Selling LangSec

Tales from the Alchemist's Apprentice

Felix ‘FX’ Lindner

Invent & Verify

My Story with LangSec

Spirits that I've cited
My commands ignore

How a blind chicken found a corn

FORMAT NORMALIZATION

Invent & Verify

Blitzableiter

- Adobe Flash SWF Format defense layer
  - Read, Recognize, Remove, Rebuild
  - Support for AVM1 and AVM2 code
- Released under GPLv3 in 2010
  - Successfully prevents all exploits since release, without a single change, iff their class was in scope
    - Predictable and deterministic defense component
    - As a byproduct, vulnerabilities exploiting bug classes not covered are significantly harder to exploit
  - Output quality above all of Adobe's own tools, according to Adobe's own tests
  - Fully integrated for firewall and proxy use (ICAP)
  - Fully integrated in NoScript for Firefox

#FAIL

- Nobody ever uses Blitzableiter
- Papers and talks to explain the concept
  - People are nodding and don't get it
- Decades of conditioning by the detection paradigm industry
  - anti-virus, IDS, IPS and all the other expensive ways to get pwned
- Failed to overcome the "scanning" notion

How That Felt Like

And the apprentice said to the alchemist: "Gods creation is so rich and things interact with so much complexity, he must have used Turing-complete machines to build it."

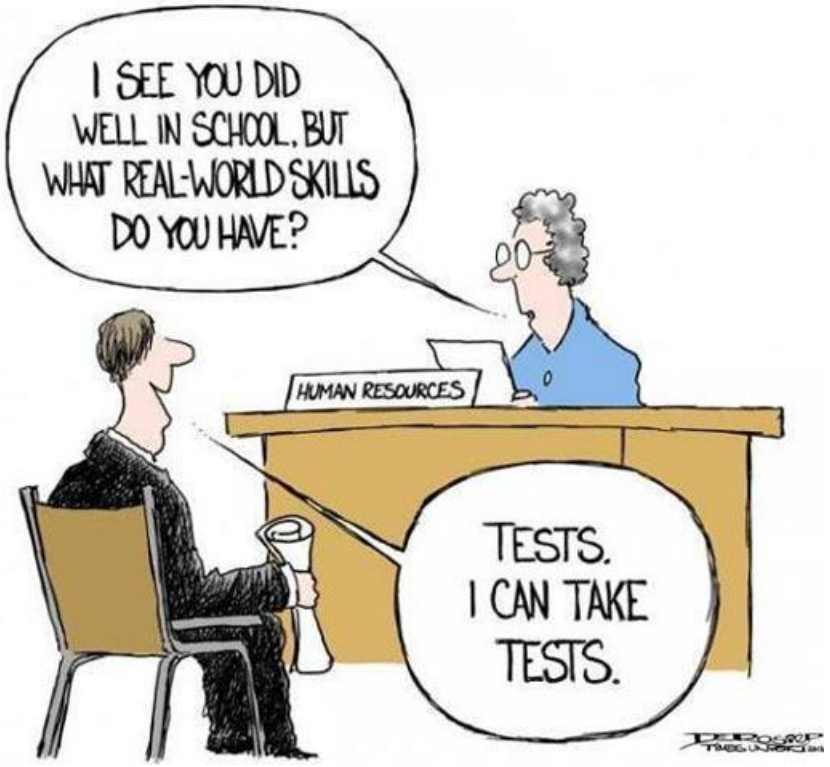
The alchemist thought about that and answered: "No, young padawan. What he used was mathematics."

Terminology #FAIL
When People Hang Up On You

- Language-**theoretic** Security
  - Impossible to convey how practical LangSec is if the recipient repudiates theory
  - In theory, theory and practice are the same. In practice, they are not.
    - Let's call it Language-practical Security ;)
- **Formally verified** is tainted with #FAIL
  - Exception: verification people ☺
- **Automaton** is not a word for many people
- **Grammar** reminds people of their ugly Russian language teachers at school

Helmbrecht's Law

- Whoever uses a car-comparison or crash testing analogy in a discussion about software security, is immediately wrong.



Jason Knowles

More: Bio, Facebook, Twitter, News Team

April 29, 2014 (WLS) -- The ABC7 I-Team is learning more about the "heartbleed virus" and how you can be a victim without even knowing it.

The popular software used to protect your personal information has been compromised, but that threat is confusing some people.

This not something you should blow off.

Related Content

MORE: E-mail the I-Team
MORE: LIKE ABC7Chicago on Facebook
MORE: Follow ABC7Chicago on Twitter

Technology experts say that the "Heartbleed Virus" is widespread and hit 66 percent of all websites over the past two years.

So the I-Team wanted to know what people are doing to stop the bleeding.

Heartbleed. The term comes from the communication between two so-called "hearts" on a server which verify your security as you shop, check e-mails and bank statements. There is now a backdoor break-in between those hearts, and it's bleeding.

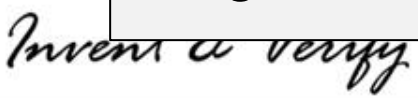
That sounds not very agile!

MAKING BUSINESS CASES

The Sorcerer's Apprentice Develops an API

That old alchemist has vanished
And for once has gone away!
Spirits called by him, now banished,
My commands shall soon obey.
Every step and saying
That he used, I know,
And with web sockets obeying
My arts I will show.

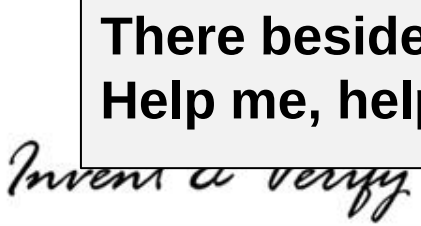
Stop now, hear me!
Ample measure
Of your treasure
We have gotten!
Ah, I see it, dear me, dear me.
LangSec's word I have forgotten!

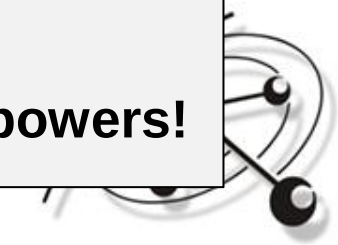


The Sorcerer's Apprentice Develops an API

The bug returns, more 0day dragging!
Now I'll throw myself upon you!
Soon, 0 goblin, you'll be sagging.
Crash! This sharp patch has undone you.
What a good blow, truly!
There, it's fixed, I see.
Hope now rises newly,
And my breathing's free.

Woe betide me!
New bugs scurry
In a hurry,
Rise like towers
There beside me.
Help me, help, oh LangSec powers!





The Stability Argument

- Business suffers from large costs when APIs need to be changed
  - Example: Apple iOS address book API
- API changes for security are even worse
- Stable APIs increase agility of development for the hipster apps
- Unstable APIs cause an explosion of development cost
  - Ask Fabs about the Linux Kernel

The Generator Argument

- Grammars scare people
  - Generating code automatically makes them wanting grammars
- Product Houses in enterprises know the cost of not having a grammar
  - Hence XML
- Providing a process to agree on interface grammars is providing a strong business incentive to the people that matter
  - If you save someone money, they don't ask how you did that, they just do as you tell them

The Agreement Machine

- Given a set of strong data types…
- For each product group…
  1. List information to handle
  2. Strongly type all fields
  3. Send to all product groups
  4. Request signoff
  5. If not signed off, goto 1
- Generate code for all product groups: Nail it

1	Name	var String
2	SpargelSize	var int

1	Name	var UTF8
2	SpargelSize	var unsigned int

1	Name	var UTF8
2	SpargelSize	unsigned int32

1	Name	UTF8[200]
2	SpargelSize	unsigned int32

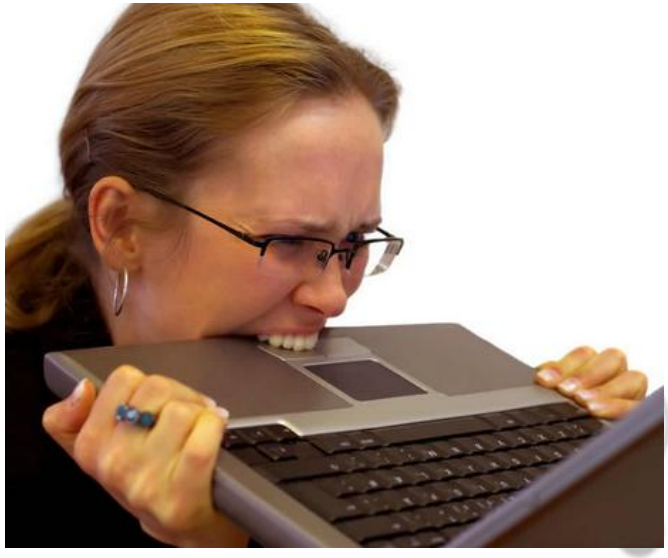
Unfortunately, MLP pointed out NP.

The Agreement Machine Scales

- Standardization Committees have the same problem: n^2
- The standard solution is to agree on disagreement, also known as Vendor Extension
  - IPv6 is a prime example

The Liability Argument

- Lack of Product Liability is the root cause
  - The business case is in selling broken software
- Liability will come back in one form or another
  - Regulation is liability
  - Lean back and watch me go
- Liability flips the business case towards selling working software
- LangSec allows small components to be composed safely
  - Agile trust architectures deal with the authorization



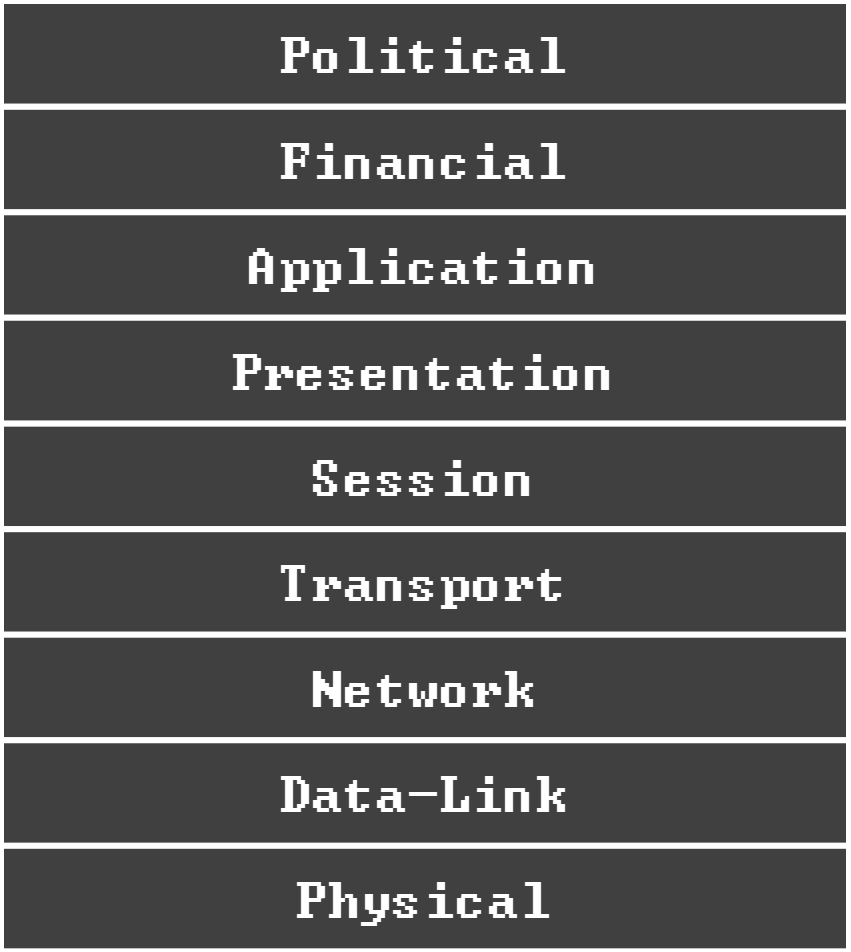
Dear Academia, I have some wishes for Xmas …

WHAT WE NEED NOW

The Stack Is A Lie

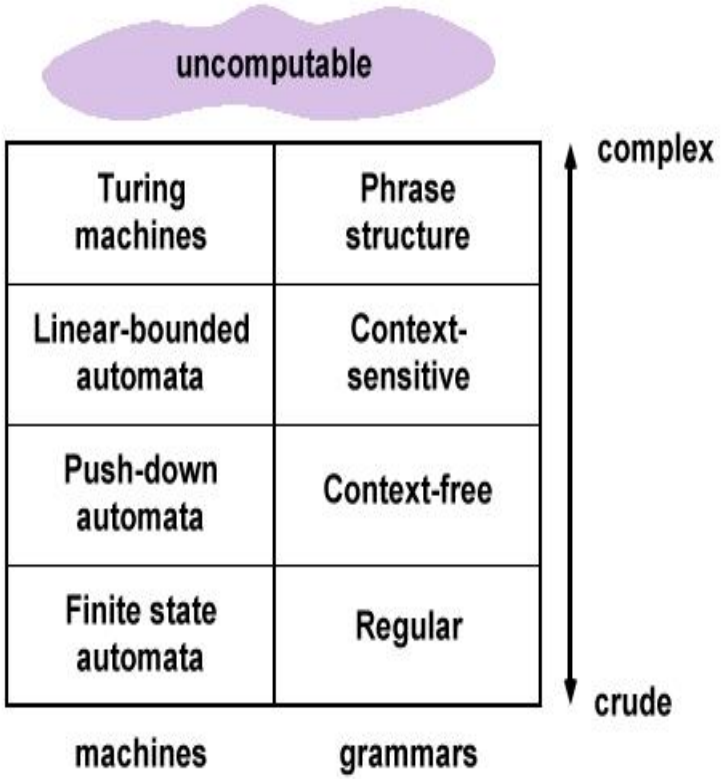
- Systems are composed, not stacked
- Composition works best when the properties of the instruments are known
  - Sound properties
  - Physical properties
- We need a standard reference model:

The LangSec Orchestra



Language Complexity Proof

- Andreas Bogk's Proof Engineering request seconded
- The Agreement Machine only works if we can automatically and reliably tell language complexity



To all you war waging retirees
All you bot herders and runners
All you Comment Group soldiers
And FinFishing Simon coward liars

To all you listening Stasi dealers
All you forum egos, trolls and leakers
All you Data Retention law abiders
And you C-board data protection liars

Form Up and Brace Yourself!

Then Watch LangSec Ruining Your Day!

Thank You!

Felix ´FX´ Lindner
Head

fx@recurity-labs.com

Recurity Labs GmbH, Berlin, Germany
http://www.recurity-labs.com

Invent & Verify