First steps into security engineering

DevConf.CZ 2019 / Brno 2019-01-26
Christian Heimes
Principal Software Engineer

christian@python.org / cheimes@redhat.com
@ChristianHeimes
Agenda & Goals
Disclaimer

This talk is

- opinionated
- subjective
- biased
- incomplete
- edutainment
1. think
2. learn
@ChristianHeimes: Nobody likes security engineers. Don't fix bugs, they hate you; fix it, they still hate you...because it's usually a breaking change! 😅

#DevConfIN #definefuture
Motivation

Why should you care?

(Recap DevConf.CZ 2018)
Yahoo hack: 1bn accounts compromised by biggest data breach in history

The latest incident to emerge - which happened in 2013 - is probably distinct from the breach of 500m user accounts in 2014

https://www.theguardian.com/technology/2016/dec/14/yahoo-hack-security-of-one-billion-accounts-breached

Verizon scrapes $350 million off deal to buy Yahoo

After its disclosures about massive security breaches, Yahoo apparently wasn't worth the original $4.83 billion price tag.

Hacking risk leads to recall of 500,000 pacemakers due to patient death fears

FDA overseeing crucial firmware update in US to patch security holes and prevent hijacking of pacemakers implanted in half a million people

Propositions & Statements
Security is a feature.

Security is a selling point.
Attackers just need one vulnerability, defenders need to be perfect.
Users don't care about security.

They are ignorant, disregardful, and responsible for security incidents.
wrong
dangerous
arrogant

(I used to think like that.)
We fight for the users!
(Tron)
0. attitude

1. think

2. learn
Security is not a feature
“Our cars are less likely to explode than competing products.”
Security is not dichotomous.
Alex Gaynor

The worst truism in information security

Attackers just need one vulnerability,
defenders need to be perfect

But what about the exploding cars?
“unbreakable” encryption
absolute security
threat model

cost–benefit analysis

documentation
Threat Model: biometrics
What you think security is: Picking the best post-quantum TLS cipher suites
What security actually is: Making sure none of your production FTP passwords are the name of a vegetable
Mitigation: Defense in depth
AIRLINE SAFETY: 2017 WAS SAFEST YEAR IN HISTORY FOR PASSENGERS AROUND WORLD, RESEARCH SHOWS

That an Air France A380 lost an engine over the Atlantic and landed safely this year is 'testament to the robustness' of the aircraft / AFP/Getty Images

Amazon Says One Engineer's Simple Mistake Brought the Internet Down

2017-02-28
Please mind the user between the chair and the keyboard.
I've said it before, and I'll say it again: if you work in security and you think users are the problem, you should read nspw.org/2009/proceedin....

And then apologise.

So Long, And No Thanks for the Externalities:
The Rational Rejection of Security Advice by Users
Cormac Herley, Microsoft Research
Human factor

- Social engineer
  - CEO scam: Ubiquiti Networks victim of $39 million
  - Password in exchange for chocolate (up to 47.9%)
    Université du Luxembourg, Computers in Human Behavior, 2016; 61: 372 DOI: 10.1016/j.chb.2016.03.026
- dissatisfied employees
- ignorant management
Chad Loder @chadloder

We have a huge credibility problem in information security and it's time we addressed it. We #infosec experts spend too much time asking "How do we get users to care more about security?" - and not enough time asking "How do we get security to care more about users?"
Your grandmother has installed Flash.
User Interface

Lion Air Flight 610:

Pilots fought automatic safety system before plane plunged
0. attitude

1. think

2. learn
Professionally paranoid
be creative
&
learn from the past
Consider leaky abstraction layers
Example: Memory safety
Hardware security

RSA Key Extraction via Acoustic Cryptanalysis

https://www.tau.ac.il/~tromer/acoustic/
Physical security against intru-deers

https://twitter.com/DCFurs/status/1087663240421593089
cybersquirrel1.com – attacks on power grid

<table>
<thead>
<tr>
<th>Agent</th>
<th>Success</th>
</tr>
</thead>
<tbody>
<tr>
<td>Squirrel</td>
<td>1228</td>
</tr>
<tr>
<td>Bird</td>
<td>635</td>
</tr>
<tr>
<td>Snake</td>
<td>116</td>
</tr>
<tr>
<td>Raccoon</td>
<td>114</td>
</tr>
<tr>
<td>Rat</td>
<td>52</td>
</tr>
<tr>
<td>Cat</td>
<td>26</td>
</tr>
<tr>
<td>Marten</td>
<td>25</td>
</tr>
<tr>
<td>Jellyfish</td>
<td>13</td>
</tr>
<tr>
<td>Monkey</td>
<td>12</td>
</tr>
<tr>
<td>Human</td>
<td>3*</td>
</tr>
</tbody>
</table>

http://cybersquirrel1.com/
Ethics and responsibility

Boy: I LOVE YOU
Girl: I HAVE A BOYFRIEND
Boy: SUDO I LOVE YOU
Girl: BOY IS NOT IN THE SUDOERS FILE. THIS INCIDENT WILL BE REPORTED.
twitter.com/addelindh/stat …

11:26 AM - 5 Mar 2018
0. attitude

1. think

2. learn
I know that I know nothing

(Socratic paradox)
Skill #1
Communication
Stop reading, start doing!

Parisa Tabriz
So, you want to work in security?

https://medium.freecodecamp.org/so-you-want-to-work-in-security-bc6c10157d23
Available for free: https://www.cl.cam.ac.uk/~rja14/book.html
Human Computer Interaction

UI / UX
“Soft” skills

- team work / team diversity
- locate and evaluate information
- law / legal affairs
- ethics & compliance
- rhetoric
- read and write documentation
Social Engineering

- The Social Engineering Framework
  https://www.social-engineer.org/framework/
- Social Engineering, The Art of Human Hacking
  Christopher Hadnagy (2010)
- The Art Of Deception
Digital self-defense

- secure your hardware
  - disk encryption
- privacy
  - ad-blocker
  - email provider
- good passwords / 2FA
- update, update, update!

https://freedom.press/training/
Operating Systems

- man pages
- Advanced Programming in the UNIX Environment
  Stevens / Rago (2013)
Computer networks and system tools

- IPv4, IPv6, routing, TCP, UDP, DNS, firewall
- auditing, logging
- SELinux
- analysis and pentesting tools
  - wireshark
  - nmap
  - metasploit
  - IDA Interactive Disassembler
Software
General Resource

- OWASP: Open Web Application Security Project
- CWE: Common Weakness Enumeration
- CVE: Common Vulnerabilities and Exposures
- IETF RFCs
Top 10 bugs

- injection attacks (SQL, LDAP, JSON, XQuery, XPath, ...)
- broken authentication and access control
- Cross-Site scripting (XSS)
- XML entities
- Insecure Deserialization (images, documentations, ASN.1)
Unicode

>>> import unicodedata
# homograph / homoglyphic confusion attack
>>> unicodedata.name('Python'[0])
CYRILLIC CAPITAL LETTER ER
# persistent XSS with wide unicode normalization
>>> wide = '<script>'
>>> safe = wide.replace('<', '&lt;')  # quote
>>> unicodedata.name(safe[0])
'FULLWIDTH LESS-THE A N SIGN'
>>> unicodedata.normalize('NFKD', safe)
'<script>'
Programming languages

• C
• Assembly
• eBPF, BPF

• Go
• Java
• JavaScript
• Python
• Rust
Cryptography
Cryptography

- The Code Book, Simon Singh
- Cryptography Engineering, Ferguson/Schneier/Tadayashi
- Serious Cryptography, JP Aumasson
Cryptography

free online resources

- Cryptography I, Dan Boneh
  https://www.coursera.org/learn/crypto  Enroll now
- The cryptopals crypto challenges
  https://cryptopals.com/
- Crypto 101, LvH,
  https://www.crypto101.io/
- Mathematics of Public Key Cryptography,
  Steven Galbraith (2012)
TLS/SSL, Certificates

- Bulletproof SSL and TLS, Ivan Ristic
- CA/Browser Forum Baseline Requirements
  https://cabforum.org/
- Mozilla Server Side TLS
  https://wiki.mozilla.org/Security/Server_Side_TLS
Passwords / Authentication

- NIST 800-63-3: Digital Identity Guidelines
- OAuth, OpenID Connect
- 2FA (FIDO, WebAuthn)
- Troy Hunt, https://haveibeenpwned.com/
Misc
News, blogs

- Linux Weekly News https://lwn.net/
- Troy Hunt https://www.troyhunt.com/
- Krebs on Security https://krebsonsecurity.com/
- Bruce Schneier https://www.schneier.com/
- https://www.feistyduck.com/bulletproof-tls-newsletter/
Conference videos

- Chaos Communication Conference (e.g. 35C3)
- Black Hat
- DEFCON
- Real World Crypto
Security people

- Adam Langley
- Alex Gaynor
- Brian Krebs (Krebs On Security)
- Bruce Schneier
- Dan Bernstein (djb)
- Frank Denis
- Hanno Böck
- JP Aumasson
- Katie Moussouris
- Matt Blaze

- Matthew Green
- Nick Sullivan
- Parisa Tabriz
- Ryan Sleevi
- Tanja Lange
- Tavis Ormandy
- Thomas Ptacek
- Tony Arcieri
- Troy Hunt
Summary
Summary

- Mind the user
- Keep learning
- Get experience
  Write your own crypto (don't use it in production)

Please send your suggestions
christian@python.org / @ChristianHeimes
THANK YOU

plus.google.com/+RedHat

linkedin.com/company/red-hat

facebook.com/redhatinc

twitter.com/RedHat

youtube.com/user/RedHatVideos