No pictures during this presentation please
Slides will be made available

Hacker Mindset

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

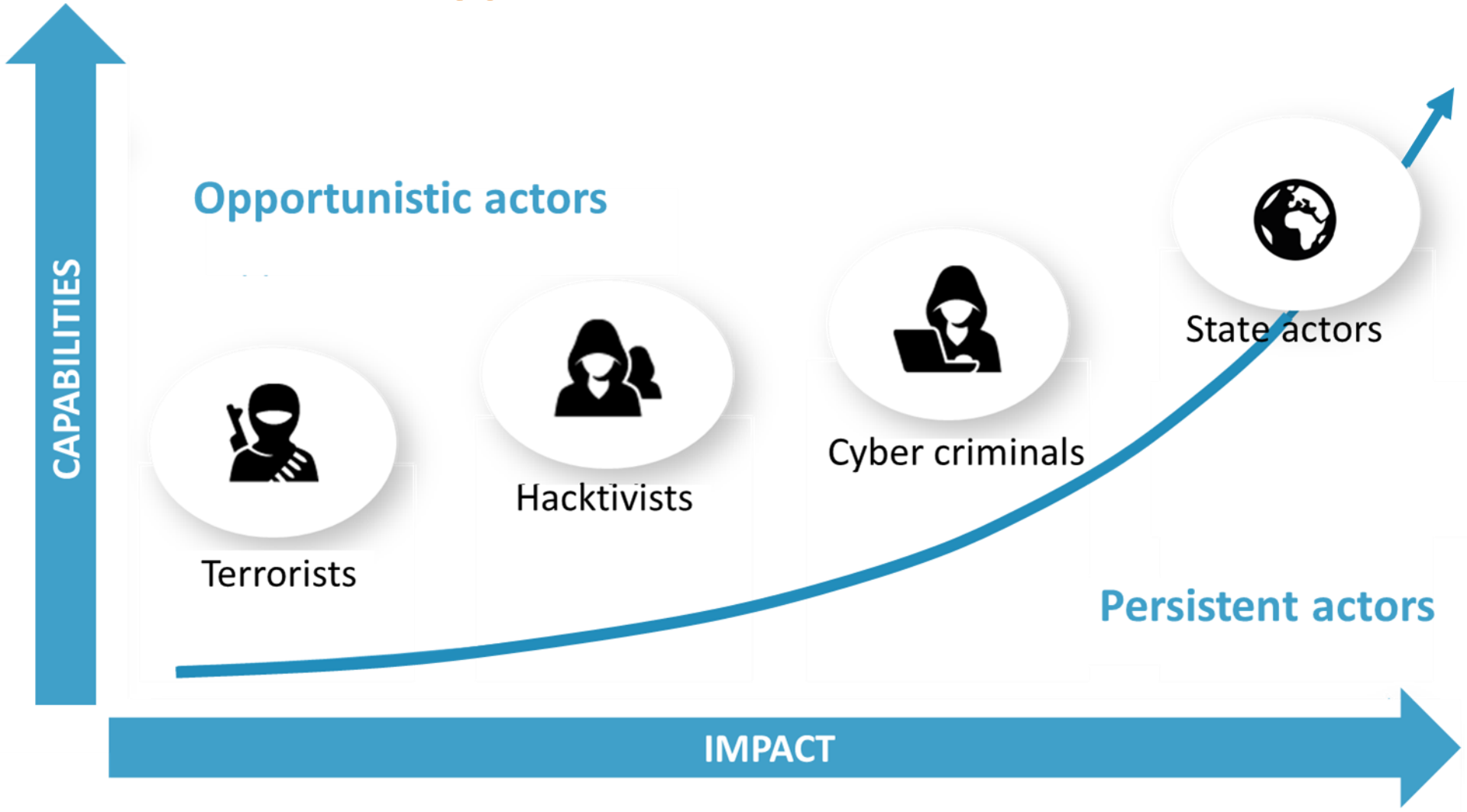
Context: Why is the AIVD contributing to this event?

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

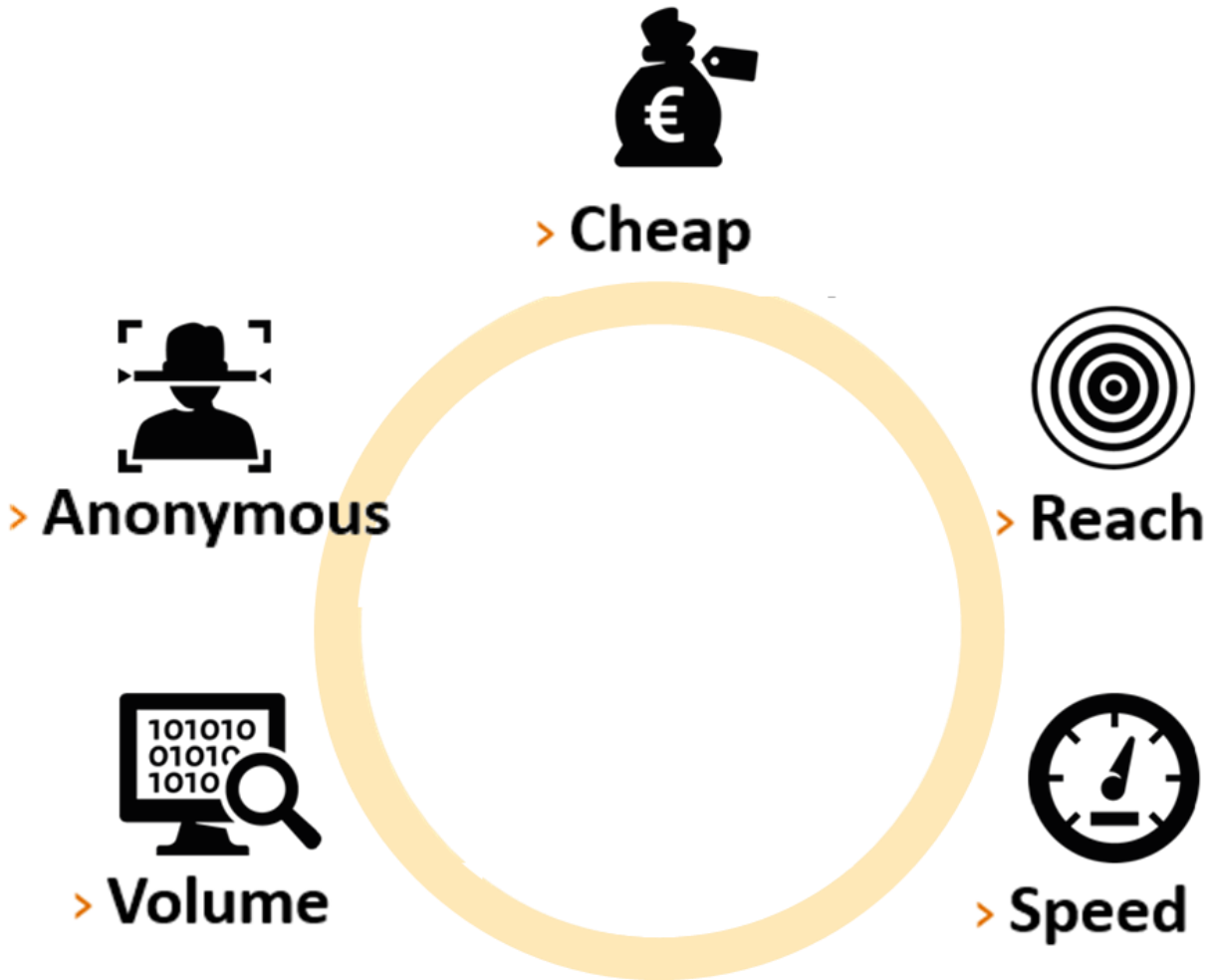
To do so the AIVD…

- 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

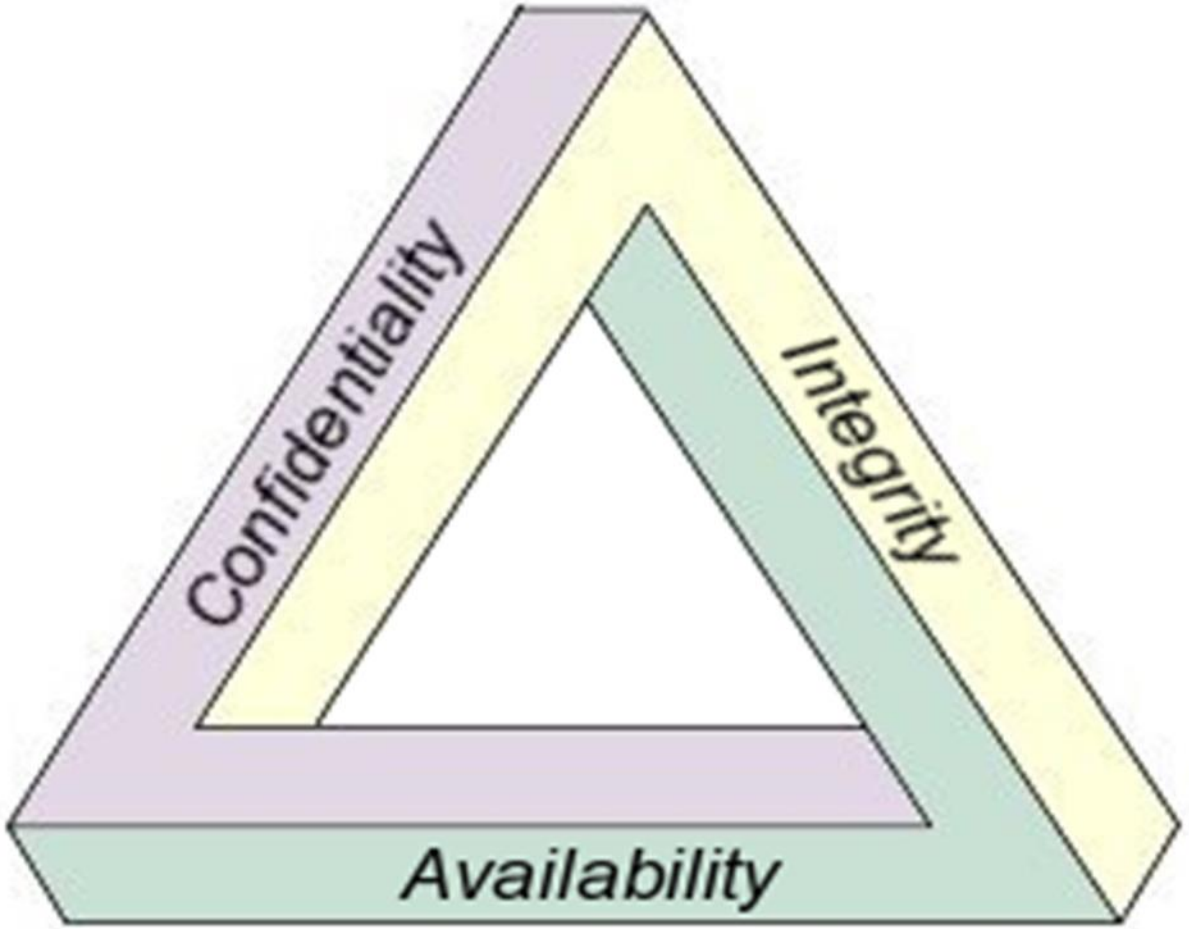


Internet has proven to be a game changer

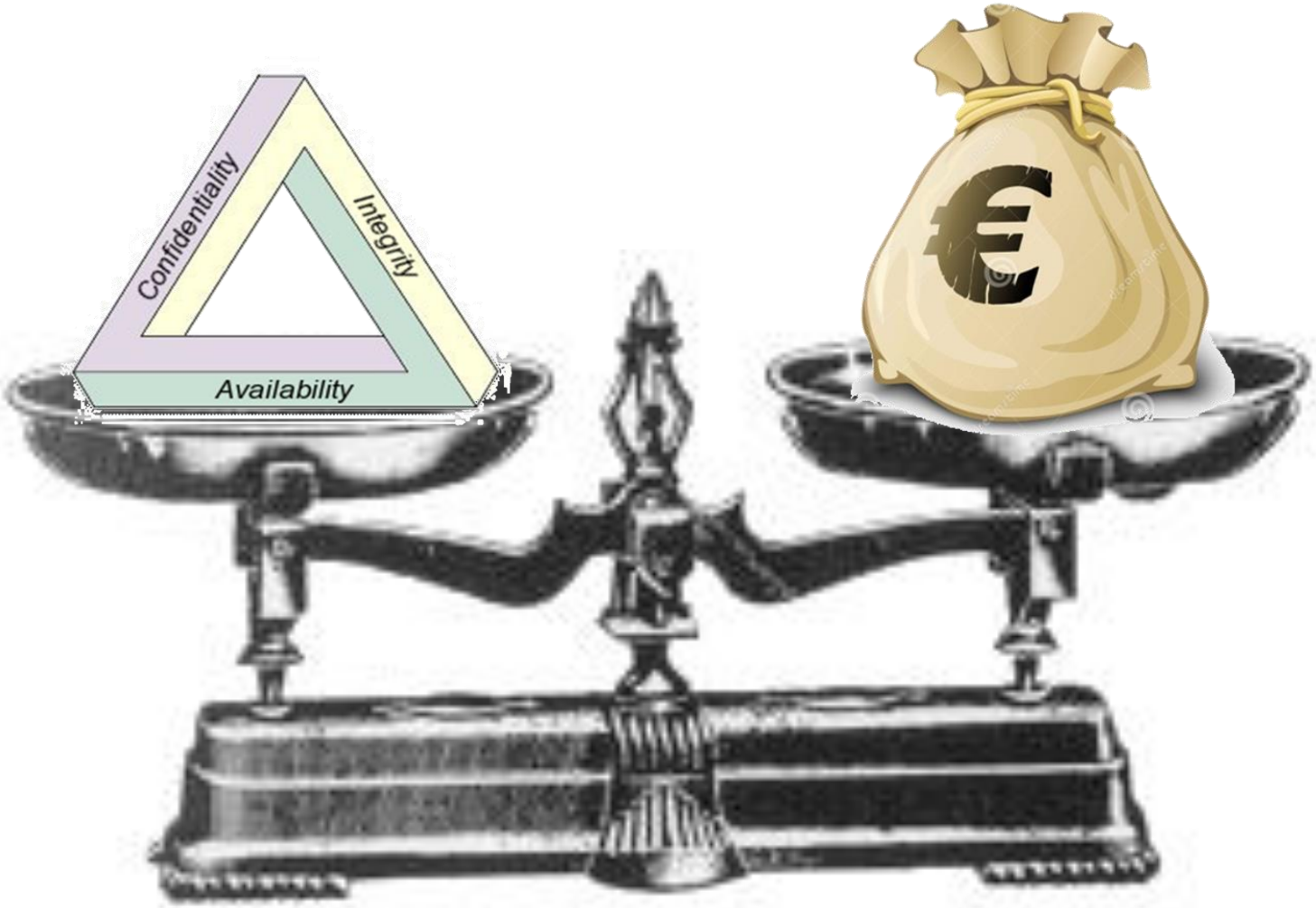


Physical threats vs Digital threats

Three main goals of any IT-security strategy



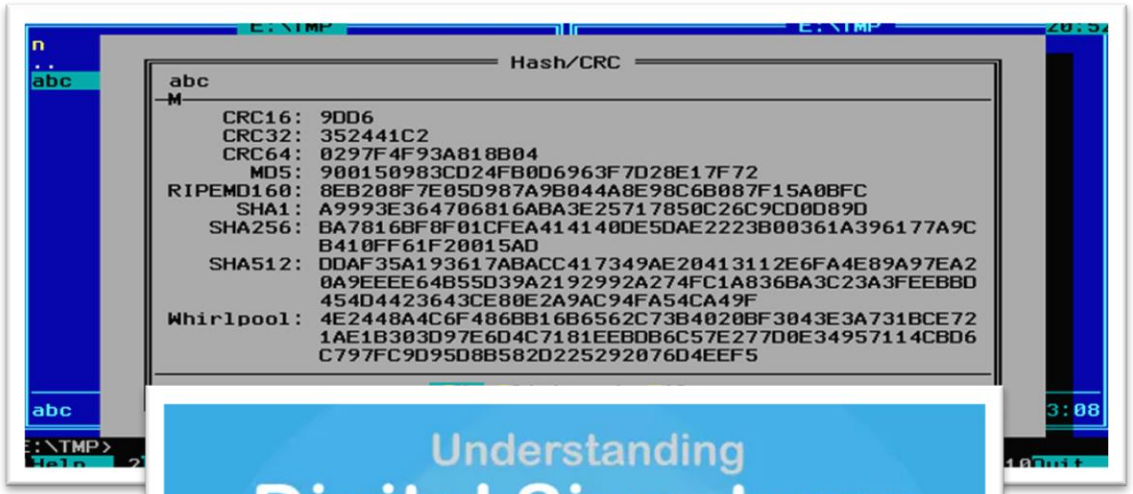
What requirements should be met by your products and services?



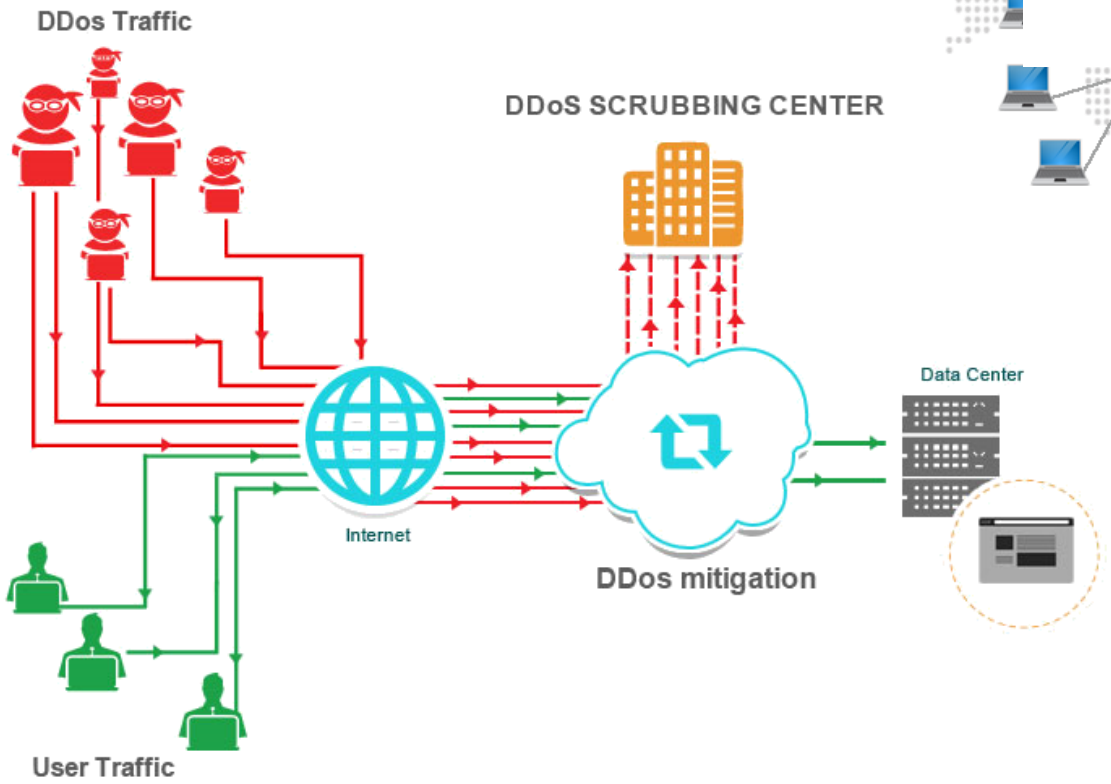
What might you do to increase Confidentiality?

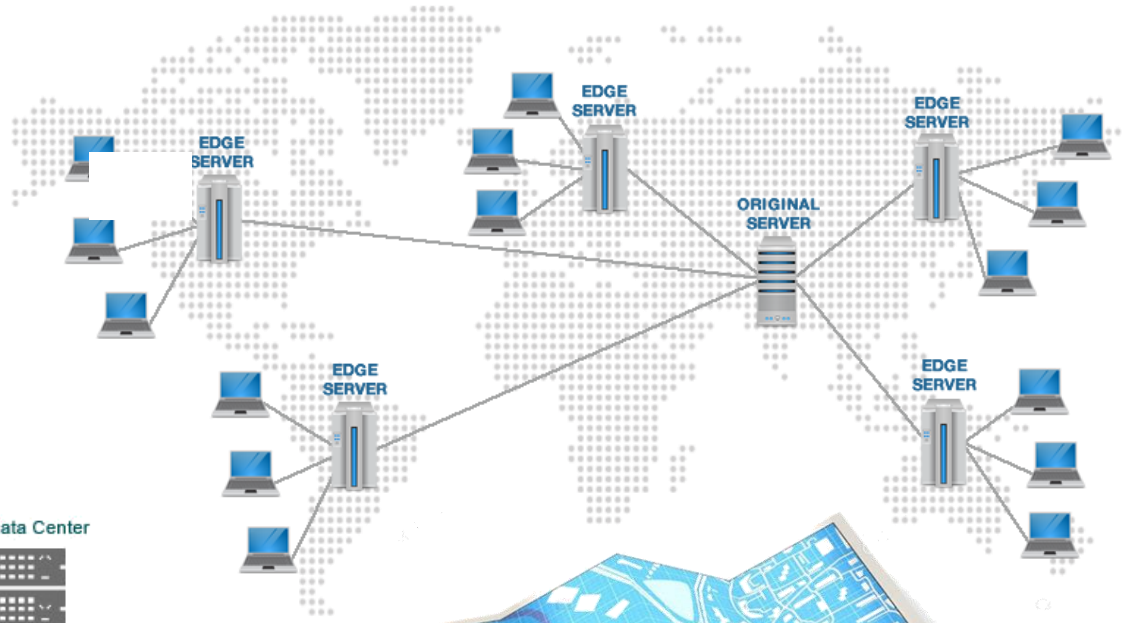
Security principle:
"Least privilege"

What might you do to increase Integrity?



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

Get short URL

Published time: 28 Feb, 2017 20:52

© 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.

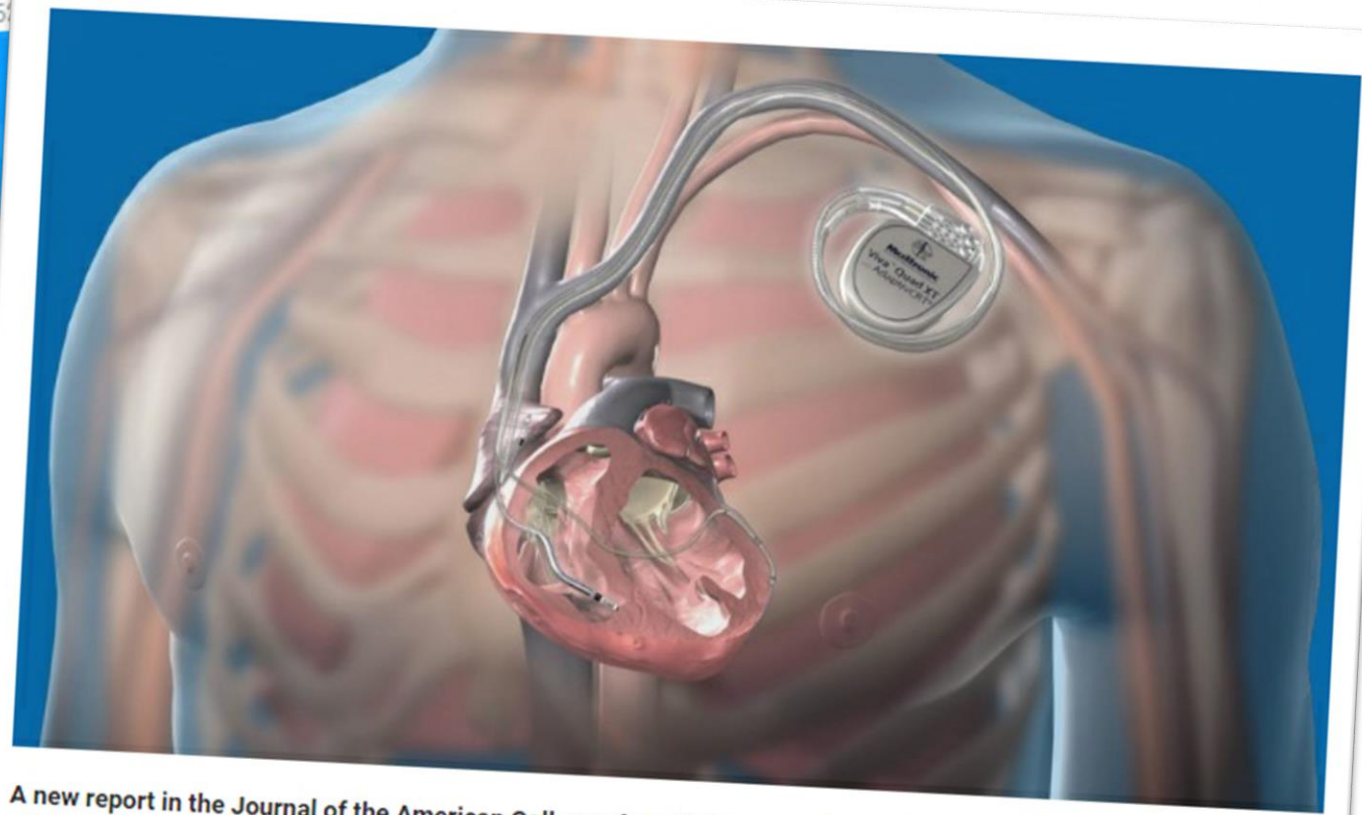
‘Smart’ Teddy be
children at risk

Published time: 28 Feb, 2017 20:5

© cloudpets.com

Spiral Toys, the com
million individual rec

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: P
s can be
shows
The internet of dildos is here, and it's vulnerable as hell
TechRepublic.
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
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.
© cloudpet
Spiral Toy
million inc
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.

Home › Wireless Security

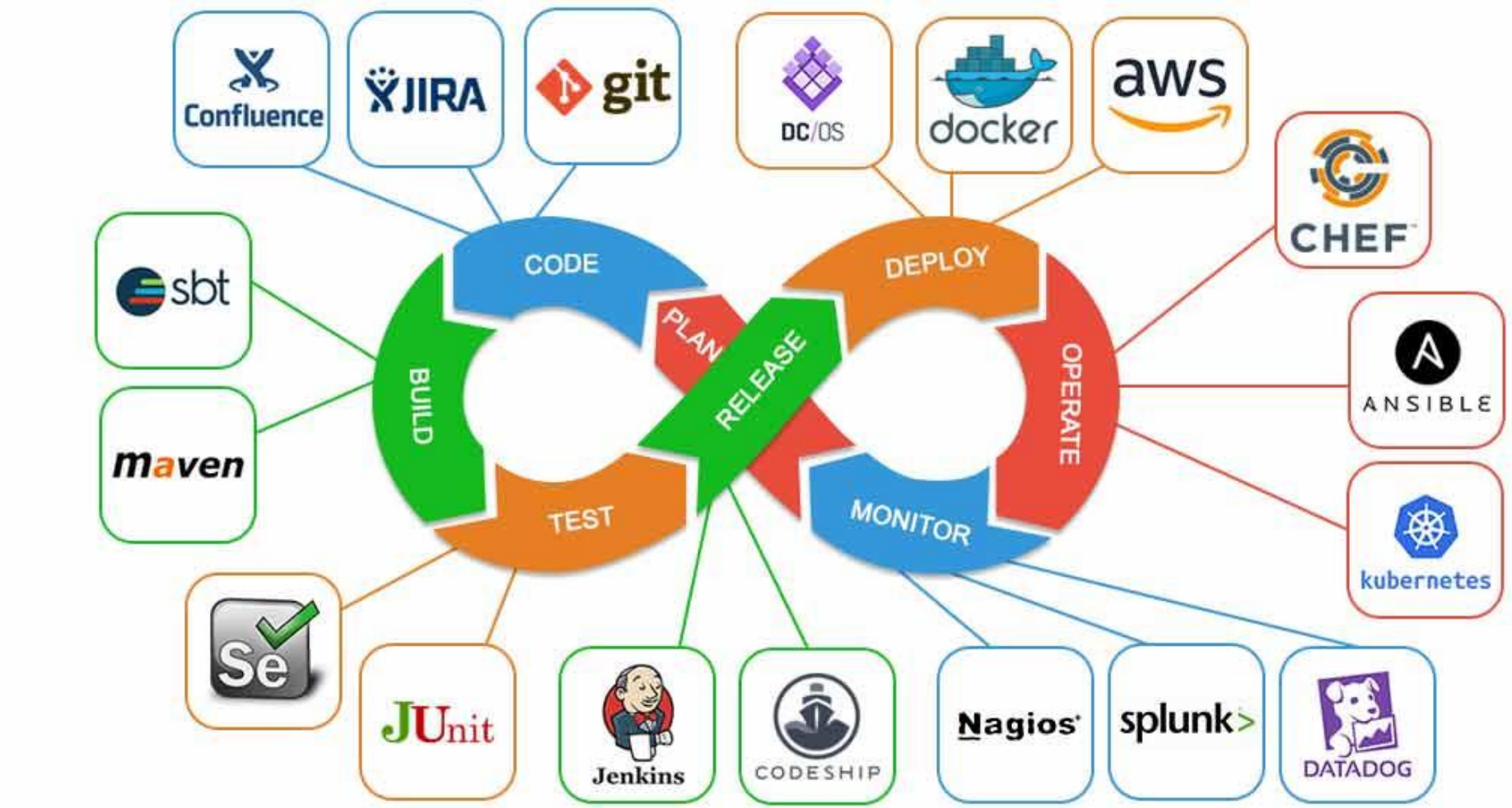
Tesla Car Hacked Remotely From Drone via Zero-Click Exploit

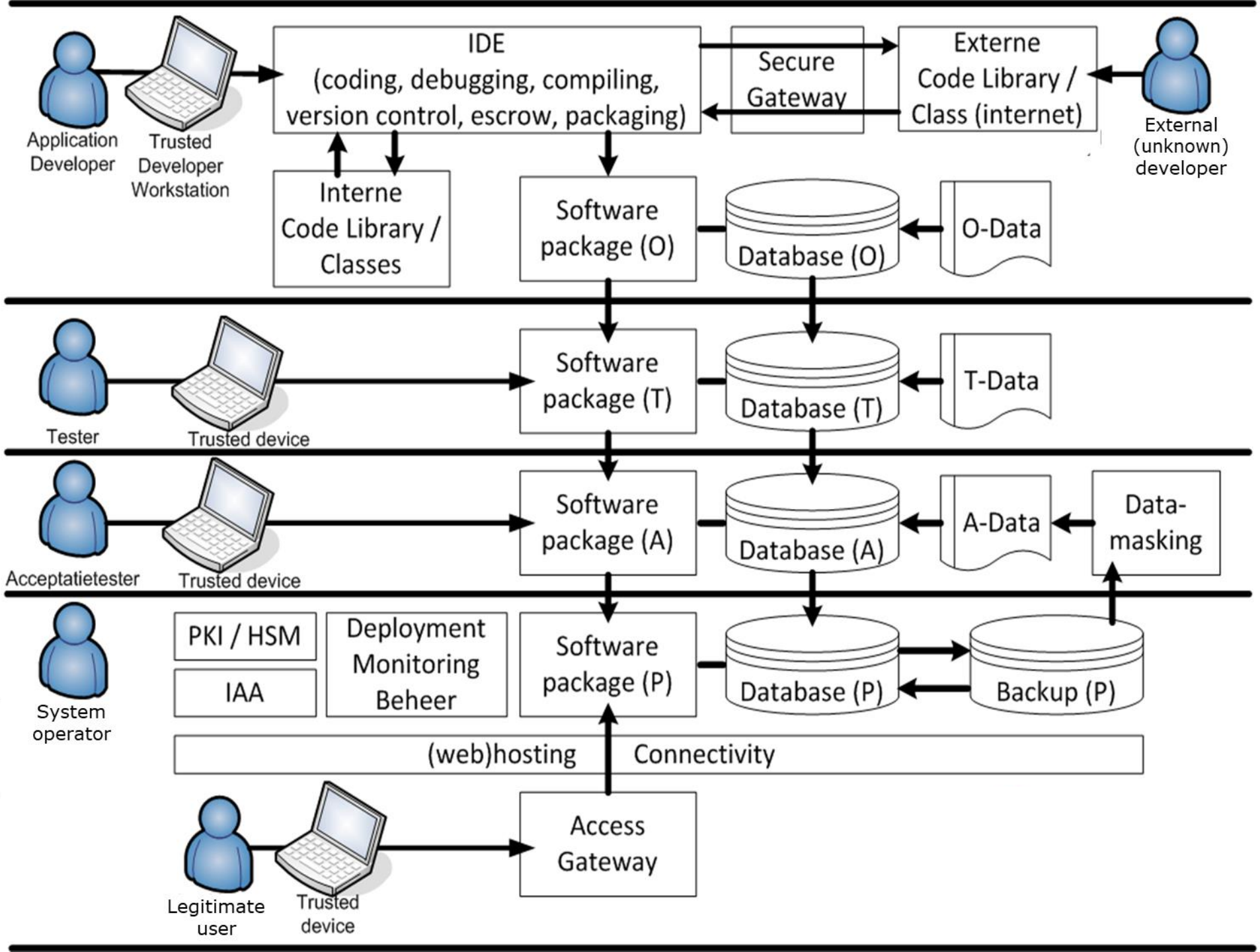
By Eduard Kovacs on May 03, 2021

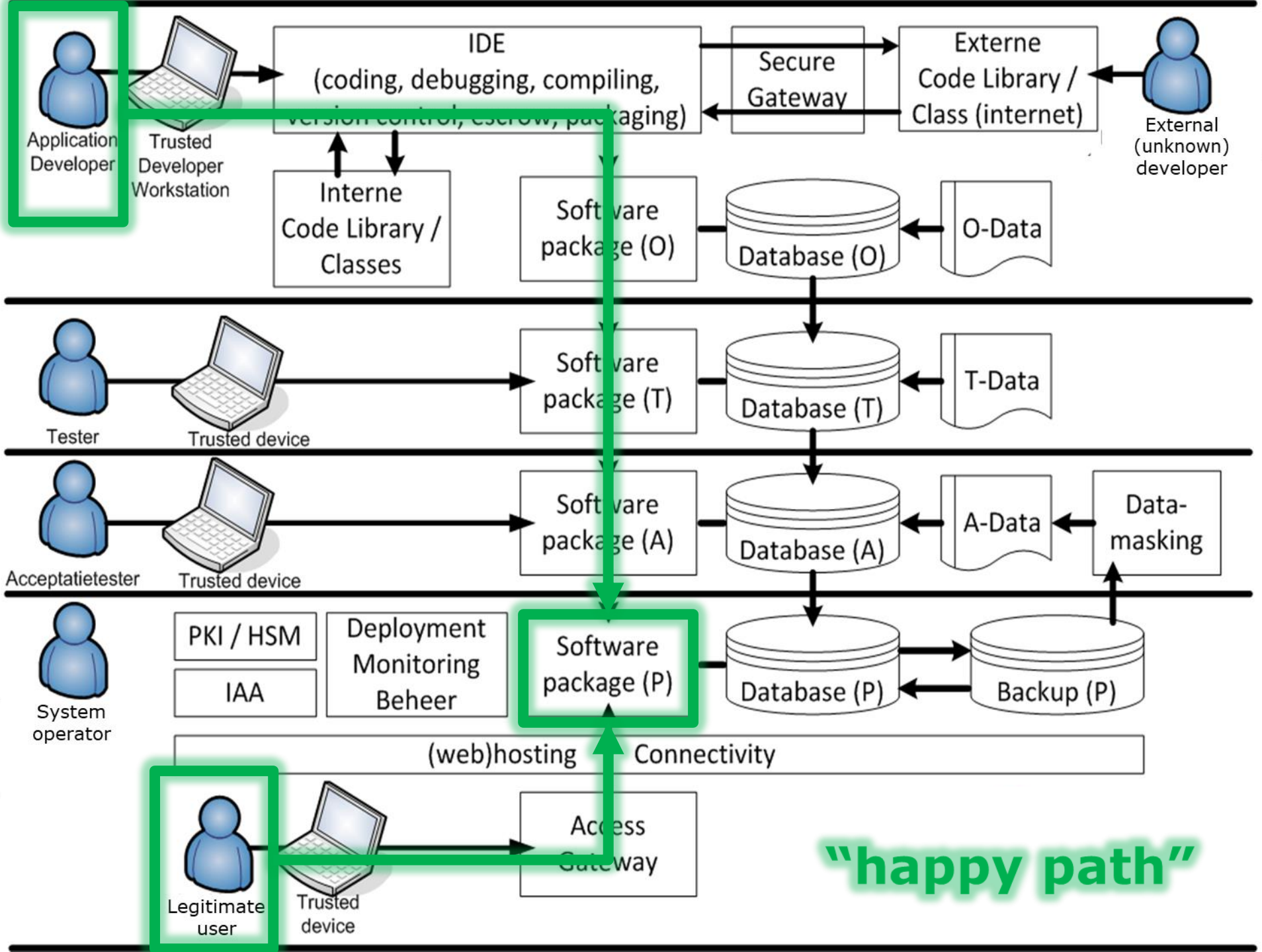
Share Tweet RSS

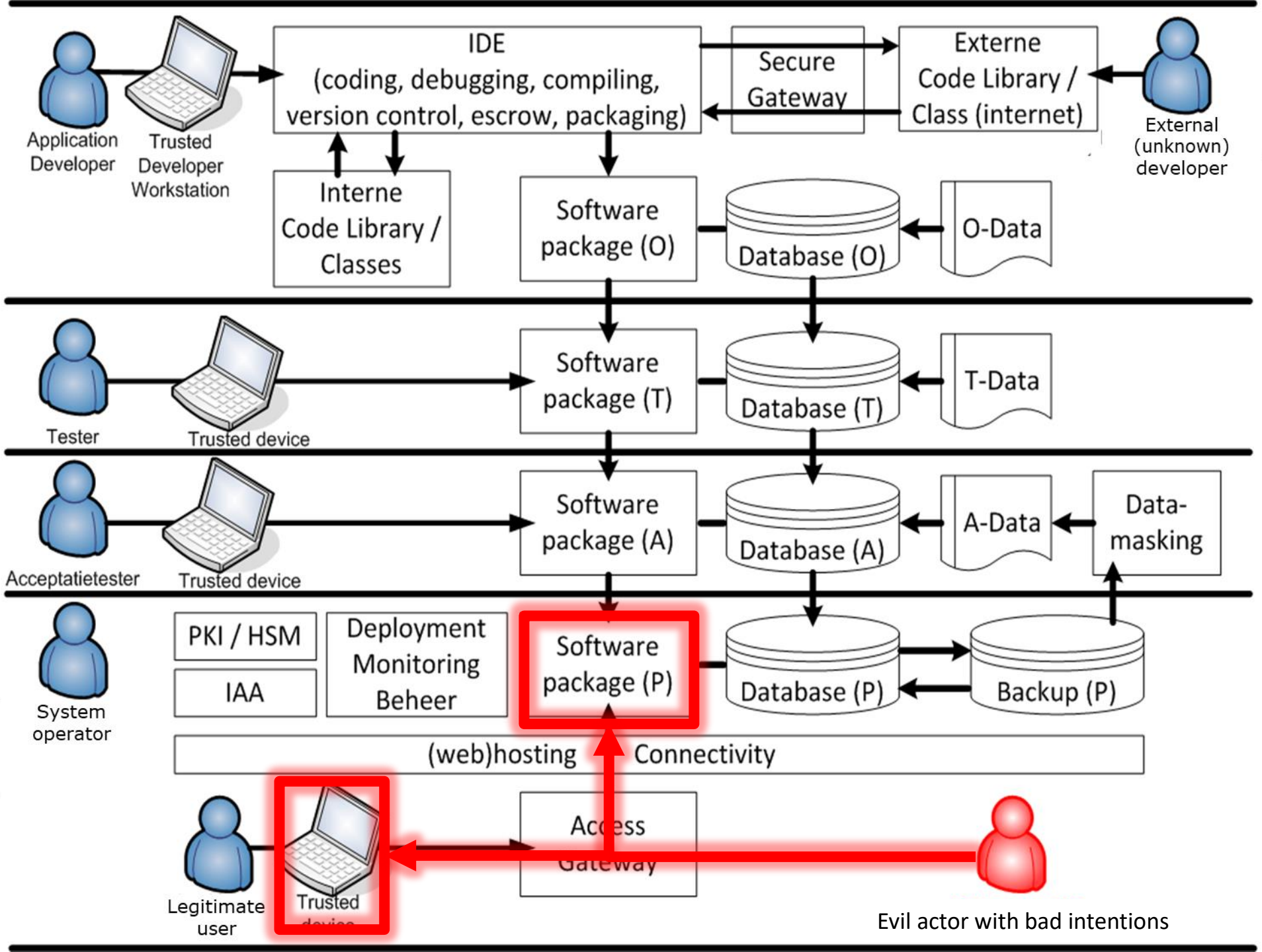
Two researchers have shown how a Tesla — and possibly other cars — can be hacked remotely without any user interaction. They carried out the attack from a drone.

So what should you do when developing new systems?



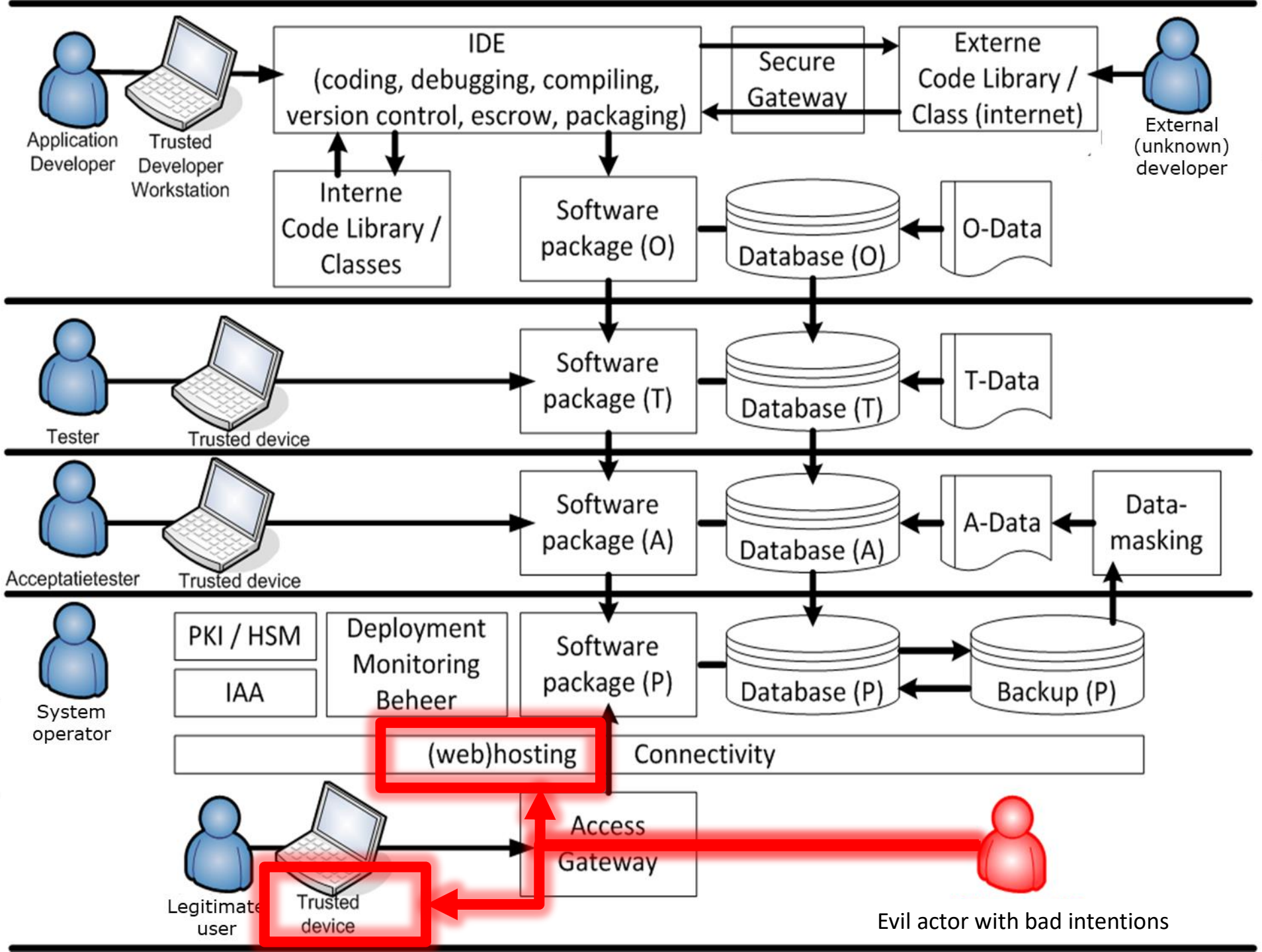

IDE
(coding, debugging, compiling, version control, escrow, packaging)
Secure Gateway
Externe Code Library / Class (internet)
External (unknown) developer
Application Developer
Trusted Developer Workstation
Interne Code Library / Classes
Software package (O)
Database (O)
O-Data
Tester
Trusted device
Software package (T)
Database (T)
T-Data
Acceptatietester
Trusted device
Software package (A)
Database (A)
A-Data
Data-masking
System operator
PKI / HSM
IAA
Deployment Monitoring Beheer
Software package (P)
Database (P)
Backup (P)
(web)hosting
Connectivity
Legitimate user
Trusted device
Access Gateway


Application Developer
Trusted Developer Workstation
IDE
(coding, debugging, compiling,
Secure Gateway
Externe Code Library / Class (internet)
External (unknown) developer
Interne Code Library / Classes
Software package (O)
Database (O)
O-Data
Tester
Trusted device
Software package (T)
Database (T)
T-Data
Acceptatietester
Trusted device
Software package (A)
Database (A)
A-Data
Data-masking
System operator
PKI / HSM
IAA
Deployment Monitoring Beheer
Software package (P)
Database (P)
Backup (P)
(web)hosting
Connectivity
Legitimate user
Trusted device
Access Gateway
"happy path"

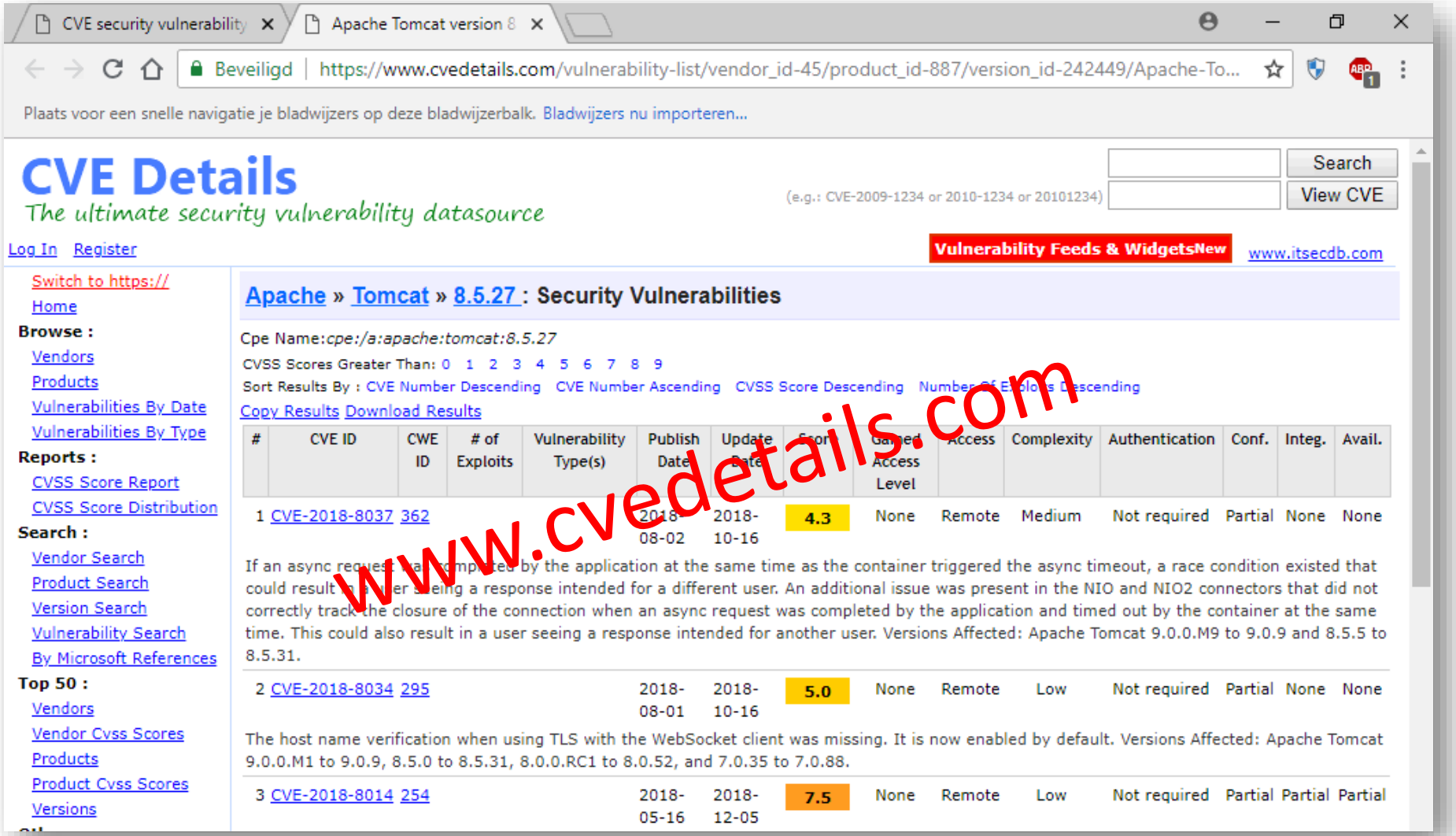

IDE
(coding, debugging, compiling, version control, escrow, packaging)
Secure Gateway
Externe Code Library / Class (internet)
Application Developer
Trusted Developer Workstation
External (unknown) developer
Interne Code Library / Classes
Software package (O)
Database (O)
O-Data
Tester
Trusted device
Software package (T)
Database (T)
T-Data
Acceptatietester
Trusted device
Software package (A)
Database (A)
A-Data
Data-masking
System operator
PKI / HSM
IAA
Deployment Monitoring Beheer
Software package (P)
Database (P)
Backup (P)
(web)hosting
Connectivity
Legitimate user
Trusted device
Access Gateway
Evil actor with bad intentions

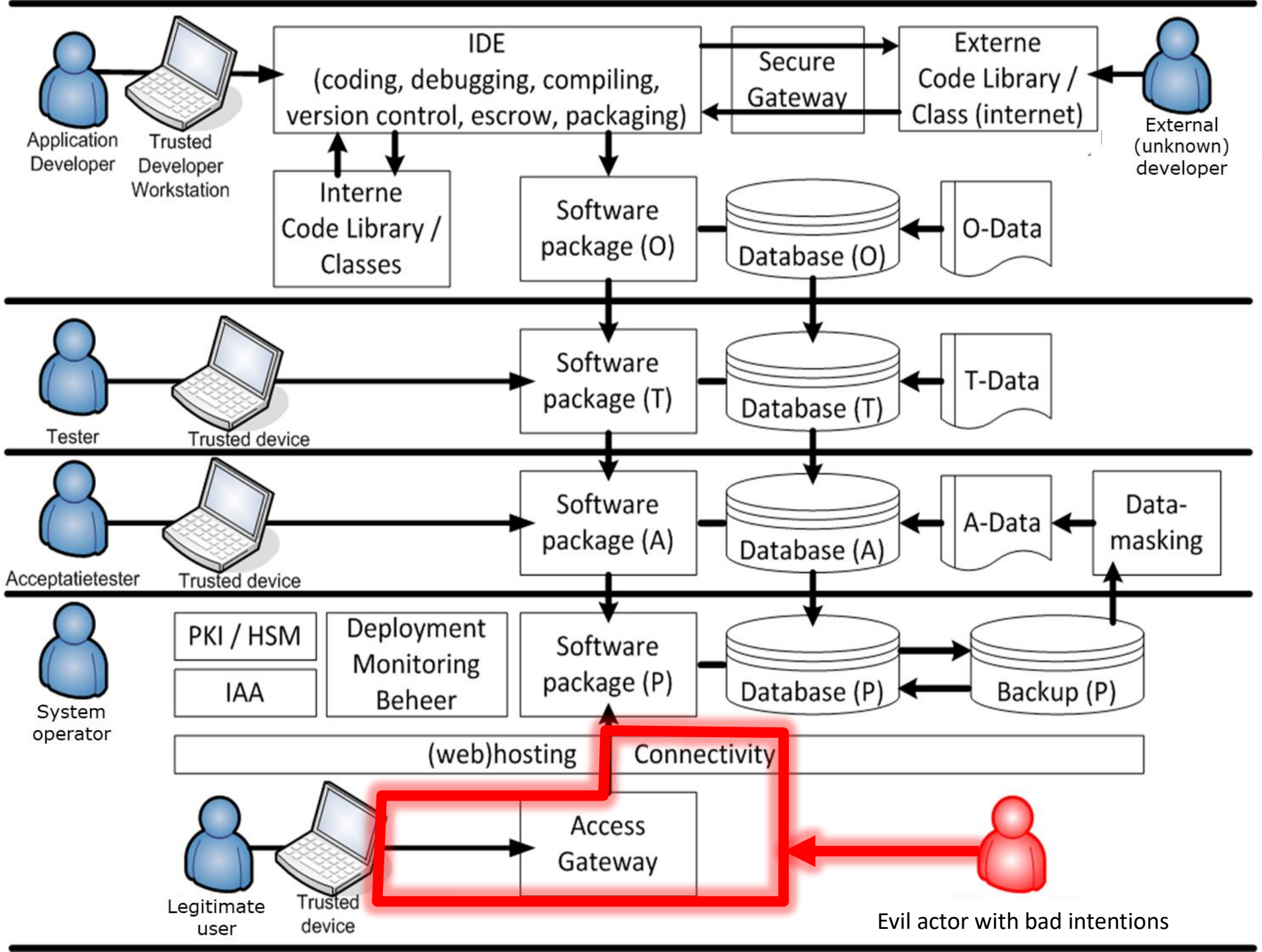
Basic (obvious) security measures

- 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- of Cookie-manipulation / etc… etc…
- See OWASP.org, featuring:
  - OWASP Top 10 (2021)
  - OWASP Dependency Check
  - OWASP Security Knowledge Framework
  - OWASP Application Security Verification Standard


IDE
(coding, debugging, compiling, version control, escrow, packaging)
Secure Gateway
Externe Code Library / Class (internet)
Application Developer
Trusted Developer Workstation
External (unknown) developer
Interne Code Library / Classes
Software package (O)
Database (O)
O-Data
Tester
Trusted device
Software package (T)
Database (T)
T-Data
Acceptatietester
Trusted device
Software package (A)
Database (A)
A-Data
Data-masking
System operator
PKI / HSM
IAA
Deployment Monitoring Beheer
Software package (P)
Database (P)
Backup (P)
(web)hosting
Connectivity
Access Gateway
Legitimate user
Trusted device
Evil actor with bad intentions

Security measure: keep ALL software up to date



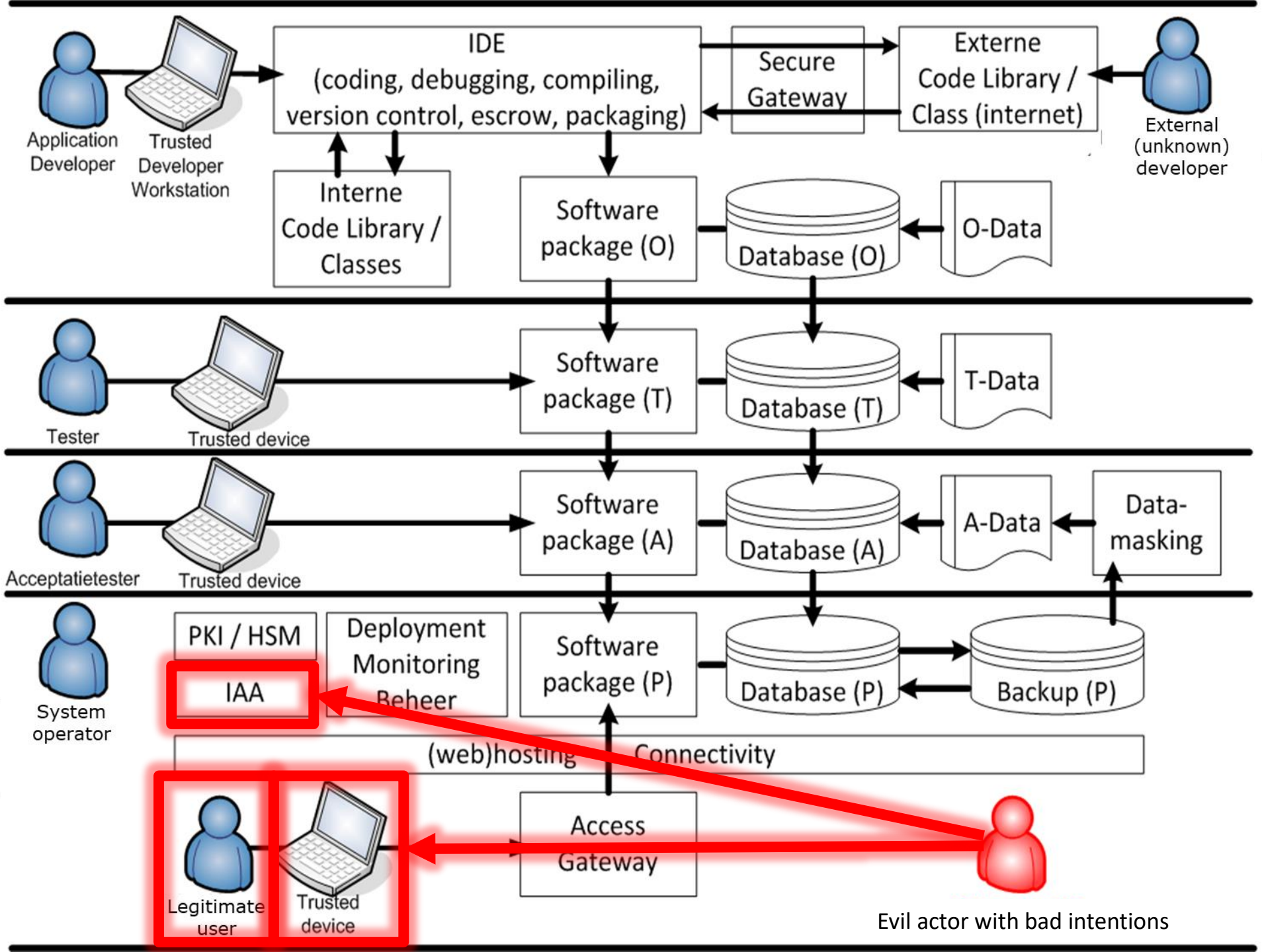

IDE
(coding, debugging, compiling, version control, escrow, packaging)
Secure Gateway
Externe Code Library / Class (internet)
External (unknown) developer
Application Developer
Trusted Developer Workstation
Interne Code Library / Classes
Software package (O)
Database (O)
O-Data
Tester
Trusted device
Software package (T)
Database (T)
T-Data
Acceptatietester
Trusted device
Software package (A)
Database (A)
A-Data
Data-masking
System operator
PKI / HSM
IAA
Deployment Monitoring Beheer
Software package (P)
Database (P)
Backup (P)
(web)hosting
Connectivity
Legitimate user
Trusted device
Access Gateway
Evil actor with bad intentions

Security measures

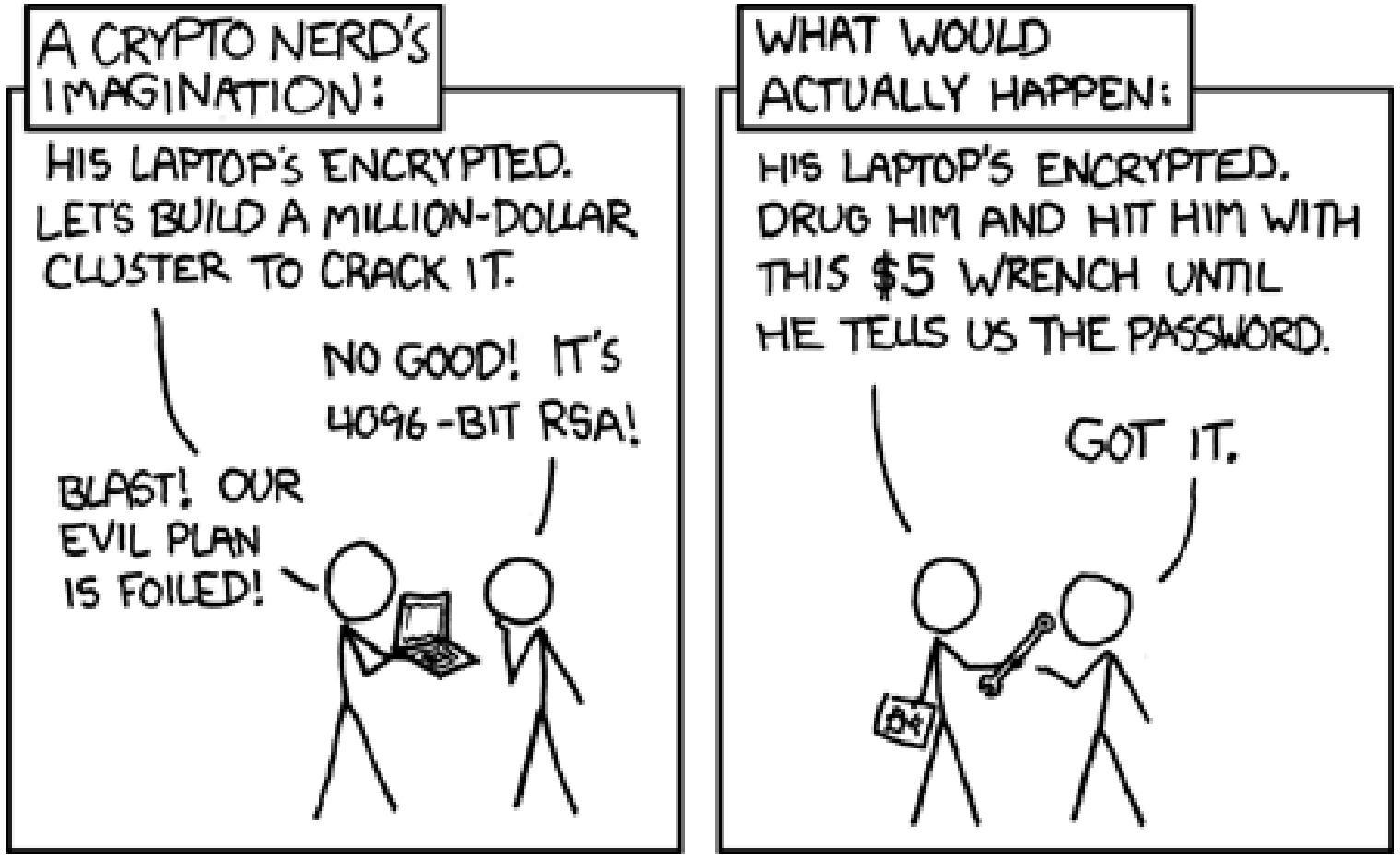
Prevent Man in the Middle attacks:

- 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?


IDE
(coding, debugging, compiling, version control, escrow, packaging)
Secure Gateway
Externe Code Library / Class (internet)
External (unknown) developer
Application Developer
Trusted Developer Workstation
Interne Code Library / Classes
Software package (O)
Database (O)
O-Data
Tester
Trusted device
Software package (T)
Database (T)
T-Data
Acceptatietester
Trusted device
Software package (A)
Database (A)
A-Data
Data-masking
System operator
PKI / HSM
IAA
Deployment Monitoring Beheer
Software package (P)
Database (P)
Backup (P)
(web)hosting
Connectivity
Access Gateway
Legitimate user
Trusted device
Evil actor with bad intentions

Is the authenticated end-user actually trustworthy?



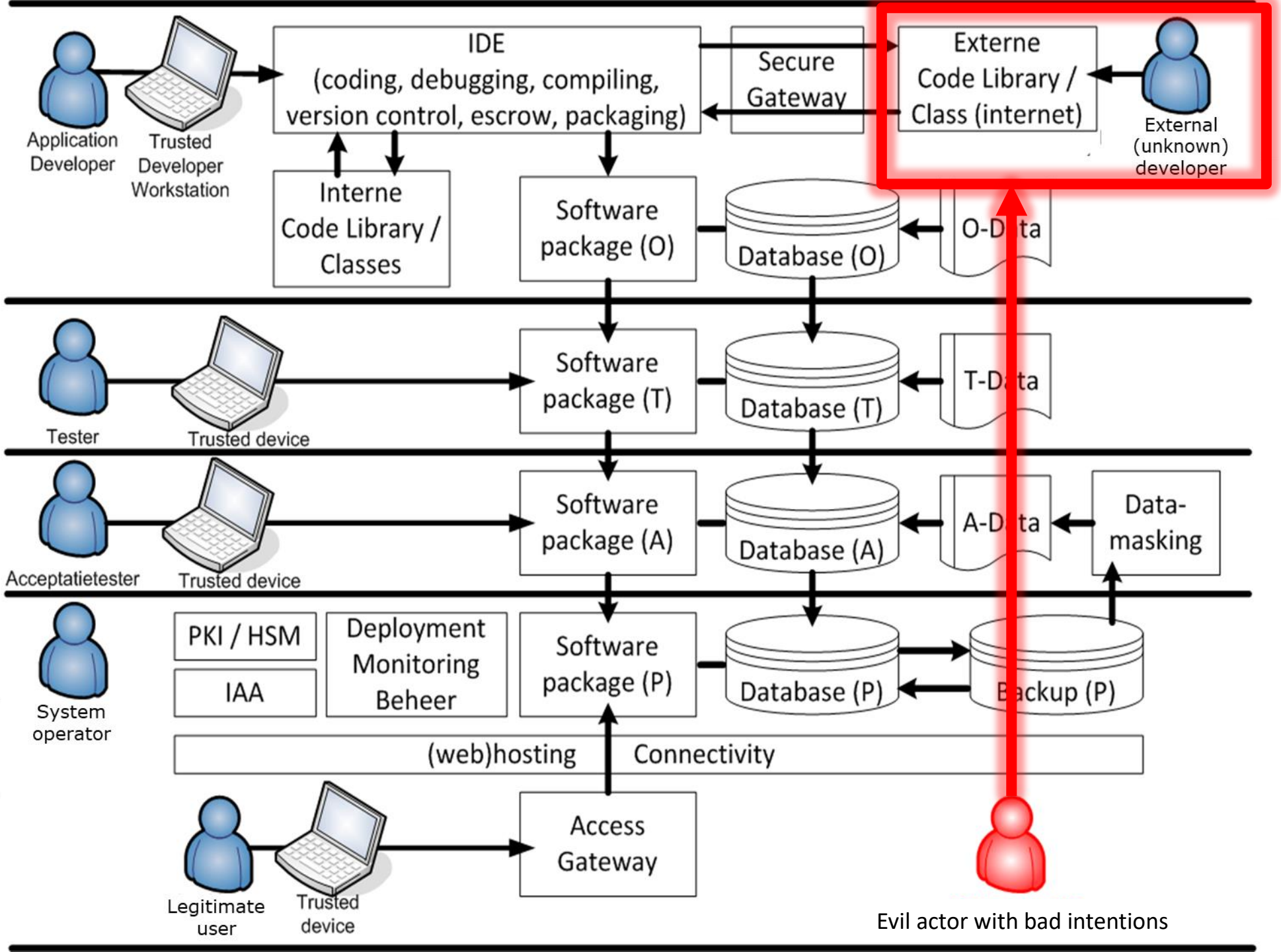
Measure: User and Entity Behavior Analytics (UEBA)

Detecting Hacked Twitter Accounts based on Behavioural Change

Meike Nauta[1], Mena Habib[2] and Maurice van Keulen[1]
[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

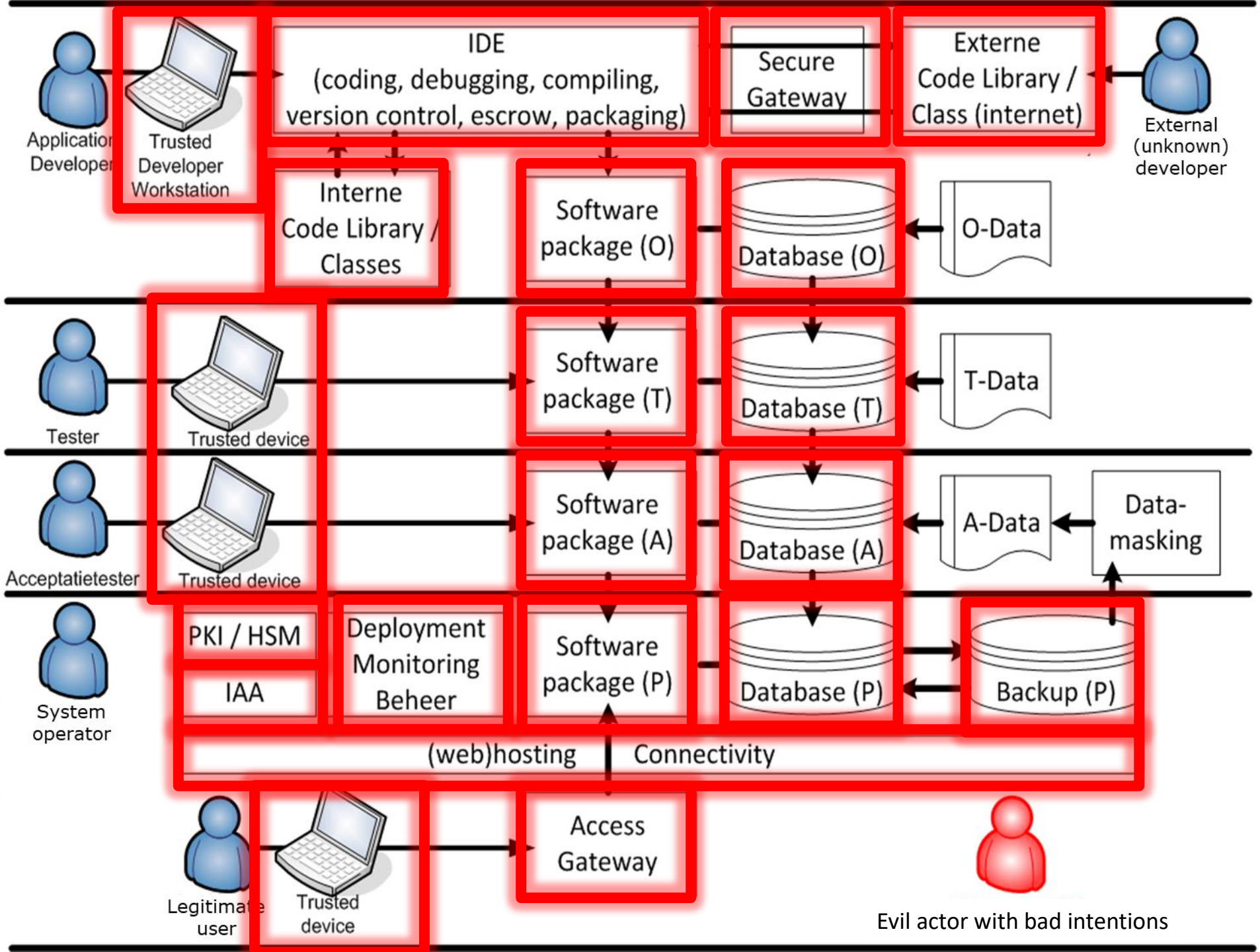
Abstract: Social media accounts are valuable for hackers for spreading phishing links, malware and spam. Furthermore, some people deliberately hack an acquaintance to damage his or her image. This paper describes a classification for detecting hacked Twitter accounts. The model is mainly based on features 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 use 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.


IDE
(coding, debugging, compiling, version control, escrow, packaging)
Secure Gateway
Externe Code Library / Class (internet)
External (unknown) developer
Application Developer
Trusted Developer Workstation
Interne Code Library / Classes
Software package (O)
Database (O)
O-Data
Tester
Trusted device
Software package (T)
Database (T)
T-Data
Acceptatietester
Trusted device
Software package (A)
Database (A)
A-Data
Data-masking
System operator
PKI / HSM
IAA
Deployment Monitoring Beheer
Software package (P)
Database (P)
Backup (P)
(web)hosting
Connectivity
Legitimate user
Trusted device
Access Gateway
Evil actor with bad intentions

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



Evil actor with bad intentions

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

c|net

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.

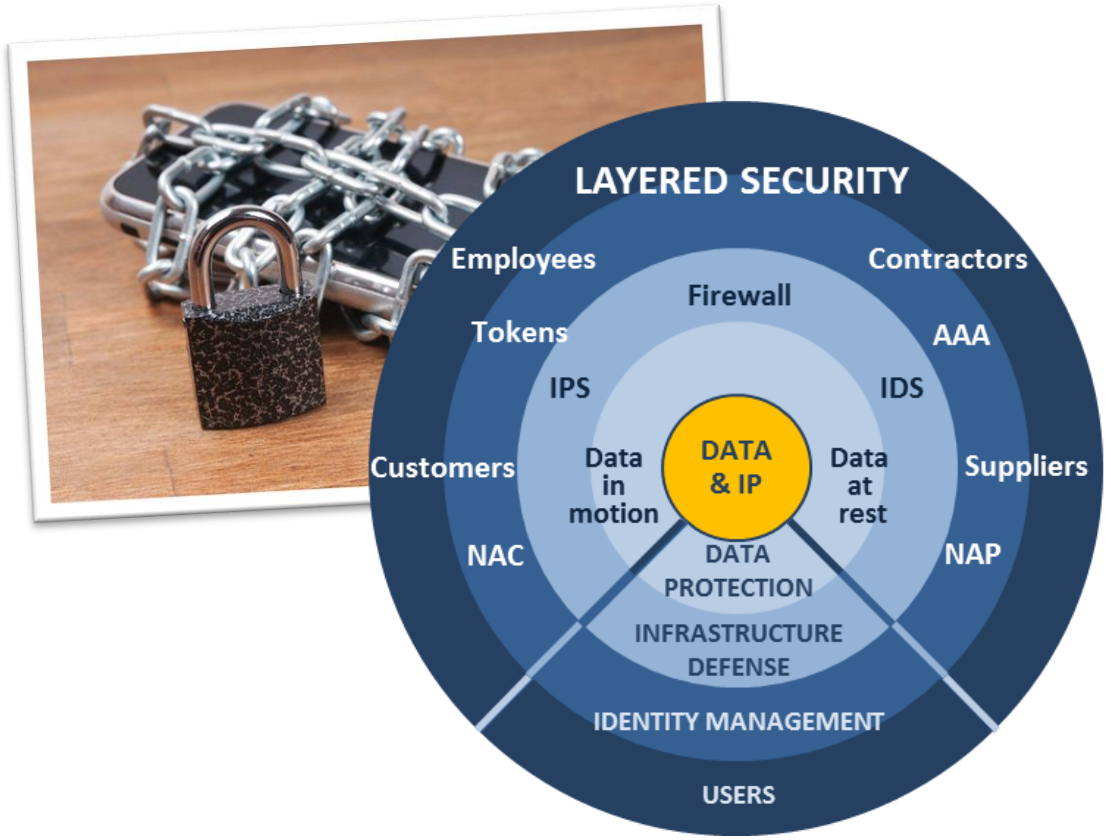
Three overarching principles…

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!

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