„Something, that is allegedly secure is not necessarily secure, Something, that is allegedly known might turn out to be unknown. Appearance can be deceptive, our senses can deceive us. Even though experience and knowledge can limit errors, reality also limits those.“

*Inspired by Berthold Brecht*

Author: unknown
Learning from the Human Immune System: Artificial T-cells as a Response to Cyber Attacks

Michael Spranger and Dirk Labudde
Sonntag, 9. Juli 2017
Experimental Data → Protein Structure Analysis → DNA Sequence Analysis → Computational Analysis & Gain of Knowledge
FoSIL – Forensic Sciences

General Forensics

Digitalization

Case Data

Computational Analysis & Gain of Knowledge

IT-Forensics
Digital Forensics

Crime Scene Investigations
Biological Data
Digital Data

Visualization

Analysis

© by Grustentier
FoSIL – Expert Opinions

Audio Analysis

Social Engineering

Video Analysis

Scientific-Technical Report

Person Identification

Customized Examinations

Various Calculations

Movement Profiles
Bioinformatics and Forensics - How today's Life Science Technologies can shape the Crime Sciences of tomorrow
The lift in the human body

- organism
- organ
- tissue
- cell
- organelle
functional and structural unit
The cell and the surrounding signaling pathway of EGF

Human Protein Reference database http://www.hprd.org
A human cell and the surrounding omnis celula e celula

- Signal transduction
- Metabolic pathways
- Gen regulation
- Protein-protein-interaction
- Infections
- Specific reactions
- Immune reaction
Why does this work in a cell?

Why can we not implement this in a technical manner?
How does the immune system work?
Transfer pathogens to people

- droplet
- water
- Contact
- Blood and tissue
The Antigen (Virus) and Anti-body

Pattern/signatures for recognition and binding
Pattern recognition

Methods for information extraction
What does this mean for cyber attacks?
Infection of „computer-networks“

Hacker hits on U.S. power and nuclear targets spiked in 2012

Number of annual cyber attacks in the years 2009 to 2014 (in millions)
Targets for critical infrastructure

- Energy
  - Chemical
  - Dams
  - Defense Industrial Base

- Communications
  - Commercial Facilities
  - Financial Services
  - Critical Manufacturing
  - Government Facilities
  - Healthcare and Public Health
  - Information Technology
  - Nuclear Reactors, Materials, and Waste

- Emergency Services
- Food and Agriculture
- Transportation Systems
- Water and Wastewater Systems
Types of Malware

- Virus
- Adwares
- Dialers
- Backdoors
- Keyloggers
- Spywares
- Troyanos
- Gusanos
- Otros
Common characteristics

Malware is similar to a software: it consists of a program code that can perform various actions when it is activated or started.

In contrast to serious software, however, the unwanted code usually tries to spread unintentionally. This can be done independently or with the help of other programs/functions.

After infection, the malware continues to hide (to download program codes from the Internet, to send SPAM or to spy on personal data), or to identify itself by trying to blackmail the user, delete files, or encrypt and unwanted ones Web pages.

A computer virus regularly consists of three parts.
• replication unit
• trigger
• Payload
Malware

- time-independent detection
- Specific and adaptive antibodies
- isolation

Current security systems:

- Virus Scanner
- Real-time protection
- firewall management
- mail protection

Problems: signatures too old, Adaption to slow (there is no really adaption), heuristics not good enough (minimal true positives)
Virus Scanner – new/old ideas

Real time scanning (continuously)
- all components
- random access memory
- Known signatures
- Algorithms for the prediction of unknown signatures (Genetic algorithms)
- code scanner (emails, documents) – new software fragments (quarantine)
- Automatic (semi-automatic) penetration tests

New independent components
- Information units for the whole network
- Scanning of trigger units - Logical network
Virus Scanner – new/old ideas

Adaption of the biological process

New independent component
Virus Scanner – new/old ideas

New independent component

<table>
<thead>
<tr>
<th>Non-specific Response</th>
<th>Specific Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pathogen</td>
<td>T-killer cell</td>
</tr>
<tr>
<td>Macrophage 1. digests pathogen</td>
<td>activates</td>
</tr>
<tr>
<td>2. presents fragments of pathogen (antigens)</td>
<td>Antigen-Receptor</td>
</tr>
<tr>
<td>T-helper cell</td>
<td>B-lymphocyte</td>
</tr>
<tr>
<td></td>
<td>forms</td>
</tr>
<tr>
<td></td>
<td>Plasma cell</td>
</tr>
<tr>
<td></td>
<td>produces Antibodies</td>
</tr>
<tr>
<td></td>
<td>Memory cell stores characteristics of pathogen</td>
</tr>
</tbody>
</table>

Classical Virus Scanner

Signature modulation

Σ modulations

activation

elimination

isolation
Topology encapsulates
THE INFILTRATION GAME

Artificial Immune System for the Exploitation of Crime Relevant Information in Social Networks

Securing the signal transduction of the socio-technical environment: Social network (Facebook)
“Most massive attack in Leipzig since the Pogrom Night in November 1938”

[LVZ 12th January 2016]
Are we able to predict such incidents?

Yes, by monitoring of social networks?
Rage announced and stoked by Social Networks

“Area-wide terrorists attack blonde German women by Muslim asylum seekers.”

Storm on Leipzig!

“Rapefugees not welcome!”
SoNA: A Prototype

SoNA - Social Network Analyzer

Visualization

Contact Network

Press T or P to switch between Transforming and Poking mode.

Outline

Post

Date: Thu Sep 22 13:08:08 CET 2016

Author: PEGIDA

Message

PEGIDA - Schauplatz

Passend zum letzten Posting, die realitätsbetroffenen Neuenmenschen bilden in Bautzen eine Lichterkette vom Kommorkun zum Lichterkante der Meinungs, blind er den Untergang, ja, das können diese Menschen, es ist unfassbar.....

--- Nach Ausschreibung: Bautzen Lichterkette für Toleranz

Zudem wird die Ausgangssperre und das Alkoholverbot für unbegleitete, minderjährige Ausländer wieder aufgehoben.

Challenge – vast amount of profiles
Challenges – closed/secret groups
This is just like pathogens, isn’t it?

Remember, what does the human body do?
Human Immune Response System

**Non-specific Response**
- Pathogen
- Macrophage
  - 1. digests pathogen
  - 2. presents fragments of pathogen (antigens)

**Specific Response**
- T-killer cell
  - destroys infected body cell
- T-helper cell
  - activates
- B-lymphocyte
  - forms Plasma cell
- Antigen-Receptor
- Antigen-Antibody reaction
- Produces Antibodies
- Digestion
- Macrophage
- Memory cell stores characteristics of pathogen
Can we do this for social networks in the same way?

Are we able to construct an artificial immune system?
Agent-based Social Network Analysis

**Agency**

\[ P^C = \{ \text{Candidates} \} \]  \[ f^A (P^C) \]  \[ f^E (A) \]

**Ensemble**

\[ p_j \]

**Agent Generators**
Conclusion

Classical Virus Scanner

Signature modulation

Σ modulations

activation

elimination
FEEL FREE TO ASK QUESTIONS

VISIT US AT: www.bioforscher.de/FoSIL