

Try Harder 2 Be Yourself

Individuality is Key

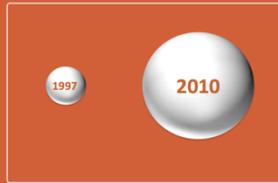
Phenoelit

Why Do We Hack?

Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%

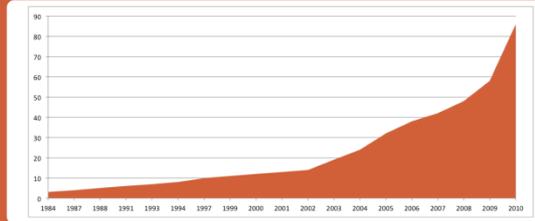
- 00000
- 00010 ■ It used to be all about curiosity
- 00020
- 00030 ■ Access to rare stuff
- 00040
- 00050 ■ “How the fuck did he do that?”
- 00060
- 00070 ■ “I wonder if I could ...?”
- 00080
- 00090 ■ Also: getting vendors to move
- 000A0
- 000B0 ■ Today’s reasons are different
- 000C0
- 000D0 ■ Publicity + career points
- 000E0
- 000F0 ■ Bug bounty programs
- 00100
- 00110 ■ Exploit sales
- 00120
- 00130 ■ Hacktivism
- 00140
- 00150 ■ Speaking at conferences
- 00160

Setec Astronomy Setec Confer Moan (yo!..)



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

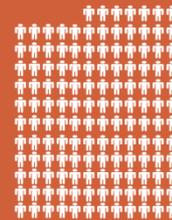
Number of Conferences per year (1984-2010)



The Established Conferences keep getting bigger...



Speakers (BlackHat 1997)



Speakers (BlackHat 2010)

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



Why Do We Go To Conferences?

```
Text View: K:\KEYNOTE.EXE          Col 0          270,650 Bytes          0%
00000  ■ Commonly cited reasons:
00010  ■ “To meet other like-minded people”
00020  ■ “Meet old friends”
00030  ■ “Meet new people”
00040  ■ Actual reasons:
00050  ■ “I like alcohol and 0day!”
00060  ■ “I’m getting paid to talk to those people
00070  that like alcohol and zero day.”
00080  ■ Essentially, we ask to be influenced
00090  ■ That’s a good thing!
00100  ■ self-reflection
00110  ■ Respect
00120  ■ Learning
00130
00140
00150
00160
1Help  2Unwrap  3  4ASCII  5  6  7Search  8Viewer  9Print  10Quit
```

What Speaking Means (to me)

Text View: K:\KEYNOTE.EXE

Col 0

270,650 Bytes

0%

00000
00010
00020
00030
00040
00050
00060
00070
00080
00090
000A0
000B0
000C0
000D0
000E0
000F0
00100
00110
00120
00130
00140
00150
00160

- Not speaking:
Do strange research you love
vs.
- Speaking:
Do strange research you love
and present it to people smarter
than yourself
 - The people in the audience are
offering you an hour of their life
time to review your shit!
 - This might be embarrassing
 - Halvar to me: “You fucked up every Turing
reference you did. So give me a cigarette.”

How Hacking Is Done

Know Your History

Hacking in the 1960

Text View: K:\KEYNOTE.EXE

Col 0

270,650 Bytes

0%

00000
00010
00020
00030
00040
00050
00060
00070
00080
00090
000A0
000B0
000C0
000D0
000E0
000F0
00100
00110
00120
00130
00140
00150
00160

- Username: system
Password: manager



1 Help 2 Unwrap 3 4 ASCII 5 6 7 Search 8 Viewer 9 Print 10 Quit

Hacking in the 1980s

```
Text View: K:\KEYNOTE.EXE          Col 0          270,650 Bytes  0%
00000
00010  ■ UNIX r-services
00020
00030  ■ NFS exports
00040
00050  ■ RPC services
00060
00070  ■ Anonymous FTP servers
00080
00090  ■ Default passwords
000A0    ■ Or none at all for SGI Irix
000B0
000C0
000D0
000E0  ■ Password guessing ("GOD")
000F0
00100  ■ Sendmail .forward pipes
00110
00120
00130
00140
00150
00160
1Help  2Unwrap  3  4ASCII  5  6  7Search  8Viewer  9Print  10Quit
```

Hacking in the 1990s

Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%

- 00000
- 00010 ■ Read BugTraq, hack sendmail (again)
- 00020
- 00030 ■ ping -l 65510
- 00040
- 00050 ■ Microsoft windows 9x and NT
- 00060
- 00070 ■ Sun Solaris
- 00080
- 00090 ■ SCO UNIX
- 000A0
- 000B0 ■ Novell Netware
- 000C0
- 000D0 ■ Apple Mac
- 000E0
- 000F0 ■ cd ~/some/open/source && grep
- 00100 strcpy *.c
- 00110
- 00120
- 00130 ■ Also: Port Scanning!!1!
- 00140
- 00150
- 00160

1 Help 2 Unwrap 3 4 ASCII 5 6 7 Search 8 Viewer 9 Print 10 Quit

Hacking in the 2000s

Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%

- 00000
- 00010 ■ cd ~/some/open/source && grep -E -e
- 00020 'printf\s*\([^"]+[, \)]' *.c
- 00030
- 00040 ■ 7350 x2
- 00050
- 00060 ■ solaris sadmind
- 00070
- 00080 ■ Cisco UDP echo
- 00090
- 000A0 ■ Worms!!1!
- 000B0
- 000C0 ■ Heap Spraying
- 000D0
- 000E0 ■ Fuzzing
- 000F0
- 00100 ■ Rise of the client-side attacks
- 00110
- 00120 ■ Rise of the web application bugs
- 00130
- 00140
- 00150
- 00160



Hacking in the 2000s

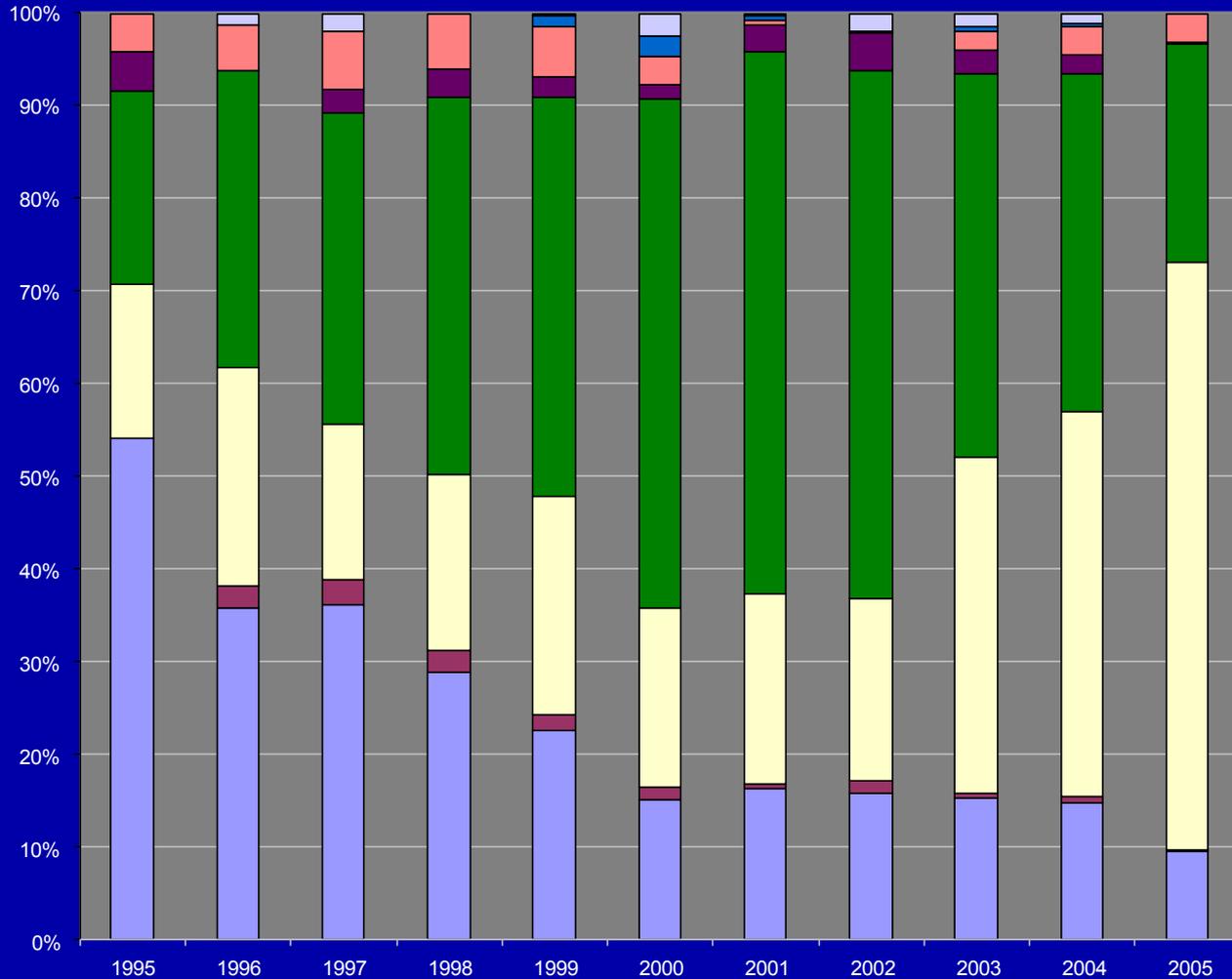
Text View: K:\KEYNOTE.EXE

Col 0

270,650 Bytes

0%

00000
00010
00020
00030
00040
00050
00060
00070
00080
00090
000A0
000B0
000C0
000D0
000E0
000F0
00100
00110
00120
00130
00140
00150
00160



- Other
- Encryption module
- Communication protocol
- Hardware
- Server application
- Non-Server application
- Network Protocol Stack
- Operating System

1 Help 2 Unwrap 3 4 ASCII 5 6 7 Search 8 Viewer 9 Print 10 Quit

Also...

Text View: K:\KEYNOTE.EXE

Col 0

270,650 Bytes

0%

00000
00010
00020
00030
00040
00050
00060
00070
00080
00090
000A0
000B0
000C0
000D0
000E0
000F0
00100
00110
00120
00130
00140
00150
00160



1 Help 2 Unwrap 3 4 ASCII 5 6 7 Search 8 Viewer 9 Print 10 Quit

Hacking in the 2010s

```
Text View: K:\KEYNOTE.EXE          Col 0          270,650 Bytes  0%
```

- 00000 ■ W^X, DEP, ASLR, KASLR, Safe-SEH,
00010 stack cookies, fortify source
- 00020
- 00030
- 00040 ■ ROP goes mainstream
- 00050
- 00060 ■ Jailbreaks
- 00070
- 00080 ■ Kingcope's BSD telnetd Remote Root
- 00090
- 000A0 ■ Java client side bugs
- 000B0
- 000C0 ■ for i in \$(cat emails.txt);do(cat
000D0 fish.txt|mail -s "Facebook Account
000E0 Verification" \$i);done
- 000F0
- 00100
- 00110 ■ Google, Dropbox, Amazon, iCloud
- 00120
- 00130
- 00140 ■ Anonymous!!1!
- 00150
- 00160

1Help 2Unwrap 3 4ASCII 5 6



And Now?

where Are We Heading?

What Is Big Right Now: The Cloud

Text View: K:\KEYNOTE.EXE

Col 0

270,650 Bytes

0%

- 00000 ■ The Cloud™ means virtualization
00010 technologies everywhere
- 00020 ■ OS virtualization
- 00030 ■ Network virtualization
- 00040 ■ Storage virtualization
- 00050 ■ Several metric tons of management
- 00060 ■ The change in “ownership” is
00070 important for the researcher
- 00080 ■ Even if you don’t “own” the software,
00090 testing, fuzzing and debugging a local
000A0 copy is pretty hard to prevent
- 000B0 ■ Testing and playing with the cloud can
000C0 land you in jail pretty quickly
- 000D0 ■ Plus, you might hand your 0day over the moment
000E0 you find it
- 000F0 ■ Few clouds allow testing (e.g. Microsoft)
- 00100
- 00110
- 00120
- 00130
- 00140
- 00150
- 00160

1 Help 2 Unwrap 3 4 ASCII 5 6 7 Search 8 Viewer 9 Print 10 Quit

What Is Big Right Now: The Cloud

Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%

- 00000 ■ The Cloud™ means that hacking goes
00010 back to a mainframe host scenario
00020
 - 00030 ■ There are two reasons that mainframe
00040 exploits are so rare:
00050
 - 00060 1. They were actually designed and built with a
00070 lot of security in mind
 - 00080 2. They were pretty hard to get to
- 00090 ■ IMHO, hacking PAS and SAS will tend
000A0 to be much more observation centric
000B0 than testing centric
000C0
 - 000D0 ■ Observation is hard to prevent
 - 000E0 ■ Few and far between testing is hard to
000F0 detect
- 00100 ■ IAS comes down to finding Xen
00110 breakouts and building the image
00120
00130
00140
00150
00160

What Is Big Right Now: Mobile Devices

```
Text View: K:\KEYNOTE.EXE          Col 0          270,650 Bytes  0%
00000  ■ Mobile devices are the natural
00010  counter-point to Cloud services
00020
00030  ■ The security models differ
00040  significantly depending on the goal
00050  of the vendor
00060
00070  ■ Apple protects their business model
00080  ■ Google protects the user's believes
00090
000A0  ■ Mobile Apps roll software security
000B0  back to the 90s
000C0
000D0  ■ written by former Adobe Flash coders
000E0
000F0  ■ Mass produced in numbers never seen before
00100
00110  ■ Objective-C is a programming language that
00120  could not have been designed worse if it
00130  were intentional
00140
00150  ■ Many underestimated attack vectors
00160
1Help  2Unwrap  3  4ASCII  5  6  7Search  8Viewer  9Print  10Quit
```

What Is Big Right Now: SCADA !!1!

Text View: K:\KEYNOTE.EXE

Col 0

270,650 Bytes

0%

- 00000 00010 00020 00030 00040 00050 00060 00070 00080 00090 000A0 000B0 000C0 000D0 000E0 000F0 00100 00110 00120 00130 00140 00150 00160
 - SCADA and ICS are the new hotness after Stuxnet was discovered
 - SCADA has a couple of fun aspects:
 - Most environments are un-patchable
 - Most vendors consider software security as something Microsoft must do
 - Most ICS engineers consider themselves invincible to any hacker due to their arcane domain knowledge
 - A lot of protocols are transported and proxied over TCP/IP now (see Metasploit)
 - ICS are very interesting things to learn about, if you have patience
 - You will also find dancing monkeys

1 Help 2 Unwrap 3 4 ASCII 5 6 7 Search 8 Viewer 9 Print 10 Quit

Also...

Text View: K:\KEYNOTE.EXE

Col 0

270,650 Bytes

0%

00000
00010
00020
00030
00040
00050
00060
00070
00080
00090
000A0
000B0
000C0
000D0
000E0
000F0
00100
00110
00120
00130
00140
00150
00160



SORRY MARIO
THE PRINCESS
IS IN ANOTHER
CASTLE

1 Help 2 Unwrap 3 4 ASCII 5 6 7 Search 8 Viewer 9 Print 10 Quit

Military Hacking

Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%

- 00000 00010 00020 00030 00040 00050 00060 00070 00080 00090 000A0 000B0 000C0 000D0 000E0 000F0 00100 00110 00120 00130 00140 00150 00160
 - Military and intelligence hacking is nothing new
 - Neither the practice nor the targets
 - Stuxnet, Gaus, Flame etc. only allowed the general public a glimpse
 - The difference is in the resources, tactics and techniques
 - The military industrial complex now invests more in attack technologies than the cybercrime market
 - This opens a lot of possibilities for the attackers in terms of R&D
 - Case in point: Nobody pulls a new MD5 collision attack out of their ass
 - Depending on international developments, it might also be the only area of unpunished in-the-wild hacking for a while

1 Help 2 Unwrap 3 4 ASCII 5 6 7 Search 8 Viewer 9 Print 10 Quit

What Might Get Big

Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%

- 00000 ■ Cryptography Bugs
 - 00010 ■ Cryptography is still considered fairy dust: Have crypto, be secure!
 - 00020
 - 00030
 - 00040 ■ Check Greg's excellent talk "Non-obvious bugs by example"
 - 00050
 - 00060
- 00070 ■ Parallel Execution Bugs
 - 00080
 - 00090 ■ Very hard to spot in source code
 - 000A0 ■ Almost impossible to find by fuzzing
 - 000B0
 - 000C0 ■ Almost everything today has multiple cores or CPUs or both
 - 000D0
 - 000E0
- 000F0 ■ Lower level processors
 - 00100 ■ Trusted by the application CPU
 - 00110 ■ Already started with GSM Baseband research
 - 00120 ■ System Management Controllers, ILO, etc.
 - 00130
 - 00140 ■ There is a ton of this in today's devices
 - 00150
 - 00160

When Bug Count Isn't Everything

Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%

- 00000 00010 00020 00030 00040 00050 00060 00070 00080 00090 000A0 000B0 000C0 000D0 000E0 000F0 00100 00110 00120 00130 00140 00150 00160
 - when hacking, I believe one can also do something for the common good:
 - Before Barnaby Jack publicly hacked insulin pumps, only one medical device vendor cared
 - Before Dillon Beresford took a deeper look at Siemens PLCs, no vendor cared about their base operating system
 - Now Siemens is the only one not caring
 - Nils' PinPadPwn demonstration should change quite a few payment systems
 - while hackers, we are also humans
 - At some point, even you and me will have to use a PIN-Pad to pay for stuff

When Bug Count Isn't Everything

Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%

- 00000
- 00010 ■ Product Security is a cost center
- 00020 for the vendor – it makes no money
- 00030
- 00040
- 00050 ■ They need a Backup-Effect in order to
- 00060 justify the expenses to do it:
- 00070 Only when data is lost do people care
- 00080 about and invest in backups.
- 00090
- 000A0
- 000B0
- 000C0 ■ This is called passion!
- 000D0
- 000E0 ■ Maybe money isn't everything?
- 000F0
- 00100 ■ A hacker does for love what others
- 00110 can't even do for money.
- 00120
- 00130
- 00140
- 00150
- 00160

Target Selection

Where Individuality Shines

Stay Naïve

Text View: K:\KEYNOTE.EXE

Col 0

270,650 Bytes

0%

- 00000 ■ Naivety was always an important part
00010 of hacking
- 00020
- 00030
- 00040 ■ Remember the movie “Hackers”? The kiddy
00050 was the one hacking the Gibson.
- 00060
- 00070 ■ Whether you think that you will find
00080 a vulnerability or not, you will be
00090 right.
- 000A0
- 000B0
- 000C0 ■ Stubbornness is pretty useful
- 000D0
- 000E0 ■ It also compensates for talent ;)
- 000F0
- 00100 ■ Hacking is often about frustration
00110 resilience more than anything else
- 00120
- 00130 ■ Or about not getting frustrated in the
00140 first place, a.k.a. expectation management
- 00150
- 00160

1 Help 2 Unwrap 3 4 ASCII 5 6 7 Search 8 Viewer 9 Print 10 Quit

Target Selection

Text View: K:\KEYNOTE.EXE

Col 0

270,650 Bytes

0%

00000
00010
00020
00030
00040
00050
00060
00070
00080
00090
000A0
000B0
000C0
000D0
000E0
000F0
00100
00110
00120
00130
00140
00150
00160

- It helps to find targets that genuinely interest you
 - Targets that are boring you to death are missing the inherent motivation
 - Rage can be pretty motivating
- Don't hack things just because everyone else is hacking them
 - Unless you are hunting for bug bounties
- Understand whether your target environment is competitive by nature
 - Act accordingly

1 Help 2 Unwrap 3 4 ASCII 5 6 7 Search 8 Viewer 9 Print 10 Quit

Size Does Matter

Text View: K:\KEYNOTE.EXE

Col 0

270,650 Bytes

0%

00000

00010 ■ Bigger targets are usually juicier

00020

00030 ■ More code =

00040

00050 ■ More attack surface =

00060

00070 ■ More chances for vulnerabilities

00080

00090 ■ Average of vulnerability per lines
000A0 of source code is relatively stable
000B0

000C0

000D0 ■ Bigger targets are admin bitches

000E0

000F0 ■ Harder to set up and configure right

00100

00110 ■ Your tools will have a harder time

00120

00130 ■ More code to wade through, because
00140 it's not relevant
00150

00160

1 Help

2 Unwrap

3

4 ASCII

5

6

7 Search

8 Viewer

9 Print

10 Quit

Means To An End

Text View: K:\KEYNOTE.EXE

Col 0

270,650 Bytes

0%

00000
00010
00020
00030
00040
00050
00060
00070
00080
00090
000A0
000B0
000C0
000D0
000E0
000F0
00100
00110
00120
00130
00140
00150
00160

Purpose	Methods
Criminal	Browser injectors Kernel rootkits and key logger AV evasion Fishing and C&C site management
Bug bounties vulnerability sales	Fuzzing at scale & in .fi style Automation and industrialization Static analysis
Exploit sales	Targeted fuzzing Static and runtime analysis Exploit reliability
Publicity	Fancy target selection Hardware hacking Output frequency
Fun	☺

1 Help 2 Unwrap 3 4 ASCII 5 6 7 Search 8 Viewer 9 Print 10 Quit

A Word About Fuzzing

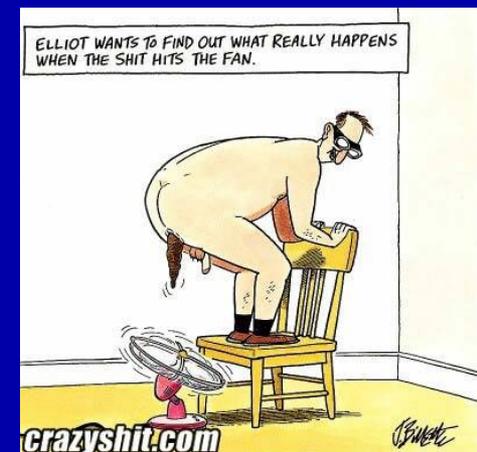
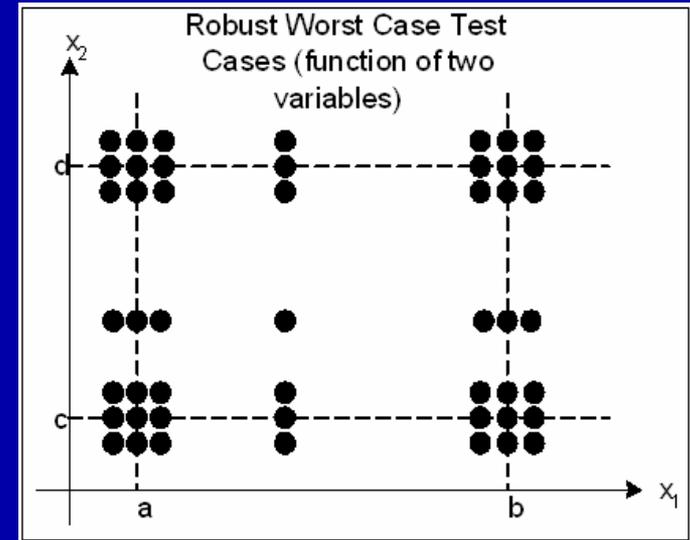
Text View: K:\KEYNOTE.EXE

Col 0

270,650 Bytes

0%

- 00000 ■ I concur that fuzzing
00010 finds a lot of bugs
00020 these days
- 00030 ■ Especially in complex
00040 software (e.g.
00050 Browsers)
- 00060 ■ That doesn't prove
00070 fuzzing to be superior
00080 – it only proves the
00090 shitty state our
000A0 software is in
- 000B0 ■ What you are doing is
000C0 called Robust Worst
000D0 Case Testing
- 000E0 ■ It has an exponential
000F0 effort grow with the
00100 number of variables
00110 being the exponent
00120
00130
00140
00150
00160



crazyshit.com

Method Selection

Text View: K:\KEYNOTE.EXE

Col 0

270,650 Bytes

0%

- 00000 ■ There are many ways to find
- 00010 vulnerabilities:
- 00020
- 00030 ■ Manual testing
- 00040 ■ Fuzzing
- 00050 ■ Static source code analysis
- 00060 ■ Static binary code analysis
- 00070 ■ Runtime analysis
- 00080 ■ Diffing
- 00090 ■ Reading Specifications
- 000A0
- 000B0
- 000C0
- 000D0
- 000E0
- 000F0 ■ The key is to do what suites you best
- 00100 ■ Not everyone reads code like Halvar
- 00110 ■ Not everyone breaks crypto like Greg
- 00120
- 00130
- 00140 ■ Be individual!
- 00150
- 00160

1Help 2Unwrap 3 4ASCII 5 6 7Search 8Viewer 9Print 10Quit

Bad News

Text View: K:\KEYNOTE.EXE

Col 0

270,650 Bytes

0%

00000
00010
00020
00030
00040
00050
00060
00070
00080
00090
000A0
000B0
000C0
000D0
000E0
000F0
00100
00110
00120
00130
00140
00150
00160

- There is no silver bullet in Computer Security
 - Yes, that includes offense!



1 Help 2 Unwrap 3 4 ASCII 5 6 7 Search 8 Viewer 9 Print 10 Quit

And You?

Where Do You Stand?

Don't Let Anyone Tell You What To Do

Text View: K:\KEYNOTE.EXE

Col 0

270,650 Bytes

0%

00000

00010

00020

00030

00040

00050

00060

00070

00080

00090

000A0

000B0

000C0

000D0

000E0

000F0

00100

00110

00120

00130

00140

00150

00160

- Most people that lecture you on ethics don't follow those themselves
 - Digital human rights activists who also head companies selling to military or criminal mob
 - People bashing Microsoft while sitting at their campus getting paid by them
 - People writing spy software for oppressive governments while claiming to be left wing activists
 - Do you think Adrian Lamo is an exception?
- There are many aspects to consider
 - Other people's opinion isn't one of them

1Help

2Unwrap 3

4ASCII 5

6

7Search

8Viewer

9Print

10Quit

To Sell or Not To Sell?

Text View: K:\KEYNOTE.EXE

Col 0

270,650 Bytes

0%

- 00000 00010 00020 00030 00040 00050 00060 00070 00080 00090 000A0 000B0 000C0 000D0 000E0 000F0 00100 00110 00120 00130 00140 00150 00160
 - Is selling exploits like selling weapons?
 - Do you think it should be illegal?
 - Do you think you can control what your exploit is used for?
 - Do you care?
 - what about regulating use?
 - Is it better or worse than leaking docs to wikileaks?
 - „Do whatever you want. Trust your guts, your humanly feelings, your very limited knowledge. This is best effort.” – Julio Auto

1 Help

2 Unwrap 3

4 ASCII 5

6

7 Search

8 Viewer

9 Print

10 Quit

Vendor Communication?

```
Text View: K:\KEYNOTE.EXE          Col 0          270,650 Bytes  0%
00000  ■ Should you talk to the vendor?
00010      ■ Do they even have a contact address?
00020      ■ Did you consider their previous track record?
00030      ■ Maybe ask someone with prior experience?
00040      ■ If in doubt, hand it off to a CERT.
00050  ■ How much time should you allow for a fix?
00060      ■ RFPolicy 2.0 calls for 2 weeks warning
00070      ■ Most fix times declared by vendors are bullshit
00080          ■ Some are not
00090          ■ Use your best judgment and gut feeling
000A0      ■ Can you accept being beaten by someone else
000B0          releasing before you?
000C0          ■ If the vendor half-releases, that's going to happen
000D0  ■ Don't let a vendor scare you away from
000E0  disclosure with legal threats
000F0      ■ I have not heard of a successful legal action
00100          that didn't have another aspect
00110          ■ If you violated NDAs, you are fucked anyway
00120
00130
00140
00150
00160
1Help  2Unwrap  3  4ASCII  5  6  7Search  8Viewer  9Print  10Quit
```

To Anonymous or Not To Anonymous?

Text View: K:\KEYNOTE.EXE

Col 0

270,650 Bytes

0%

00000

- Which Anonymous are we talking about?

00010

00020

00030

00040

00050

00060

00070

00080

- Considerable risk

00090

000A0

000B0

000C0

000D0

000E0

000F0

00100

00110

- A highly personal decision

00120

00130

00140

00150

00160

- One that should probably be kept private
- One that can have significant consequences

1 Help

2 Unwrap

3

4 ASCII

5

6

7 Search

8 Viewer

9 Print

10 Quit

To Cyberwar or Not To Cyberwar?

Text View: K:\KEYNOTE.EXE

Col 0

270,650 Bytes

0%

- 00000 ▪ Militaries and intelligence services
00010 around the world are dying for skilled
00020 personal
00030
 - 00040 ▪ Their demand probably exceeds the currently
00050 available global supply
- 00070 ▪ Not everyone's favorite idea of a
00080 working place
00090
 - 000A0 ▪ "Plush Bunker"
- 000B0 ▪ Depending on your country, quitting
000C0 might not be an option
000D0
 - 000E0 ▪ Once intelligence, always intelligence
 - 000F0 ▪ Security clearances can become chain on your
00100 leg for life
- 00120 ▪ Still, a surprising number of people
00130 choose this path
00140
 - 00150 ▪ See Military Hacking
- 00160

Why I Always Stayed Legal & Public

Text View: K:\KEYNOTE.EXE

Col 0

270,650 Bytes

0%

- 00000
- 00010 ■ It's easier to reason with others
- 00020 ■ Defends against politician's arguments
- 00030
- 00040 ■ It's better paid
- 00050 ■ No need to monetize but plenty of options
- 00060 ■ It's a global business, no need to sell
- 00070 locally
- 00080
- 00090
- 000A0
- 000B0 ■ It's more relaxing
- 000C0 ■ OpSec is pretty annoying over time
- 000D0 ■ when you get older, you want it easy
- 000E0
- 000F0
- 00100
- 00110 ■ You get to talk to other people
- 00120 without being worried that they fuck
- 00130 you over
- 00140
- 00150
- 00160

1Help 2Unwrap 3 4ASCII 5 6 7Search 8Viewer 9Print 10Quit

Some Things Cannot Be Individualized

why I loved PTS-DOS,
but don't like Kaspersky.

Know Your Basics

Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%

```
00000 #!/usr/bin/perl --machine=fullturing
00010 $n=<>;
00020 while($n!=1){
00030   if($n%2==0){$n=$n/2;}
00040   else{$n=3*$n+1;}
00050   printf("%u\n",$n);
00060 }
00070
00080
00090
00100
```

- 00110 ■ Credits:
 - 00120 ■ Alan Turing
 - 00130 ■ Lothar Collatz

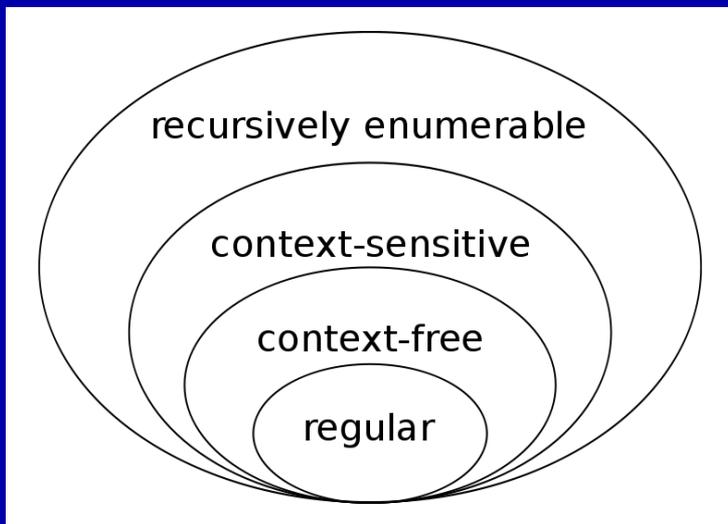
1Help 2Unwrap 3 4ASCII 5 6 7Search 8Viewer 9Print 10Quit

Know Your Basics

Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%

00000
00010
00020
00030
00040
00050
00060
00070
00080
00090
000A0
000B0
000C0
000D0
000E0
000F0
00100
00110
00120
00130
00140
00150
00160

- “Never bring a regular expression to a context-free grammar fight.”
 - Meredith L. Patterson
 - If you build defense, this is vital
 - If you build offense, this is more relevant than you would think



1Help 2Unwrap 3 4ASCII 5 6 7Search 8Viewer 9Print 10Quit

Know Your Basics

Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%

- 00000
- 00010
- 00020
- 00030
- 00040
- 00050
- 00060
- 00070
- 00080
- 00090
- 000A0
- 000B0
- 000C0
- 000D0
- 000E0
- 000F0
- 00100
- 00110
- 00120
- 00130
- 00140
- 00150
- 00160
- If you ignore proven facts, you will keep looking for the philosopher's stone of hacking
 - "I have build this automated fuzzing framework that will use coverage testing to run every code path with my input!"
 - "Iterating through all possible inputs that match this regular expression will find me all possible bugs in this code!"
- Those are the only things that should limit your individuality
 - Unless, of course, you can prove them wrong ;)

Be Yourself

And (optionally) get paid for it.

You And The Community

Text View: K:\KEYNOTE.EXE

Col 0

270,650 Bytes

0%

00000
00010
00020
00030
00040
00050
00060
00070
00080
00090
000A0
000B0
000C0
000D0
000E0
000F0
00100
00110
00120
00130
00140
00150
00160

- cultivate relations to others with respect for them
 - It's OK to loose the respect later if they don't deserve it
 - Respect is a symmetric connection: priority and limits work both ways
- Most people share your ideals
 - But they might have other needs, motivations or interests

1 Help 2 Unwrap 3 4 ASCII 5 6 7 Search 8 Viewer 9 Print 10 Quit

Working in InfoSec

Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%

- 00000 00010 00020 00030 00040 00050 00060 00070 00080 00090 000A0 000B0 000C0 000D0 000E0 000F0 00100 00110 00120 00130 00140 00150 00160
 - Working in InfoSec is often said to suck monkey balls
 - I call bullshit
 - In a professional environment, the rules change a little
 - Be fair and professional
 - Don't let anyone use you
 - Don't fool yourself into submission
 - "The job sucks but the team is so nice!"
 - You should not fall for charlatans
 - My rule of thumb: The more often the person appears in shitty TV shows, the more likely that person is a charlatan.

Working in InfoSec

Text View: K:\KEYNOTE.EXE

Col 0

270,650 Bytes

0%

00000

00010

00020

00030

00040

00050

00060

00070

00080

00090

000A0

000B0

000C0

000D0

000E0

000F0

00100

00110

00120

00130

00140

00150

00160

- In every work environment, you find 100 types of people:
 - 00: asshole
 - 01: asshole considered nice
 - 10: nice considered asshole
 - 11: nice
- That doesn't make InfoSec any better or worse than other jobs
- Also: If you find yourself in a hole, stop digging.
 - If a job sucks, find a new one

1Help

2Unwrap 3

4ASCII 5

6

7Search

8Viewer

9Print

10Quit

Working in InfoSec

Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%

- 00000
- 00010 ■ A good company fosters your
- 00020 development as an individual to the
- 00030 same extend that you foster the
- 00040 development of the overall team
- 00050
- 00060
- 00070
- 00080
- 00090 ■ Figure out your motivation and find
- 000A0 a company that shares it
- 000B0
- 000C0
- 000D0 ■ If in doubt, start you own
- 000E0
- 000F0
- 00100
- 00110
- 00120
- 00130
- 00140
- 00150
- 00160

1Help 2Unwrap 3 4ASCII 5 6 7Search 8Viewer 9Print 10Quit

Done.

Text View: K:\KEYNOTE.EXE

Col 0

270,650 Bytes

0%

00000 Thanks for listening

00010

00020

00030

00040

00050

00060

00070

00080

00090

000A0

000B0

000C0

000D0

000E0

000F0

00100

00110

00120

00130

00140

00150

00160

The Norton Commander

Do you want to quit the Norton Commander?

Yes

No

Greetz and Shouts:

Phenoelit, Phonoelit, Halvar Flake, HD Moore

1 Help

2 Unwrap 3

4 ASCII 5

6

7 Search

8 Viewer

9 Print

10 Quit