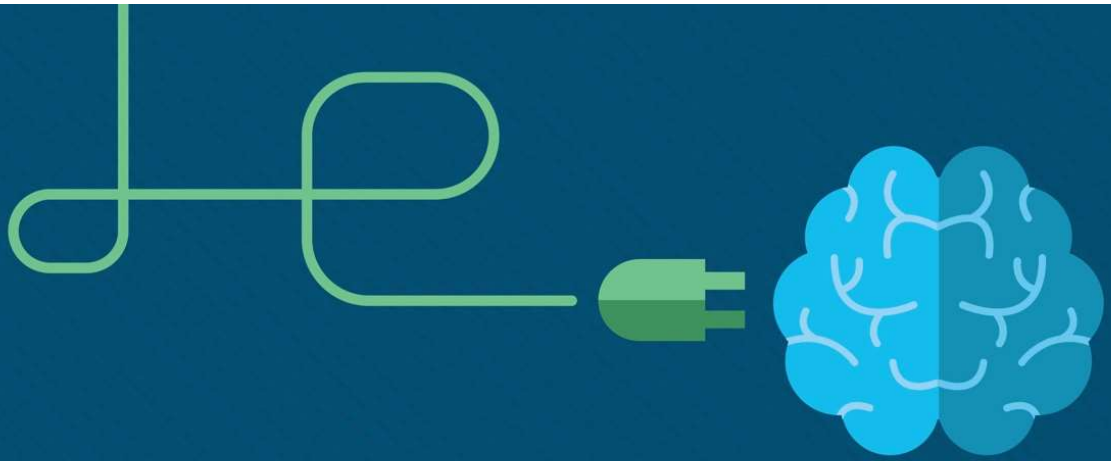


Webinar: Identity and access management developments

Een samenwerking tussen de Cisco Networking Academy, KIVI en Stysec

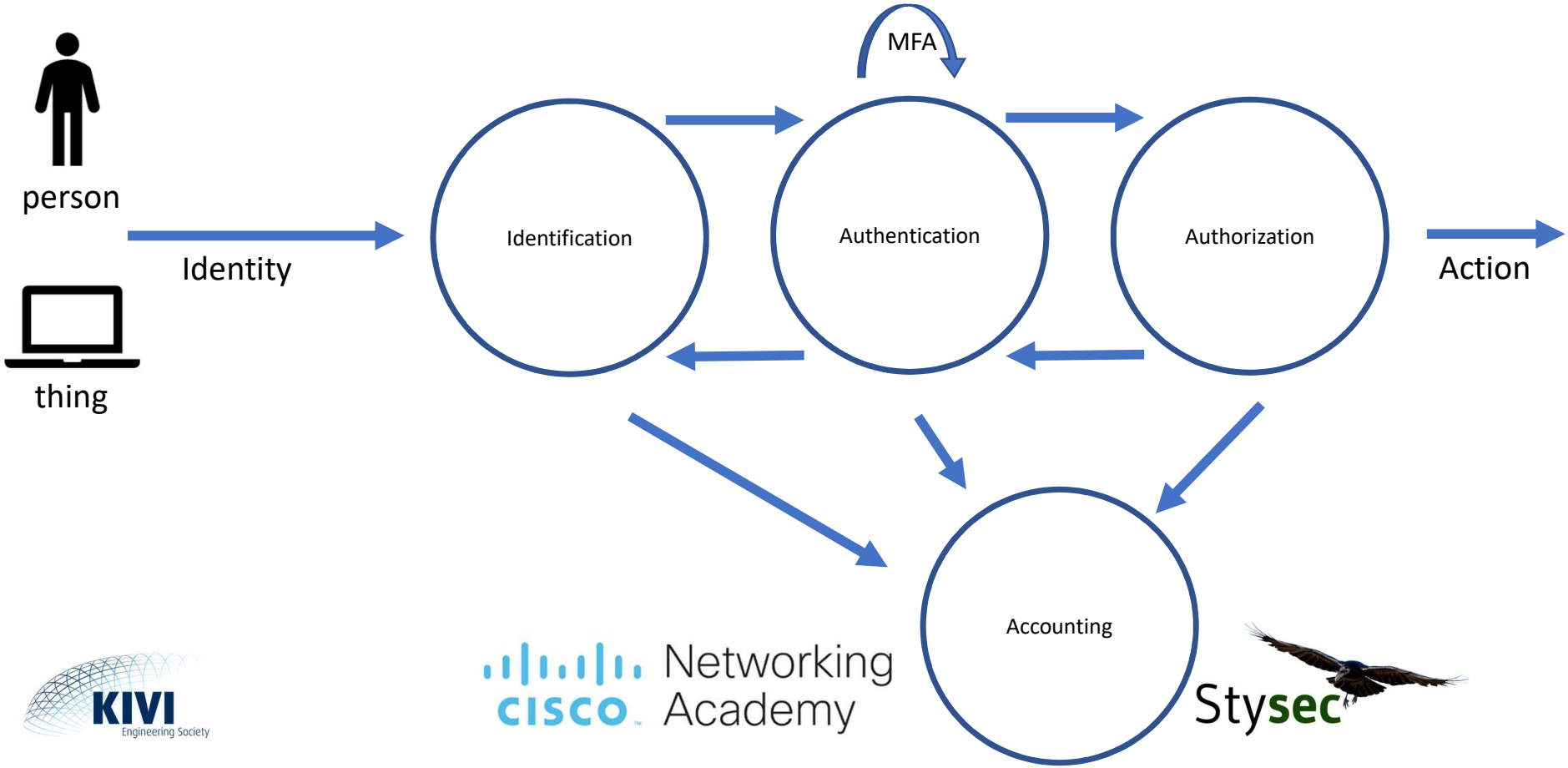
Dinsdag 19 mei 2020

Drs Ing René Pluis MBA MBI – rpluis@cisco.com

Cyber Security Lead CDA-NL program

Overview IAA&A:

Identity – Identification – Authentication – Authorization – Accounting



KIVI Engineering Society

CISCO Networking Academy

Stysec

IAA&A in real life, examples

Used for all kind of processes where IAA&A are needed:

- official processes like
  - Passports, driver license and other official (picture) documents which can be used as ‘official ID’
  - Proof of age and / or identity (visits to bar, casino, … and signing official documents like mortgage, bank accounts, …)
- (un)official day to day processes like
  - Access to restricted areas (employee ID for office, membership cards, …)

Unofficial processes often not (automatically) enforced in day to day practice, people get to recognize other people and will deploy ‘implicit soft’ IAA. Accounting often not in place.

Several levels of IAA possible depending on classification or safety levels, accounting important

Automated processes (especially between things) faster but can be weaker than a security guard…

KIVI Engineering Society

Networking Academy

Stysec

IAA&A – closer look

Identity and Identification – to identify the requestor

- how to strongly connect an identity to a person? Bio-metrics?
- how to strongly connect an identity to a device / thing? Physic-metrics?
- how to verify that the offered identity is indeed related to the person / device offering the identity?

Authentication – to verify the provided identity

- multi factor – something you know, something you have, something you are, something you …
- multiple times / continuous authentication

KIVI Engineering Society

Networking Academy

Stysec

IAA&A – closer look

Authorization – given a proven identity, provide approval

- in principle independent of IA – Identification and Authentication process
- ‘zero trust’ approach – re-authenticate before granting approval, each time
- not always static – context like location, time, behavioral, etc. start playing a role too
- broader scope, not only IA but also security posture taken into account
  - RBAC – Role Based Access Control
  - ABAC – Attribute Based Access Control
  - PBAC – Policy Based Access Control
  - Behavioral / context based access control (for example password less)

Accounting or Accountability

- often overlooked but most important (detection, anomalies, legal aspects, enforcement, …)

KIVI Engineering Society

Networking Academy

Stysec

IAA&A – closer look

Persons

- often an interactive process where an identity is provided and authenticated by providing proof
  - most used to provide identity: account or user name, smart card, token, ...
  - most used to authenticate identity: password (by far), finger print, facial scan, iris scan, token, …
  - authorization either via 'local username password file' construct or central active directory and RBAC
  - persons not involved and not aware with accounting

Things

- must be automatic or passive
  - Stronger authentication often based on certificates and other cryptographic technology (hashing / digital signatures)

Spoofing always a danger (Identity theft, man in the middle, address spoofing, …)

KIVI Engineering Society

Networking Academy

Stysec

IAA&A – network deployment examples

Persons using the network, devices, applications

- CLI – Command Line Interface, username (identification) / password (authentication) and TACAS or RADIUS (authorization), challenge response, sometimes token needed (‘something you have’)
- GUI – Graphical User Interface, stronger IA and PBAC / MFA
- zero trust, MFA when and where needed (‘MFA for workforce’)

Things connecting to each other

- ‘mutual authentication’ mechanisms (e.g. route updates via certificates & encrypted links)
- MFA – Multi Factor Authentication, MFA for workplace and MFA for workloads
- ‘director’ environments, one dashboard, configure at one place and propagate through network

KIVI Engineering Society

Networking Academy

Stysec

IAA&A – challenges

Certificates

- they expire / interoperability problems
- complex – much (central) administration, CRLs – Certification Revocation Lists, interoperability
- outdated cryptographic strength, key length, different technology, quantum
- 'official' counterfeits, e.g. DigiNotar hack (read the book†)

Hardware tokens

- expensive, you can loose them, can get stolen

General problems

- pre-configuration tasks, not easy to replace during runtime, expensive, etc.

† "Het is oorlog maar niemand die het ziet" – Huib Modderkolk, link

KIVI Engineering Society

Networking Academy

Stysec

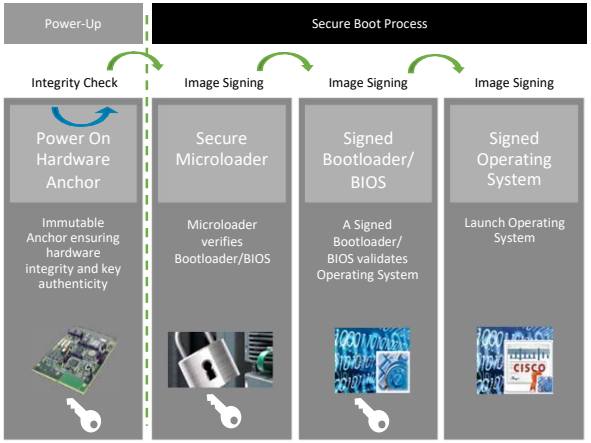
IAA&A – new developments

Hardware Identity

- PUF – Physical Unclonable Function, a way to authenticate electronic devices or chips and generate cryptographic keys from their unclonable silicon fingerprint. It uses uncontrollable deep-submicron variations from manufacturing to derive a stable, unclonable silicon fingerprint.

Trust anchor

- verification ‘identity’ of the device is not changed!



KIVI Engineering Society

Networking Academy

Stysec

IAA&A – new developments

Context based authentication / authorization

- towards ‘password less’ era, e.g. retail pick & place authorization based on handheld ID, location, task, value, etc. → no authorization needed by password

Possible scenario

- personal access card is activated by bio-metric authentication
- access card gives access to hazardous area by
  - person is authorized to access that area because:
    - based on the role the person has
    - there is an existing and valid workorder
    - the necessary certifications are in place and valid

KIVI Engineering Society

Networking Academy

Stysec

IAA&A – new deployments

Possible scenario – work in hazardous area

- personal access card is activated and strongly tied to person by bio-metric authentication
- via access card access to hazardous area is determined on basis of:
  - person is authorized to access that area because:
    - based on the role the person has
    - there is an existing and valid workorder
    - the necessary certifications are in place and valid
  - necessary support is present and available
  - right time and location
- continuous monitoring, training, remote expert, calamity management, etc.

KIVI Engineering Society

Networking Academy

Stysec

IAA&A – observations and conclusions

In the early days there was implicit trust and everybody knew each other

- loosely coupled identity, no authentication, no authorization, no accounting
- proof of protocol / algorithm / program higher priority than IAA&A
- after Internet scale up and commercial interests unique identification more important
- more important processes automated / connected stronger IAA&A necessary

Still IAA&A not sexy and more complex than on first look

Due to developments renewed interest (misuse, privacy, fraud, law & regulations, …)

Active research topic

- article: "*User Categorization using Fuzzy Logic towards PUF based Two-Phase Authentication of Fog assisted IoT devices*"

KIVI Engineering Society

Networking Academy

Stysec


Thank You!
Any Questions?


CISCO