GOETHE UNIVERSITÄT FRANKFURT AM MAIN

DIGITAL SECURITY

THE THREAT ECOSYSTEM AND CYBER DEFENSE

MASTER SEMINAR | GOETHE UNIVERSITY FRANKFURT | SUMMER 2019 | DR. GÖKHAN BAL

About Gökhan Bal

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

1983

Computer Science

Doctorate

Outer Space

Frankfurt

mail@goekhanbal.de

Science Fiction

Marriage

Digital Security

Child(ren)

cyberandresistant.de

Deutsche Bahn

GOAL: YOU KNOW ABOUT…

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Cyber Threat Ecosystem

- Threat Actors
- Major Cyber Attacks
- Attack Strategies & Techniques

Attack Targets

- Human
- Machine
- Impacts

Cyber Defense

- Security Operations
- Threat Intelligence
- Incident Response

WARM-UP

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

- Grab your smartphones
- Open https://kahoot.it

DOT-DASH-DISS OF 1903: FIRST HACK EVER?

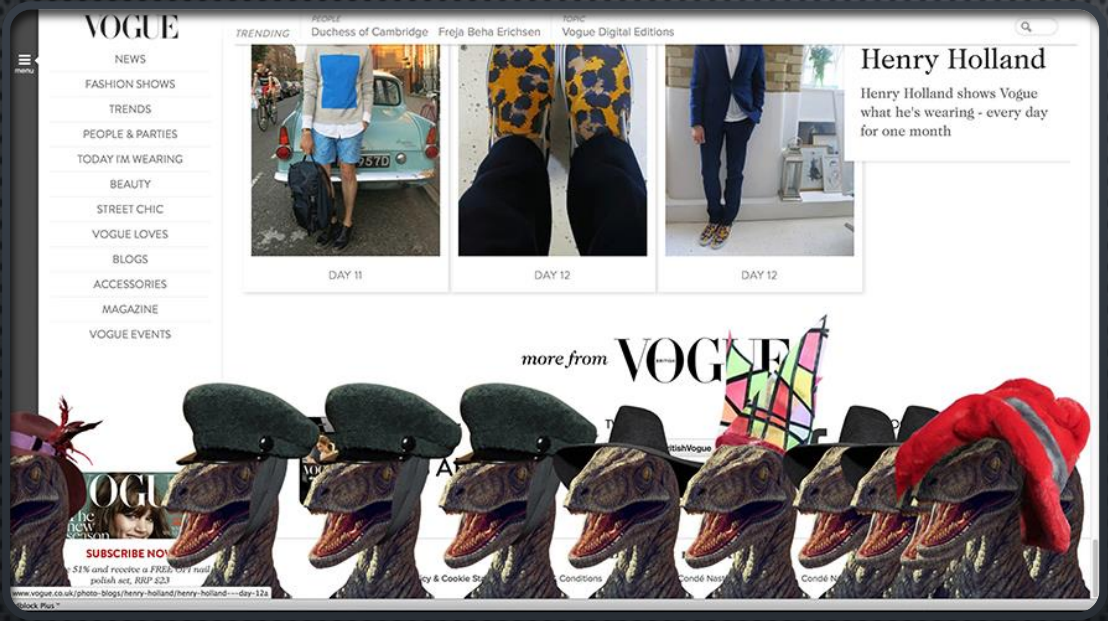
GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Magician Nevil Maskelyne used Morse code insults to disrupt a public demo of a wireless telegraph

He justified his actions on the grounds of the security holes it revealed for the public good.

https://www.newscientist.com/article/mg21228440-700-dot-dash-diss-the-gentleman-hackers-1903-lulz/

HACK EXAMPLE 2: WEB DEFACEMENT



Velociraptor parade
Unknown hackers injected some extra visuals to Vogue UK's website in 2013

https://www.core77.com/posts/25201/thanks-to-hacker-vogue-uks-new-fashion-rage-dinosaurs-in-hats-25201

HACK EXAMPLE 3: PRIVATE DATA LEAKS (1)

Hackers repeatedly published private photographs of major celebrities, including Jennifer Lawrence, Kim Kardashian, Kate Upton and Kirsten Dunst, e.g. by hacking thousands of Apple's iCloud accounts

https://thehackernews.com/2017/03/fappening-emma-watson.html

HACK EXAMPLE 4: PRIVATE DATA LEAKS (2)

Image from: https://www.bbc.com/news/world-europe-46757009

20-year old German publishes private data of many German politicians and celebrities ("doxing")

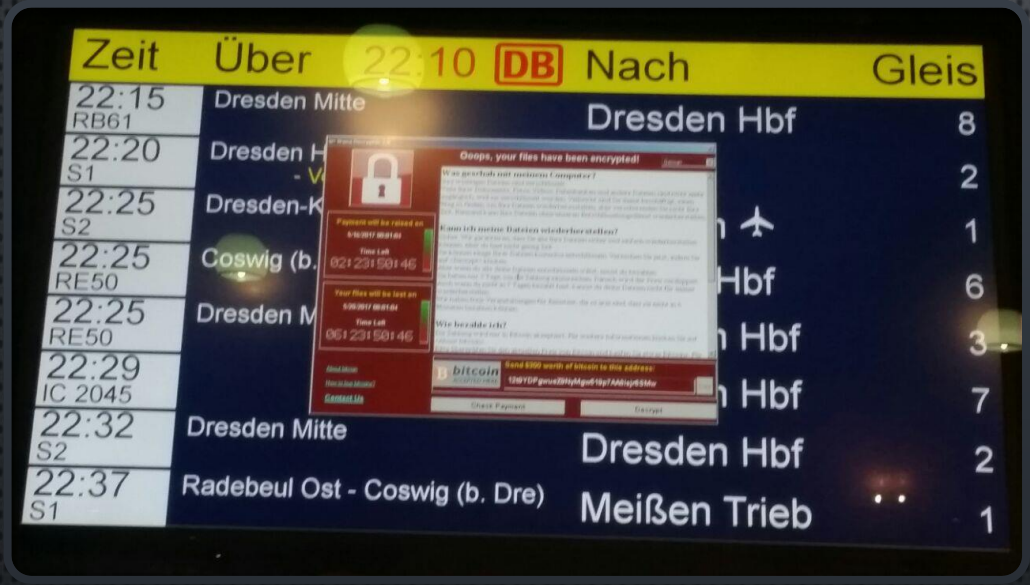
HACK EXAMPLE 5: MASSIVE DDOS ATTACK

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

A distributed denial of service (DDoS) attack from the "Mirai" botnet brought down much of America's internet in 2016. It was likely the largest of its kind in history.

https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

HACK EXAMPLE 6: WANNACRY & (NOT)PETYA RANSOMWARE WAVE OF 2017



The ransomwares "WannaCry" and (Not)Petya" hit many organizations worldwide. Deutsche Bahn was one of the most prominent victims in Germany.

Image from: https://www.heise.de/imgs/18/2/2/0/1/2/4/4/wannacry-bahn-martin-wiesner-a718e18efcf3ef8e.jpeg

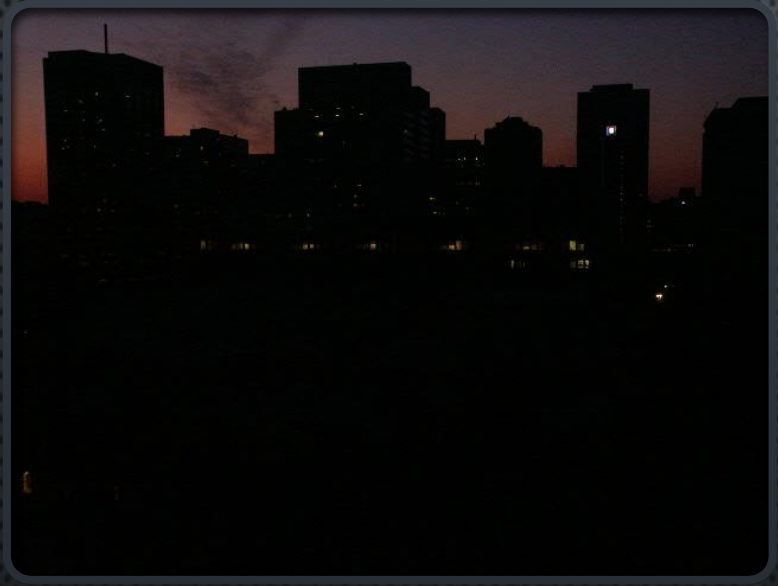
HACK EXAMPLE 7: STUXNET

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

"Stuxnet targets SCADA systems and is believed to be responsible for causing substantial damage to Iran's nuclear program [in 2010]. "

https://en.wikipedia.org/wiki/Stuxnet

HACK EXAMPLE 8: BLACKOUT IN UKRAINE



"A power failure that plunged parts of western Ukraine into the dark last month was caused by a cyberattack."

https://phys.org/news/2016-01-experts-ukraine-blackout-cyberattack.html

NOT A DEFINITION OF HACKING

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

HACKING IS ABOUT MANIPULATING PEOPLE AND/OR MISUSING INFORMATION TECHNOLOGY TO HARM PEOPLE, ORGANIZATIONS OR STATES

THE IMPACTS ARE NOT „CYBER“

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

PRIVACY INVASION

REPUTATION LOSS

FINANCIAL DAMAGE

MISINFORMATION

IMPACT

PHYSICAL OR PSYCHOLOGICAL HARM

IDENTITY THEFT

ACTIVISM

INFORMATION LOSS

THE SEMINAR TOPICS

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

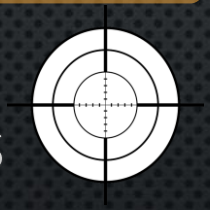
Topics 1+2

Cyber Threat Ecosystem

- Threat Actors
- Major Cyber Attacks
- Attack Strategies & Techniques

Topics 3+4

Attack Targets



- Human
- Machine
- Impacts

Topic 5

Cyber Defense

- Security Operations
- Threat Intelligence
- Incident Response

TOPIC 1: THREAT ACTORS & ECOSYSTEM

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

- Who are the threat actors (categories, groups)?
- What are their Motivations?
- What are their strategies, Tactics and techniques?
- How is the cybercrime ecosystem organized?
- What is "cybercrime as a service"?
- What were major hacks and cyber attacks?

TOPIC 2: HUMAN HACKING: SOCIAL ENGINEERING

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

- What is Social Engineering (SE)?
- What are techniques of SE?
- What are famous examples and players of SE?
- How to protect against social engineering?

TOPIC 3: HUMAN RESISTANCE

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

- What is the „Human Factor“ of Security?
- Why is the human the „weakest link“ of security?
- What are methods to increase human resistance against cyber attacks (Security training & Awareness)?
- What are usability issues of security technologies?
- Design of a small security awareness campaign for students

TOPIC 4: MACHINE VULNERABILITY

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

- What are technical vulnerabilities?
- What is the role of vulnerabilities in cyber attacks / hacks?
- What methods exist to increase machine resistance against cyber attacks?
- What are 0-day-exploits?
- What is the „vulnerability ecosystem“?
- What is a bug bounty program?

TOPIC 5: CYBER DEFENSE

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

- What are organizational measures for cyber defense?
- What is a SOC / CERT / CSIRT?
- What is Security Monitoring (SIEM[1]), Threat Hunting and Incident Response?
- What is Threat Intelligence?
- What is a Penetration test / Red Team Attack?

[1] Security Information and Event Management

Topic Assignment

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

- Topics are assigned to Groups of 3-4 Students
- Groups narrow down Topics
- Topics are worked out by the groups
- Results are presented by the groups (details follow)

TOPIC OVERVIEW

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

1 Threat Ecosystem

- Who are the threat actors?
- What are their Motivations?
- What are their strategies, Tactics and techniques?
- How is the cybercrime ecosystem organized?
- What are major hacks and cyber attacks?

2 Social Engineering

- What is Social Engineering?
- What are techniques of Social Engineering?
- What are famous examples and players of SA?
- How to protect against social engineering?

3 Human Resistance

- What is the „Human Factor“ of Security?
- How is the human the „weakest link“ of security?
- What are methods to increase human resistance against cyber attacks?
- Design of a small security awareness campaign

4 Machine Vulnerability

- What are technical vulnerabilities?
- What is the role of vulns in cyber attacks / hacks?
- What methods exist to increase machine resistance against cyber attacks?
- What is a bug bounty program?

5 Cyber Defense

- What are organizational measures for cyber defense?
- What is a SOC / CERT / CSIRT?
- What is Security Monitoring, Threat Hunting and Incident Response?
- What is Threat Intelligence?
- What is a Red Team Attack?

ORGANIZATIONAL - DATES

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

- 15.04.19, 10:00 – 14:00 — Kick-Off | HoF E.01 (Dt. Bank)
- 14.05.19: 10:00 – 14:00 — scientific working essentials / Q&A
- 24.06.19: 10:00 – 18:00 — Presentations (Day 1) | RuW 2.202
- 25.06.19: 10:00 – 18:00 — Presentations (Day 2) | RuW 2.202
- 07.07.19: 23:59:59 (CEST) — Paper Submission (via e-mail)

You are here

ORGANIZATIONAL - PRESENTATIONS

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

- Present the essentials of your topics
- You chose the format (pptx, Flipchart, Quiz, Dialogues, Role playing, Mix,…)
- Interactivity
- Minimal „talk“
- No need to submit upfront
- Evaluation of group performance
- Weight: 40%

Organizational – Paper

- Submission of a scientific paper
- Format: Word or compatible
- length: ca. 30-40 pages (without Appendices, indices and references
- Evaluation criteria: Content, Format, language, References, Quality of citations (scientific criteria
- Statement about individual contributions
- Submission of concept (Optional): 09.05.19, 23:59:59 (CEST) e-mail
- Submission (Final): 07.07.19, 23:59:59 (CEST) via e-mail
- Weight: 60%

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

QUESTIONS?

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Enjoy!