



**No pictures during this presentation please
Slides will be made available**





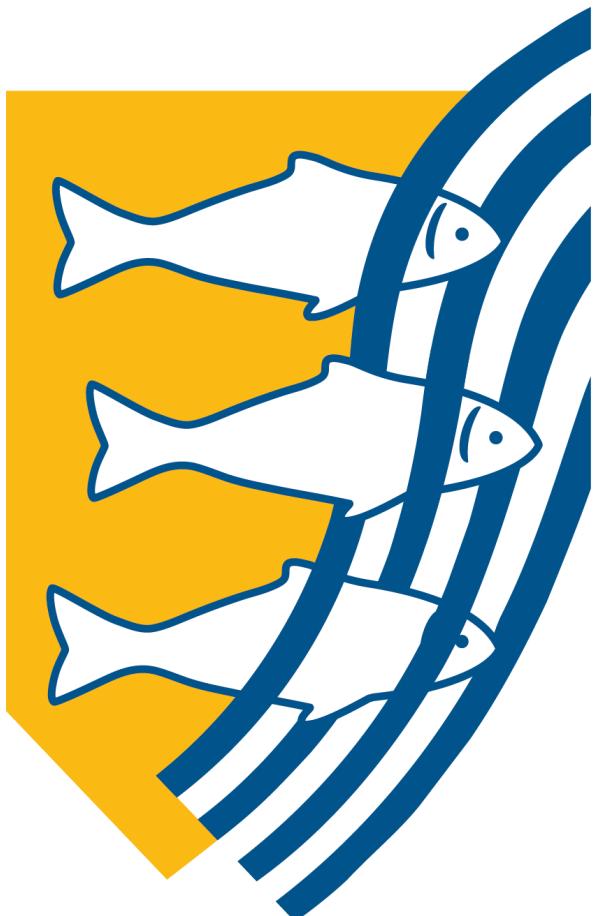
Hacker Mindset



Unprecedented, previously unimaginable new opportunities meet unprecedented, previously unimaginable new threats



Context: Why is the AIVD contributing to this event?



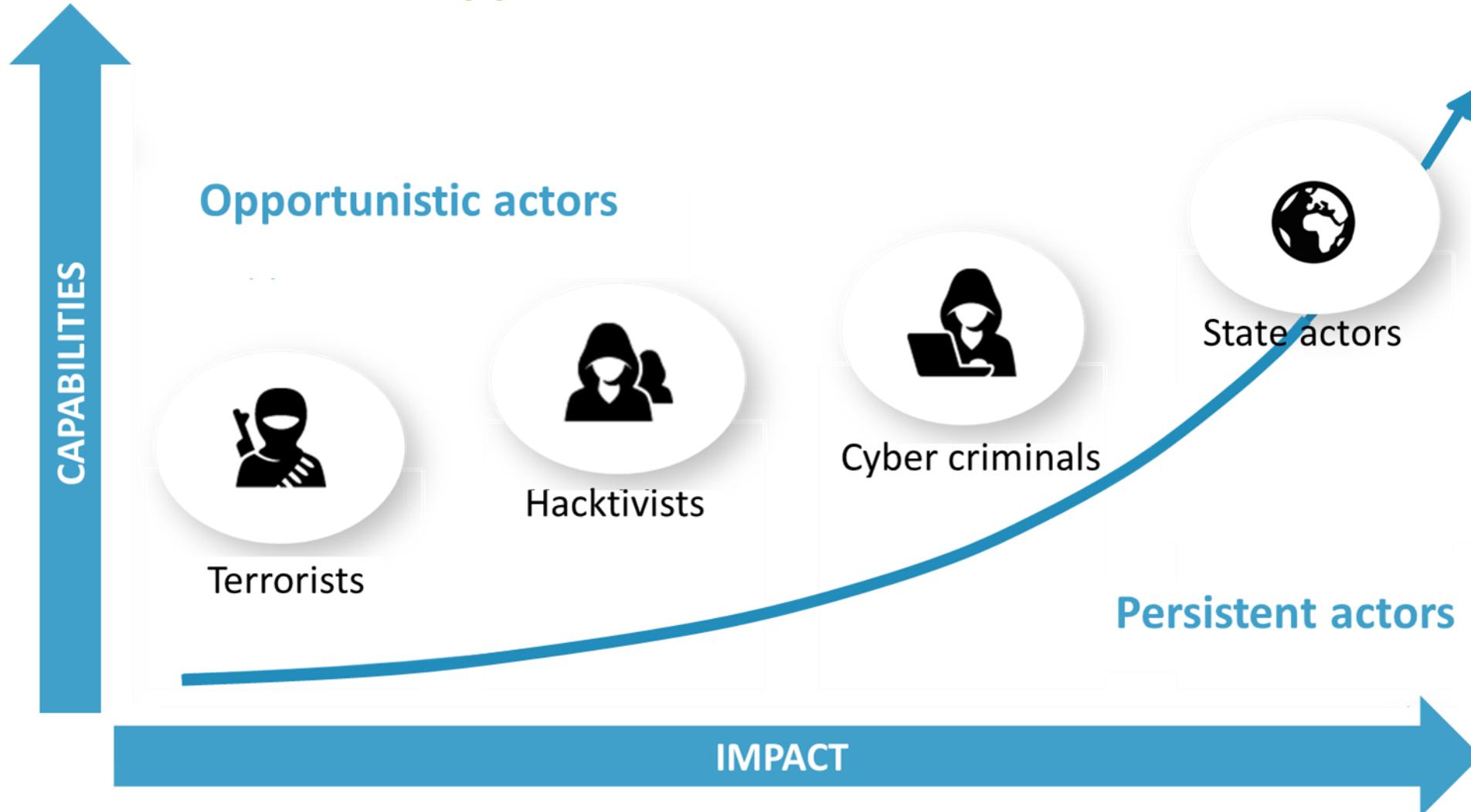
The AIVD **contributes to our national security** and **protects our democracy** against national and international threats

To do so the AIVD...

- › investigates Jihadist terrorism and other forms of extremism
- › investigates proliferation of weapons of mass destruction
- › maps known and unknown threats
- › reports on these threats to its partners
- › performs security screening of persons in vital sectors
- › investigates **(digital) espionage** and **covert (digital) influencing**
- › detects **(digital) sabotage** of vital infrastructure
- › **promotes and contributes to (information) security**

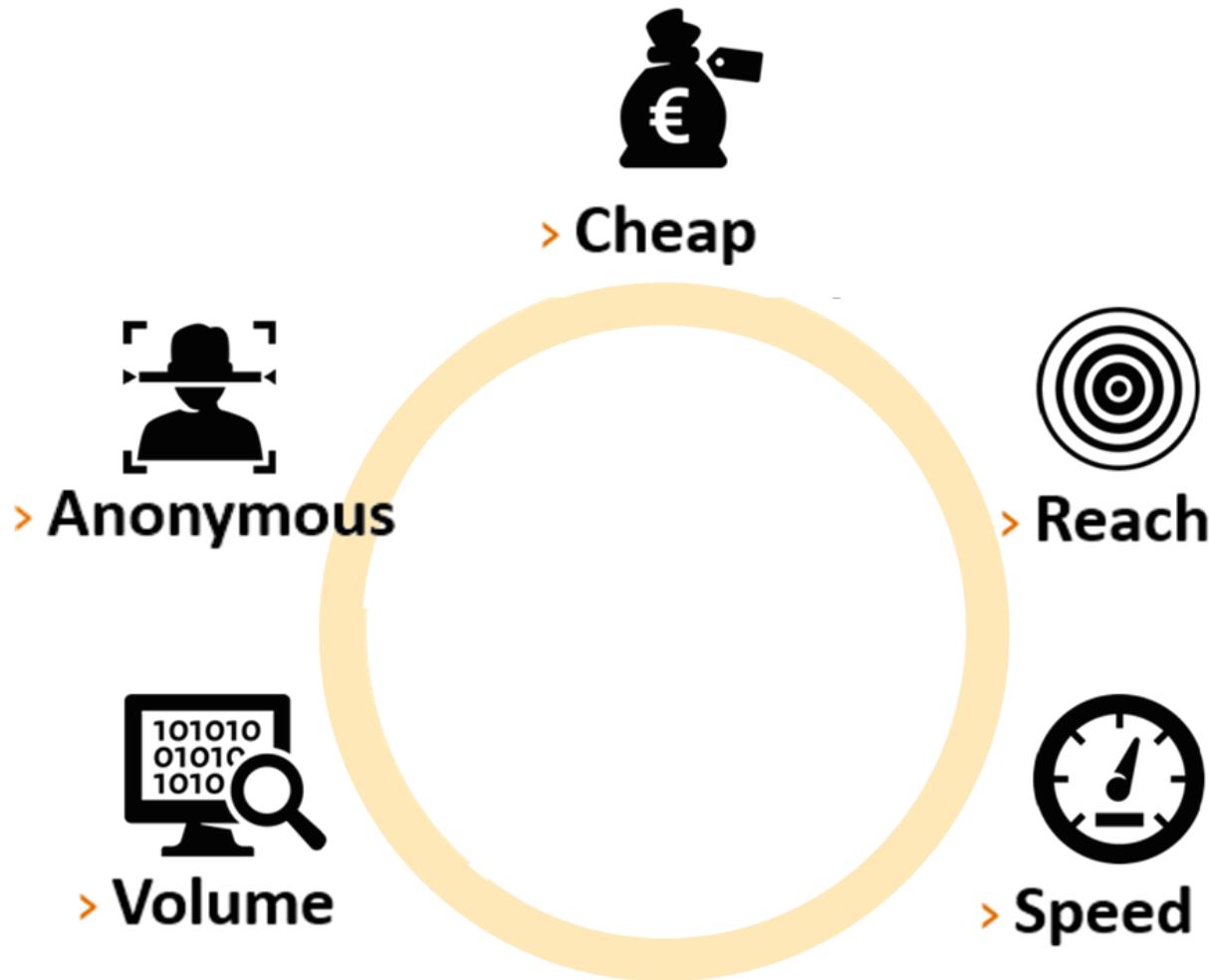


Types of threat actors





Internet has proven to be a game changer



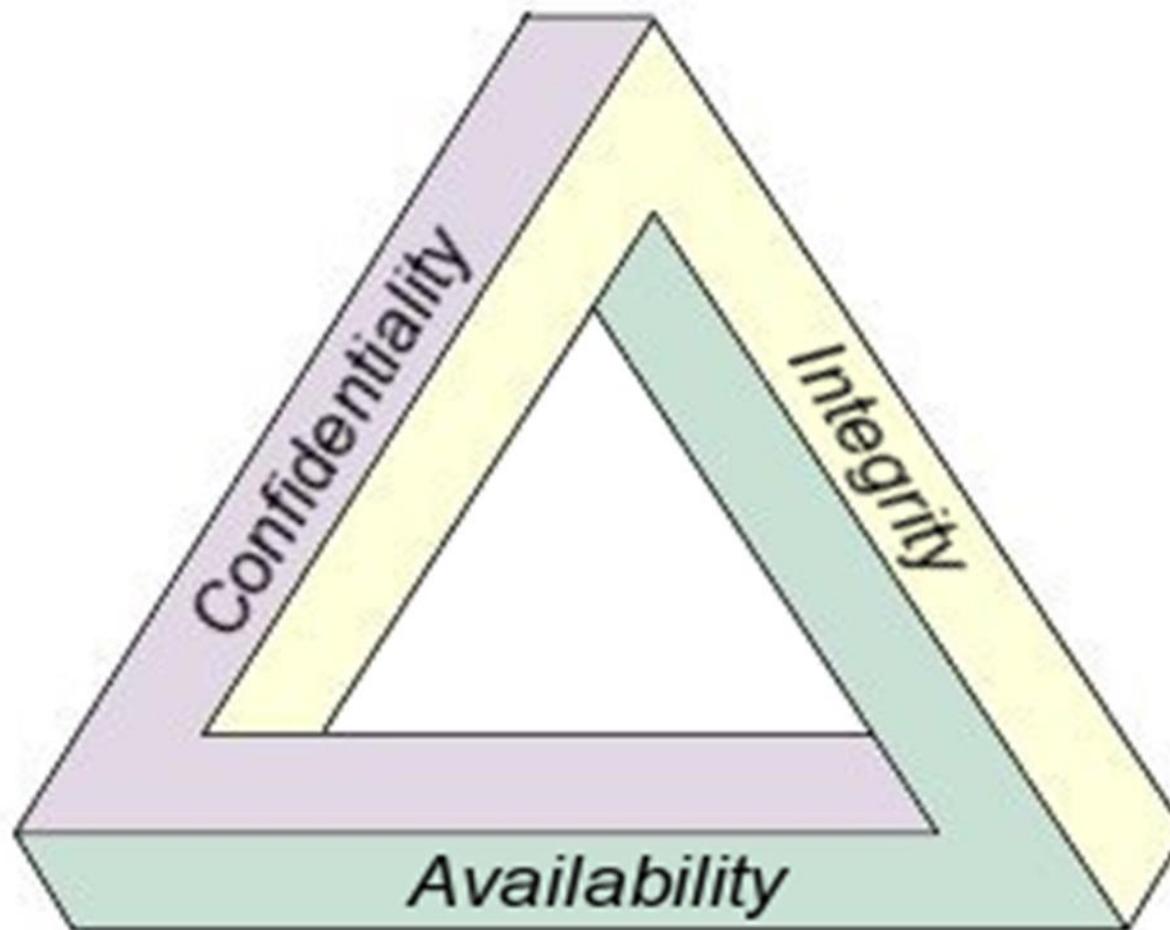


Physical threats vs Digital threats



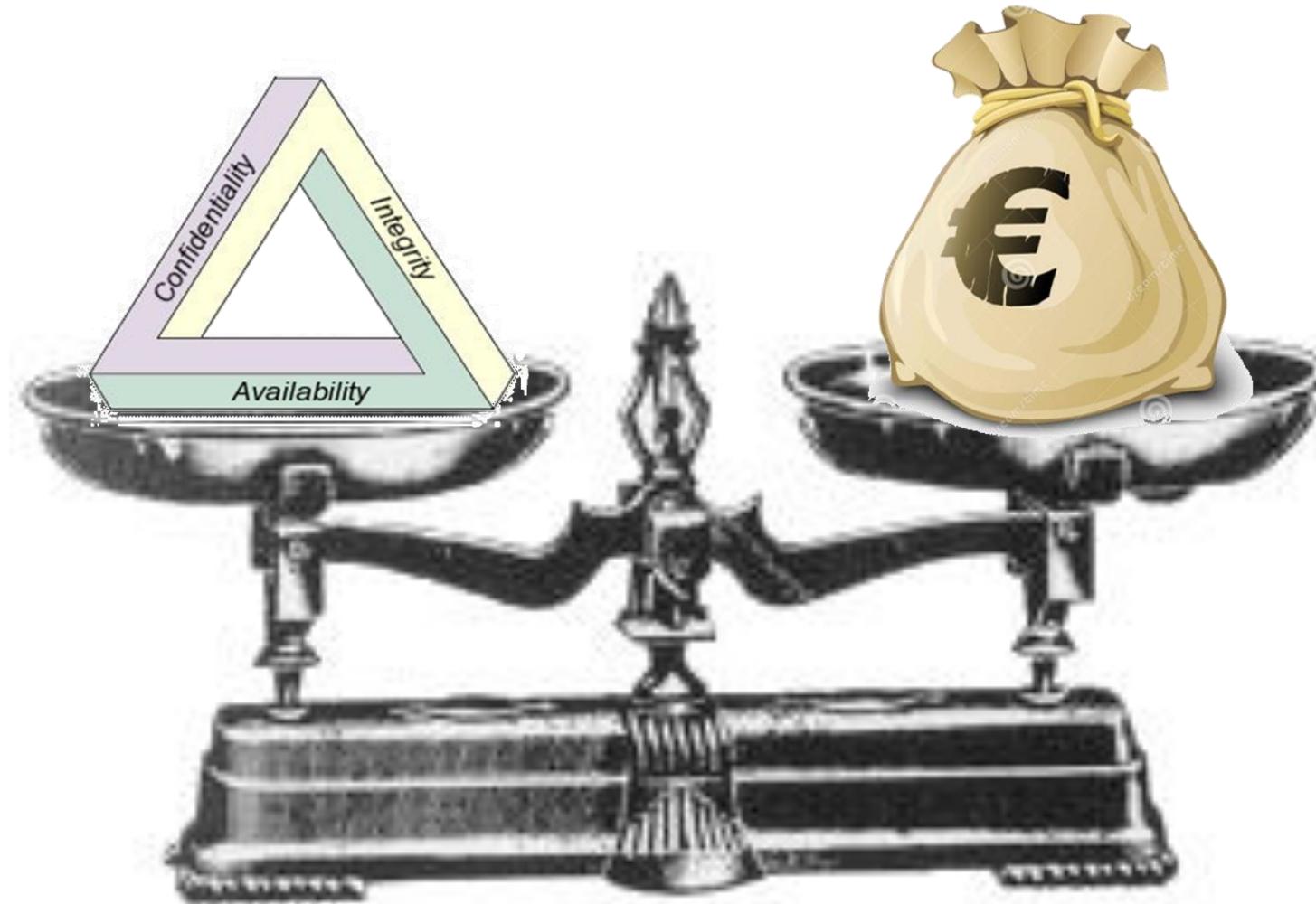


Three main goals of any IT-security strategy





What requirements should be met by your products and services?



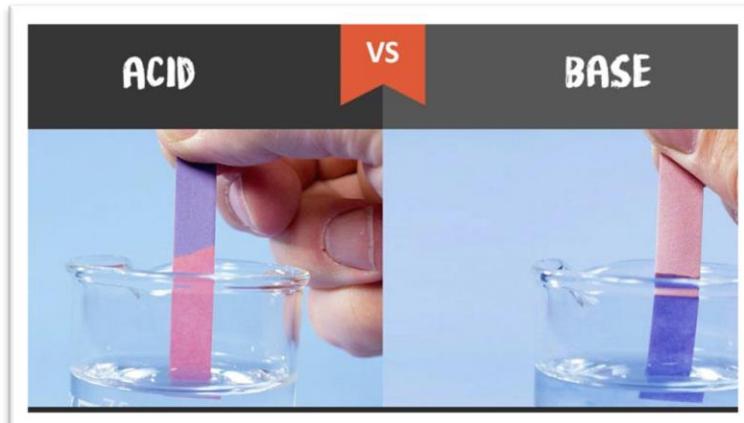
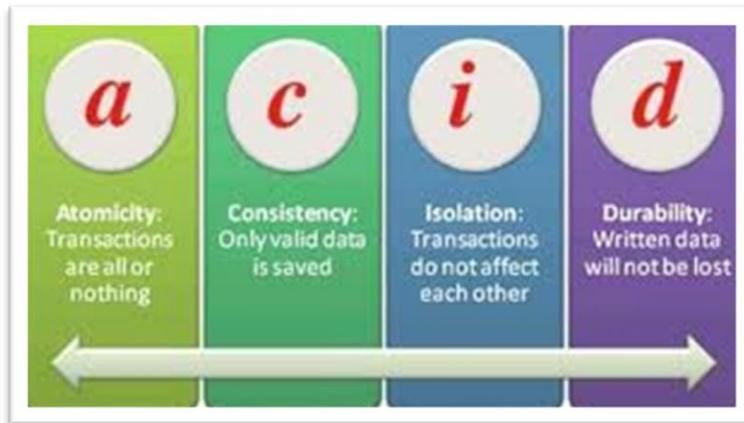


What might you do to increase Confidentiality?





What might you do to increase Integrity?



```
E:\>MD5 abc
E:\>CRC abc
E:\>RIPEMD160 abc
E:\>SHA1 abc
E:\>SHA256 abc
E:\>SHA512 abc
E:\>Whirlpool abc
```

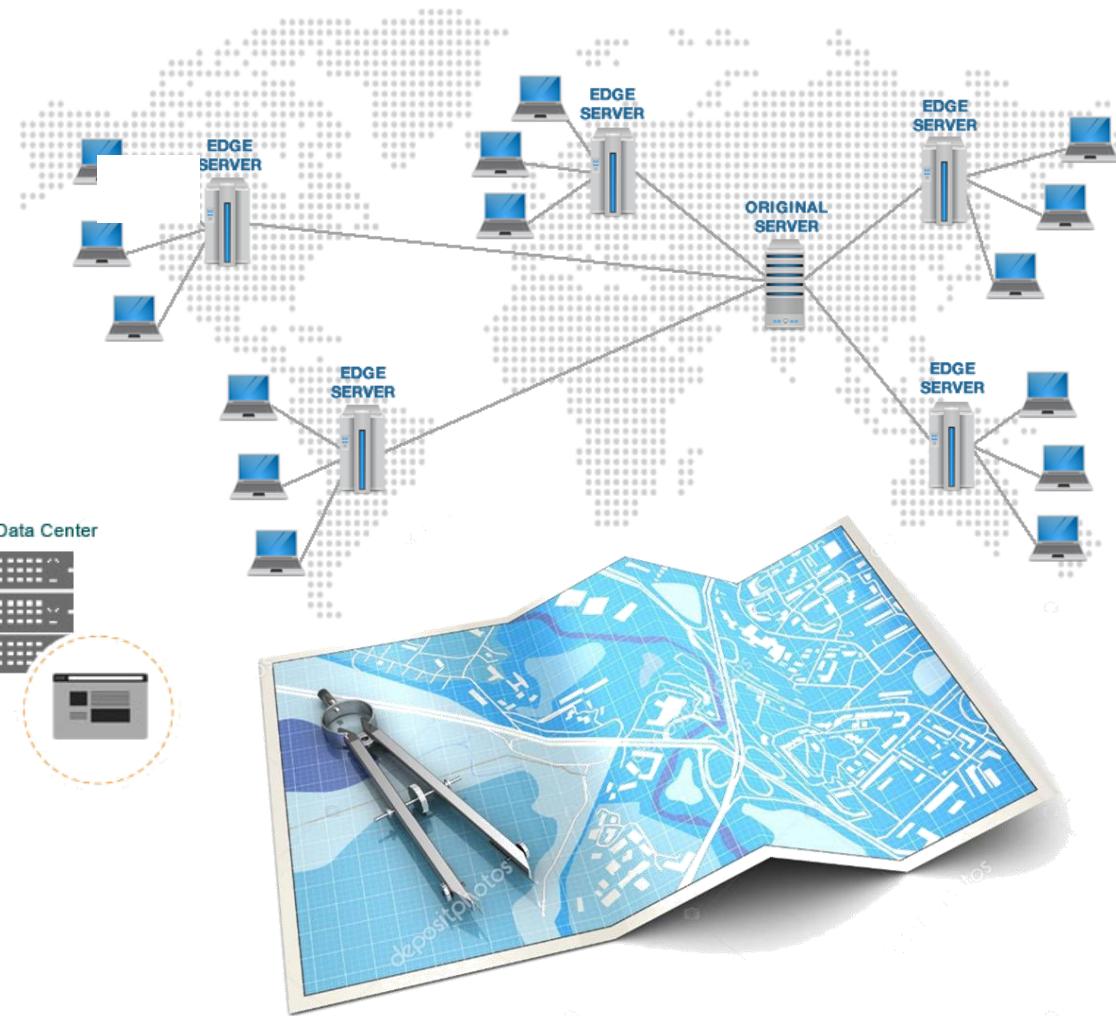
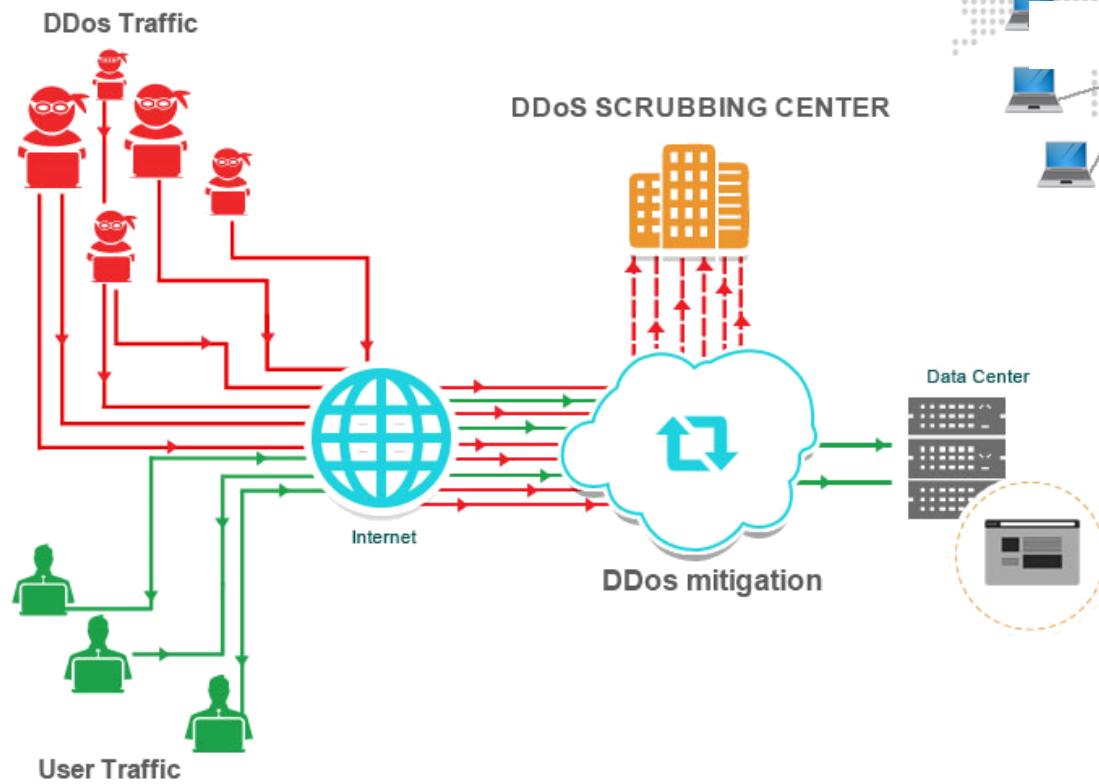
The terminal window displays the results of applying different hash functions to the string "abc". The results are as follows:

| Hash Function | Result |
|---------------|--|
| CRC16 | 9DD6 |
| CRC32 | 352441C2 |
| CRC64 | 0297F4F93A818B04 |
| MDS | 900150983CD24FB0D6963F7D28E17F72 |
| RIPEMD160 | 8EB208F7E05D987A9B044A8E98C6B087F15A0BFC |
| SHA1 | A9993E364706816ABA3E25717850C26C9CD0D89D |
| SHA256 | BA7816BF8F01CFEA414140DE5DAE2223B00361A396177A9C |
| SHA512 | B410FF61F20015AD |
| Whirlpool | D0AF35A193617ABACC417349AE20413112E6FA4E89A97EA2 0A9EEEE64B55D39A2192992A274FC1A836BA3C23A3FEEBB0 45D04423643CE80E2A9AC94FA54CA49F 4E2448A4C6F486BB16B6562C73B4020BF3043E3A731BCE72 1AE1B303D97E6D4C7181EEBDB6C57E277D0E34957114CBD6 C797FC9D95D8B582D225292076D4EEF5 |





What might you do to increase Availability?





What is the greatest adversary of secure implementations?

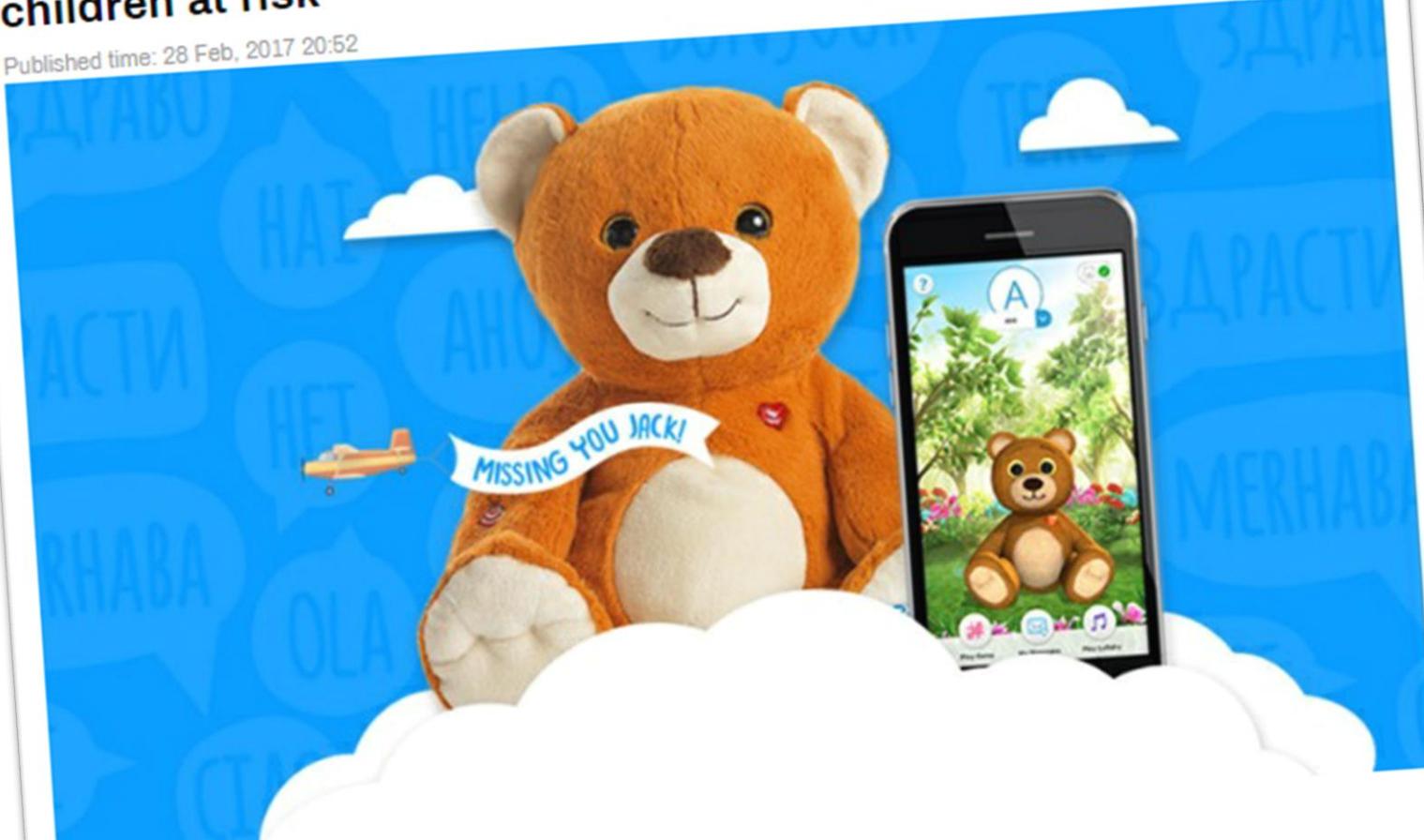




'Smart' Teddy bears hacked, 2mn private recordings leaked, children at risk

Published time: 28 Feb, 2017 20:52

[Get short URL](#)



© cloudpets.com



Spiral Toys, the company behind the CloudPets 'smart' teddy bears, left data of up to 800,000 customers, including two million individual recordings, unprotected on their servers for anyone to listen in on or view.

'Smart' Teddy bears could leave children at risk

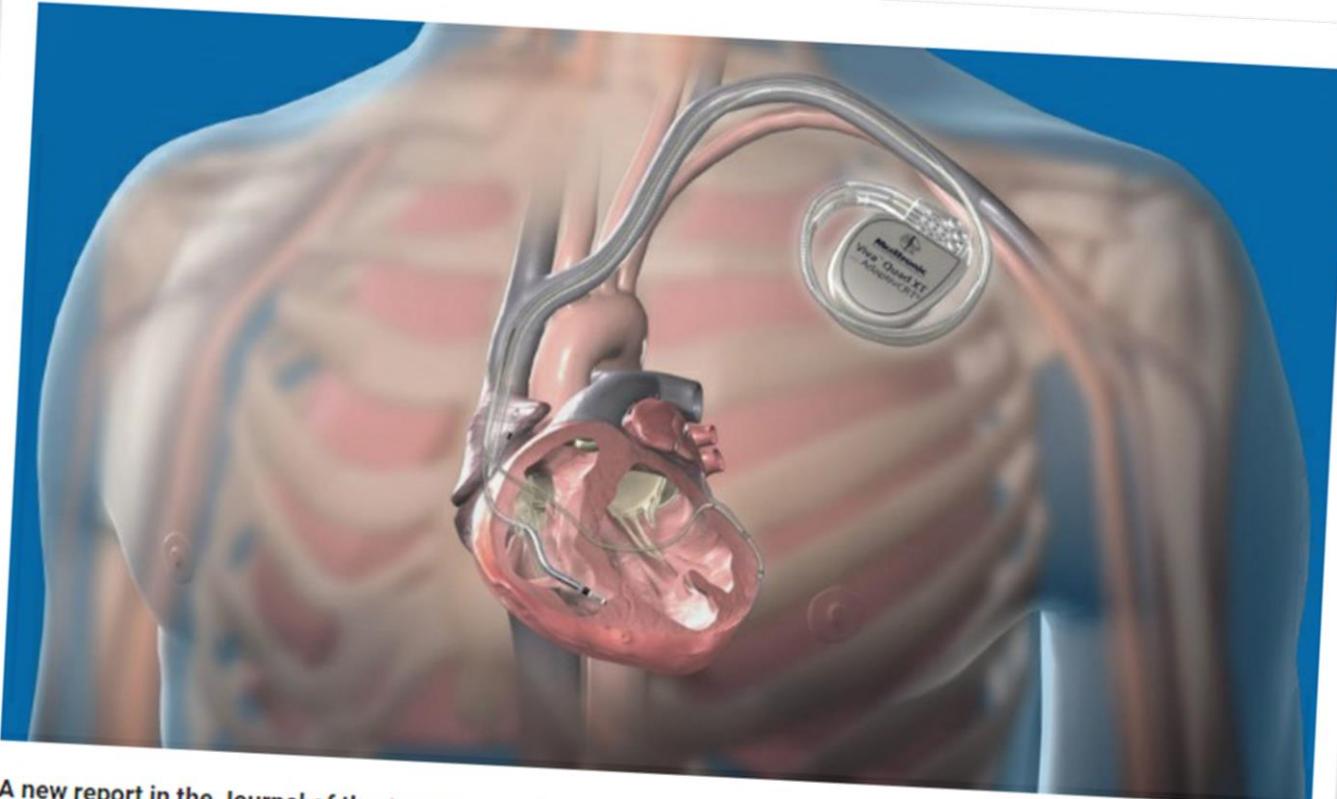
Published time: 28 Feb, 2017 20:51

© cloudpets.com



Spiral Toys, the company behind the world's first million individual recorded teddy bears, has revealed that

Heart alert: Pacemakers can be hacked, new research shows



A new report in the Journal of the American College of Cardiology says there is a possibility that pacemakers and other electrical medical devices could be hacked. (© Medtronics / SWNS.com)

A new study is warning that pacemakers and other electrical medical devices could be targeted by hackers for political, financial or personal gain.

'Smart' T
children

Published time: 2

Heart alert! D

The internet of dildos is here,
and it's vulnerable as hell

s can be
shows



SEARCH



Cloud Big Data AI IoT Cybersecurity More ▾

SECURITY



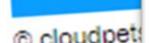
DDoS attacks increased 91% in 2017 thanks to IoT

In Q3 2017, organizations faced an average of 237 DDoS attack attempts per month. And with DDoS-for-hire services, criminals can now attack and attempt to take down a company for less than \$100.

IMAGE: GETTY IMAGES/ISTOCKPHOTO

BY JACK MORSE

FEB 02, 2018



Spiral Toy
million inc

When your internet-connected lightbulb gets hacked, a [university gets DDoS'd](#).

But when the same thing happens to your internet-connected vibrator? Well, let's just say the ramifications are a tad more *personal*.

that pacemakers and

al devices could

Keyless car theft: what you need to know



Alice Campion - 13 Sep 2021



Keyless cars are great to drive, but do they put you at a higher risk of theft? Here we explain what makes vehicles vulnerable to being stolen and how to keep your keyless car safe.



Police chiefs have warned keyless car owners are at risk, following a spike in thefts across the UK. Keyless entry thefts soared after the first lockdown.

Criminals are using "relay technology" to access keyless cars and drive them away. If you've got a keyless access car, don't panic.

'Smart
child

Published



s

D

In
wi
co

© c

•

Sp
m

Home > Wireless Security

'Smart
child'



Tesla Car Hacked Remotely From Drone via Zero-Click Exploit

By Eduard Kovacs on May 03, 2021

RSS

Share

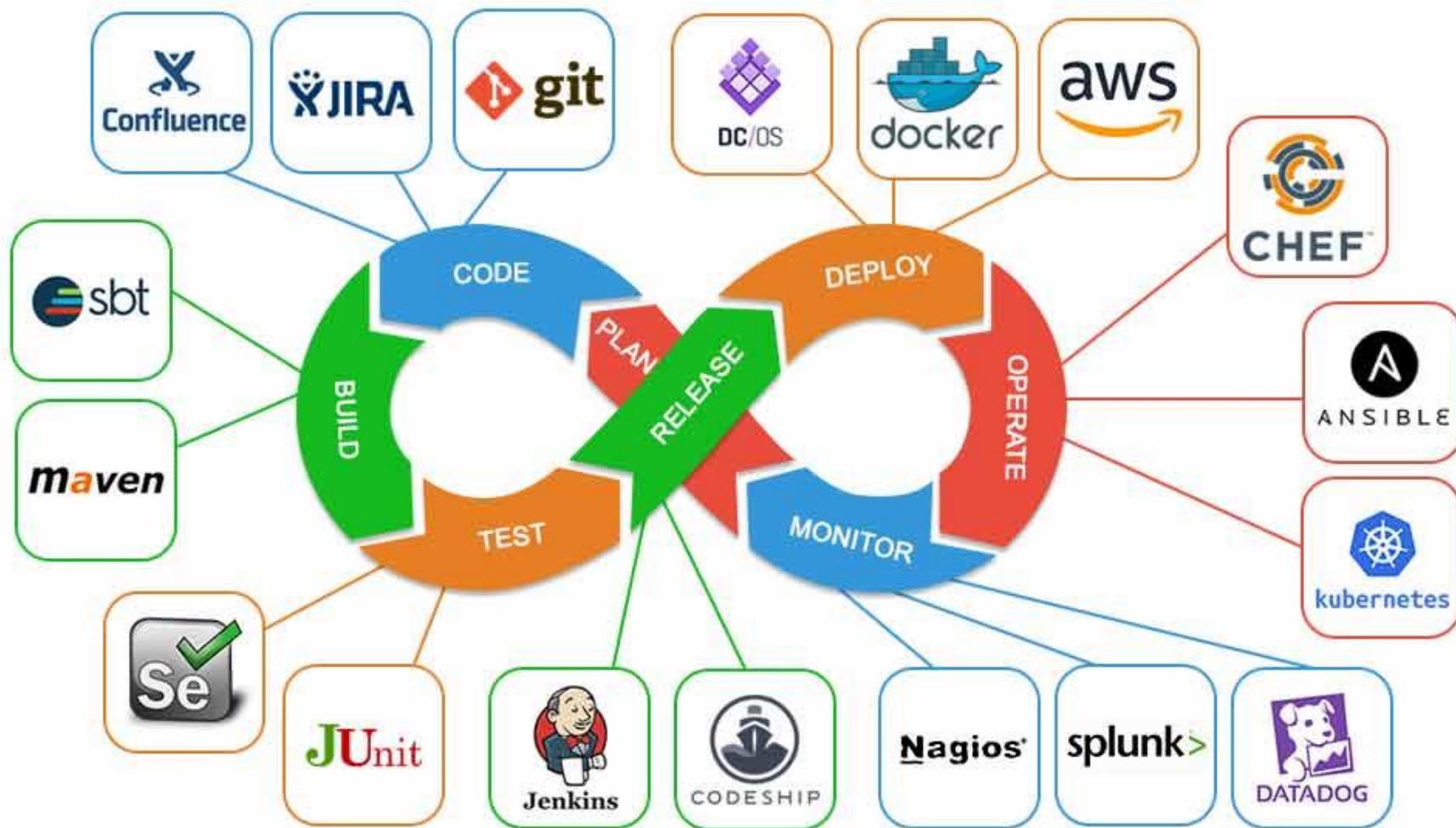
Tweet

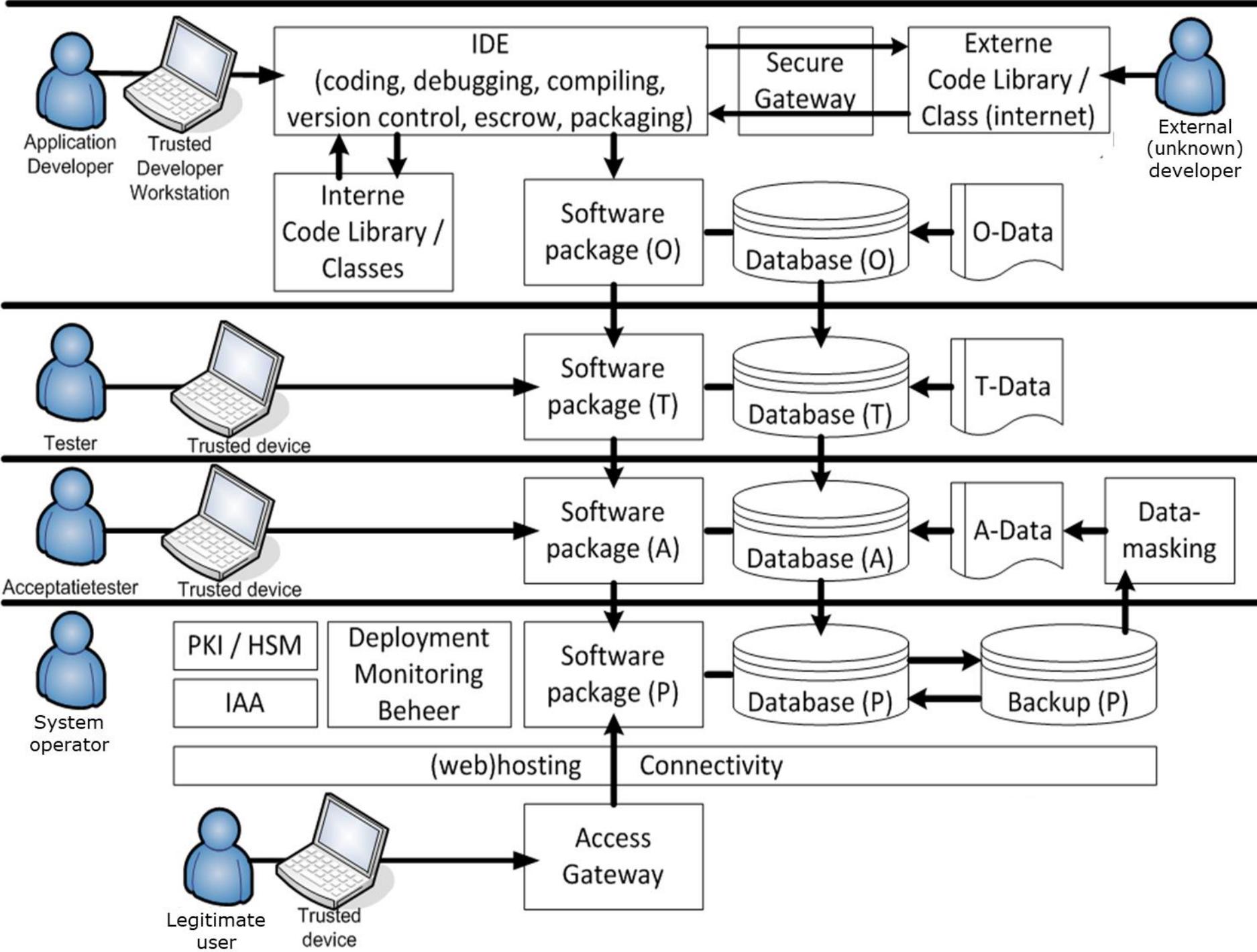


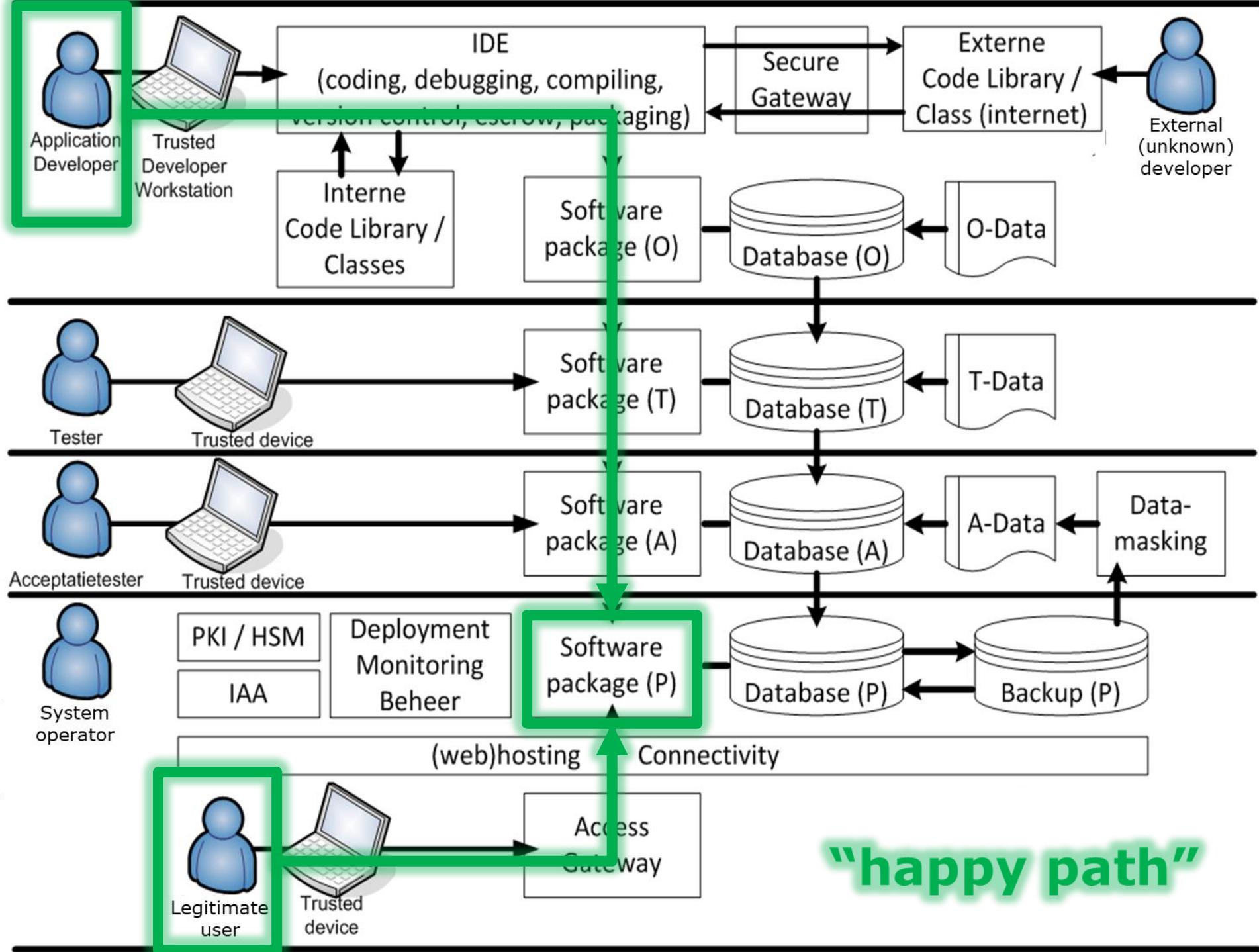
Two researchers have shown how a Tesla – and possibly other cars – can be hacked remotely without any user interaction. They carried out the attack from a drone.

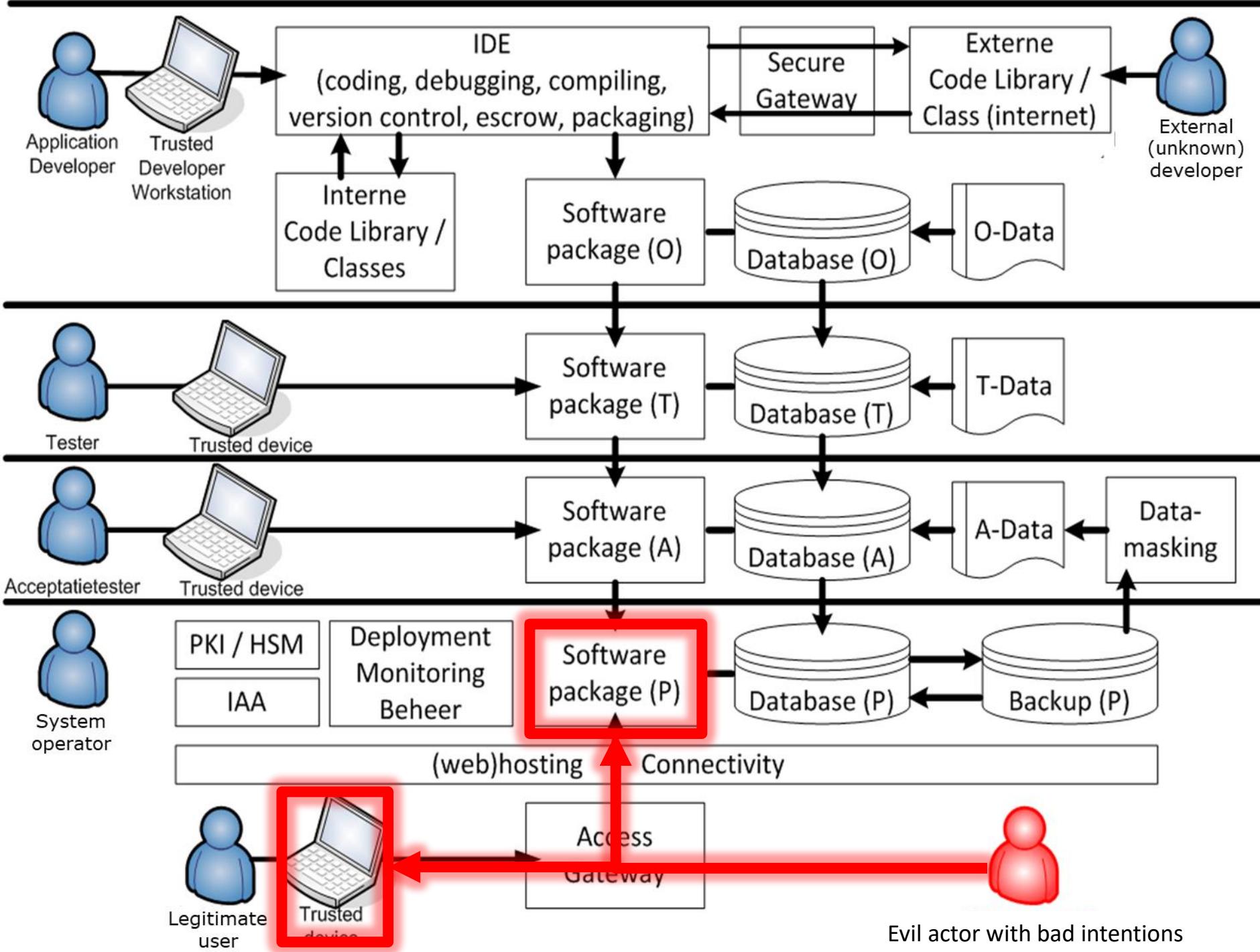


So what should you do when developing new systems?









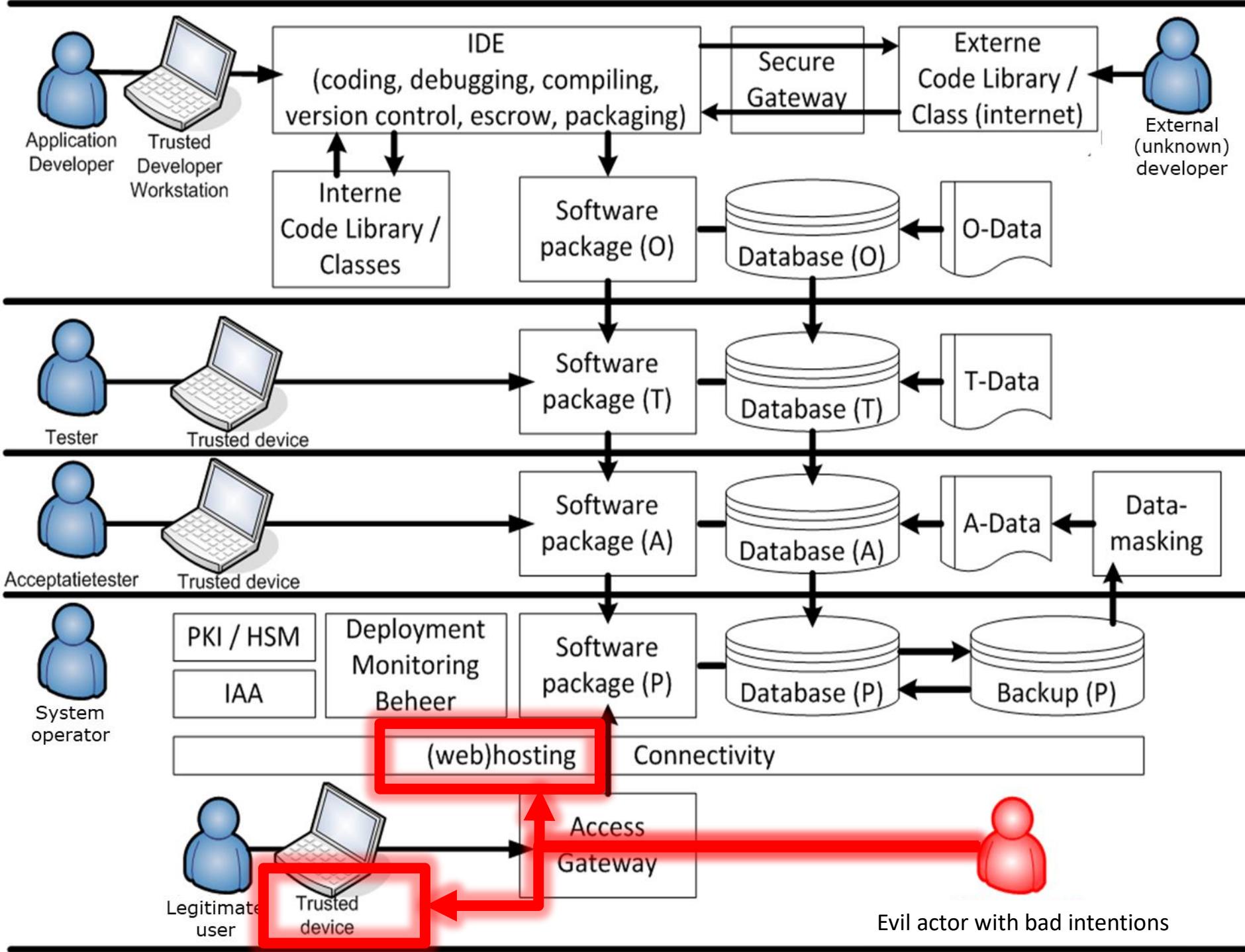


Basic (obvious) security measures

- › Strong, multi-factor user authentication
- › Ensure that your product is hardened against attacks like:
 - SQL-injection / LDAP-injection / OS-call injection /
 - Cross Site Scripting / Cross Site Request Forgery /
 - Path traversal / Token replay / Session hijacking /
 - URL-, HTTP-header- or Cookie-manipulation / etc... etc...
- › See OWASP.org, featuring:
 - OWASP Top 10 (2021)
 - OWASP Dependency Check
 - OWASP Security Knowledge Framework
 - OWASP Application Security Verification Standard



OWASP
Open Web Application
Security Project





Security measure: keep ALL software up to date

CVE security vulnerability Apache Tomcat version 8

Beveiligd | https://www.cvedetails.com/vulnerability-list/vendor_id-45/product_id-887/version_id-242449/Apache-To... ☆ ADB 1

Plaats voor een snelle navigatie je bladwijzers op deze bladwijzerbalk. Bladwijzers nu importeren...

CVE Details

The ultimate security vulnerability datasource

[Log In](#) [Register](#)

[Switch to https://](#) [Home](#)

Browse :

- [Vendors](#)
- [Products](#)
- [Vulnerabilities By Date](#)
- [Vulnerabilities By Type](#)

Reports :

- [CVSS Score Report](#)
- [CVSS Score Distribution](#)

Search :

- [Vendor Search](#)
- [Product Search](#)
- [Version Search](#)
- [Vulnerability Search](#)
- [By Microsoft References](#)

Top 50 :

- [Vendors](#)
- [Vendor Cvss Scores](#)
- [Products](#)
- [Product Cvss Scores](#)
- [Versions](#)

Vulnerability Feeds & Widgets [New](#) [www.itsecdb.com](#)

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234) [Search](#) [View CVE](#)

Apache » Tomcat » 8.5.27 : Security Vulnerabilities

Cpe Name:cpe:/a:apache:tomcat:8.5.27

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

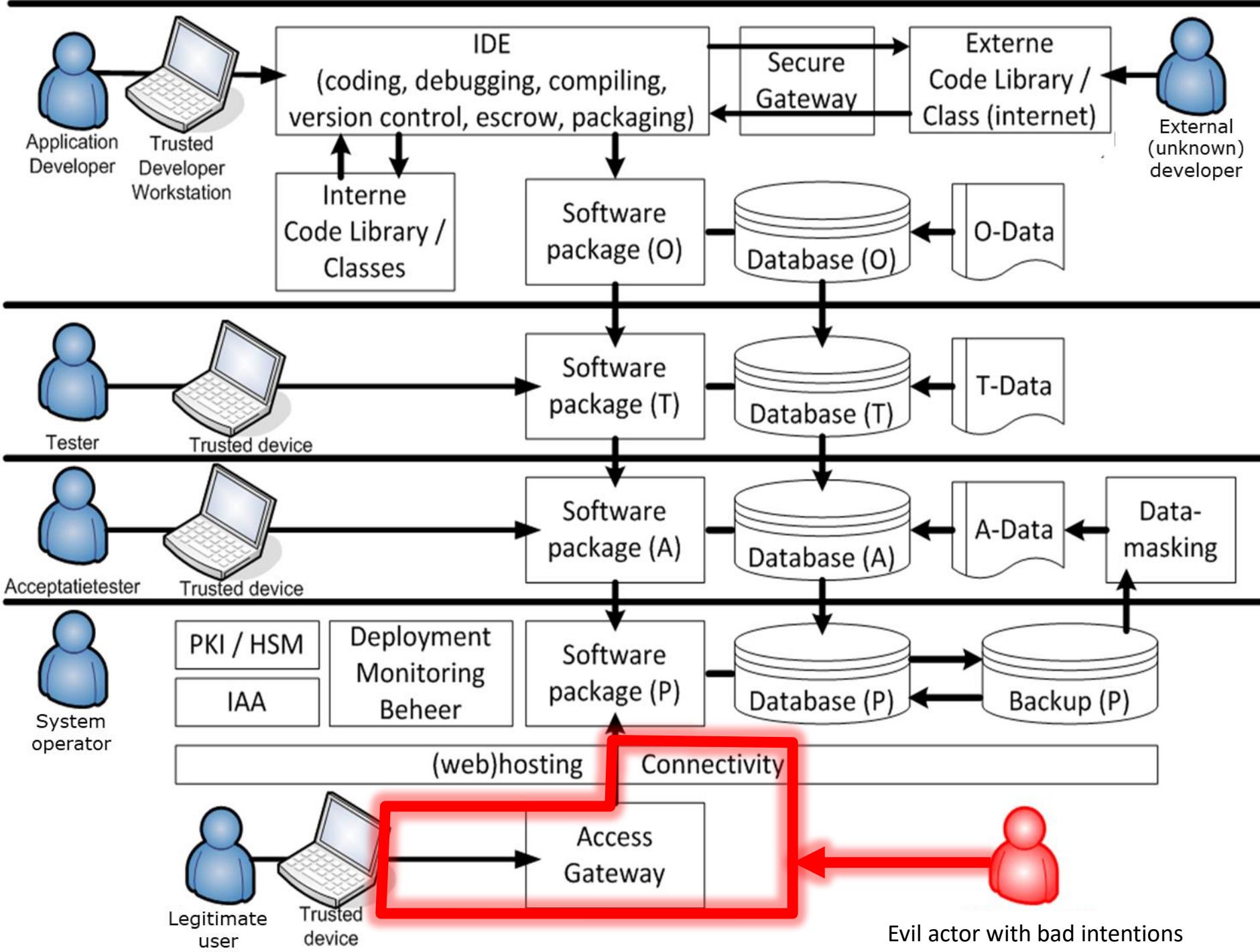
[Copy Results](#) [Download Results](#)

| # | CVE ID | CWE ID | # of Exploits | Vulnerability Type(s) | Publish Date | Update Date | Score | Gained Access Level | Access | Complexity | Authentication | Conf. | Integ. | Avail. |
|---|-----------------------------------|--------|---------------|-----------------------|--------------|-------------|-------|---------------------|--------|------------|----------------|---------|---------|---------|
| 1 | CVE-2018-8037_362 | | | | 2018-08-02 | 2018-10-16 | 4.3 | None | Remote | Medium | Not required | Partial | None | None |
| 2 | CVE-2018-8034_295 | | | | 2018-08-01 | 2018-10-16 | 5.0 | None | Remote | Low | Not required | Partial | None | None |
| 3 | CVE-2018-8014_254 | | | | 2018-05-16 | 2018-12-05 | 7.5 | None | Remote | Low | Not required | Partial | Partial | Partial |

If an async request was completed by the application at the same time as the container triggered the async timeout, a race condition existed that could result in a user seeing a response intended for a different user. An additional issue was present in the NIO and NIO2 connectors that did not correctly track the closure of the connection when an async request was completed by the application and timed out by the container at the same time. This could also result in a user seeing a response intended for another user. Versions Affected: Apache Tomcat 9.0.0.M9 to 9.0.9 and 8.5.5 to 8.5.31.

The host name verification when using TLS with the WebSocket client was missing. It is now enabled by default. Versions Affected: Apache Tomcat 9.0.0.M1 to 9.0.9, 8.5.0 to 8.5.31, 8.0.0.RC1 to 8.0.52, and 7.0.35 to 7.0.88.

www.cvedetails.com





Security measures

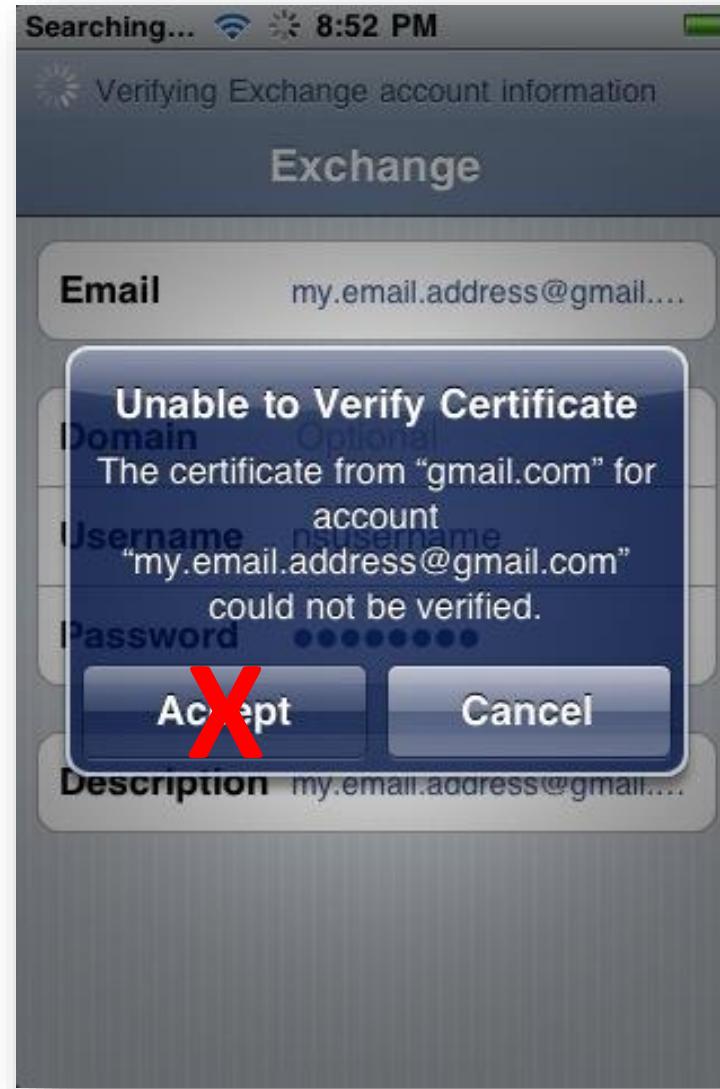
› Prevent Man in the Middle attacks:

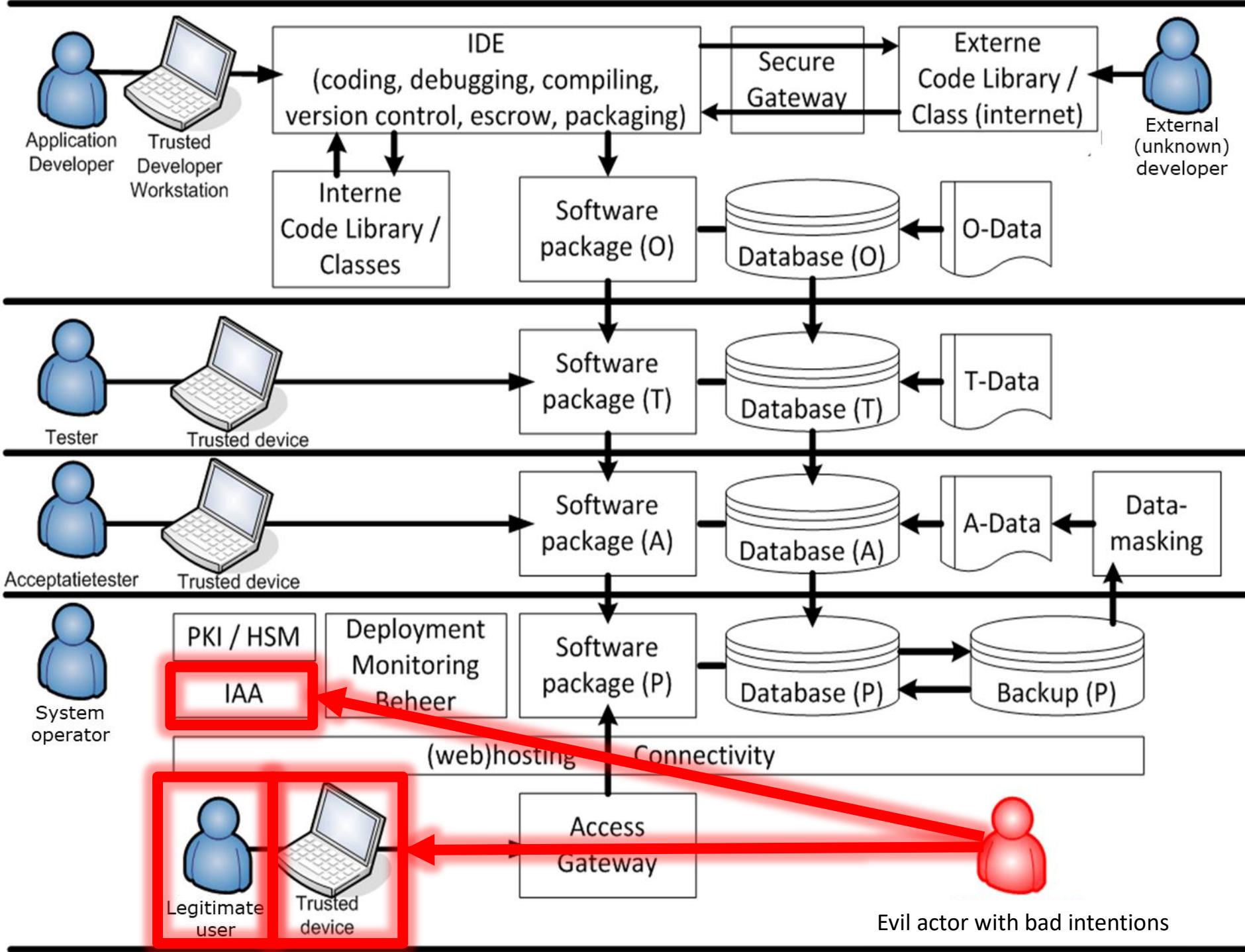
- Use (mutual) TLS-authentication between all components
- Use (trusted, validated) PKI-certificates
- Validate certificates (!!!)
- Train end user awareness to be mindful





Quiz: What is fundamentally wrong with this dialogue?







Is the authenticated end-user actually trustworthy?





Measure: User and Entity Behavior Analytics (UEBA)

Detecting Hacked Twitter Accounts based on Behavioural Change

Meike Nauta¹, Mena Habib² and Maurice van Keulen¹

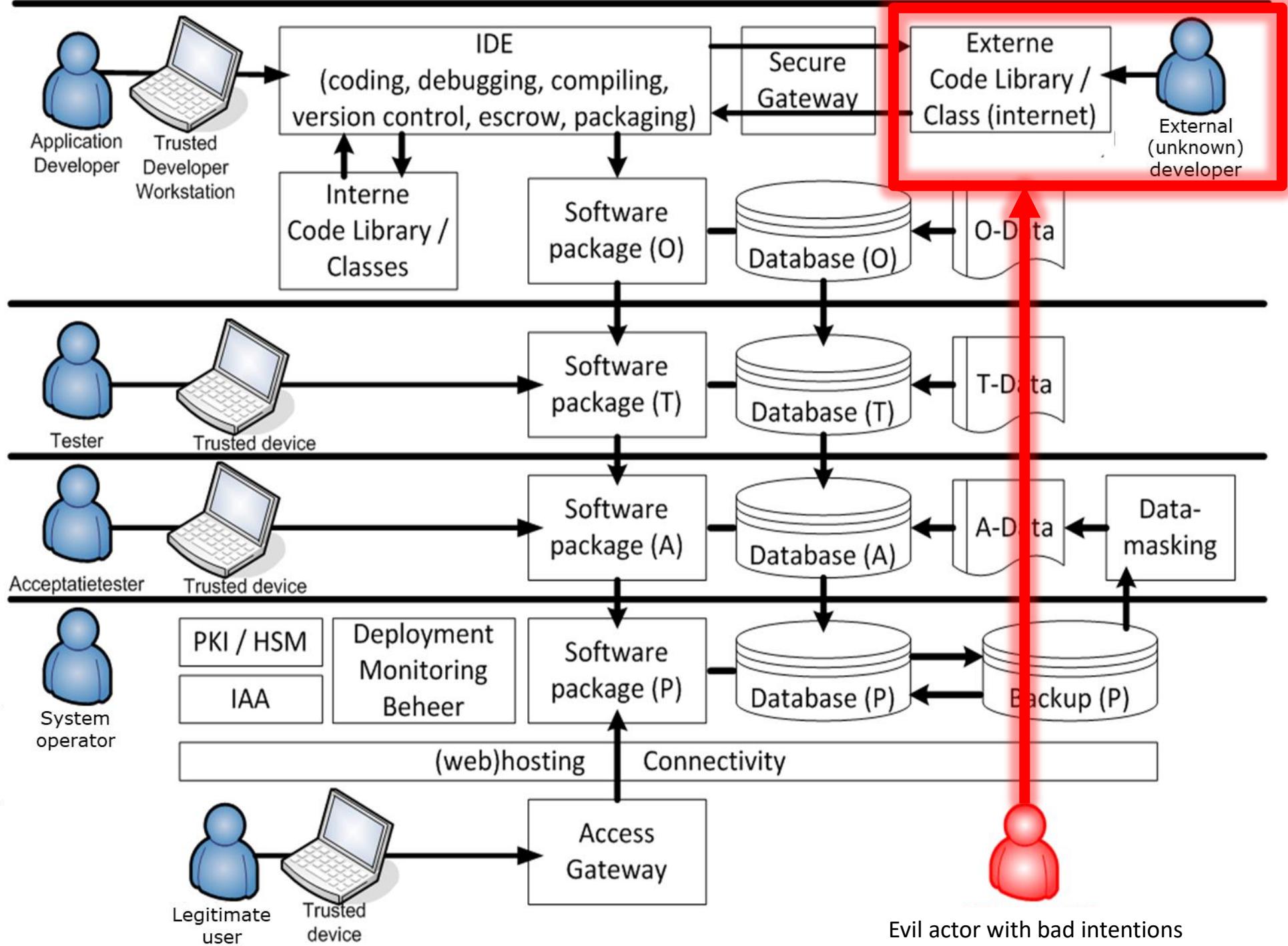
¹*University of Twente, The Netherlands*

²*Maastricht University, The Netherlands*

{m.nauta@student.utwente.nl, m.habib@maastrichtuniversity.nl, m.vankeulen@utwente.nl}

Keywords: Hacked Account Detection, Social Media

Abstract: Social media accounts are valuable for hackers for spreading phishing links, malware and spam. Furthermore, some people deliberately hack an acquaintance to damage his or her image. This paper describes a classification for detecting hacked Twitter accounts. The model is mainly based on features associated with behavioural change such as changes in language, source, URLs, retweets, frequency and time. We experiment with a Twitter data set containing tweets of more than 100 Dutch users including 37 who were hacked. The model detects 99% of the malicious tweets which proves that behavioural changes can reveal a hack and that anomaly-based features perform better than regular features. Our approach can be used by social media systems such as Twitter to automatically detect a hack of an account only a short time after the fact allowing the legitimate owner of the account to be warned or protected preventing reputational damage and annoyance.

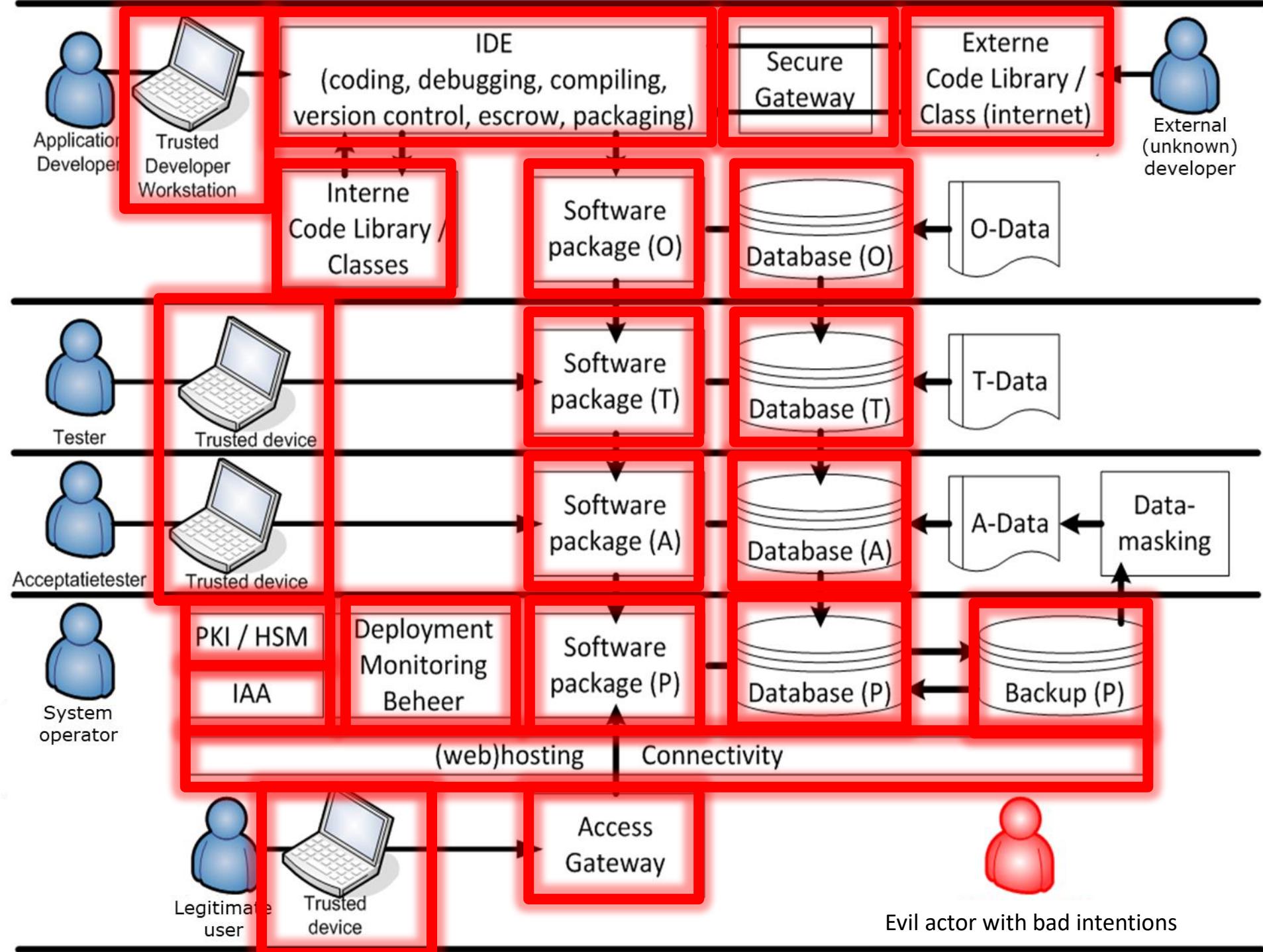




Security measures

- › Know the software/code/libraries you are downloading and using!
- › Consider risks related to downloading and using these components
- › Use a secure gateway and manage which components to download (and which not to)
- › Validate the source and its trustworthiness (website authenticity)
- › Check software integrity (signature / hash / checksum)
- › Check CVE's!!!

- › And once the software has been successfully downloaded, use:
 - Source code scan / analysis /
 - Vulnerability assessment tooling





Assume the system is compromised!

› Monitoring by a professional Security Operations Center:

- What **dataflows** should be allowed?
(not on allow-list? → cause for alarm)
- What **services** should be running?
(not on allow-list? → cause for alarm)
- What **log-events** should trigger an alarm?
(input validation / http header validations)

... and:

- Safeguard logging integrity
- Automated incident response...





SOC without incident response

The screenshot shows a news article from CNET. At the top left is the CNET logo. To its right is a horizontal navigation bar with links: REVIEWS, NEWS, VIDEO, HOW TO, SMART HOME, CARS, DEALS, and DOWNLOAD. The main title of the article is "How Target detected hack but failed to act -- Bloomberg". Below the title is a summary paragraph: "Despite alerts received through a \$1.6 million malware detection system, Target failed to stop hackers from stealing credit card numbers and personal information of millions of customers, Bloomberg reports." The article continues with two more paragraphs: "The November data breach that affected as many as 110 million Target customers could have been stopped in its tracks, according to a story published Thursday by Bloomberg." and "A team of security professionals was set up in Bangalore to monitor Target's network servers and alert security operators in Minneapolis of any detected malware. And this process worked as expected during the November hack. After detecting the hack, the people in Bangalore alerted the people in Minneapolis. But that's where the ball got dropped, according to Bloomberg. The hack continued on its merry way." The bottom right corner of the screenshot contains the number "35".

REVIEWS NEWS VIDEO HOW TO SMART HOME CARS DEALS DOWNLOAD

How Target detected hack but failed to act -- Bloomberg

Despite alerts received through a \$1.6 million malware detection system, Target failed to stop hackers from stealing credit card numbers and personal information of millions of customers, Bloomberg reports.

The November data breach that affected as many as 110 million Target customers could have been stopped in its tracks, according to a story published Thursday by Bloomberg.

A team of security professionals was set up in Bangalore to monitor Target's network servers and alert security operators in Minneapolis of any detected malware. And this process worked as expected during the November hack. After detecting the hack, the people in Bangalore alerted the people in Minneapolis. But that's where the ball got dropped, according to Bloomberg. The hack continued on its merry way.



Three overarching principles...

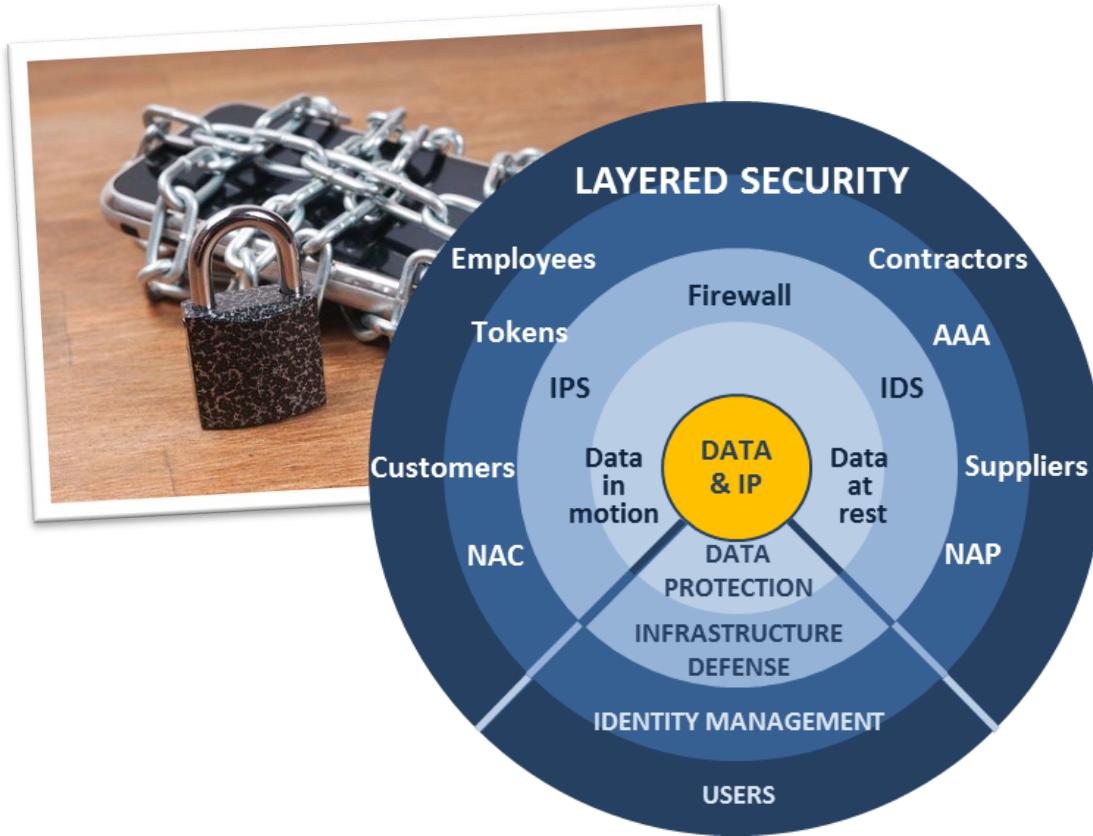
1. Security by design





Three overarching principles...

1. Security by design
2. Defence in depth





Three overarching principles...

1. Security by design
2. Defence in depth
3. Assume breach





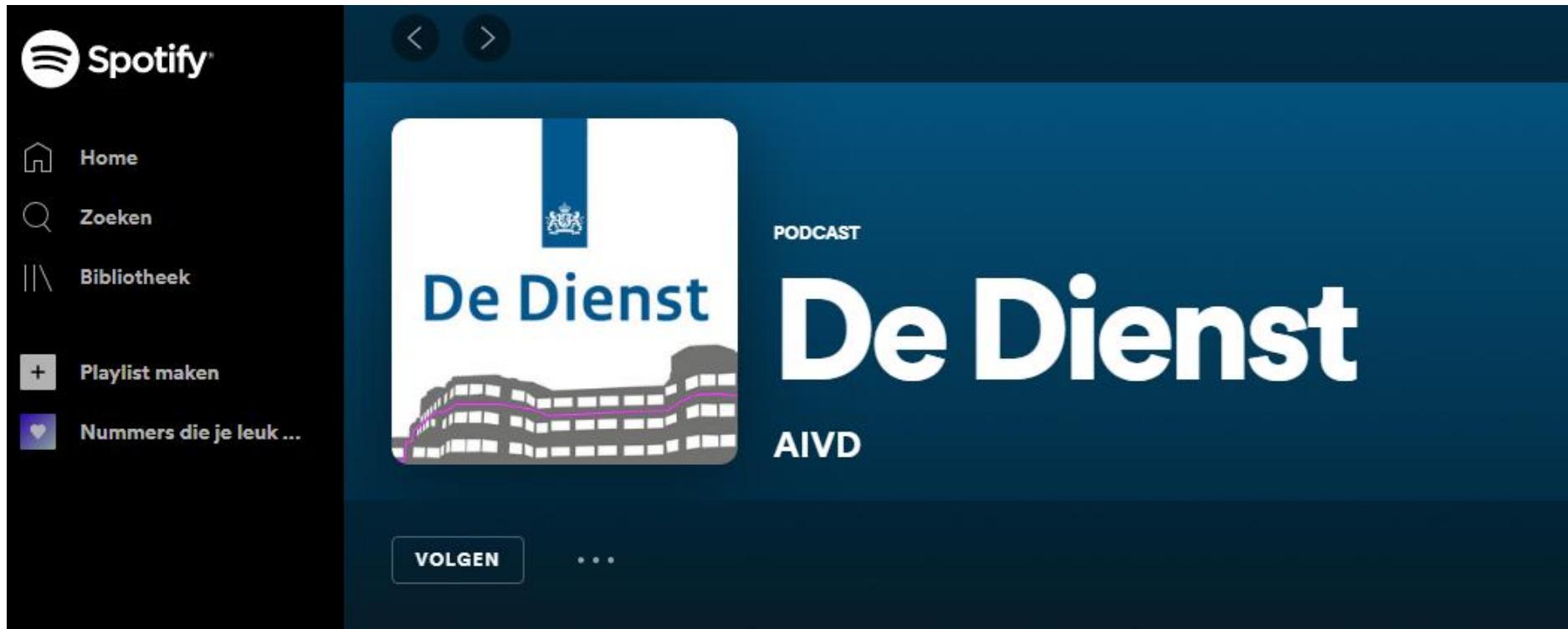
Hacker Mindset: Think like a hacker!



TO BEAT A HACKER YOU NEED
TO THINK LIKE A HACKER



Getting to know the AIVD: listen to our podcast!



- › Podcast “**De Dienst**” – now available on **Spotify**
- › New “**Cyber podcast**” – will launch Q1 2022





Do you wish to contribute to national security?



www.werkenbijdeaivd.nl / jscu.summerschool.sh / www.werkenvoornederland.nl

Relatiemanager AIVD: **Guido van Hulzen**



guido.vanhulzen@minbzk.nl