Zero Trust in Zero Trust?

(The good, the bad, and the ugly of the zero-trust buzzword)

Virgil D. Gligor
ECE Department and CyLab
Carnegie Mellon University
Pittsburgh, PA 15213

Center for Cyber Defense and Information Security
KTH Stockholm
May 24, 2022

Outline

1. Trust (~ 10 min)

- minimum trust, zero trust, and trust establishment
- security

2. "zero trust" in NIST's architecture (~ 15 min)

- what is it and what is missing
- why is "zero trust" a "buzzword"

3. The Good, the Bad, and the Ugly . . . (~ 15 min)

4. Q & A - discussion (~5 min)

5. Optional: Beyond "zero trust" (~10 min)

– how to secure compromised enterprise endpoints

1. Trust

Oxford English Dictionary: **trust** (noun)

1. Firm belief in the reliability, truth, ability, or strength of someone or something.

   1.1. *Acceptance of the truth of a statement <u>without</u> evidence* or *investigation*.

Liability? Minimize trust: decrease *unjustified beliefs*

=> some ***metric(s) of beliefs*** must exist

minimum trust: minimization is *no longer possible or practical*

"minimum trust = 0:" *<u>all</u> beliefs are fully justified*; **zero liability left**

"minimum trust ≠ 0" => **Trust(worthiness) Establishment**

- *beliefs of trustworthiness are* created by *<u>some</u>* evidence
- *risk aversion* is decreased
- *betrayal aversion* decreased

Trust Establishment (TE) is *fundamental*; e.g., see behavioral economics

Security: **trust** (noun)

Unjustified belief in a *security property* of a system or network *component*

belief in a *security property of a system* <u>*without*</u> *any evidence*
e.g., *without* verification or monitoring

minimize trust: *decrease unjustified beliefs in security properties*
=> some ***metric(s) of beliefs*** *in security properties* must exist

minimum trust: minimization is *no longer possible or practical*

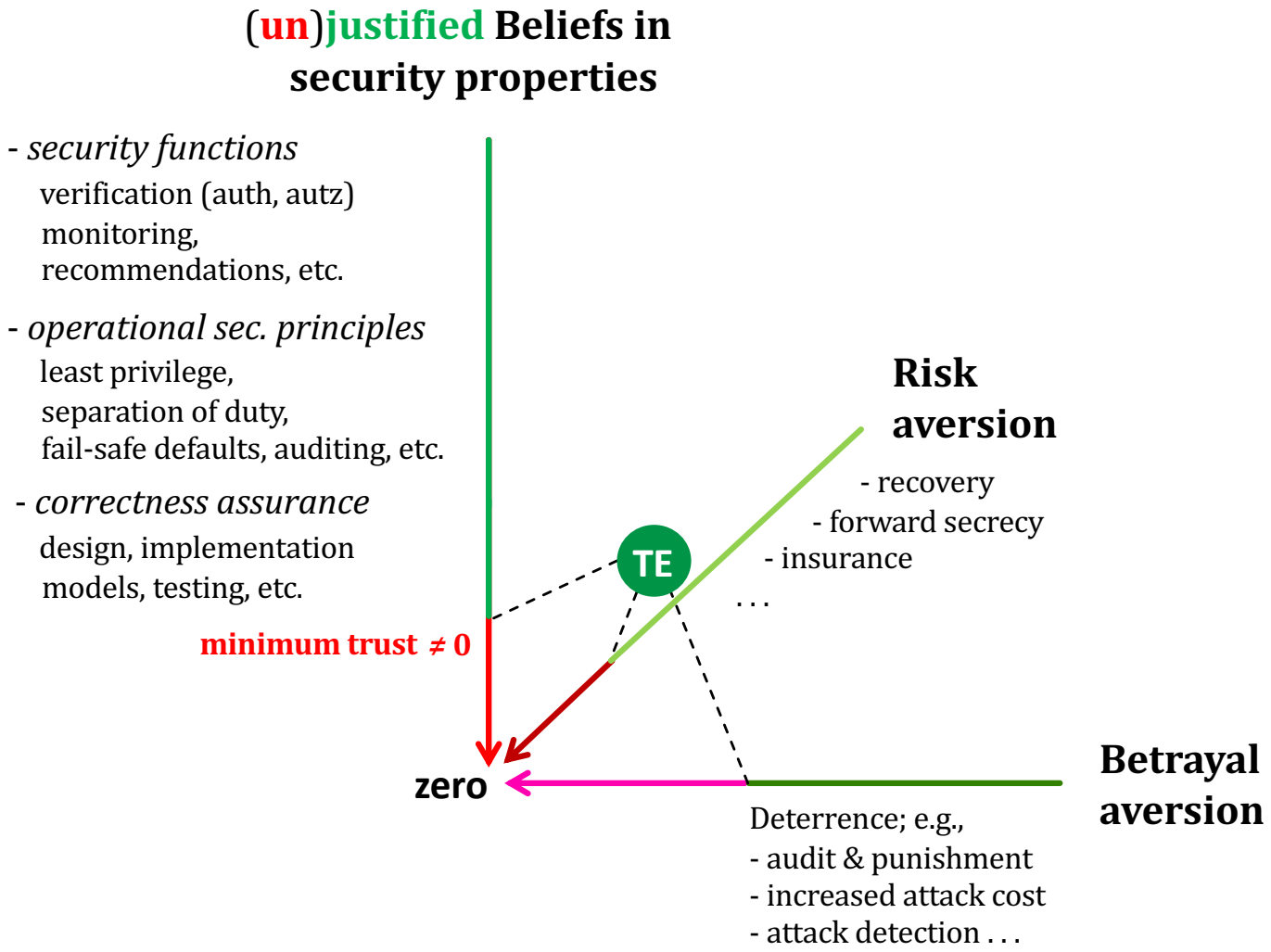
"***zero trust***:" <u>*all*</u> *beliefs in* <u>*all*</u> *sec. properties are fully justified*

"***non-zero trust***" **=> Trust(worthiness) Establishment**

- <u>*some*</u> *beliefs of trustworthiness are created* by <u>*some*</u> evidence
- *risk aversion* is decreased
- *betrayal aversion* decreased

Trust Establishment (TE) in security: how to do it?

TE in security



trust minimization => *add* security functions & op. sec. principles & correctness assurances

minimum trust => *all* security functions & ***all*** operational sec. *principles* & ***highest*** assurances

2. “zero trust” in NIST’s architecture

What is "zero trust" architecture ?

Motivation: eliminate reliance on single-perimeter protection

- *large* implicit trust zone allows an adversary's "lateral" movement

How to get it?

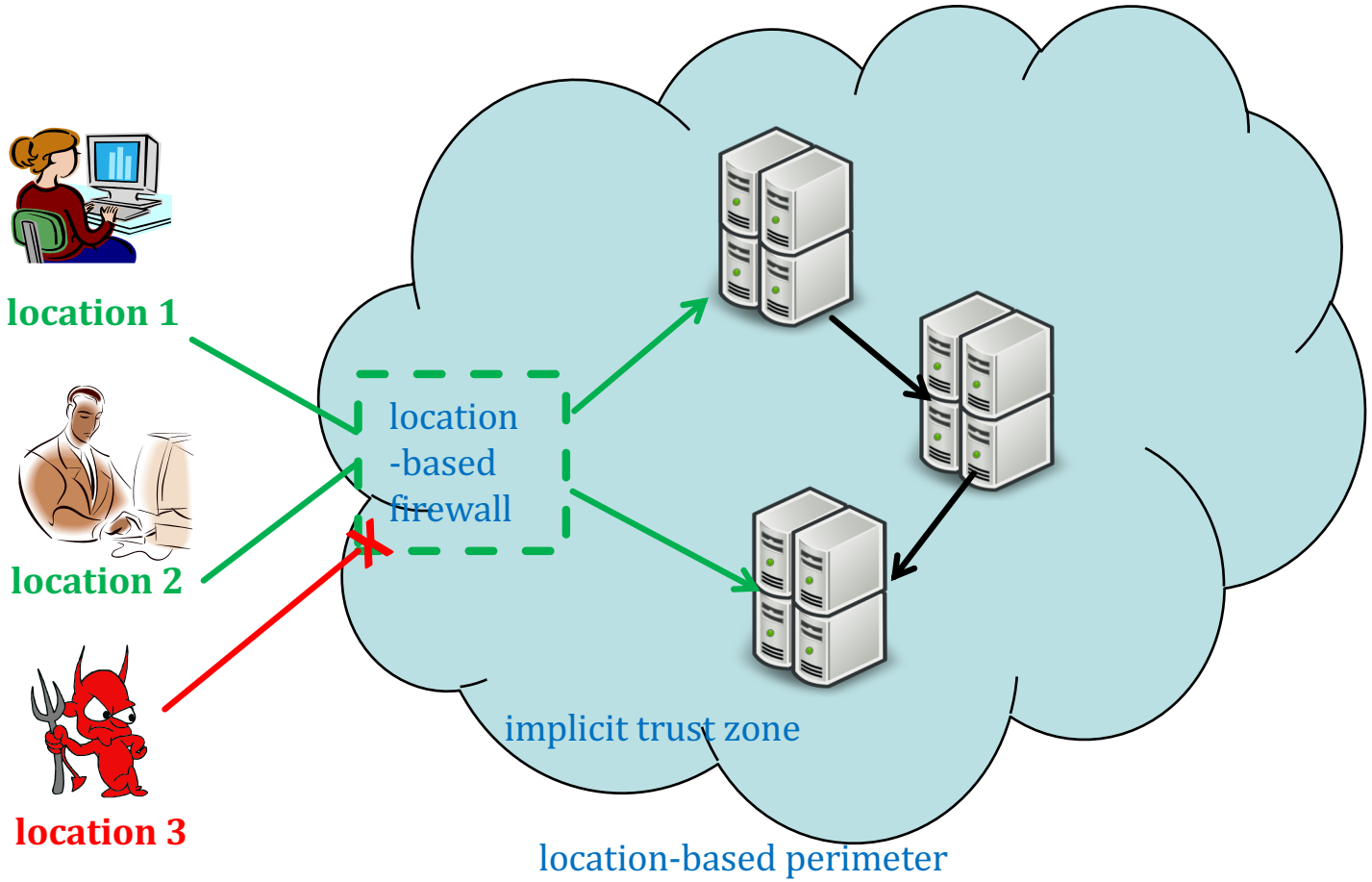
- *continuous verification* of subject's attributes (e.g., roles, permissions, access levels) & *monitoring* behavioral patterns in granting access.
  never-trust-always-verify

- *enforcement of operational security principles*,
  e.g., least privilege, separation of privileges/duties, fail-safe defaults, and auditing
  always *assume you've been hacked*

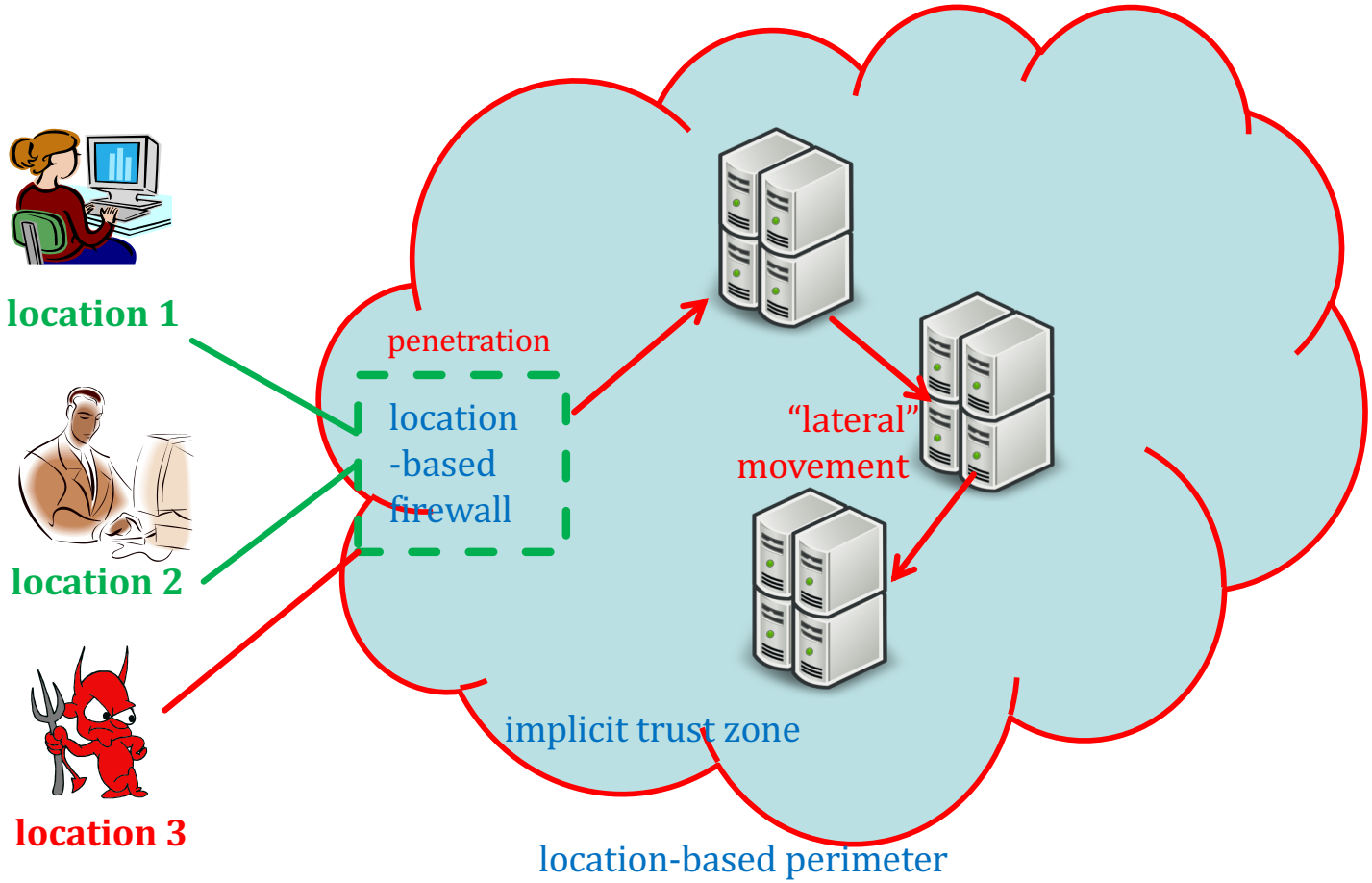
- *reduce/shrink implicit trust zones*
  minimum trust zone = single device

Goal: limit attack effects to *small* a implicit trust zone
=> deny adversaries' "lateral" movement *across trust zones*

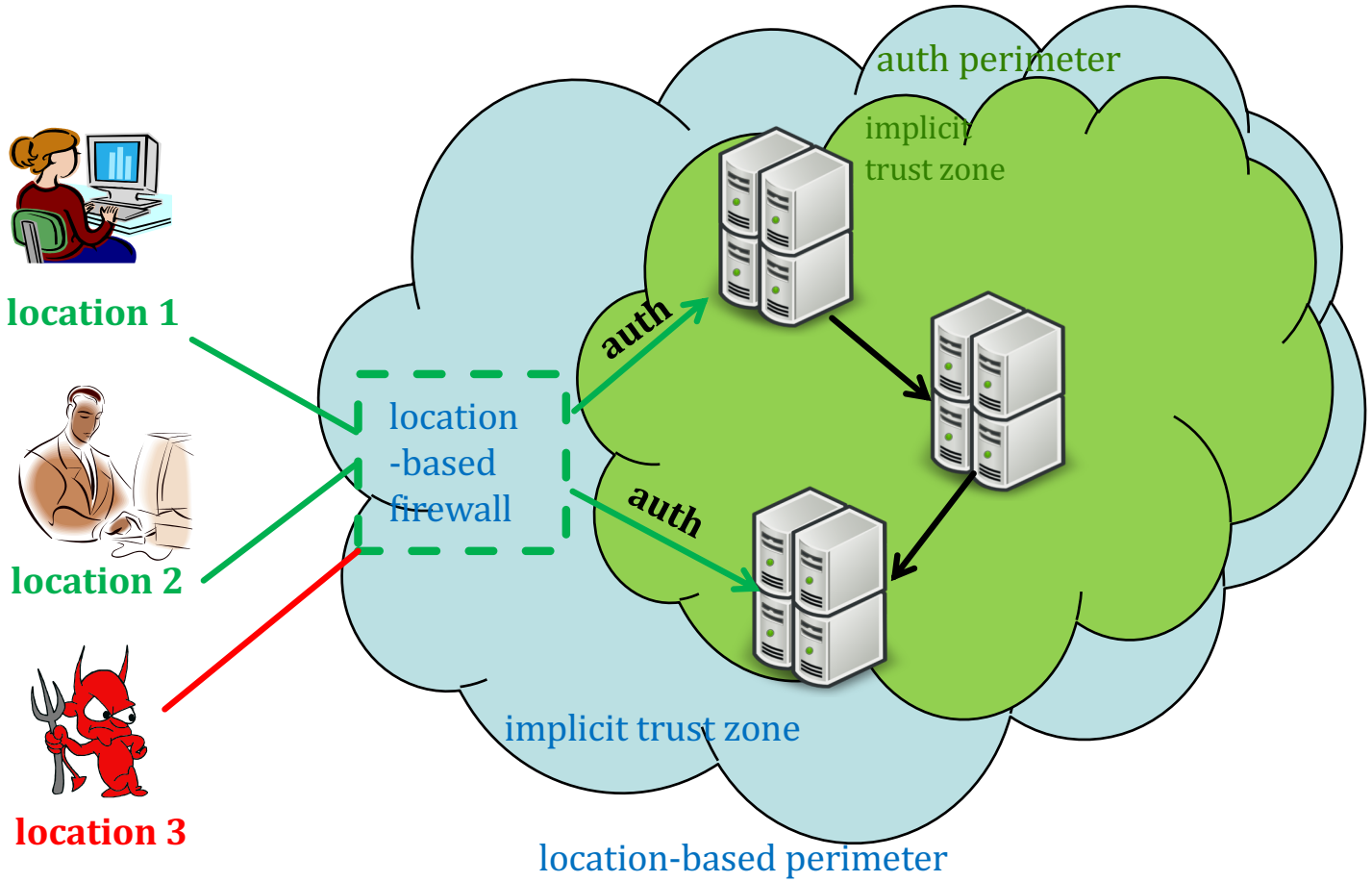
Enterprise network: fixed configuration (no red access)



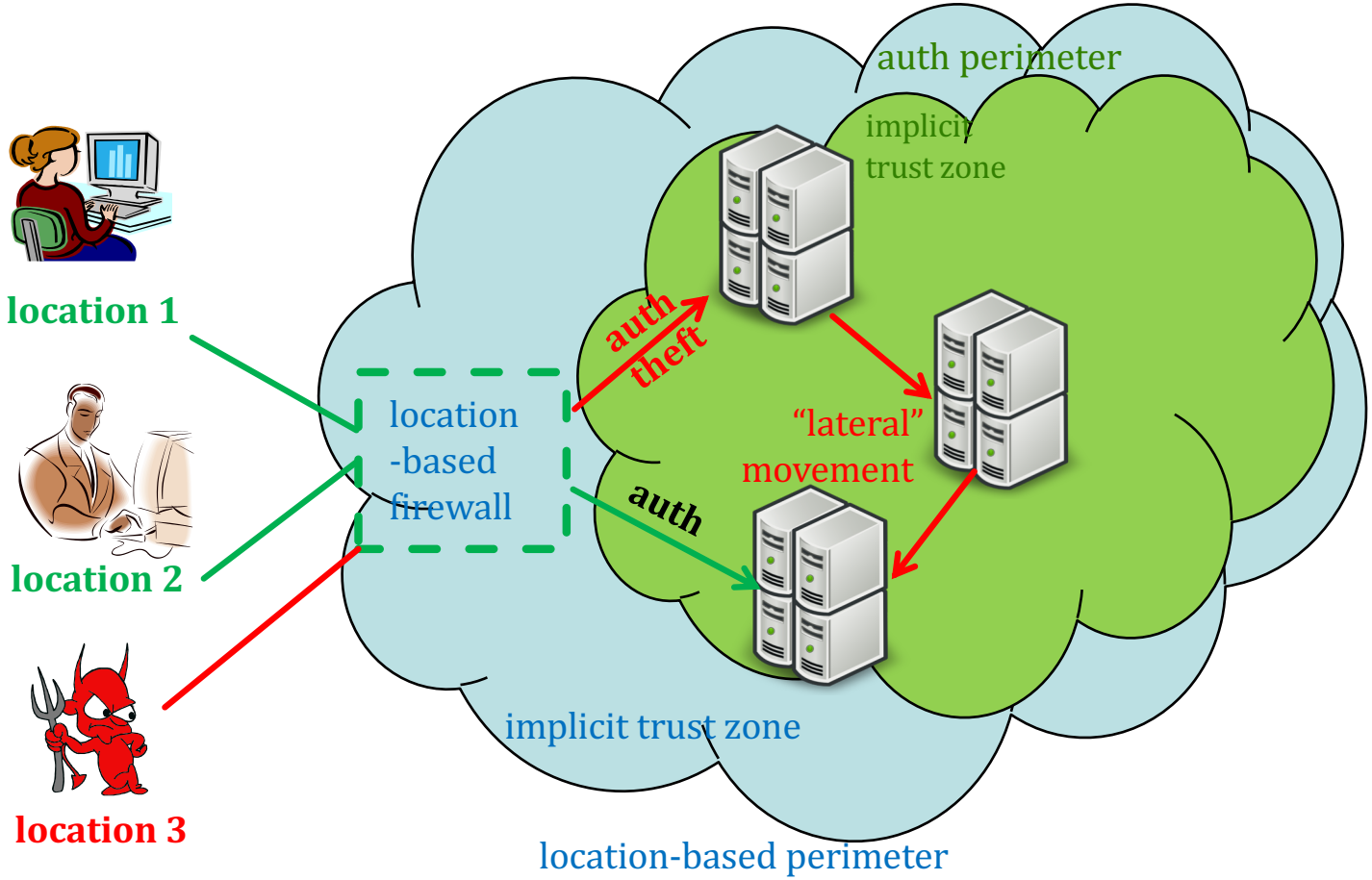
Enterprise network: fixed configuration (penetration + lateral moves)



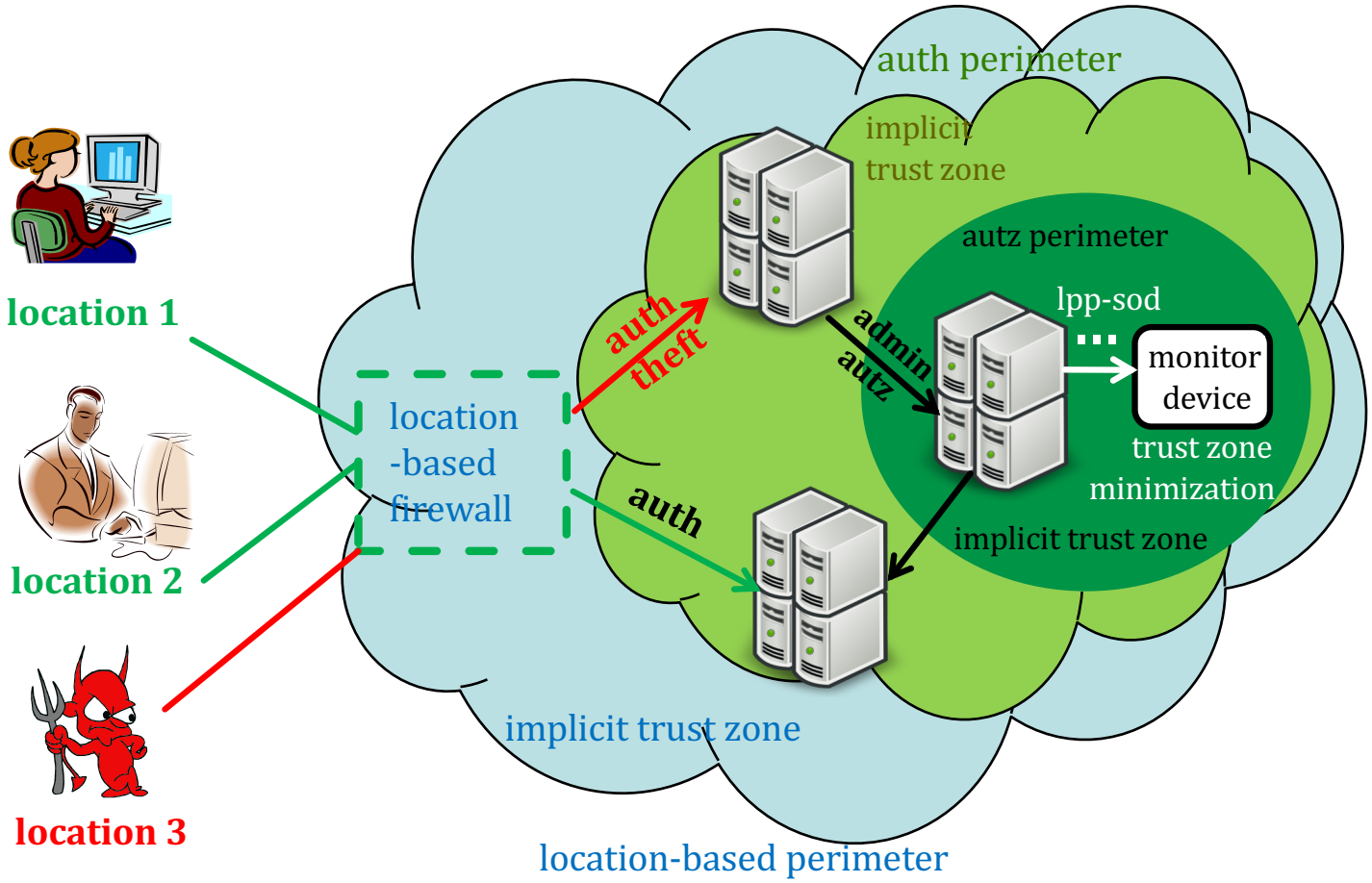
Enterprise network: fixed configuration (shrink implicit trust zone)



Enterprise network: fixed configuration (auth theft + lateral moves)



Enterprise network: fixed configuration (deny lateral moves)



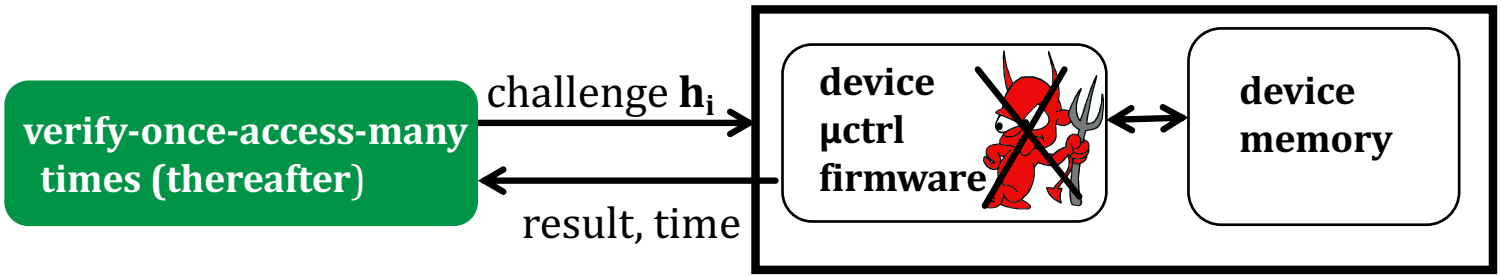
a) *verification* & *monitoring* + security principles => ***implicit trust zone minimization***
≠ trust minimization

b) *"**zero trust**"* (=> *highest assurance cost => highest opportunity cost*) ***is impractical***

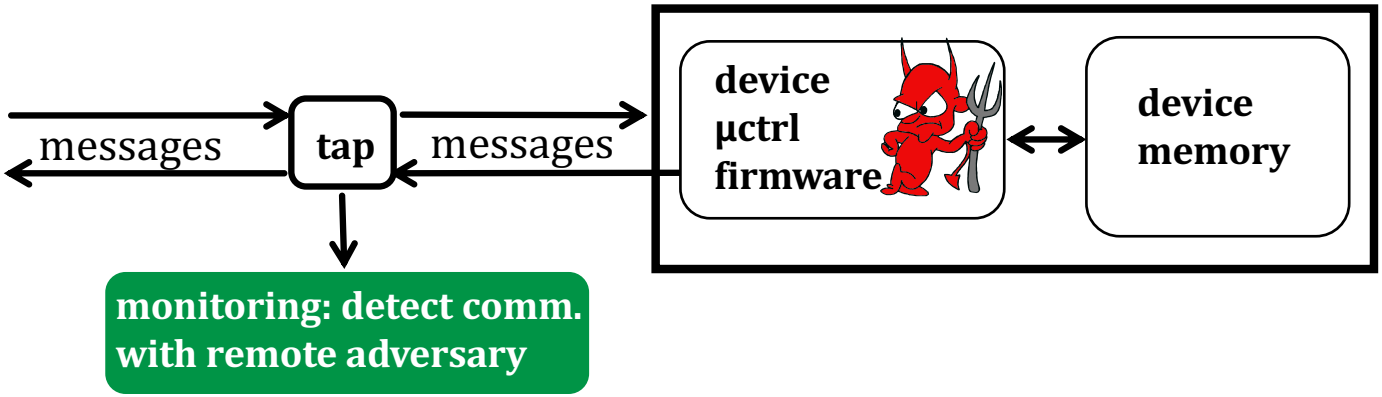
c) "zero trust" is ***impossible*** in access control

Ex.: ***min. trust zone*** = "**black box**" **device** ≙ access device memory **=>** execute code in **µctrl** firmware

security property: malware-free device *µ*ctrl firmware (*without opening* "black box")

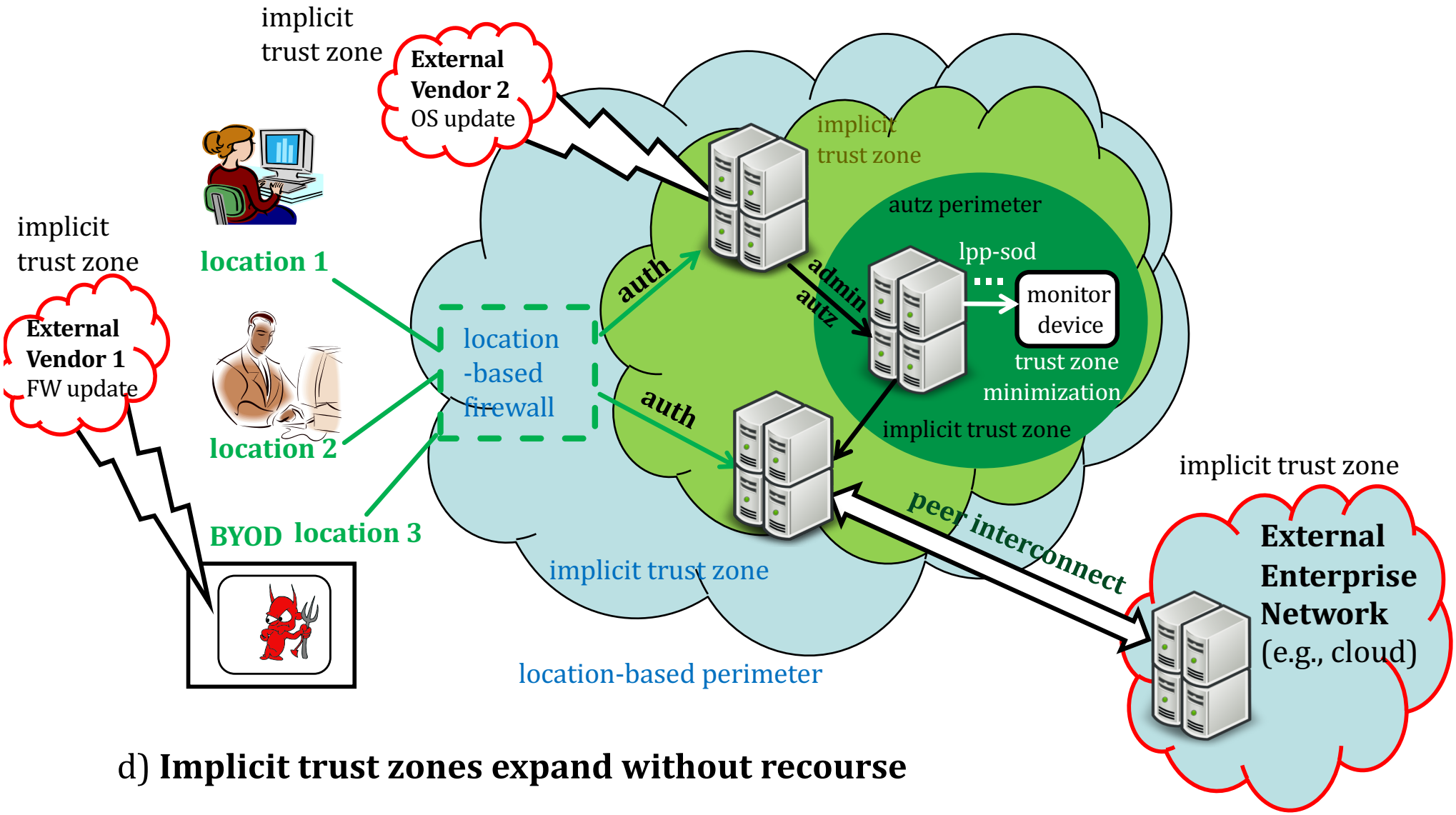


verify-once = Pr[*false negative* at i-th independent challenge h_i, i > 0] = $1/p^i \neq 0$



monitoring *fails whp*: communication is covert (e.g., stego, very rare), *if any*

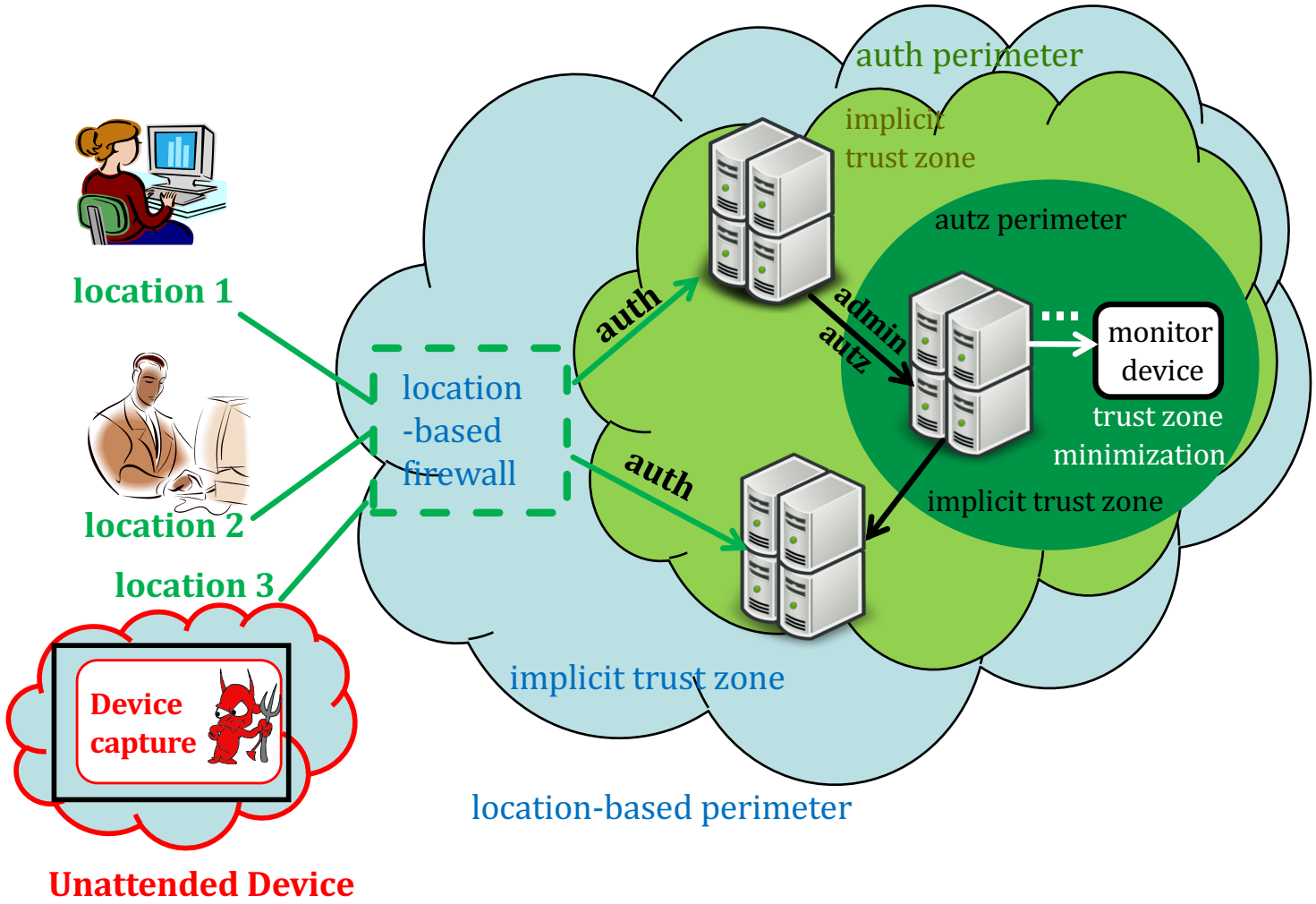
Enterprise network: variable configuration



d) **Implicit trust zones expand without recourse**

e) **Failure to require Trust Establishment**; e.g., b), c) and d)

Enterprise network: variable configuration



f) open-ended trust zones without recourse (*not* in NIST's architecture)

Summary: what is NIST missing?

a) **logic: *implicit-trust-zone minimization ≠ trust minimization***

b) **zero trust** (=> *highest assurance cost => highest opportunity cost)* **is *impractical*** (***forever***)

c) **zero trust is *impossible* in access control** (but possible outside access control)

d) **allows trust zones to expand *without recourse***

e) **fails to require Trust Establishment;** e.g., b), c) and d)

f) *open-ended* trust zones without recourse (*not* in NIST's architecture)

"Zero trust" is a "buzzword"

David Parnas (IFIP 1974) defined a "buzzword;" i.e., hierarchical structure

"Buzzwords" *lack clear definitions* and their users:

- assign different meanings to them in different systems;

ex.: enterprise networks with *fixed*, *variable*, and *unattended-device* configurations

- do not explain them (e.g., their consequences) to others;

ex.: failure of logic; impractical/impossible of zero trust; trust expansion w/o recourse; no concept of *trust establishment*

- are unable to rule out inadequate alternatives;

ex. *device integrity breaches*:

APT 28 (Fancy Bear's *LoJax)*, APT 29 (Cozy Bear's *Covid-19 espionage*),
APT 41 (Double Dragon *large-scale espionage*, recent *MoonBounce*)

ex. *supply chain attacks*: Flame ('12), ShadowHammer ('19), ethical hack ('21)

ex. *no E2E security*: BYOD integrity, cloud-based "black-box" scanning, "ultimate insult"

- adopt imprecise terminology.

ex. conflates *trust-zone* with *trust* minimization; cannot relate to *trust establishment*

3. The Good, the Bad, and the Ugly . . .

3. The Good

a) A call to arms . . .

Examples:

- improved user authentication (e.g., MFA)
- removed single VPN perimeters to an enterprise
  -> tailored remote endpoint access (e.g., VDI) to corporate resources
- micro-segmentation of network resources for *least privileged* access
- increased use of hybrid-cloud based security

b) Increased Industry awareness . . .

- 83% security & risk professionals: ”zero trust” is essential to their organizations
- new ”zero trust” initiatives: $1.6 B by 2025; market share: $50 B by 2026

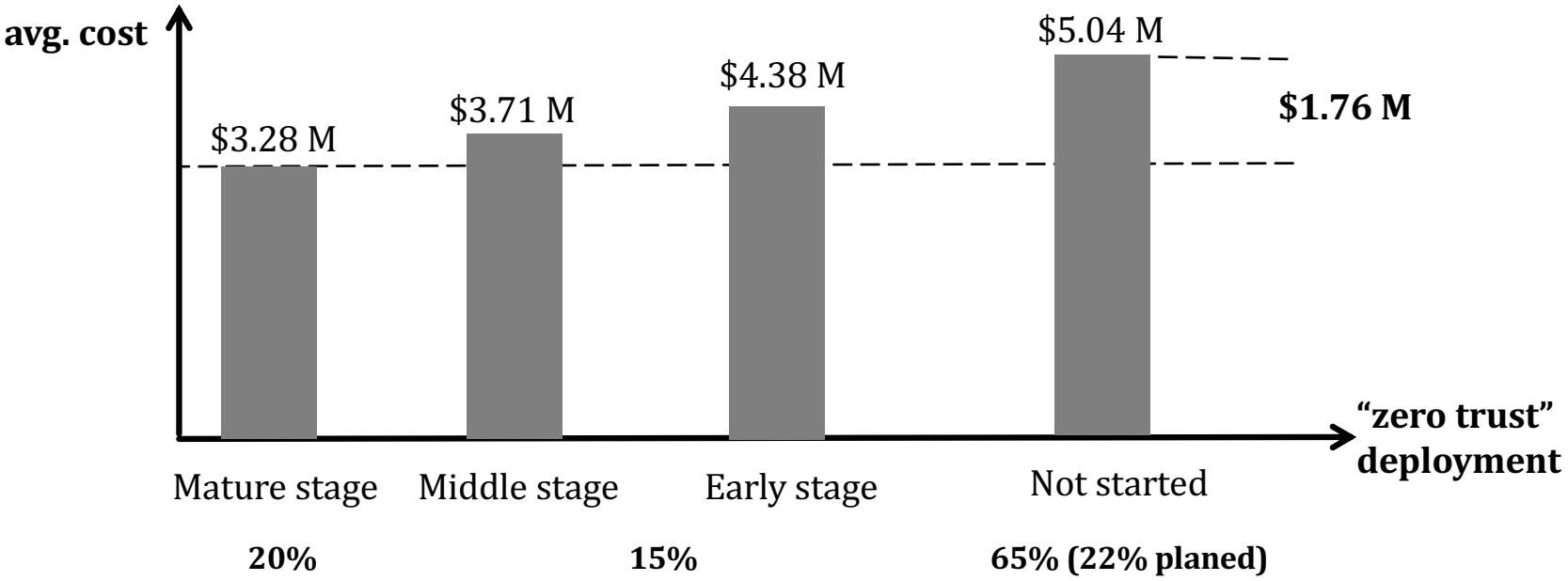
c) Increased US Government awareness and mandates. . .

- *NIST Special Publication*, 800-207, DoD Reference Architecture, NSA public embrace
- 2021 *Presidential Executive Order*, US *Office of Management & Budget* 2022 Memo

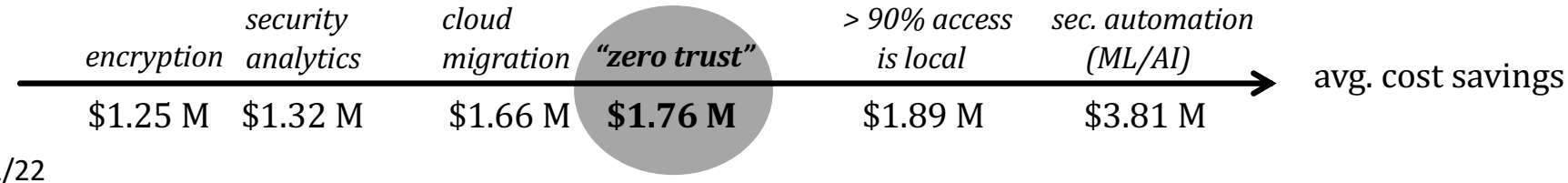
3. The Good

d) How good?

Evidence: IBM Security (via Ponemon Institute) survey (5/2020 – 3/2021):
- 537 security *breaches*, 17 countries & regions, 17 industries



- average-cost savings of "zero trust" versus other security measures



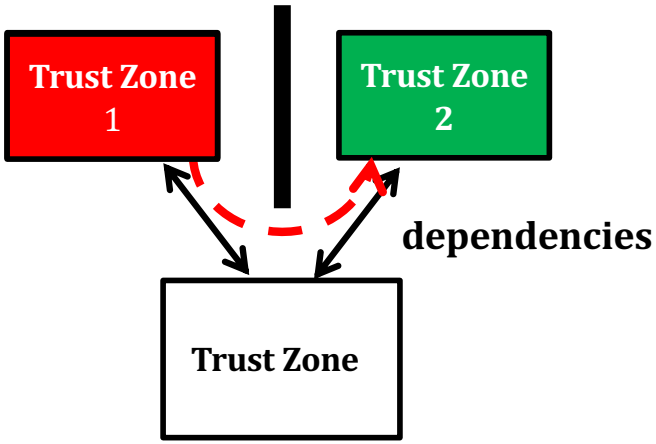
3. The Bad

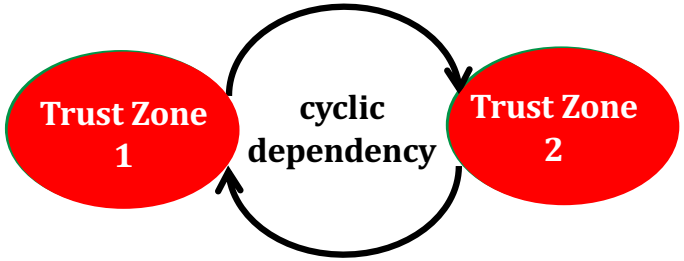
a) "zero trust" *is* ***unsound***: trust zone minimization does *not* minimize cross-zone attacks**

e.g., quadratic cross-zone ***attack growth*** is possible

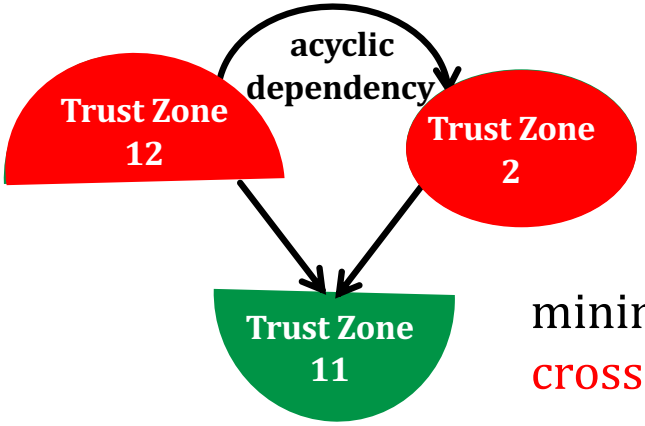
Why?

No dependencies are defined among trust zones





cross-zone attacks

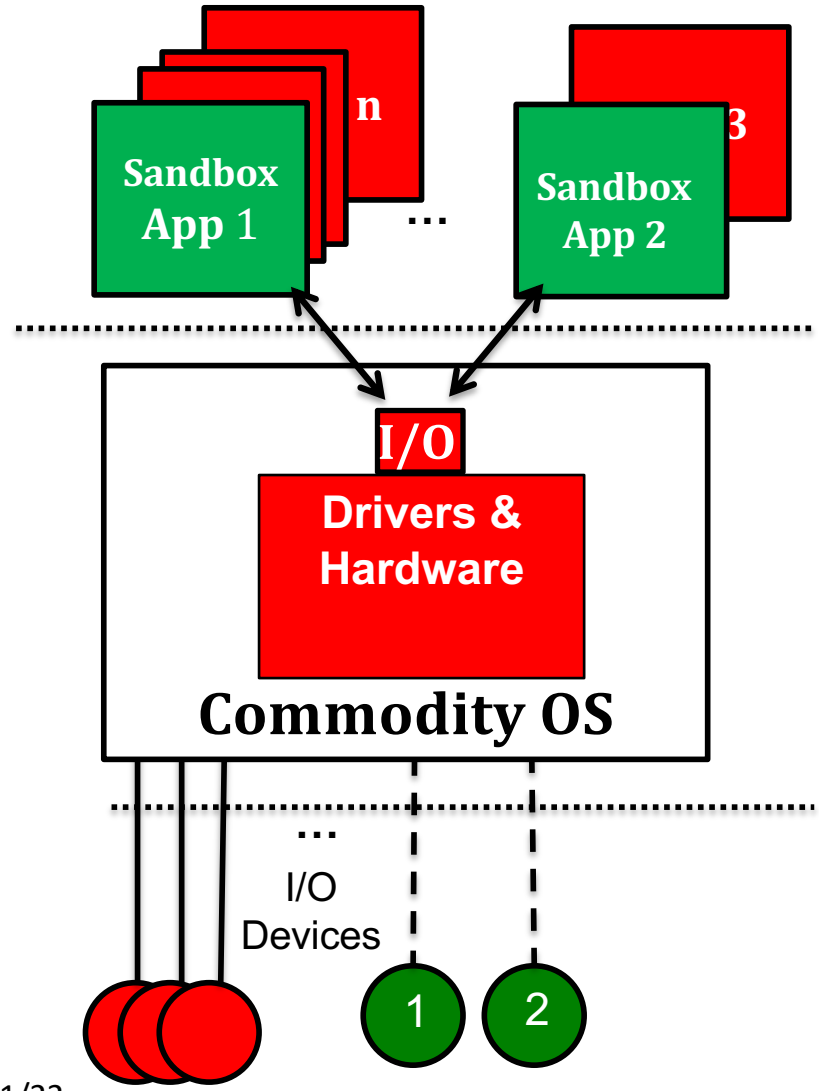


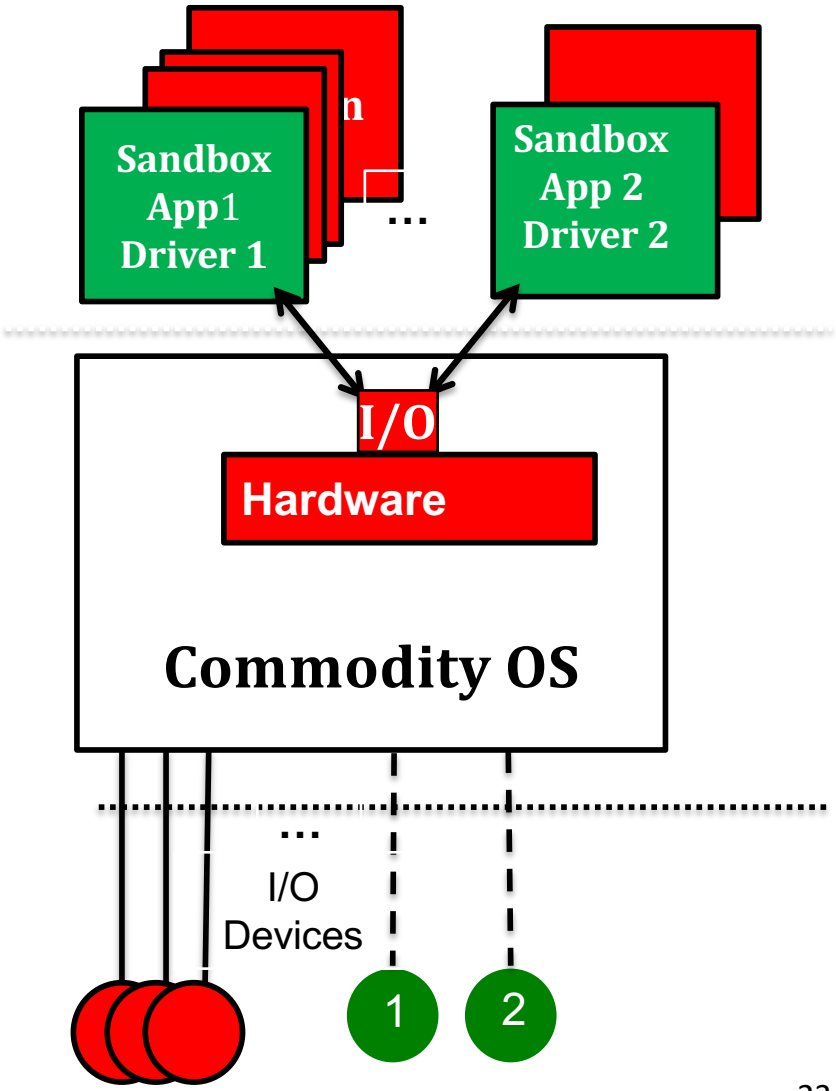
minimized cross-zone attacks

"sandwiching"

3. The Bad

I/O dependency

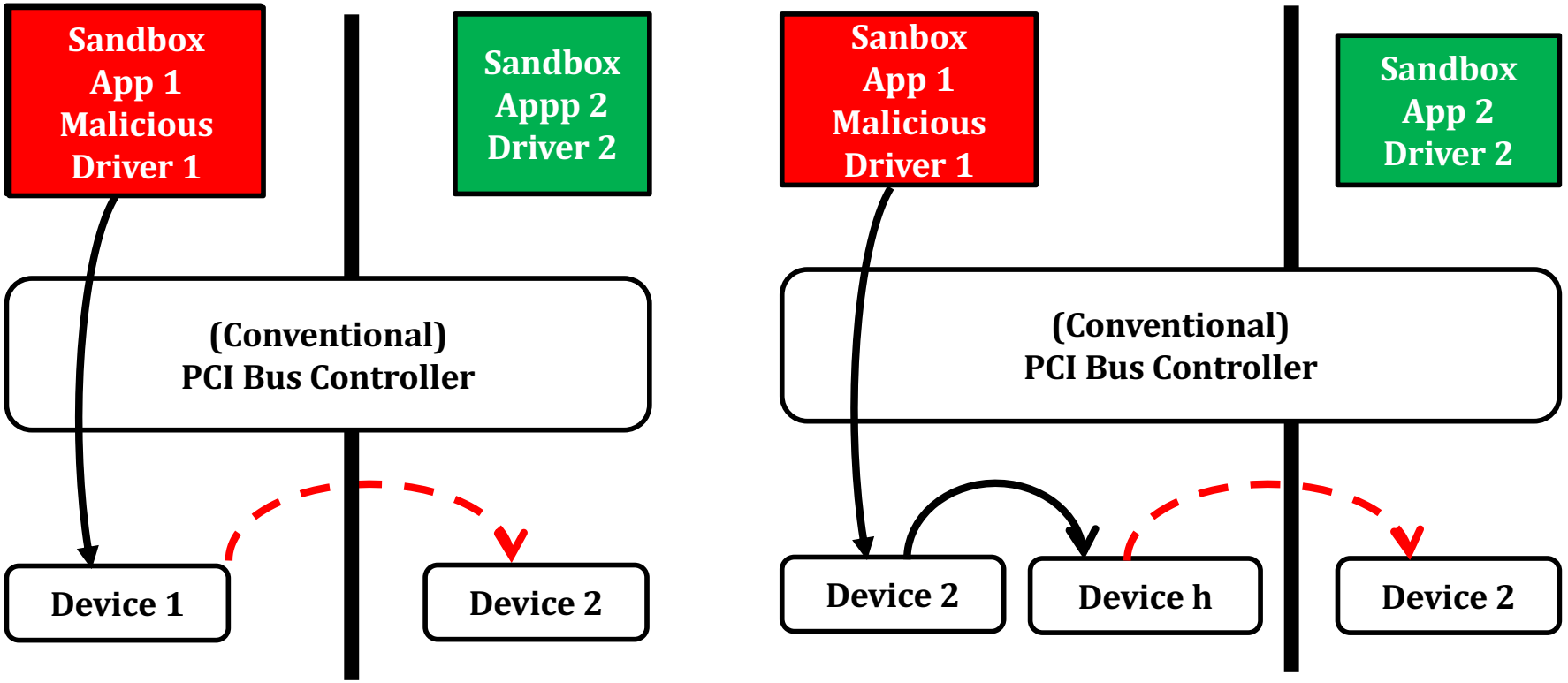




3. The Bad

Hardware dependency

no hardware authorization



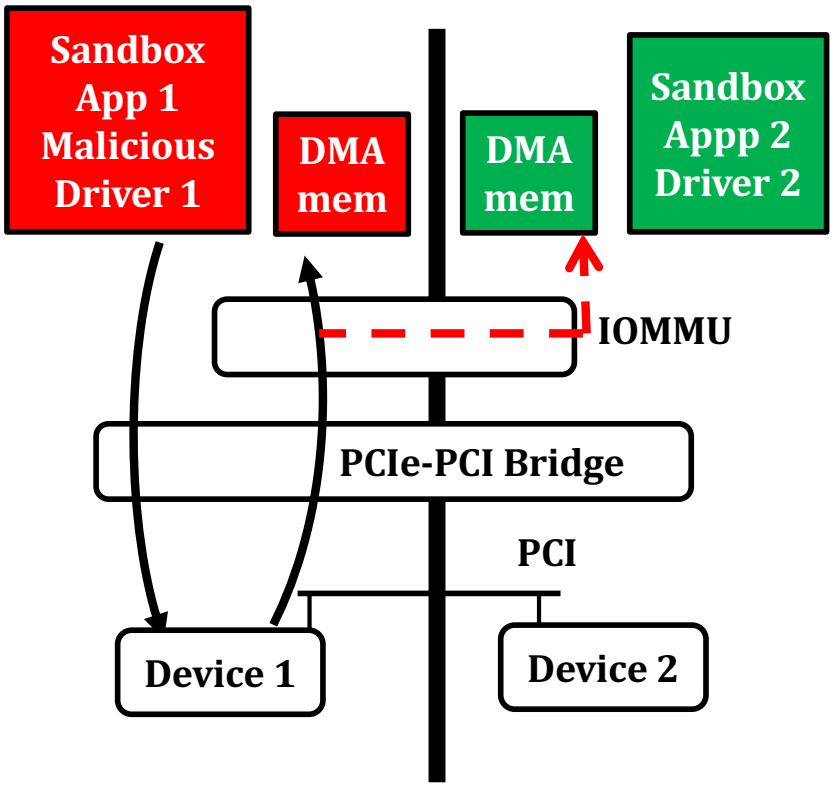
(a) *Unauthorized direct* transfers

(b) *Unauthorized indirect* transfers

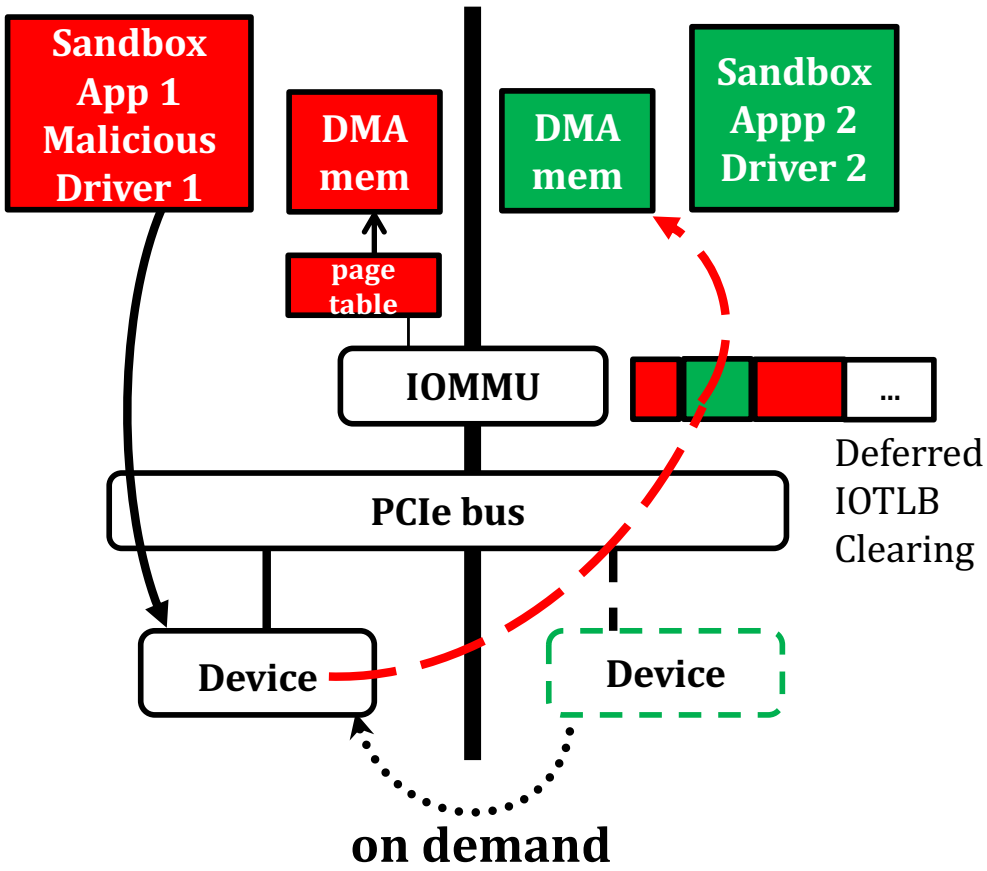
3. The Bad

Hardware dependency

Non-selective hardware



Selective-hardware failure



3. The Bad

b) "zero trust" *is* *inadequate*: it lacks basic security tenets and sound definitions

Why?

i) It **rejects "*verify-once-access-many times*"** approach to "black-box" components ***and*** **fails to define** security property **monitoring** in finite time

e.g., "*black-box*" OS/security/micro/separation *kernels*, (micro)hypervisors, devices

ii) **It *fails* to define *trust minimization***

e.g., *all* security *functions* and *operational security principles* are *insufficient*

iii) **It fails to recognize the need for *trust establishment***

e.g., risk reduction and *deterrence reduce cost and incidence* of security breaches

3. The Ugly

1. "zero trust" masquerades as an **"enterprise security model" –** yet **it *can never be one***

- unsound and inadequate

- no concept of behavioral economics, industrial organizations, law, psychology

2. "zero trust" can *never* satisfy requirements of Pres. Executive Order & OMB Memo

- "auditing of *trust relationships"* -- yet implicit trust-zone dependencies are undefined;

- *"isolate computing environments"* -- yet isolation cannot be guaranteed; e.g., I/O isolation

- "*a complete understanding of devices' operation and their security posture when granting access"*
  -- yet devices' malware freedom cannot be established.
- requirements for *trust establishment*
  - "security and integrity of software that performs functions critical to trust,"
  - "trusted source code supply chains," and
  - "ensure and attest to the integrity and provenance of open-source software",

  -- yet it mandates "*zero trust*."

3. "buzzword" -> *slogan*: millions of Google references to "zero trust"

4. Q & A -- Discussion