

25-Sep-2019



# Information security: Agents, Attacks, and Tools

Joseph Bugeja

## ABOUT ME



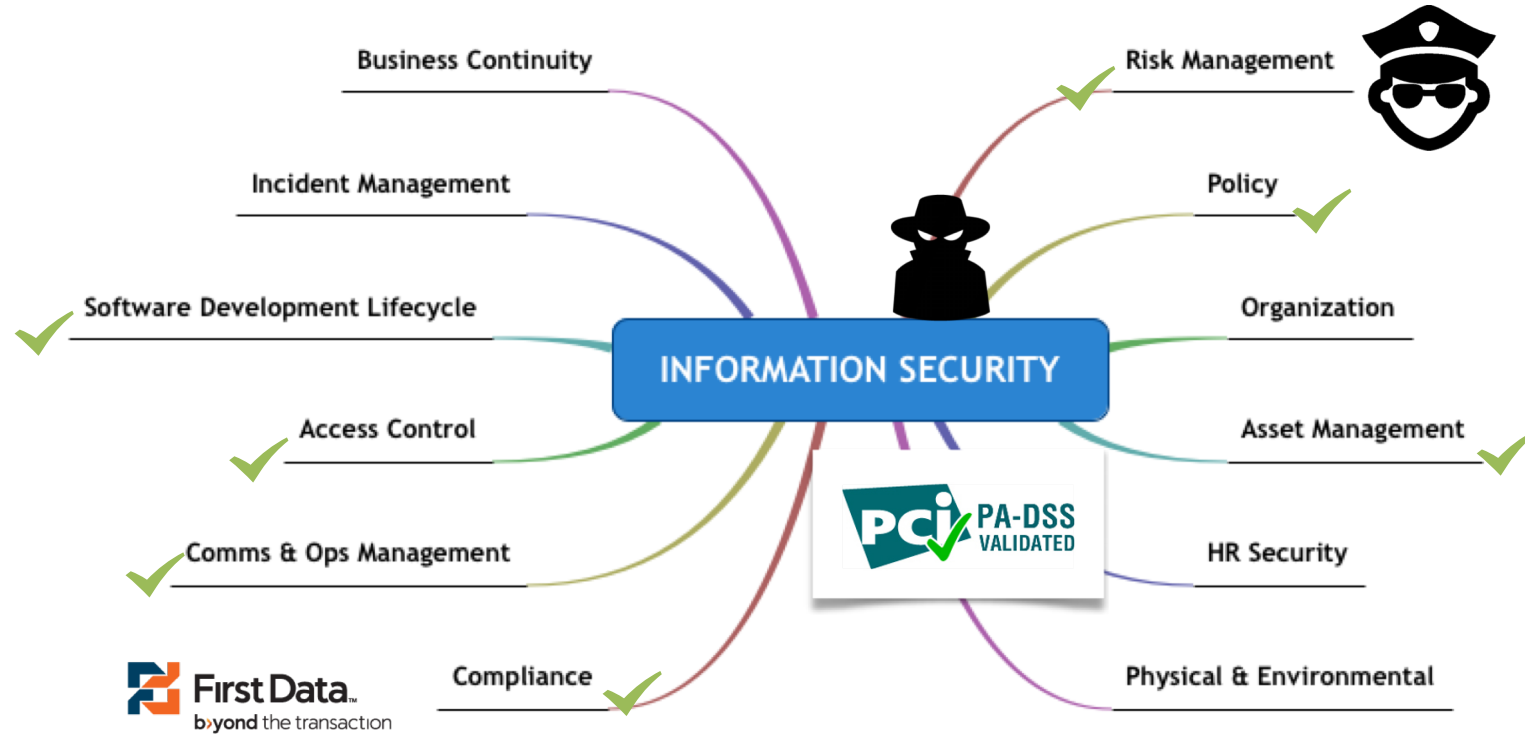
- ✓ Lic in Computer Science, MSc in Information Security
- ✓ 14 years working in the software industry

- ✓ Phd student in Computer Science
- ✓ Main research themes: security, privacy, and Internet of Things



# PROFESSIONAL INFORMATION SECURITY DUTIES

## ✓ Information Security Management Duties



# TEACHING RESPONSIBILITIES AT MALMÖ UNIVERSITY

Start / Training / Computer Science: Information Security

COURSE BASIC LEVEL 7.5 CREDITS

## COMPUTER SCIENCE: INFORMATION SECURITY

[Summary](#)


[Syllabus](#)

[plug](#)

[Registration](#)

Source: <https://edu.mah.se/sv/Course/DA351A>


# AGENDA



**Introduction**




**Malicious Threat Agents**



**Practical**



**The Internet of Things**



**Attacks and Tools**



# INTRODUCTION

# A WHILE AGO AND STILL



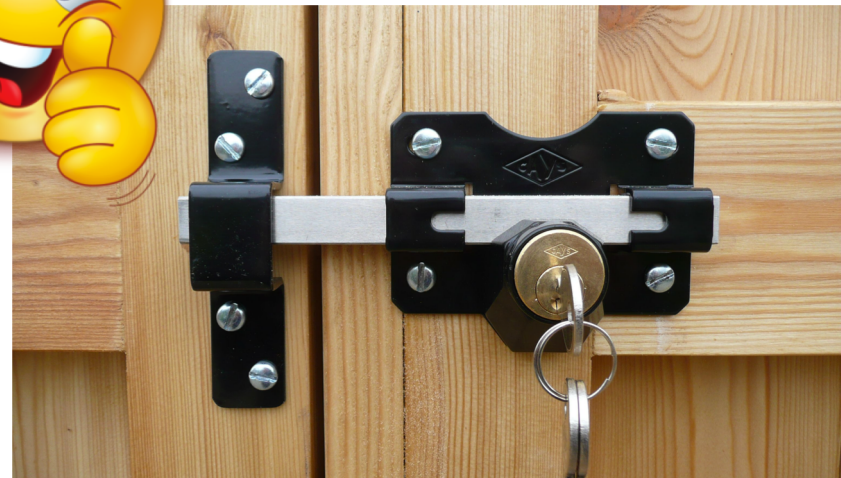
Fences



Seals



Signatures



Locks

Do you think this is  
enough to be secure  
nowadays?





# THE SITUATION NOWADAYS

How can we 'lock' these things?



Smart speakers



Wearables



Drones



Smart toys

# SECURITY THINKING

**Physical**

**Informational**

**+**

**People**

# INFORMATION SECURITY JOBS

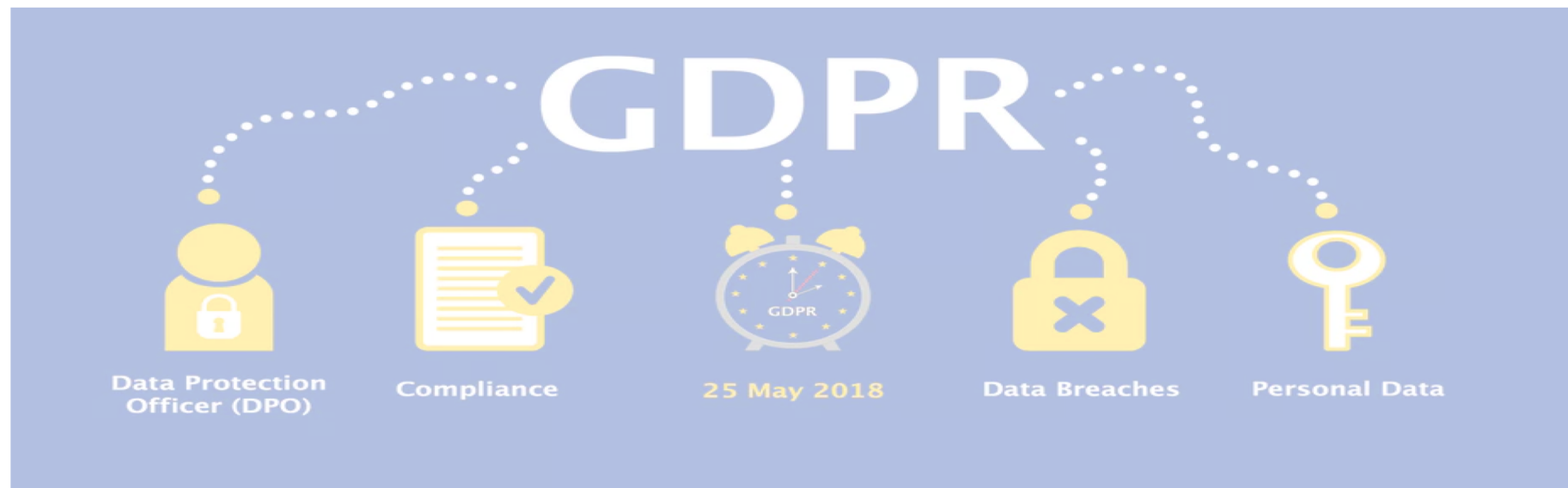
The image shows a side-by-side comparison of job listings from Dice.com and LinkedIn. The Dice.com interface on the left features a search bar with 'Information Security' entered, a filter section for 'Recent Searches' (Cyber Security Jobs), and a 'Filter Results' sidebar with categories like Company Segment, Title, Location, Company, Employment Type, and Work From Home Available. The main job list on Dice.com shows 'Information Security jobs' with 40,276 positions, listing roles such as 'Information Security Analyst' and 'Senior Information Security' from employers like Louisiana Economic Development and CBS. The LinkedIn interface on the right shows a search for 'Information security in Sweden' with 222 results. It lists several job postings, including 'Information Security Specialist' at NetEnt, 'Cyber security Tester' at Volvo Group, 'Senior Information Security Engineer' at Robert Walters, 'Information Security Architect' at Verisure Securitas Direct, 'Information Security and Governance Consultant' at Cybercom Group, 'Group Information Security Architect' at NCC, 'Teknisk Projektledare, Retail' at STANLEY Security Sverige AB, and 'Information Technology Security Consultant' at Zitac.

Source: Dice

Source:LinkedIn

# GDPR introduces a new job position: The data protection officer

IAPP says that as many as 75,000 DPOs may be required worldwide to comply with the regulation.



# SECURITY AND PRIVACY OF CITIZENS IS AT RISK

- ✓ 73,000 private video cameras leaking live footage (2014)



# SECURITY AND PRIVACY OF CITIZENS IS AT RISK

- ✓ Smart devices may jeopardize your security and privacy



*“Hackers could steal personal information and turn the microphone of the doll into a surveillance device”*

*“A hacker could crank up the temperature of a smart thermostat to a sweltering 99 degrees”*

Ransomware PoC FTW!

#Defcon24 #wargames @IoTville

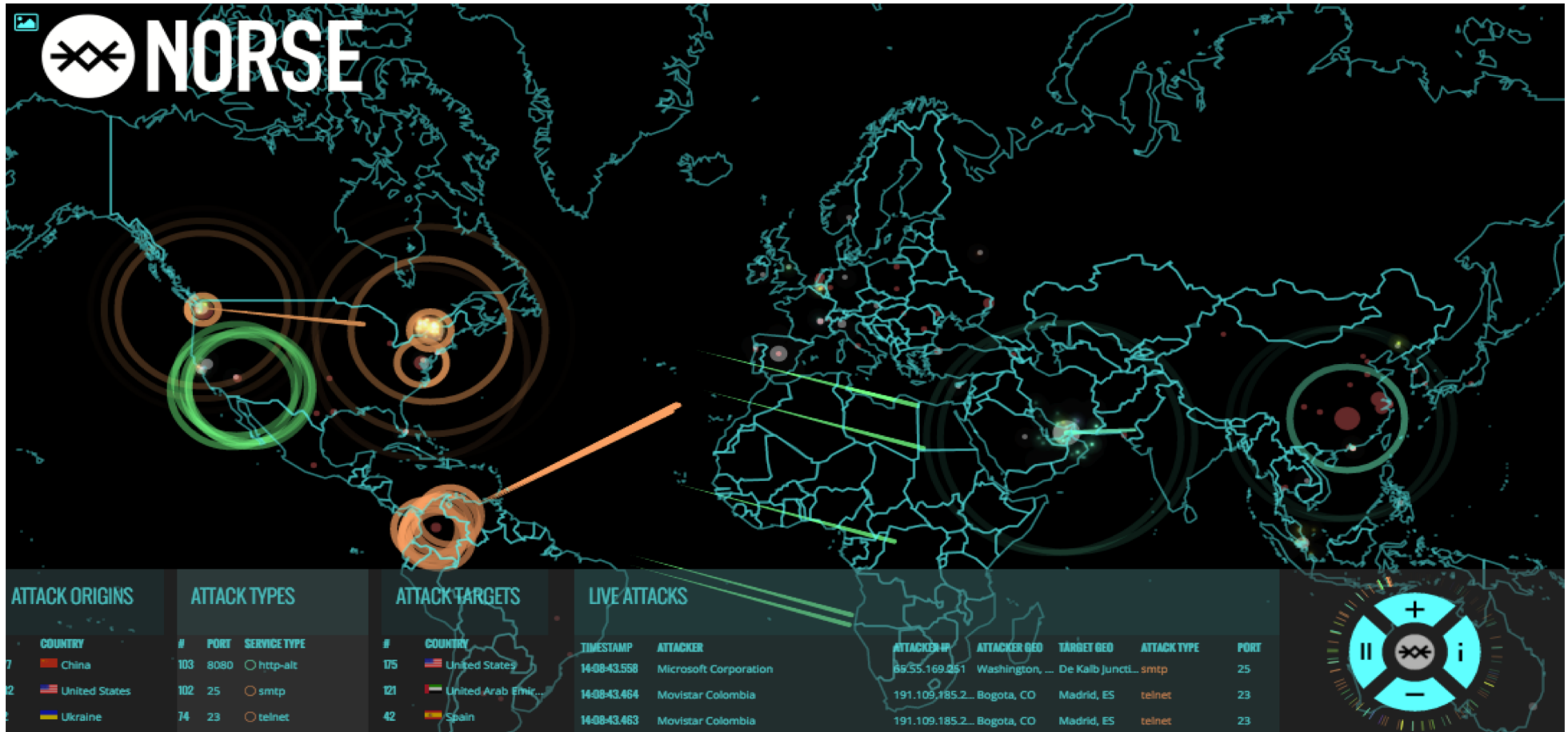


Hackers demonstrated first ransomware for IoT thermostats at DEF CON



*“After hearing the anchor’s comment, their own devices also tried to order pricey dollhouses”*

# EXAMPLES OF LIVE ATTACKS



<http://map.norsecorp.com/#/>

# HAVE YOU BEEN HACKED!?

The screenshot shows the homepage of the 'Have I Been Pwned' website. At the top, there is a dark navigation bar with a logo on the left and several menu items: Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. Below the navigation bar is a large teal section with a white rounded rectangle containing the text '';--have i been pwned?'. Underneath this is a subtitle: 'Check if you have an account that has been compromised in a data breach'. A search form follows, consisting of a white input field with the placeholder text 'email address' and a dark button labeled 'pwned?'. Below the search form is a promotional banner for 1Password, featuring an information icon, the text 'Generate secure, unique passwords for every account', and a blue button that says 'Learn more at 1Password.com'. Underneath the banner is a link 'Why 1Password?'. At the bottom of the page, there is a dark footer with four statistics: '340 pwned websites', '6,474,028,664 pwned accounts', '87,797 pastes', and '96,330,127 paste accounts'.

Source: <https://haveibeenpwned.com/>



# WHAT YOU MAY THINK IS INFORMATION SECURITY

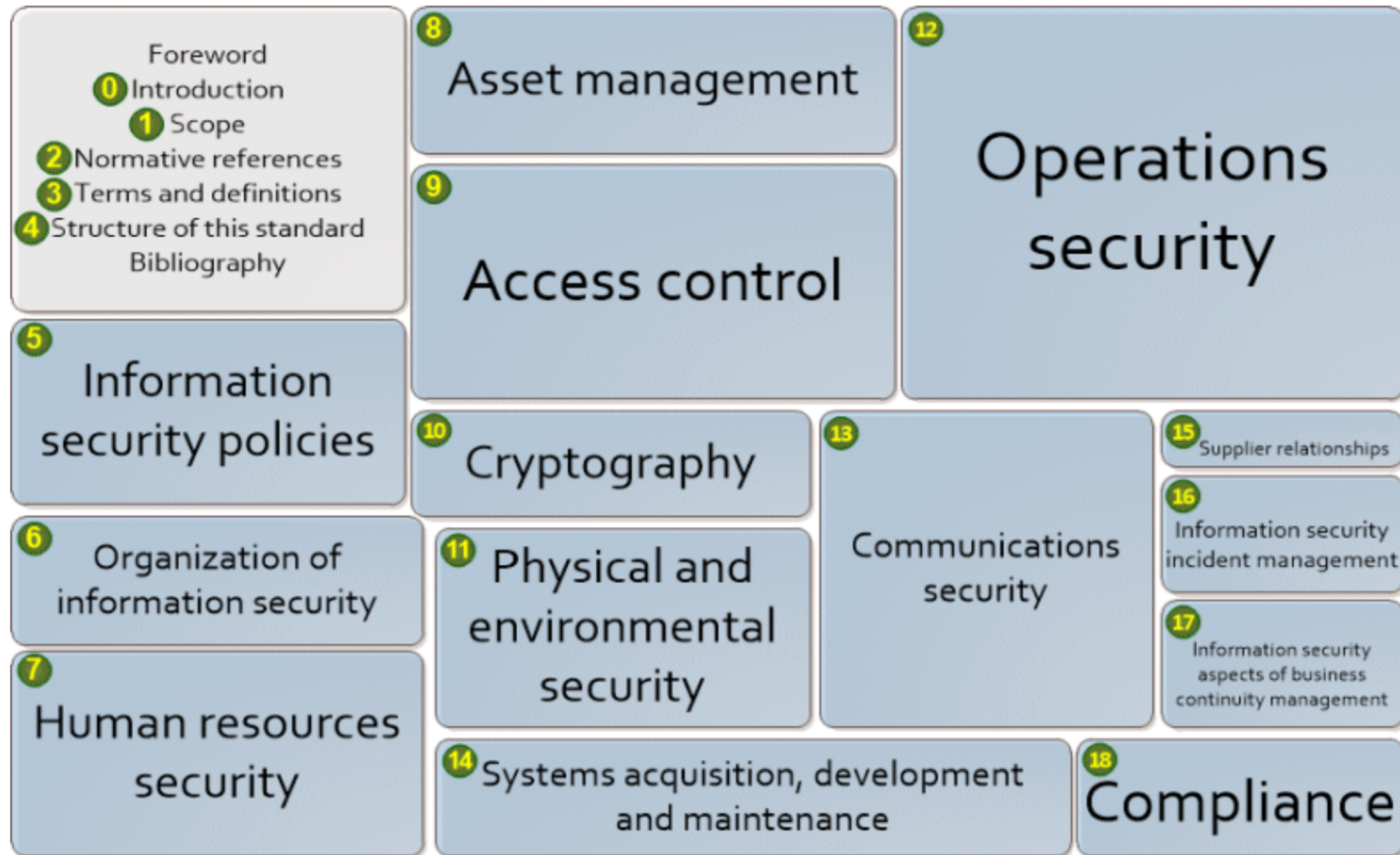


Joseph Bugeja

Doktorander i Lärande

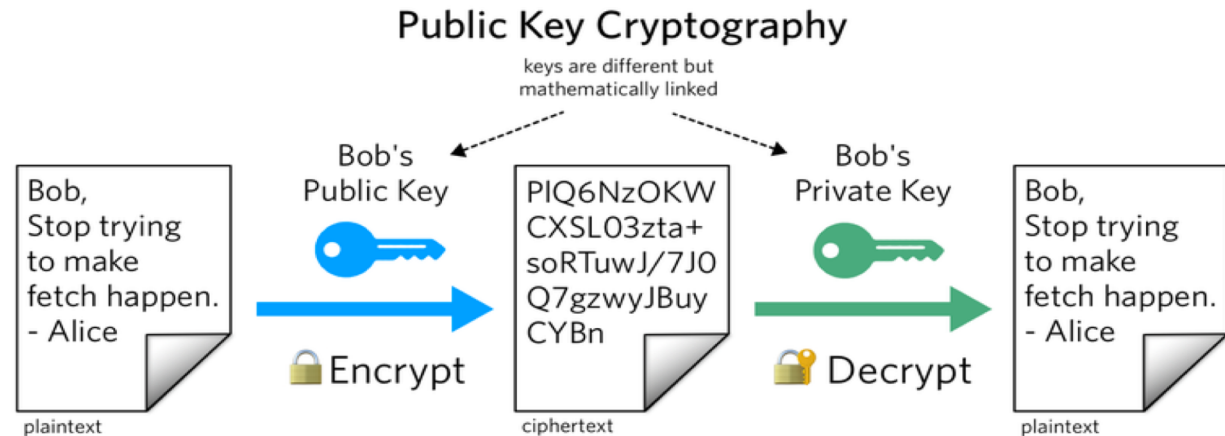
Information Security

# THE DIFFERENT DIMENSIONS OF INFORMATION SECURITY



# SECURITY INCORPORATES A WIDE SPECTRUM OF SKILLS

## MATHEMATICAL



## MANAGERIAL

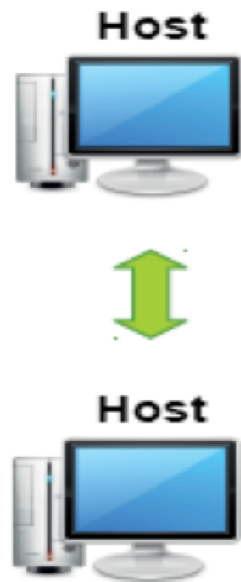




# The Internet of Things

# THE EVOLUTION OF NETWORKING

Network



The Internet



# THE EVOLUTION OF NETWORKING

Mobile-Internet

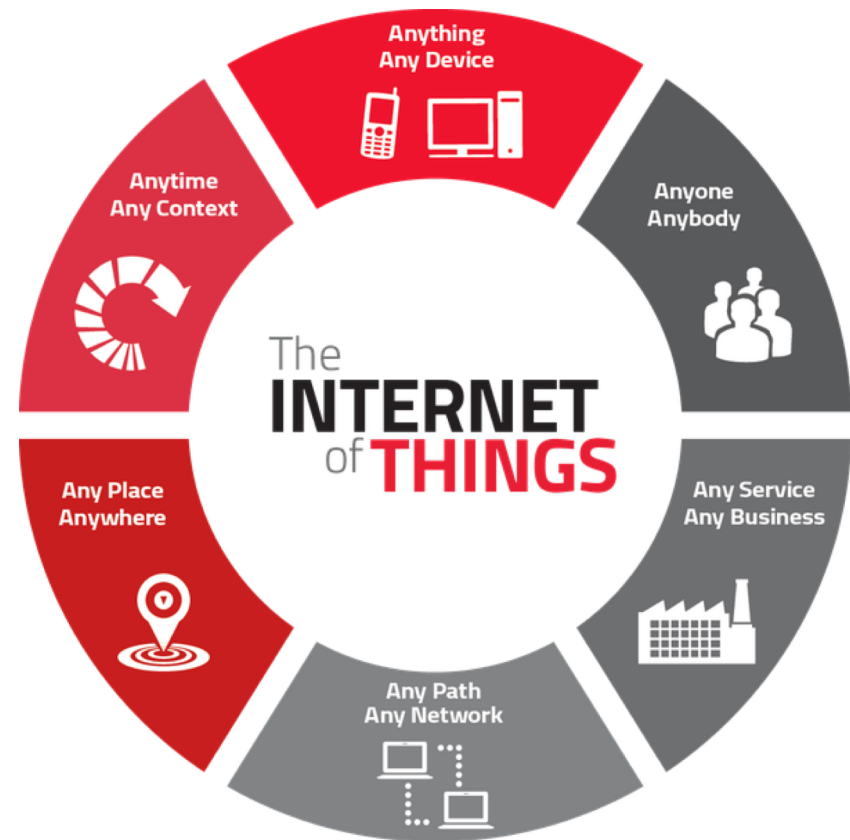


Mobiles + People + PCs



# THE INTERNET OF THINGS

## Internet of Things







# THE INTERNET OF THINGS

✓ **Over 20 billion** Internet of Things (IoT) devices by 2020

✓ Internet-connected devices will **outnumber people** at least 2:1

✓ **Global market size of about \$457B** by 2020



# THE TRADITIONAL HOME



- ✓ Well-defined (solid) perimeter
- ✓ Mostly, uses wired technologies
- ✓ Human persons accessing the home

# THE SMART CONNECTED HOME

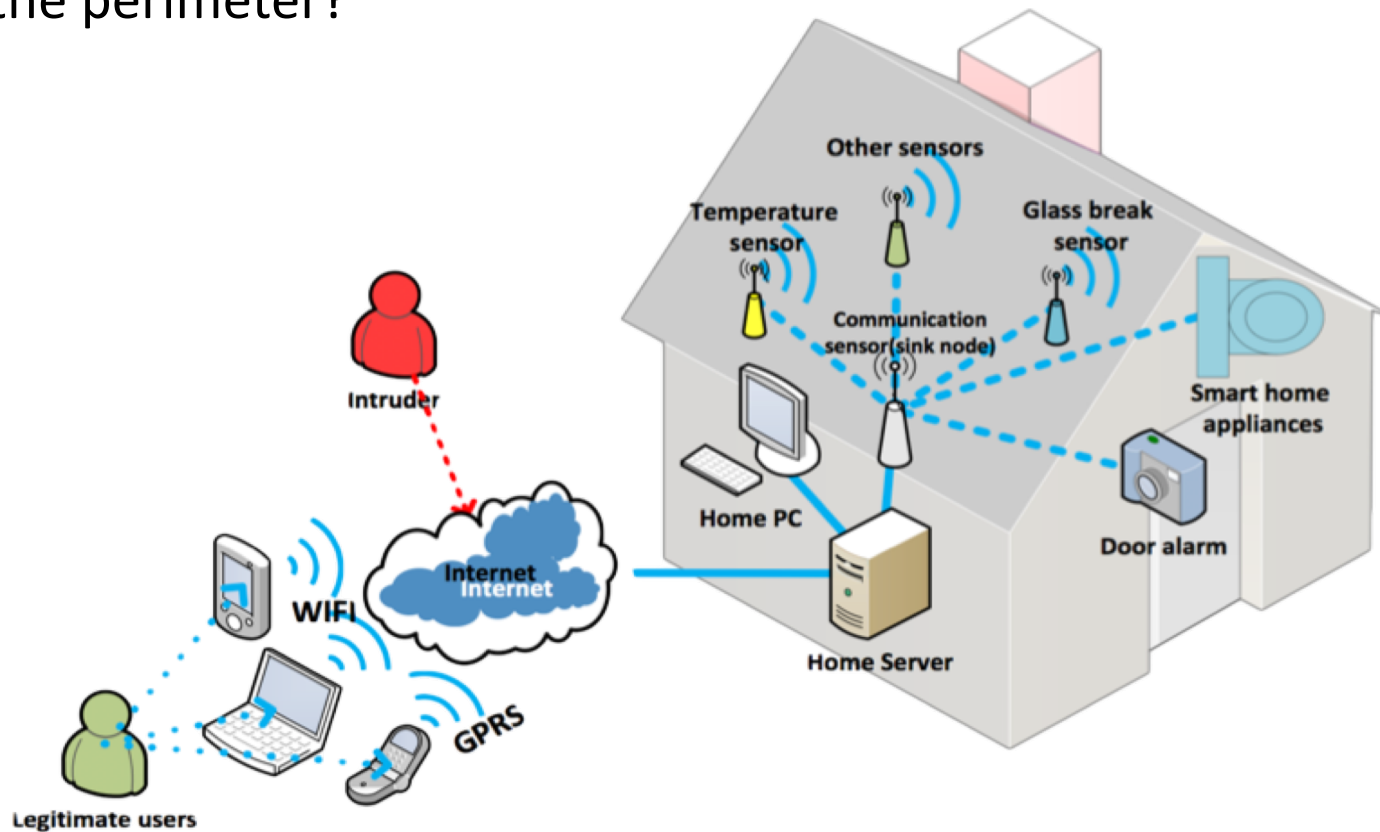
- ✓ A smart connected home leverages IoT technologies to improve the quality and efficiency of life to the residents



Image: Shutterstock

# THE SMART CONNECTED HOME

✓ Where is the perimeter?



✓ Where is my guest list?



# MALICIOUS THREAT AGENTS

## FOCUS ON THE ENEMIES

*“Know your enemy and know yourself and you can fight a thousand battles without disaster”*

*- Sun Tzu*



# LICENTIATE THESIS

STUDIES IN COMPUTER SCIENCE NO 7. LICENTIATE THESIS

JOSEPH BUGEJA



## SMART CONNECTED HOMES: CONCEPTS, RISKS, AND CHALLENGES



# MALICIOUS THREAT AGENTS





# HACKERS

- ✓ Individuals (“hobby hackers”) that include malicious persons, script kiddies, and nosy employees of an organization



- ✓ Viruses, worms, phishing

- ✓ Primarily motivated by curiosity
- ✓ Skill-level: Apprentice



Low

# THIEVES

- ✓ Opportunistic individuals that are associated with stealing mostly for personal financial gain



- ✓ System/physical intrusion, DoS, spoofing

- ✓ Main motive is monetary gain
- ✓ Skill-level: Apprentice



Low

# HACKTIVISTS

- ✓ Individuals or members of a larger group that pursue a political or social agenda



- ✓ DoS, fraud, and identity theft

- ✓ Primarily aim to promote and publicize their cause

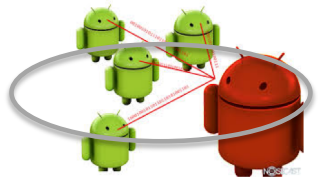
- ✓ Skill-level: Apprentice



Low

# COMPETITORS AND ORGANIZED CRIME

- ✓ Commercial competitors that compete for revenues or resources, and private criminal organizations



- ✓ Botnets, ransomware, and inside information

- ✓ Competitive advantage, CI, and monetization
- ✓ Skill-level: Journeyman



Moderate

# TERRORISTS

- ✓ Individuals that rely on violence or fear-related behavior to support personal socio-political agenda



- ✓ Damage/loss, outages, and physical attacks

- ✓ Terrorism
- ✓ Skill-level: Master



High

# NATION STATES

- ✓ Highly sophisticated individuals that are funded by governments and associated with a military unit
- ✓ Customized malware, spear phishing attacks, and zero-day attacks
- ✓ Cyber warfare, (counter-)intelligence
- ✓ Skill-level: Master

ADVANCED  
PERSISTENT  
THREAT



High

# THREAT AGENT SKILLS

## Low

Minimal technical skills



Largest number of attackers

Easiest to defend against

## Medium

Sufficient technical skills



Locate new vulnerabilities

Threat agents with such skills are likely found in all classes

## High

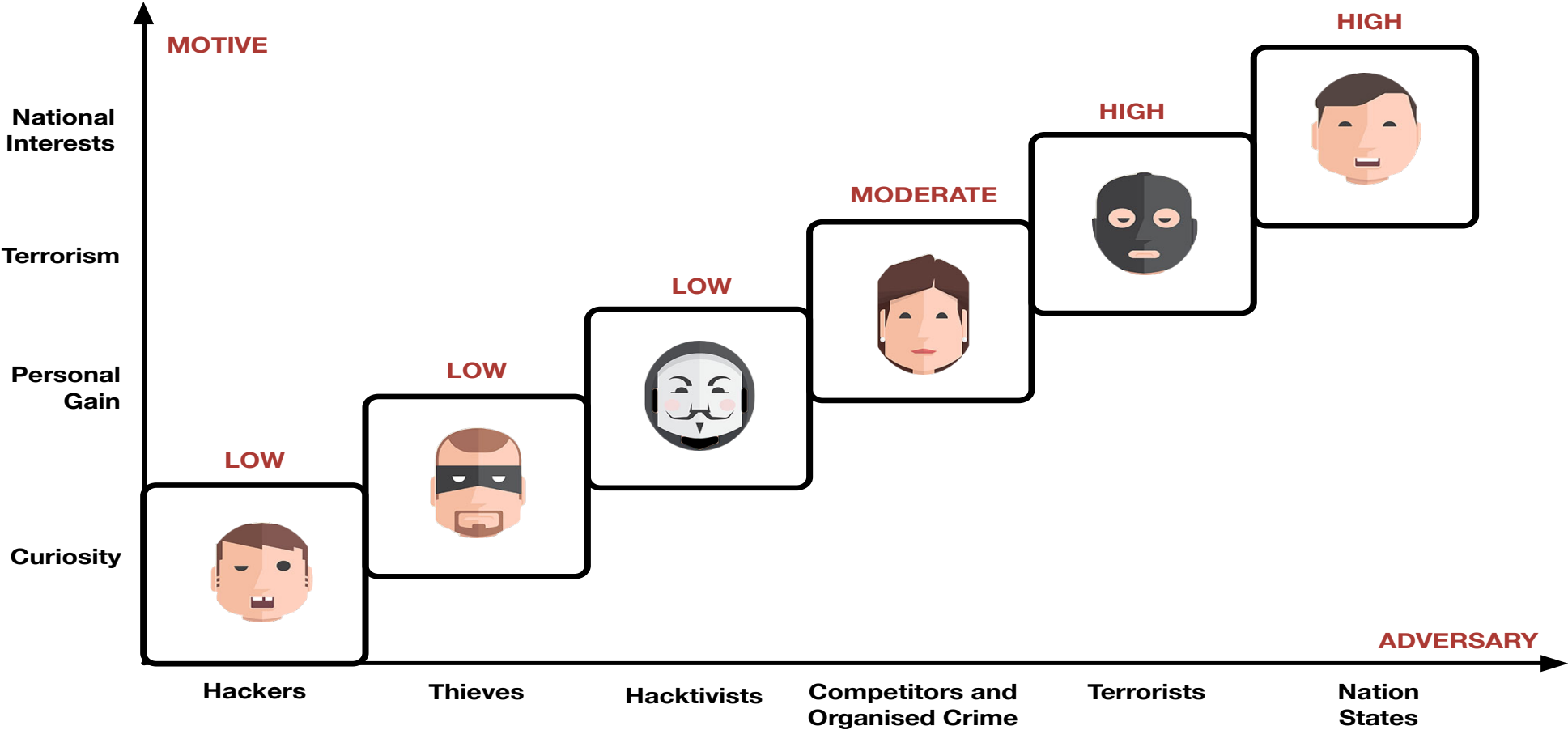
High-level technical skills



Write new powerful attack toolkits

Hardest to defend against

# THREAT MODEL

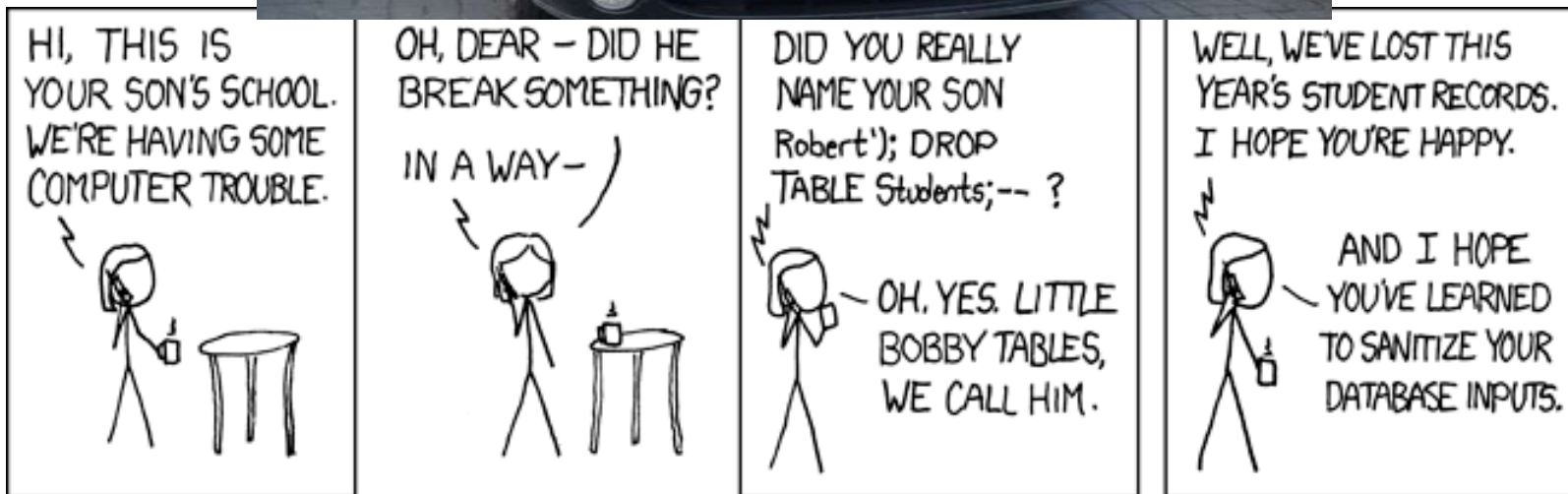




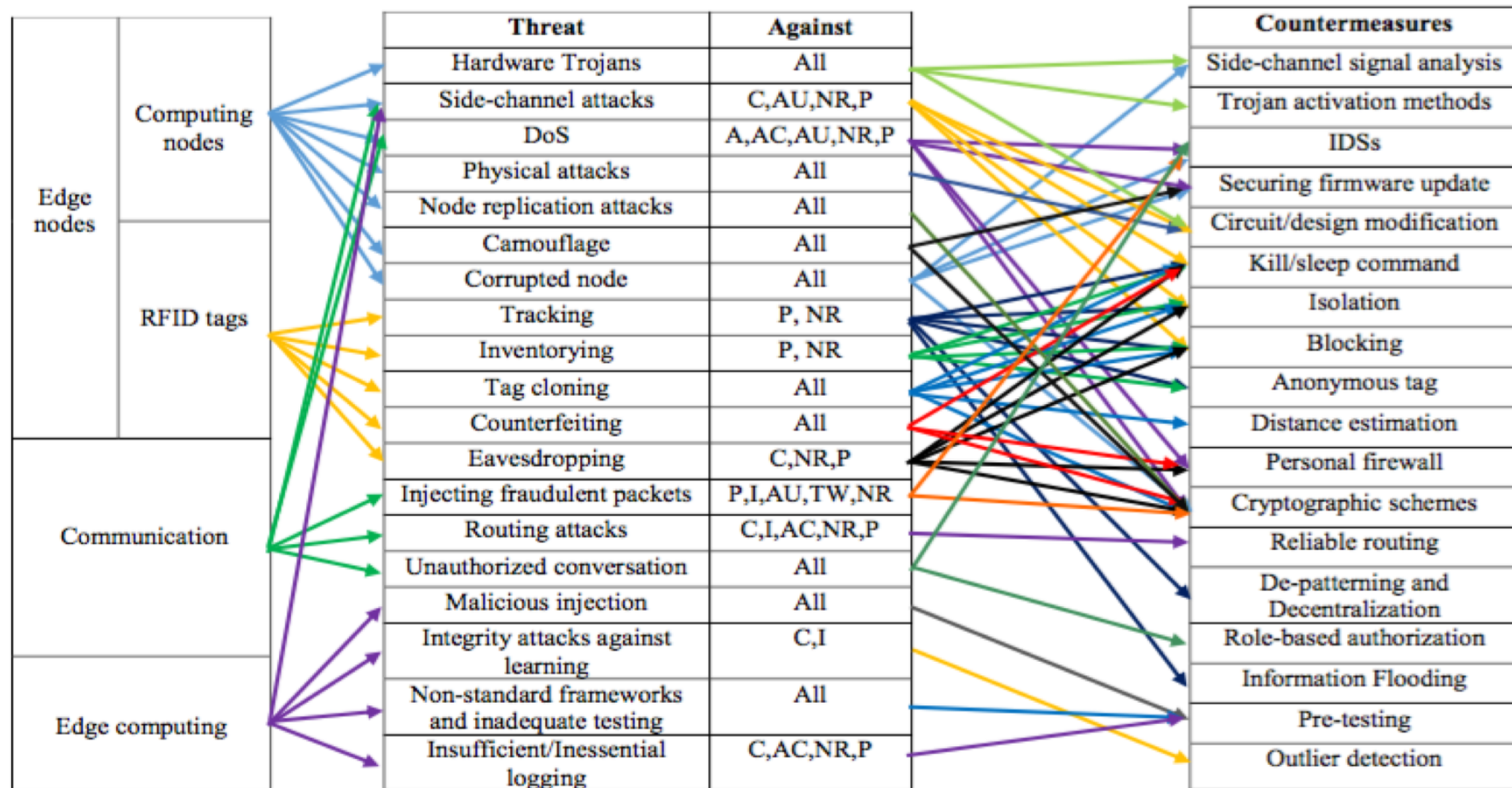


# ATTACKS AND TOOLS

# SQL INJECTION ATTACKS

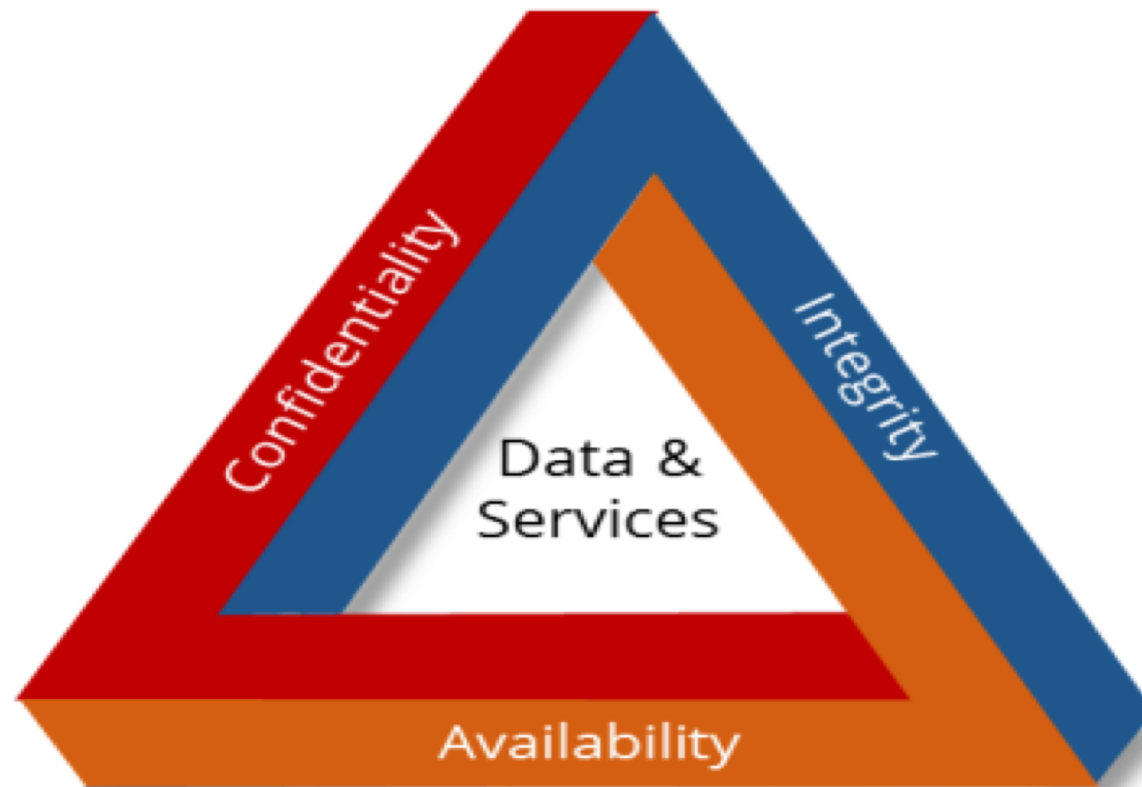


# IOT ATTACKS AND COUNTERMEASURES



Source: Mosenia et al. "A comprehensive study of security of internet-of-things." *IEEE Transactions on Emerging Topics in Computing* 5.4 (2016): 586-602.

# THE CIA TRIAD





## SECURITY TESTING TOOLS

- ✓ There are a variety of toolsets used by security professionals that could also be used for malicious purposes
- ✓ These toolsets are used by penetration testers when testing the security posture of a system
- ✓ The same tools in the hands of an adversary can be used for malicious purposes


# KALI LINUX



# OPENVAS VULNERABILITY SCANNER

Greenbone Security Assistant

Version 7.0.



Username:

Password:

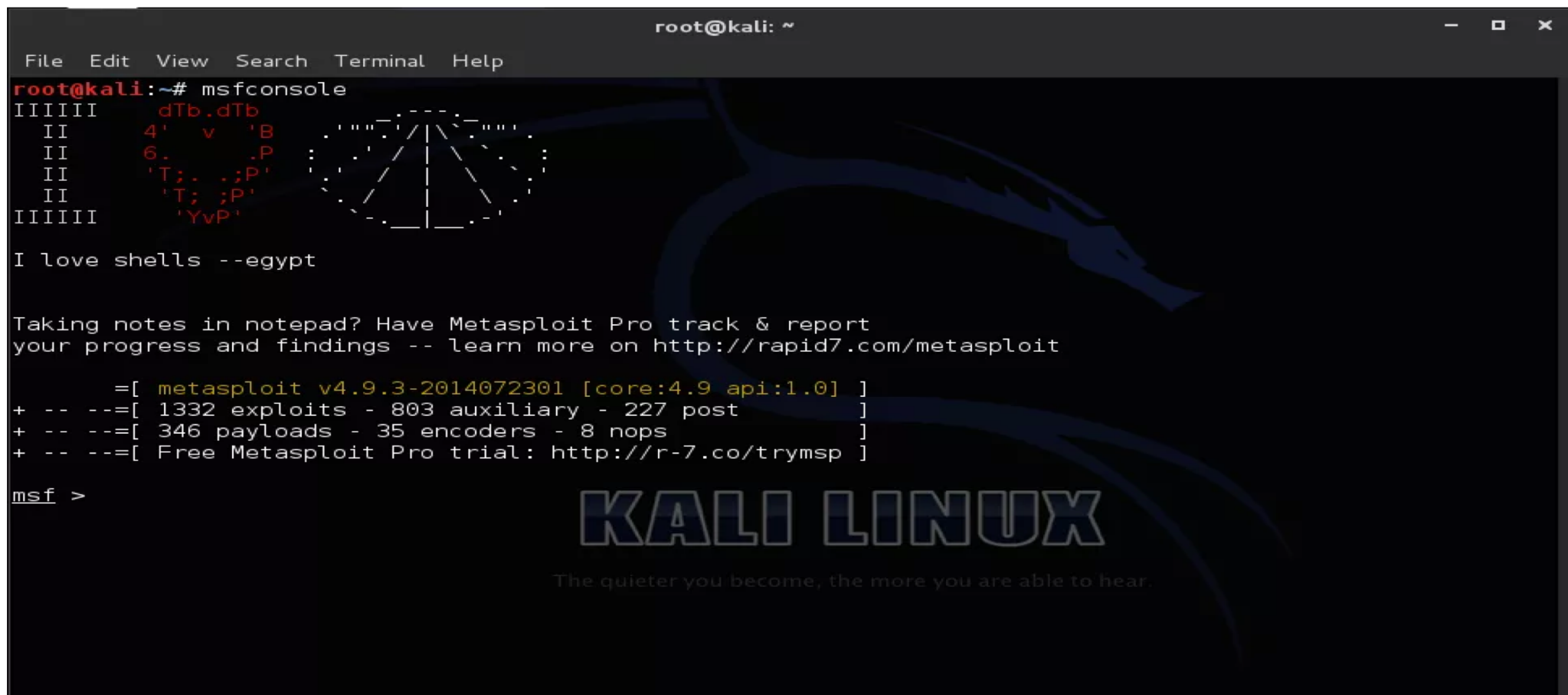
Login



[www.bujarra.com](http://www.bujarra.com)

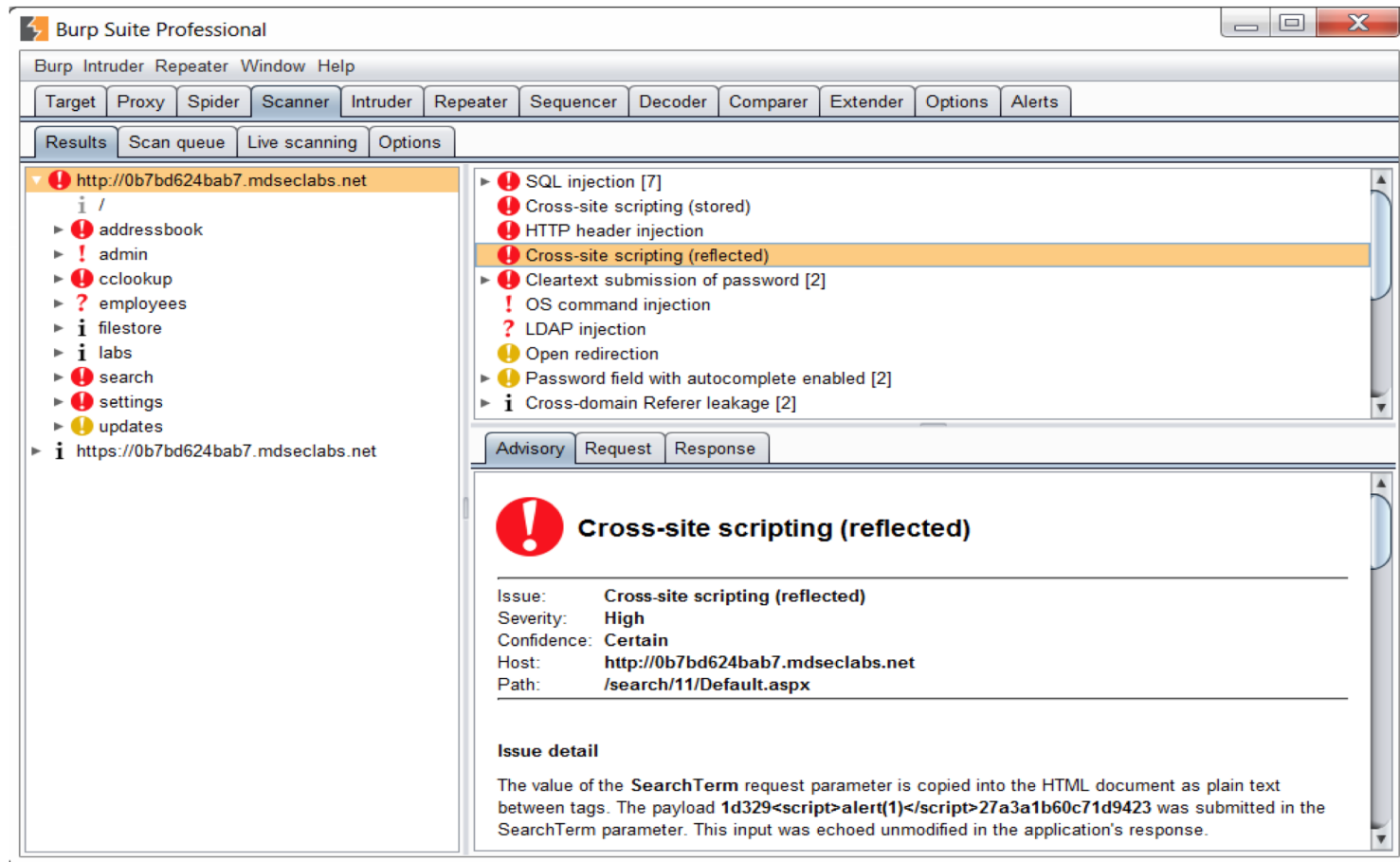
# METASPLOIT

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# msfconsole  
IIIIII      dTb.dTb  
 II      4' v 'B  
 II      6. .P  
 II      'T: .;P'  
 II      'T: ;P'  
IIIIII      'YvP'  
  
I love shells --egypt  
  
Taking notes in notepad? Have Metasploit Pro track & report  
your progress and findings -- learn more on http://rapid7.com/metasploit  
  
      =[ metasploit v4.9.3-2014072301 [core:4.9 api:1.0] ]  
+ -- --=[ 1332 exploits - 803 auxiliary - 227 post      ]  
+ -- --=[ 346 payloads - 35 encoders - 8 nops        ]  
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]  
  
msf >
```

The image shows a terminal window with a dark background. In the background, there is a faint, stylized dragon logo, which is the Kali Linux logo. The terminal output shows the Metasploit console interface, including version information, a list of available exploits, auxiliary modules, payloads, encoders, and nops. The text "KALI LINUX" is displayed in a large, outlined font, and below it, the slogan "The quieter you become, the more you are able to hear." is visible.



# BURP SUITE



The screenshot displays the Burp Suite Professional interface. The main window shows a scan of the target `http://0b7bd624bab7.mdseclabs.net`. The left sidebar lists various endpoints, including `/`, `/addressbook`, `/admin`, `/cclookup`, `/employees`, `/filestore`, `/labs`, `/search`, `/settings`, and `/updates`. The right pane shows a list of detected issues, with **Cross-site scripting (reflected)** highlighted. Below this, the details for the selected issue are shown:

**Advisory** Request Response

**Cross-site scripting (reflected)**

Issue: **Cross-site scripting (reflected)**  
Severity: **High**  
Confidence: **Certain**  
Host: `http://0b7bd624bab7.mdseclabs.net`  
Path: `/search/11/Default.aspx`

**Issue detail**

The value of the `SearchTerm` request parameter is copied into the HTML document as plain text between tags. The payload `1d329<script>alert(1)</script>27a3a1b60c71d9423` was submitted in the `SearchTerm` parameter. This input was echoed unmodified in the application's response.

# METASPLOITABLE

```
Metasploitable-2
Suspend Snapshots Devices Enter Unity
* Starting deferred execution scheduler atd [ OK ]
* Starting periodic command scheduler crond [ OK ]
* Starting Tomcat servlet engine tomcat5.5 [ OK ]
* Starting web server apache2 [ OK ]
* Running local boot scripts (/etc/rc.local)
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out' [ OK ]

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: _
```



PRACTICAL

# SHORT DEMONSTRATION

John



Fortinet Threat Map



Shodan



**THANK YOU  
FOR *YOUR*  
ATTENTION!**

FULLCIRCLE SECURITY

Expertise. Knowledge. Success.

[bugejajoseph.com](http://bugejajoseph.com)

[HOME](#) / [ACADEMIC](#) / [PRESENTATIONS](#) / [SERVICES](#) / [ABOUT](#) / [CONTACT](#)