20. Mai. 2015

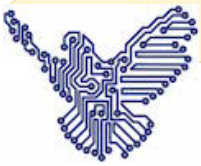
von gast

in Cyber Security, Security Culture

Kommentare (0)

Why language matters – The inherent insecurity of languages and what we can do against it

by Florian Grunert



Part VIII of our series on cyberpeace

The prefix *cyber*, prepended onto terms like war, peace, security, and so on, results in interesting word combinations which we construct with our spoken language. Many scholars, from political to social science, have discussed the terms and the semantics of it in order to understand the problem and to create some scientific value out of it. But this article will not be another endless discussion on whether *cyberfoo* exists [1] somewhere in any computer network at the moment or not.

The careful reader has seen that the title of this article has something to do with language – but not only with our spoken languages. What I want to discuss is a theoretical aspect of defense research regarding the inherent insecurity of computer languages and their usage in today's computers, which are programmed by human beings (most of the time). This article is an offer and maybe a response to the article How to Abolish Cyberwar by Dr. Miriam Dunn Calvelty.

Stop Weird Machines – Photoshopped by Kythera of Anevern

Dr. Cavelty outlines in her article that one of the inherent security problems is Information Technology itself, which leads her to an interesting conclusion.

> *It means changing the skewed balance between offense and defense in the favor of defense. Ultimately, the solution must be a secure and resilient cyberspace that is no longer strategically exploitable.*

SOCIAL MEDIA

SUCHE

Suche...

Suche

TWITTER FEED

Die offene Gesellschaft im Zangengriff – Was tun gegen islamistischen #Extremismus und #Islamfeindlichkeit? https://t.co/he1sNyzNRo
27. Januar 2016, 7:40 from Twitter Web Client

Diana Schubert über die Rolle von #Kommunen in der #Prävention von #Radikalisierung https://t.co/6F0QGmsxoQ #Salafismus
26. Januar 2016, 7:54 from Twitter Web Client

Fördern die Medien #Salafisten? Dynamiken, Verantwortung & Grenzen der Berichterstattung über salafistische Gruppen https://t.co/YM8phOlqdf
25. Januar 2016, 9:14 from Twitter Web Client

TAGS

BELIEBT KOMMENTARE NEU

"Die Flüchtlinge", "die Rassisten" und "Wir" – zu den Ambivalenzen

So she asks for

> *[…]investing in IT Security research and education, into the exposure of computer vulnerabilities by technologically apt people ("hackers").*

Language-Theoretic Security is one of these investments or investigations we should take seriously and which focuses on exactly what Dr. Dunn Cavelty is asking for.

Why Language-theoretic Security matters

I want to briefly outline the impact of Language-Theoretic Security and its possible impact on some security flaws we have at the moment. Let us start with some basics to understand the importance of this research.
[Disclaimer:This article is not written for technical readers who are familiar with the theory of computer languages and computation]

Every computer gets inputs (e.g. a program) which tell it to do what it should do. But sometimes the input is not correct or may be manipulated by a third entity. Both of these scenarios can cause unwanted behavior. Sometimes a user becomes aware of it because the machine freezes, and sometimes, when you are lucky, you get the so-called Blue Screen of Death (BSODs). Either way, something is going wrong. That said, obviously not all of your BSODs can be attributed to Language-Theoretic Security problems.

So the input a computer gets is an important aspect of computation and it is therefore important for the security of your computer. If somebody is able to manipulate the input at the moment you are browsing over a webpage, the person could harm your machine. But let's expand on the theory behind it a bit more. Due to the fact that most computers only understand binary (Zeros and Ones) input, we have to process our human readable programs into a binary representation which our computer can first understand and then execute.

This obviously has something to do with language, because the computer has to understand what it should execute. And so the computer parses a program written by humans into a binary representation of the actual program.
As you might know, there are a lot of different spoken languages in the world, like English, Spanish or Arabic. The same situation exists in the field of computer languages. There are thousands of different computer languages which can be used to create input for our computer. Similarly, in the field of computer languages we also have different language „families" and most of them are influenced by others.

Now, we know that a computer needs input which has to be processed into its own binary representation of the former generated input out of a computer language. Presumably, then, once this happened, the input will be executed in the way we expected it to behave, right?
Often, that is indeed what happens. But sometimes, the input can be manipulated (in computer science: crafted) and the input is doing something that it was not supposed to do, intentionally or unintentionally. And here we have the problem.

The Problem: Why is my computer not doing what I want it do?[2]

im aktuellen Flüchtlingsdiskurs

Ich bin Paris! Ich bin Muslim! Ich bin Nato? Die offene Gesellschaft und ihre Feinde nach dem 13. November.

Der Dschihad der Auslandskämpfer: Ausdruck einer Subkultur

Terroristen oder Bürgerkriegsflüchtlinge? Was wir gegen diese Verwechslung tun müssen

Fördern unsere Medien die Salafisten? Dynamiken, Verantwortung und Grenzen der Berichterstattung über salafistische Gruppen

KATEGORIEN

Außenpolitik (64)
Bürgerkriege (24)
Cyber Security (52)
Demokratisierung (14)
Drohnen (15)
Flüchtlinge (17)
Humanitäre Interventionen (15)
Innere Sicherheit (32)
Interviews (10)
Katastrophen (4)
Konferenz (29)
Militär (31)
Pandemien (2)
Podcast (7)
Popkultur (22)
Raketenabwehr (1)
Sanktionen (8)
Security Culture (27)
Sicherheits-Kommunikation (16)
Sicherheitskultur (237)
Sozialwissenschaft Online (71)
Stellenangebote (55)
Strategie (12)
Terrorismus (60)

We have two major problems here.
On the one hand we have the (inconsistent) computer languages themselves, and on the other hand we have the processing or parsing from the human readable language to the binary representation which processes this bad input. Both problems should be analyzed accordingly. The inconsistence of languages means that the languages are not correctly defined. A short example from native languages:
Everybody knows this kind of inconsistence with our spoken language. You are talking about a specific issue like „freedom“ or „love“ and if you do not define the words as accurately as possible to your conversation partner, the discussion will end really fast because your conversation partner is not able to understand (parse) your argument (language). Usually we say that „We have a communication problem“. Different researchers and thinkers have analyzed language(s) and these kind of problems thoroughly and with a high probability each one of us can remember at least one situation in their life were the communication problem occurred during a conversation with a human being. But let us focus on the communication problems inside our computers.

We have the similar problems with our computers and the input we create in form of computer programs.
Because a lot of our computer languages are also not strict enough and consistent when it comes to the creation and consumption of the input, they fail like we do. Which means at the end, our computers are insecure. Or like friends of mine always say:

> *ALL PWNED*[3]

In the paper „Exploit Programming From Buffer Overflows to „Weird Machines“ and Theory of Computation“[4]
the group of researchers describe and summarize our modern developed computers in a perfect phrase:

> *The Rise of the Weird Machines*[5]

The Big Picture

These *weird machines* make a lot of attacks possible. Most of the attacks we read about in the news everyday are results of the insecurity of computer languages. And in the context of the current discussion about IT security on a nation-state level, this gets really problematic. We use these *weird machines* to run our countries‘ infrastructure, and to make it worse; we connect them with each other. But what do most nation states do against this dilemma?

They spend money on getting and developing security flaws in our computer systems which they are not willing to fix because they want to use them for their own purpose. For example to spy on other states and their citizens, or to use them in a conflict to have an advantage. They are not spending the money on more research in the field of language security, theorem proving

Theorie (5)
Umwelt (1)
Versicherheitlichung (23)
Visualisierung (6)
Whistleblowing (8)
WikiLeaks (17)
WMD (10)
Zivilgesellschaft (67)

BLOGROLL

Arbeitskreis soziale Bewegungen
Augen geradaus
Dan Drezner
Dart-Throwing Chimp
David Campbell
de.hypotheses.org
Demokratieforschung Göttingen
Duck Of Minerva
Future and Politics
Hylaean Flow
Internet und Politik
IR Blog
Just Security Blog
justsecurity.org
Killer Apps
Kings Of War
MPC Journal – Muslim Politics and Culture
netzpolitik.org
percepticon
shabka.org
Terrorismus in Deutschland
theorieblog.de
Verfassungsblog
Vom Bohren harter Bretter
whistleblower-net.de

ARCHIV

Wähle den Monat

and so on. We humans are not really good in communicating in pure functional languages and/or mathematical logic, but computers are able to do this in a better way than we do. There is hope, because we have researchers who tackle these kind of problems.

If you are interested in the research please feel free to check http://langsec.org/. Please feel free to add more research projects in the comments if you have some in mind. We have to convince more people to invest in this area of security research.

I want to thank some people who helped me to understand the importance of this topic:
@teh_gerg, @41414141, @joernchen, @sergeybratus, @maradydd.

- [1] Foo is a metasyntactic variable, a placeholder for whatever word you want to put in.
- [2] An age-old question.
- [3] https://en.wikipedia.org/wiki/Pwn
- [4] The Halting Problems of Network Stack Insecurity“by Len Sassaman, Meredith L. Patterson, Sergey Bratus, Anna Shubina Source: http://www.langsec.org/papers/Sassaman.pdf
- [5] Exploit Programming: from Buffer Overflows to Weird Machines and Theory of Computation“, Sergey Bratus, Michael E. Locasto, Meredith L. Patterson, Len Sassaman, Anna Shubina. Source: http://www.langsec.org/papers/Bratus.pdf

Tags: it security, laguage-theory, language, programming

« CfP: Macht (in) der Wissenschaft: Kritische Interventionen in Wissensproduktion und Gesellschaft

Stellenanzeigen Mai 2/2 »

Bislang keine Kommentare

Einen Kommentar hinterlassen

Name

Email

Webseite

Kommentar

Wählen Sie alle Bilder mit Straßennamen aus.

reCAPTCHA

Bestätigen

captcha captcha

Soll die Herausforderung einfacher sein?

Datenschutz & Nutzungsbedingungen

Kommentar senden

Benachrichtige mich über nachfolgende Kommentare per E-Mail.