You & Your Research

2012 - @haroonmeer
(haroon@thinkst.com)
About: Me

@haroonmeer
haroon@thinkst.com

http://cc.thinkst.com/speaker/Meer/Haroon/timeline/
http://cc.thinkst.com/speaker/Meer/Haroon/timeline/

http://cc.thinkst.com/
**Speaker:** Mr Felix (FX) Lindner

**[Speaker-Timeline]**  **[Speaker-Links]**

Submit Patch For Speaker

<table>
<thead>
<tr>
<th>Conference</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defcon-2012 - Las Vegas</td>
<td>Hacking [Redacted] Routers</td>
</tr>
<tr>
<td>BerlinSides-2012 - Berlin, Germany</td>
<td>Apple vs. Google Client Platforms</td>
</tr>
<tr>
<td>Atheta-2012 - Athens, Greece</td>
<td>&quot;Apple vs. Google Client Platforms&quot;</td>
</tr>
<tr>
<td>Blackhat Europe-2012 - Amsterdam, The Netherlands</td>
<td>Apple vs. Google Client Platforms</td>
</tr>
<tr>
<td>hashdays-2011 - Lucerne, Switzerland</td>
<td>Targeted Industrial Control System Attacks - Lessons from Stuxnet</td>
</tr>
<tr>
<td>Blackhat Europe-2011 - Barcelona, Spain</td>
<td>Building Custom Disassemblers</td>
</tr>
<tr>
<td>Blackhats-2010 - Berlin, Germany</td>
<td>Building Custom Disassemblers</td>
</tr>
<tr>
<td>Chaos Communication Congress-27 - Berlin, Germany</td>
<td>Building Custom Disassemblers</td>
</tr>
<tr>
<td>EC2ND-2010 - Germany</td>
<td>Keynote: On Hackers</td>
</tr>
<tr>
<td>DEF CON-18 - Las Vegas, USA</td>
<td>Blitzableiter - The Release</td>
</tr>
<tr>
<td>Blackhat USA-2010 - Las Vegas, USA</td>
<td>Blitzableiter - The Release</td>
</tr>
<tr>
<td>ITWeb Security Summit-2010 - Johannesburg, South Africa</td>
<td>Panel: The Ultimate Defence - Think Like A Hacker</td>
</tr>
<tr>
<td>ITWeb Security Summit-2010 - Johannesburg, South Africa</td>
<td>Security Is Easy, In Theory</td>
</tr>
<tr>
<td>Blackhat Europe-2010 - Barcelona, Spain</td>
<td>Defending The Poor</td>
</tr>
<tr>
<td>Chaos Communication Congress-26 - Berlin, Germany</td>
<td>Defending The Poor</td>
</tr>
<tr>
<td>CONFidence -2009 - Krakow, Poland</td>
<td>Developments In Cisco Ios Forensics</td>
</tr>
<tr>
<td>DEF CON-17 - Las Vegas, USA</td>
<td>Router Exploitation</td>
</tr>
<tr>
<td>Blackhat USA-2009 - Las Vegas, USA</td>
<td>Router Exploitation</td>
</tr>
</tbody>
</table>

http://cc.thinkst.com/speaker/Lindner/Felix/
About: FX

http://cc.thinkst.com/speaker/Lindner/Felix/timeline/
About: FX

http://cc.thinkst.com/speaker/Lindner/Felix/timeline/
About: FX

http://cc.thinkst.com/speaker/Bratus/Sergey/links
About: Me

http://blog.thinkst.com
@haroonmeer

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

& Your Research
For || Against

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
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!
For Good Research
What’s that?
Stuff we did the past 2 years...

<past 2 years>
Penetration Testing Considered Harmful
(haroon@thinkus.com)

PENETRATION TESTING CONSIDERED HARMFUL
44CON 2011
HAROON MEER
i’m 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 GOT 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 NAYONE

D ank Kaminsky, an archetypal hacker, was not looking for trouble when he discovered a flaw in the core of the Internet. The security researcher was using his knowledge of Internet infrastructure to come up with a better way to stream video to users. Kaminsky's expertise is in the Internet's domain name system (DNS), the protocol responsible for matching websites' URLs with the numeric addresses of the servers that host them. The same could be said for multiple servers with several addresses, and Kaminsky thought he had a great trick for directing users to the servers best able to handle their requests at any given moment.

Normally, DNS is reliable but not nimble. When a computer—say, a server that helps direct traffic across Comcast's network—requests the numeric address associated with a given URL, it stores the answer for a period of time known as "time to live," which can range anywhere from seconds to days. This helps to reduce the number of queries the server makes. Kaminsky's idea was to bypass the time to live, allowing the server to get a fresh answer every time it wanted to know a site's address. Consequently, traffic on Comcast's network would be sent to the optimal address at every moment, rather than to whatever address had already been stored. Kaminsky was sure that the strategy could significantly speed up content distribution.

It was only later, after talking casually about the idea with a friend, that Kaminsky realized his "trick" could completely break the security of the domain name system and, therefore, of the Internet itself. The time to live, it turns out, was at the core of DNS security: being able to bypass it allowed for a wide variety of attacks. Kaminsky wrote a little code to make sure the situation was as bad as he thought it was. "Once I saw it work, my stomach dropped," he says. "I thought, 'What the heck am I going to do about this? This affects everyone.'"

Kaminsky's tool began to flood Web servers with any Web page an attacker chose. The most obvious use was to send people to phishing sites (websites designed to trick people into entering banking passwords and other personal information, allowing an attacker to steal their identities) or other fake versions of Web pages. But the danger is even worse: programs such as those used to deliver e-mail or for secure communications over the Internet ultimately rely on DNS. A cooperative attacker could use Kaminsky's technique to intercept sensitive e-mail, or to create forged versions of the certificates that ensure secure transactions between users and banking websites. "Every day I find another domain," Kaminsky says. "Another thing falls over if DNS is bad... I mean, literally, you look around and see anything that's using a network—anything that's using a network—and it's probably using DNS."

Kaminsky called Paul Vixie, president of the Internet Systems Consortium, a nonprofit corporation that supports several aspects of Internet infrastructure, including the software most commonly used in the domain name system. "Usually, if somebody wants to report a problem, you expect that it's going to take a fair amount of time for them to explain it: maybe a whiteboard, maybe a Word document or two," Vixie says. "In this case, it took 30 seconds for him to explain the problem, and another 20 seconds for him to answer my objections. After that, I said, 'Okay, I am speaking to you over an unsecured cell phone. Please do not ever say to anyone what you just said to me over an unsecured cell phone again.'"

Perhaps more frightening was that because the vulnerability was not located in any particular hardware or software but in the design of the DNS protocol itself, it wasn't clear how to fix it. In secret, Kaminsky and Vixie gathered together some of the top DNS experts in the world from people from the U.S. government and
“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

Exploit Writing Tutorials
- Universal DEP/ASLR bypass with msvcr71.dll and mona.py
- Hack Notes: Ropping eggs for breakfast
- Exploit writing tutorial part 3: SEH Based Exploits - just another example
- Exploit writing tutorial part 3: SEH Based Exploits
- Exploit writing tutorial part 2: Stack Based Overflows - jumping to shellcode
- Exploit writing tutorial part 1: Stack Based Overflows

Exploits
- Metasploit Bounty – The Good, the Bad and the Ugly
- Universal DEP/ASLR bypass with msvcr71.dll and mona.py
- Hack Notes: Ropping eggs for breakfast
- Fuzzing with Metasploit: Simple FTP fuzzing
- Exploit writing tutorial part 6: Bypassing Stack Cookies, SafeSEH, SEHOP, HW DEP and ASLR
- Exploit writing tutorial part 5: How debugger modules & plugins can speed up basic exploit development
- Exploit writing tutorial part 4: From Exploit to Metasploit - The basics
- Exploit writing tutorial part 3b: SEH Based Exploits -
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
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 questions for you if you 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 you 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!

Secondly, did you always set out to be a hacker or was it just something that interested you and you 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.”
thegruqq

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.
This crackme was really hard work...fun though.
http://www.crackmes.de/users/crp/trace_q/
13 Apr 10    Favorite  t→ 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-fx0vug
Everybody who has studied creativity is driven finally to saying: “creativity comes out of your subconscious.”

http://www.paulgraham.com/top.html
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
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.”
msf > show exploits

Metasploit Framework Loaded Exploits

<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.d1l Chunked Encoding</td>
</tr>
<tr>
<td>ia_webmail</td>
<td>I.A WebMail 3.x 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_ntdll</td>
<td>IIS 5.0 WebDAV ntdll.dll Overlay</td>
</tr>
<tr>
<td>imail_ldap</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>pop3pop_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
v2.0

+    [ msfconsole v2.0 [19 exploits - 27 payloads]
msf > show exploits

Metasploit Framework Loaded Exploits
======================================

apache_chunked_win32  Apache Win32 Chunked Encoding
blackice_pam_icq       Blackice/RealSecure/Other ISS ICQ Parser Buffer Overflow
exchange2000_xexch50   Exchange 2000 MS03-46 Heap Overflow
frontpage_fp30reg_chunked Frontpage fp30reg.dll Chunked Encoding
ia_webmail             I.A WebMail 3.x Buffer Overflow
iis50_nsiislog_post    IIS 5.0 nsiislog.dll POST Overflow
iis50_printer_overflow IIS 5.0 Printer Buffer Overflow
iis50_webdav_ntdll     IIS 5.0 WebDAV ntdll.dll Overflow
imail ldap             IMail LDAP Service Buffer Overflow
msrpc_dcom_ms03_026    Microsoft RPC DCOM MS03-026
mssql2000_resolution   MSSQL 2000 Resolution Overflow
pop3top_negative_read  PoPTop Negative Read Overflow
realserver_describe_linux RealServer Describe Buffer Overflow
samba_trans2open       Samba trans2open Overflow
sambab_search_results  Sambar 6 Search Results Buffer Overflow
servu_mtdm_overflow    Serv-U FTPD MDTM Overflow
solaris_sadmind_exec   Solaris sadmind Command Execution
upnp_winxp             Universal Plug N Play Overflow
warftpd_165_pass       War-FTPD 1.65 PASS Overflow

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.

10 Aug 10
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 that 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.
Questions?

http://blog.thinkst.com
@haroonmeer

www.cs.virginia.edu/~robins/YouAndYourResearch.html