td>sambar6_search_results</td>
<td>Sambar 6 Search Results Buffer Overflow</td>
</tr>
<tr>
<td>servu_mdtm_overflow</td>
<td>Serv-U FTPD MDTM Overflow</td>
</tr>
<tr>
<td>solaris_sadmind_exec</td>
<td>Solaris sadmind Command Execution</td>
</tr>
<tr>
<td>upnp_winxp</td>
<td>Universal Plug N Play Overflow</td>
</tr>
<tr>
<td>warftpd_165_pass</td>
<td>War-FTPD 1.65 PASS Overflow</td>
</tr>
</tbody>
</table>
You should do your job in such a fashion that others can build on top of it, so they will indeed say, “Yes, I've stood on so and so's shoulders and I saw further.”
Metasploit Console v2.0 [19 exploits - 27 payloads]

`msf > show exploits`

**Metasploit Framework Loaded Exploits**

<table>
<thead>
<tr>
<th>Exploit</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>apache_chunked_win32</td>
<td>Apache Win32 Chunked Encoding</td>
</tr>
<tr>
<td>blackice_pam_icq</td>
<td>Blackice/RealSecure/Other ISS ICQ Parser Buffer Overflow</td>
</tr>
<tr>
<td>exchange2000_xexch50</td>
<td>Exchange 2000 MS03-46 Heap Overflow</td>
</tr>
<tr>
<td>frontpage_fp30reg_chunked</td>
<td>Frontpage fp30reg.dll Chunked Encoding</td>
</tr>
<tr>
<td>ia_webmail</td>
<td>IA WebMail 3.0 Buffer Overflow</td>
</tr>
<tr>
<td>iis50_nsiislog_post</td>
<td>IIS 5.0 nsiislog.dll POST Overflow</td>
</tr>
<tr>
<td>iis50_printer_overflow</td>
<td>IIS 5.0 Printer Buffer Overflow</td>
</tr>
<tr>
<td>iis50_webdav_ndll</td>
<td>IIS 5.0 WebDAV ndll.dll Overflow</td>
</tr>
<tr>
<td>imap_ldap</td>
<td>IMAP LDAP Service Buffer Overflow</td>
</tr>
<tr>
<td>msrpc_dcom_ms03_026</td>
<td>Microsoft RPC DCOM MS03-026</td>
</tr>
<tr>
<td>mssql2000_resolution</td>
<td>MSSQL 2000 Resolution Overflow</td>
</tr>
<tr>
<td>poptop_negative_read</td>
<td>Poptop Negative Read Overflow</td>
</tr>
<tr>
<td>realserver_describe_linux</td>
<td>RealServer Describe Buffer Overflow</td>
</tr>
<tr>
<td>samba_trans2open</td>
<td>Samba trans2open Overflow</td>
</tr>
<tr>
<td>sambar_search_results</td>
<td>Sambar 6 Search Results Buffer Overflow</td>
</tr>
<tr>
<td>servu_mdtm_overflow</td>
<td>Serv-U FTPD MDTM Overflow</td>
</tr>
<tr>
<td>solaris_sadmind_exec</td>
<td>Solaris sadmind Command Execution</td>
</tr>
<tr>
<td>upnp_winxp</td>
<td>Universal Plug N Play Overflow</td>
</tr>
<tr>
<td>warftpd_165_pass</td>
<td>War-FTPD 1.65 PASS Overflow</td>
</tr>
</tbody>
</table>

`msf > []`
It's very ugly; you shouldn't have to do it
I learned years ago that if you care what the public thinks about your research or ideas, you must do marketing. Sucks, but it's true.
it is not sufficient to do a job, you have to sell it.
Summary

- Work on important problems;
- Deny that it is all luck (pasteur)
- Great Thoughts
Is the effort .. worth it?
Absolutely..
The result is worth the struggle
.. because the truth is, **the value is in the struggle more than it is in the result.** The struggle to make something of yourself seems to be worthwhile in itself. The success and fame are sort of dividends, in my opinion.
so why do so many people, with all their talents, fail?
Well, one of the reasons is drive and commitment.
The people who do great work with less ability but who are committed to it, get more done than those who have great skill and dabble in it, who work during the day and go home and do other things and come back and work the next day.
You can lead a nice life; or you can be a great scientist.

If you want to lead a nice happy life with a lot of recreation and everything else, you'll lead a nice life.
The second thing is, I think, the problem of personality defects.
a .. personality defect is ego assertion..
and then most presciently..
Many a second-rate fellow gets caught up in some little twitting of the system, and carries it through to warfare.
self delusion..
There are so many alibis. Why weren't you first? Why didn't you do it right? Don't try an alibi. Don't try and kid yourself. You can tell other people all the alibis you want. I don't mind. But to yourself try to be honest.
you need to know yourself, your weaknesses, your strengths, and your bad faults, like my egotism.
Summary
(People don’t win because)

- Don’t work on important problems;
- Don’t become emotionally involved;
- Keep giving themselves alibis
- Keep saying “it’s luck”
I've told you how easy it is; furthermore I've told you how to reform. Therefore, go forth and become great.
Vragen?

http://blog.thinkst.com
@haroonmeer