THANKS!
haroon meer
@haroonmeer
What's with the cheesy title?
THE HARD THING ABOUT HARD THINGS

Building a Business When There Are No Easy Answers

BEN HOROWITZ

thinkst applied research
Saumil Shah @therealsaumil · Mar 30
@haroonmeer's #Troopers15 Keynote: "The hard thing about the hard things" - recommended weekend enlightenment!

Frank Koehntopp @koehntopp · Mar 28
Watching @haroonmeer 's talk at @WEareTROOPERS 2015 - awesome. youtube.com/watch?v=rarpym...

David Barroso @lostinsecurity · Mar 30
Recommended presentation of the day: @haroonmeer keynote at @WEareTROOPERS youtube.com/watch?v=rarpym...

mimeframe @mimeframe · Mar 28
Well, @haroonmeer delivered another awesome talk: youtube.com/watch?v=rarpym...

Daniel Hauenstein @dhauenstein · Mar 30
Good keynote at @WEareTROOPERS by @haroonmeer. Watch it. Now. All of it. youtube.com/watch?v=rarpym...

Julian Cohen @HockeyInJune · Apr 3
Haroon Meer tackles every major problem in the information security industry in under an hour. youtube.com/watch?v=rarpym...

the grugg @thegrugq · Mar 29
Go watch @haroonmeer say smart things. youtube.com/watch?v=rarpym...
but.. before we go on
Is this even a problem?
Global Commission
on Internet Governance

Global Cyberspace Is Safer than You Think: Real Trends in Cybercrime

Eric Jardine

PAPER SERIES: NO. 16 — JULY 2015

https://www.cigionline.org/sites/default/files/no16_web_1.pdf
“This paper argues that the level of security in cyberspace is actually far better than the picture described by media accounts and IT security reports.”

https://www.cigionline.org/sites/default/files/no16_web_1.pdf
"Our Cyber Security Status is Grim (and the way ahead will be hard)"
“Your cyber systems continue to function and serve you not due to the expertise of your security staff but solely due to the sufferance of your opponents.”"
“Our upcoming security apocalypse”

“a crisis of confidence”

“a simple litmus test”
“...imagine the highest value individual at your corporation”
“Can you stop a determined attacker from compromising him?”
“how ineffectual can we be?”

“For the thousands your organization spends on security, you can't protect the one guy who is most valuable to you. Worse yet, would you even know if he was popped?”

“This problem compounds, because the company boards are now increasingly aware of the Infosec problem.”

“but they are making the logical assumption that the teams of people they are paying, have the problem under control.”
“They don't know that we don't have the answers yet, that many of us are resorting to hope as a strategy, hoping desperately that when the breach eventually happens, it won't happen on our watch”
We are already there
“it’s just not evenly distributed yet”
its going to get worse...
Why?
“Courage is contagious”
Welcome to the home of the NSA Playset.

In the coming months and beyond, we will release a series of dead simple, easy to use tools to enable the next generation of security researchers. We, the security community have learned a lot in the past couple decades, yet the general public is still ill equipped to deal with real threats that face them every day, and ill informed as to what is possible.

Inspired by the NSA ANT catalog, we hope the NSA Playset will make cutting edge security tools more accessible, easier to understand, and harder to forget. Now you can play along with the NSA!


If you feel like you can contribute, please join the discussion here:

https://groups.google.com/forum/#!forum/nsaplayset

Check out Mike's HITB2014 talk here:

Complexity
It’s not a new realisation..
A Plea for Simplicity

You can't secure what you don't understand.

Bruce Schneier

*Information Security*

November 19, 1999

Ask any 21 experts to predict the future, and they're likely to point in 21 different directions. But whatever the future holds--IP everywhere, smart cards everywhere, video everywhere, Internet commerce everywhere, wireless everywhere, agents everywhere, AI everywhere, *everything* everywhere--the one thing you can be sure of is that it will be complex. For consumers, this is great. For security professionals, this is terrifying. The worst enemy of security is complexity. This has been true since the beginning of computers, and it's likely to be true for the foreseeable future.

We all know the amount of testing that goes into any major software product, and we all know the
epidemic of macro viruses shows that Microsoft Word and Excel need to be secure too. Rogue printer drivers can compromise Windows NT. Malicious attachments can tunnel through firewalls. Maintenance ports on routers can compromise networks, as can random modems. DSL and satellite modems can completely compromise security. So can Java or Microsoft Outlook. Or your recycling bin.

The networks of the future will be necessarily more complex, and therefore less secure. The technology industry is driven by the demand for features, for options, for speed. There are no standards for quality or security, and there is no liability for insecure software. Hence, there is no economic incentive to build in high quality. In fact, it's just the opposite. There is an economic incentive to create the lowest quality the market will bear. Unless customers demand higher quality and better security, this will never change.

I see two alternatives. The first is to recognize that the digital world will be one of ever-expanding features and options, of ever-faster product releases, of ever-increasing complexity and of ever-decreasing security. This is the world we have today, and we can decide to embrace it knowingly.

The other choice is to slow down, simplify and try to add security. Customers won't demand this--the issues are too complex for them to understand--so a consumer advocacy group is required. This solution might not be economically viable for the Internet, but it is the only way to get security.

BRUCE SCHNEIER is CTO of Counterpane Internet Security Inc., a company trying to bring managed security solutions to complex networks. He writes the CryptoRhythms column for Information Security, and is the author of Applied Cryptography and the Blowfish and Twofish encryption algorithms.
Linux Kernel (1991)
10,239 (loc)
In a Nutshell, Linux Kernel...

... has had \textit{612,828} commits made by \textit{14,884} contributors representing \textit{18,256,560} lines of code

... is mostly written in \texttt{C}
  with an average number of source code comments

... has a well established, mature codebase
  maintained by a very large development team
  with stable Y-O-Y commits

... took an estimated \textit{5,951} years of effort (COCOMO model)
  starting with its first commit in February, 2002
  ending with its most recent commit 3 days ago
Turns out almost every high-end DP/3D/4K screen out there has a 150 MHz x86 running inside with USB, LAN & more.

https://twitter.com/aionescu/status/615379928305963008
What Do WebLogic, WebSphere, JBoss, Jenkins, OpenNMS, and Your Application Have in Common? This Vulnerability.

By @breenmachine

Marshalling Pickles

how deserializing objects can ruin your day

Gabriel Lawrence (@gebl) and Chris Frohoff (@frohoff)

http://www.slideshare.net/frohoff1/appseccali-2015-marshalling-pickles
“the Bob Ippolito Problem”
How is access Controlled?

- Python - PyPI - Static username/password (can be stored in .pypirc)
- Ruby - Rubygems - Static username/password (API key stored in .gem/credentials)
- JavaScript - npm - Static username/password (stored in .npmrc, base64 encoded)
- PHP - packagist - Static username/password (auto-updates from repository)
- .NET - NuGet - Static username/password or API Key.

You get the picture

simplejson 3.8.1

Simple, fast, extensible JSON encoder/decoder for Python

simplejson is a simple, fast, complete, correct and extensible JSON
<http://json.org> encoder and decoder for Python 2.5+ and Python 3.3+. It is
pure Python code with no dependencies, but includes an optional C extension
for a serious speed boost.

The latest documentation for simplejson can be read online here: http://simplejson.readthedocs.org/

simplejson is the externally maintained development version of the json library included with Python 2.6 and Python
3.0, but maintains backwards compatibility with Python 2.5.

The encoder can be specialized to provide serialization in any kind of situation, without any special support by the
objects to be serialized (somewhat like pickle). This is best done with the default kwarg to dumps.

For those of you that have legacy systems to maintain, there is a very old fork of simplejson in the python2.2 branch
that supports Python 2.2. This is based off of a very old version of simplejson, is not maintained, and should only be
used as a last resort.

<table>
<thead>
<tr>
<th>File</th>
<th>Type</th>
<th>Py Version</th>
<th>Uploaded on</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>simplejson-3.8.1.tar.gz (md5, pgp)</td>
<td>Source</td>
<td></td>
<td>2015-10-27</td>
<td>74KB</td>
</tr>
</tbody>
</table>

Downloads (All Versions):
628018 downloads in the last day
4803859 downloads in the last week
17828268 downloads in the last month

Author: Bob Ippolito
For those of you that have legacy systems to maintain, there is a very old fork of simplejson in the python2.2 branch that supports Python 2.2. This is based off of a very old version of simplejson, is not maintained, and should only be used as a last resort.

**Downloads (All Versions):**
- 628018 downloads in the last day
- 4803859 downloads in the last week
- 17828268 downloads in the last month

**Author:** Bob Ippolito

specialized to post-process JSON objects with the object_hook or object_pairs_hook kwargs. This is particularly useful for implementing protocols such as JSON-RPC that have a richer type system than JSON itself.

For those of you that have legacy systems to maintain, there is a very old fork of simplejson in the python2.2 branch that supports Python 2.2. This is based off of a very old version of simplejson, is not maintained, and should only be used as a last resort.
“In a composite system there is no critical gate, everything is a gate”

We are in bad shape; It’s going to get much worse.. and..
Most enterprises are not safe

- Big Banks + other FIs
- Defense Industrial Base
- Oil and Gas
- Critical Infrastructure
- Big Tech
- Some Retail

```
FORTUNE
500
```

```
“SECURE 100”
```

```
“TOASTED 400”
```

```
Everybody Else
```

https://www.youtube.com/watch?v=-lkZMnIRuel
We've been begging people to care about security for 30 years.

Now they do, and we aren't giving them actionable advice.
Serious Question:

How many networks have you seen, where if I broke in, I wouldn't be able to own/laterally move/persist like it was 2003?
What have we been doing for the past 15 years?
We wanted to make a difference?
“At least we are doing something!”

(thats better than nothing, right?)
“Wrong! Peddling hard in the wrong direction doesn’t help just because you want it to”

http://blog.thinkst.com/2013/01/your-companies-security-posture-is.html
“If you want something new, you have to stop doing something old.”

- Peter Drucker
"We spend a lot of time helping Leaders learn what to do. We don't spend enough time helping them learn what to stop."
The 20 Habits that hold us Back

1) ...
2) ...
3) Passing Judgement
4) Making Destructive Comments
5) Starting with “No”, “But”, “However”
6) Telling the world how smart we are
7) Speaking when angry
8) Negativity, or “let me explain why that won’t work”
9) ...
10) ...
The 20 Habits that hold us Back

10) …
11) Claiming credit we don't deserve
12) Making excuses
13) Clinging to the past
14) …
15) …
16) Not Listening
17) …
18) …
19) Passing the buck
20) …
Security Anti-Patterns
Anti-pattern

From Wikipedia, the free encyclopedia

An anti-pattern (or antipattern) is a common response to a recurring problem that is usually ineffective and risks being highly counterproductive.[1][2] The term, coined in 1995 by Andrew Koenig,[3] was inspired by a book, Design Patterns, which highlights a number of design patterns in software development that its authors considered to be highly reliable and effective.
Taken some wrong turns;
Developed some bad habits;
Missing some opportunities.
Penetration Testing
Penetration Testing Considered Harmful

(haroon@thinkst.com)

PENETRATION TESTING CONSIDERED HARMFUL
44CON 2011
HAROON MEER

https://www.youtube.com/watch?v=GvX52HPAfBk
Web browsers are a constant target for attack.
When last have you used one on a pen-test?
These days we just simulate other pen-testers..

https://www.youtube.com/watch?v=GvX52HPAfBk
This is a classic example of “Draining the Swamp”

https://www.youtube.com/watch?v=GvX52HPAfBk
Possible to be perfectly pleased, perfectly pwned, and still be perfectly pwnable!
• It’s easy (these days) to sell;
• It feels like we are doing something;
• It delivers a result.
(even if its a questionable one)
how do we define risk in an org?
Deloitte Managers Made Huge $400,000+ Salaries, Hacked Documents Show

Julie Bort 攸 _GB
Dec. 3, 2014, 9:40 PM 3,014

how do we define risk in an org?
<table>
<thead>
<tr>
<th>Company</th>
<th>Year (Year)</th>
<th>Affected Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANTHEM</td>
<td>2015</td>
<td>80 million customers</td>
</tr>
<tr>
<td>JPMORGAN CHASE</td>
<td>2014</td>
<td>76 million households</td>
</tr>
<tr>
<td>TARGET</td>
<td>2014</td>
<td>70 million individuals</td>
</tr>
<tr>
<td>HOME DEPOT</td>
<td>2014</td>
<td>56 million customers</td>
</tr>
<tr>
<td>DEPT. OF VETERAN AFFAIRS</td>
<td>2006</td>
<td>26.5 million veterans</td>
</tr>
<tr>
<td>OPM</td>
<td>2015</td>
<td>4 million current and former employees (est.)</td>
</tr>
<tr>
<td>POSTAL SERVICE</td>
<td>2014</td>
<td>800,000 individuals</td>
</tr>
<tr>
<td>KEYPOINT</td>
<td>2014</td>
<td>48,000 current and former employees</td>
</tr>
<tr>
<td>SONY PICTURES</td>
<td>2014</td>
<td>47,000 current and former employees</td>
</tr>
<tr>
<td>USIS</td>
<td>2014</td>
<td>27,000 current and former employees</td>
</tr>
<tr>
<td>Company</td>
<td>Date</td>
<td>Number Affected</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>ANTHEM</td>
<td>2015</td>
<td>80 million customers</td>
</tr>
<tr>
<td>JPMORGAN CHASE</td>
<td>2014</td>
<td>76 million households</td>
</tr>
<tr>
<td>TARGET</td>
<td>2014</td>
<td>70 million individuals</td>
</tr>
<tr>
<td>HOME DEPOT</td>
<td>2014</td>
<td>56 million customers</td>
</tr>
<tr>
<td>DEPT. OF VETERAN AFFAIRS</td>
<td>2006</td>
<td>26.5 million veterans</td>
</tr>
<tr>
<td>OPM</td>
<td>2015</td>
<td>4 million current and former employees (est.)</td>
</tr>
<tr>
<td>POSTAL SERVICE</td>
<td>2014</td>
<td>800,000 individuals</td>
</tr>
<tr>
<td>KEYPOINT</td>
<td>2014</td>
<td>48,000 current and former employees</td>
</tr>
<tr>
<td>SONY PICTURES</td>
<td>2014</td>
<td>47,000 current and former employees</td>
</tr>
<tr>
<td>USIS</td>
<td>2014</td>
<td>27,000 current and former employees</td>
</tr>
</tbody>
</table>

HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM - DEMOCRATS
Threat Intelligence & Information Sharing
“Consider STUXNET, EquationGroup, These intrusion sets and countless others from sophisticated adversaries. One of their defining characteristics is the fact that they are stealthy, they evade detection. Until written about, they are virtually undetectable, because they bypass traditional defences.”
“We need pervasive and true visibility into our enterprise environments. These aren't nice to haves.. They are foundational, core requirements for any modern security program”

“If you don't have that level of security, you are only pretending to do security”
“threat intelligence.. another core requirement”
“so analysts can mostly quickly respond and identify those threats that matter most to the organisation"
Perfectly Typical
Some of the contractors that have helped OPM with managing internal data have had security issues of their own—including potentially giving foreign governments direct access to data long before the recent reported breaches. A consultant who did some work with a company contracted by OPM to manage personnel records for a number of agencies told Ars that he found the Unix systems administrator for the project "was in Argentina and his co-worker was physically located in the [People's Republic of China]. Both had direct access to every row of data in every database: they were root. Another team that worked with these databases had at its head two team members with PRC passports. I know that because I challenged them personally and revoked their privileges. From my perspective, OPM compromised this information more than three years ago and my take on the current breach is 'so what's new?'"
But what’s wrong with learning about malicious activity on other networks in near real time?
Before near-real-time learning.. how about 6-year old learning?
If you're planning on buying something you heard about from #RSAC, don't. Take that money, hire some smart engineers, and listen to them.
Most enterprises are not safe

- Big Banks + other FIs
- Defense Industrial Base
- Oil and Gas
- Critical Infrastructure
- Big Tech
- Some Retail

What are they missing?
- Secure software engineering
- Engineering focused IR
- Ability to create, not buy, solutions

https://www.youtube.com/watch?v=-IkJZMnRuel
“Can’t we just use consultants?”
You can’t outsource your thinking!
“Understand your prize jewels”
Cargo Cult Science
Cargo Cult Security
Taken some wrong turns;
Developed some bad habits;
Missing some opportunities.
“it’s not perfect, throw it out!”
Enhanced Mitigation Experience Toolkit
Bring back the Honeypots
{marco|haroon|azhar}@thinkst.com

“network utopia”
“Want Complex, Need Simple”
become super contrarian
Security as a Enabler

- Assisting teams to do their new crazy ideas - securely
- Chase solutions to difficult challenges
  - If your security engineers don't like hard problems and novel solutions you have the wrong ones
- **Incentivises** proactive engagement with Security

Etsy  @iodboi
If Security introduces blocking to the org, it will be ignored, not embraced
Security as a Blocker

- Lazy and plain ‘bad’ security teams default to blocking
- Blocking makes Security a NOP in the CD world
- You will be ignored and teams will work around you
- No’s are a Finite Resource - use them wisely

Etsy  @iodboi
Enterprise obstacles
ex·cuse

verb
3rd person present: excuses
/ɪkˈskjuːz/  

1. attempt to lessen the blame attaching to (a fault or offense); seek to defend or justify.
   "he did nothing to hide or excuse Jacob's cruelty"
   synonyms: justify, defend, condone, vindicate;  More

2. release (someone) from a duty or requirement.
   "it will not be possible to excuse you from jury duty"
   synonyms: let off, release, relieve, exempt, absolve, free
   "she has been excused from her duties"

noun
plural noun: excuses
/ɪkˈskjuːzɪz/

1. a reason or explanation put forward to defend or justify a fault or offense.
   "there can be no possible excuse for any further delay"
   synonyms: justification, defense, reason, explanation, mitigating circumstances, mitigation, vindication
   "that's no excuse for stealing"
The honest question I have is: How can an industry that so prides itself on social engineering, also claim that "management don't get it"?
If I had a dollar for everytime I got distracted, I wish I had some ice cream.
Disclosure Debates
ARE YOU COMING TO BED?

I CAN'T. THIS IS IMPORTANT.

WHAT?

SOMEONE IS WRONG ON THE INTERNET.
MEET ‘PROJECT ZERO,’ GOOGLE’S SECRET TEAM OF BUG-HUNTING HACKERS
It would seem that most criticisms of eEye are not based on fact, but are rooted in a dislike of their brash style, in-your-face advisories, and choice of hair coloring.

focus on exploits / 0day
2 0-days away from the worst day of your life?
Golden Rule / 0-day rule
“Conferences”
A Talk about Talks

thinkst applied research

{haroon|marco}@thinkst.com

44CON 2013
HTTP://44CON.COM
@44CON

https://www.youtube.com/watch?v=BlVjdUkrSFY
Chess Vs. Poker

Or: why we’re playing the wrong game

Jacob Torrey

Cyber-security Philosopher and Boffin

http://blog.jacobtorrey.com/chess-vs-poker
As the gap between the chess players and poker players grows, our contributions to the field become increasingly relevant to the majority population of the Internet and we risk becoming a marginalized group, even though we are the most capable to help raise the bar for everyone.
BeyondCorp
BeyondCorp
A New Approach to Enterprise Security

RORY WARD AND BETSY BEYER

(Note: The text is not visible in the image.)

“Researcher” count?
Alan Kay, 2015: Power of Simplicity

https://www.youtube.com/watch?v=NdSD07U5uBs
“9 1/2” Inventions

25 Researchers ~ 5 Years

~$12M/year in today's dollars

$30+ Trillion Dollars and counting

Personal Computer
GUI
WYSIWYG&DTP
Real OOP

Bit-Map Screens

Laser Printer

Postscript type
Bitmap type

Ethernet

Peer-Peer
(& Client-Server)

~ 50% of
Internet
Taken some wrong turns;
Developed some bad habits;
Missing some opportunities.
Re-examine old "truths"
Cheap Hacks Win
Most enterprises are not safe

- Big Banks + other FIs
- Defense Industrial Base
- Oil and Gas
- Critical Infrastructure
- Big Tech
- Some Retail

Everybody Else

What are they missing?
- Secure software engineering
- Engineering focused IR
- Ability to create, not buy, solutions
nobody owns the enterprise security problem
but it’s hard...
but it’s hard...

hard to go from “script.pl” to a shipping product..
but it’s hard...

hard to go from “always right consultant” to “vendor”
but come on..
So.. in Summary
• We are at an important inflection point
• We simultaneously face a crisis of relevance and a crisis of confidence
• Our current trajectory leads to disaster
Step one is to simply acknowledge this
If you are a Defender
Make sure what you are aiming at matters;
No therapeutic difference
If you are an attacker
Realise that there's a bunch of interesting hacks waiting to be pulled off playing Defense!
If you are an Researcher
We need you to show up and choose a side.
throw your hat into the ring..
THANK YOU