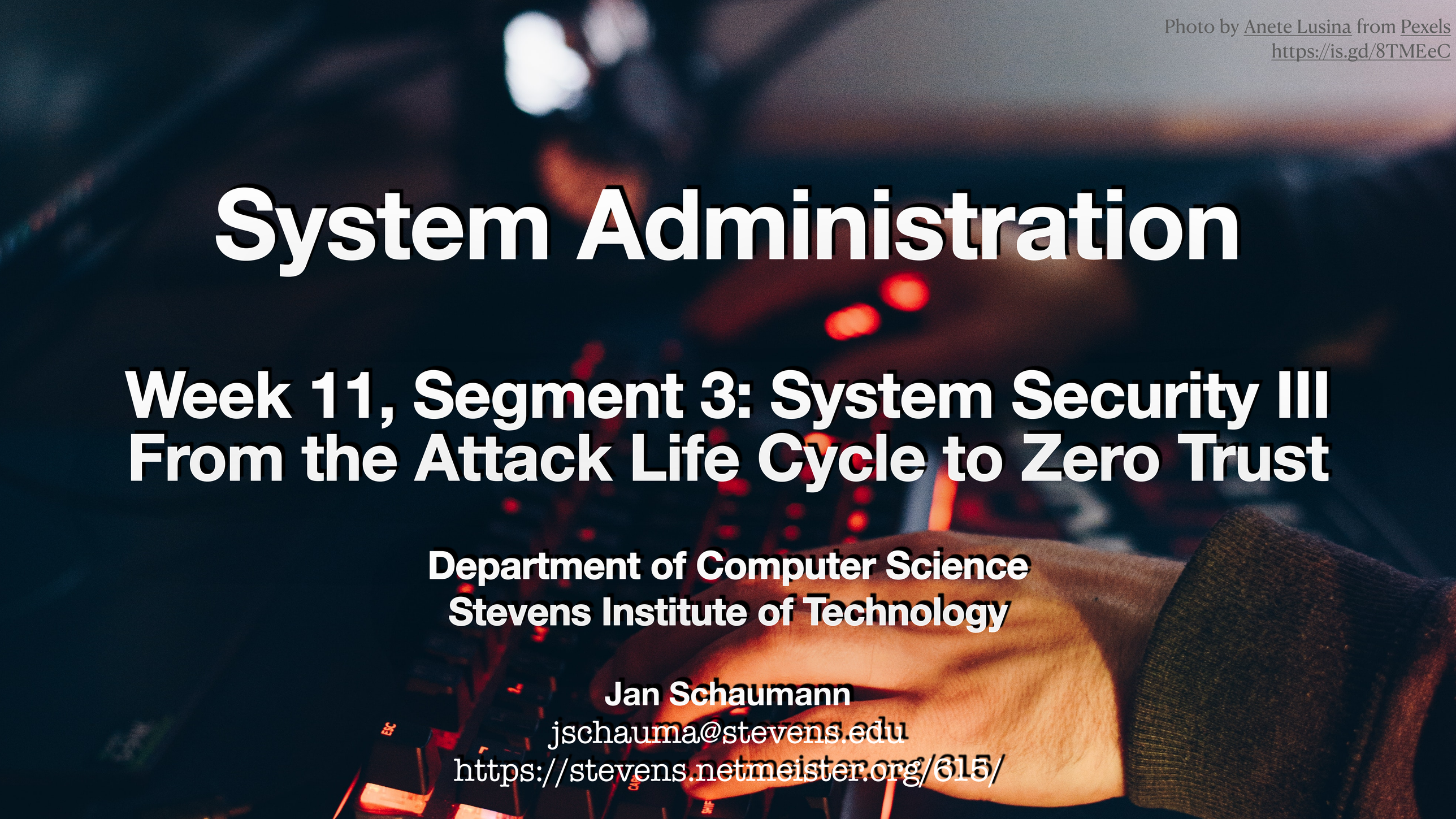


System Administration

Week 11, Segment 3: System Security III
From the Attack Life Cycle to Zero Trust

Department of Computer Science
Stevens Institute of Technology

Jan Schaumann
jschauma@stevens.edu
https://stevens.netmeister.org/615/

Defense in Depth

Security is like an onion:
the more layers you peel away, the more it stinks.

Never assume any one protection mechanism is sufficient.

Always assume the other protections you deployed
can be circumvented or broken.

The Attack Life Cycle

Initial Recon

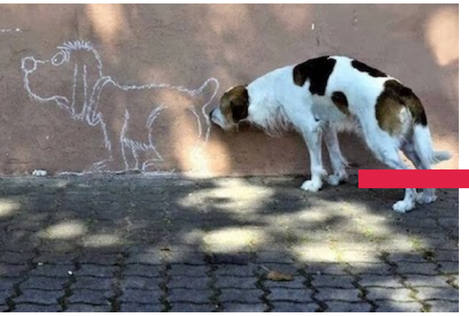
The Attack Life Cycle

Initial Compromise

Initial Recon

The Attack Life Cycle

Establish Foothold

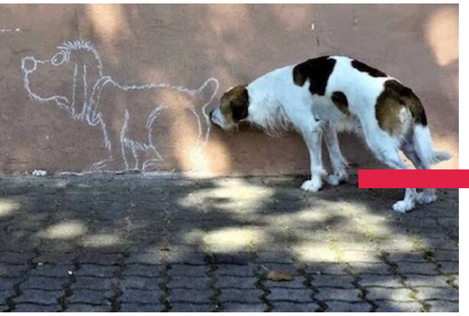


Initial Recon

Initial Compromise

The Attack Life Cyc

Escalate Privileges



Initial Recon

Initial Compromise

Establish Foothold

The Attack Life Cycle

Initial Recon

Initial Compromise

Internal Recon

Establish Foothold

Escalate Privileges

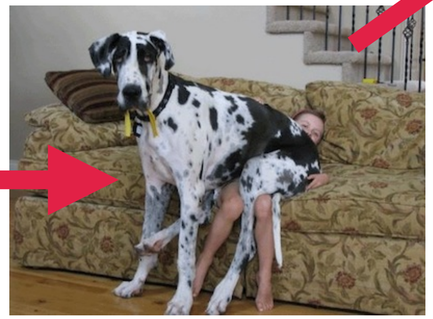
Lateral Move

Internal Recon

Initial Recon

Initial Compromise

Establish Foothold



Escalate Privileges

Maintain Presence

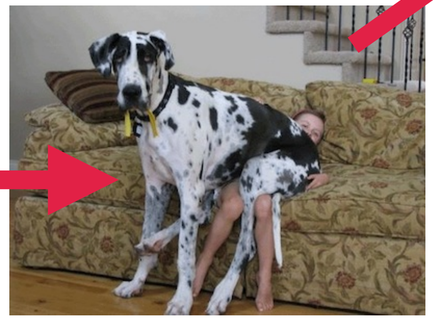
Lateral Move

Internal Recon

Initial Recon

Initial Compromise

Establish Foothold

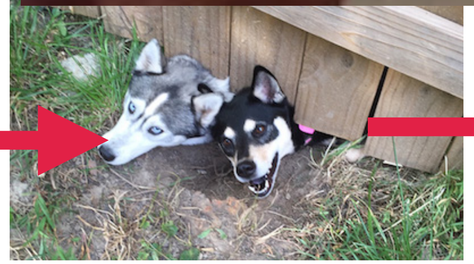


Escalate Privileges

The Attack Li

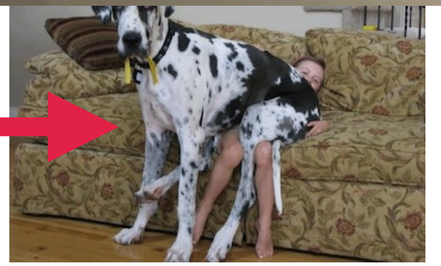
Complete Mission

Initial Recon



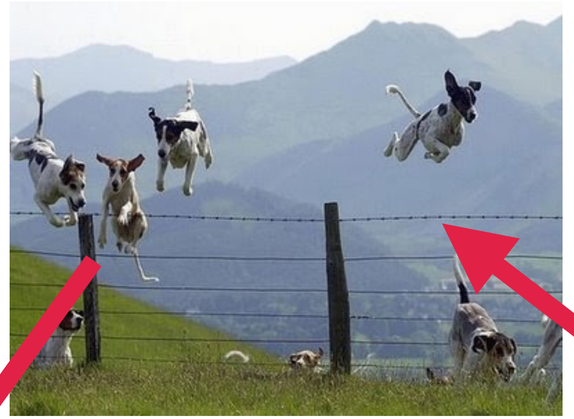
Initial Compromise

Establish Foothold



Escalate Privileges

The Attack Life Cycle



Lateral Move

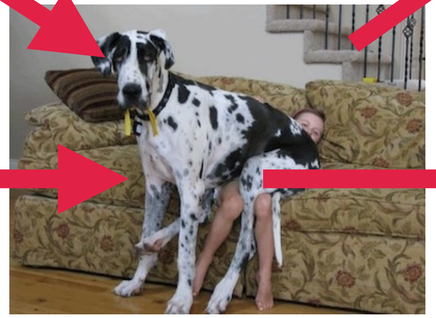
Maintain Presence

Internal Recon

Initial Recon

Initial Compromise

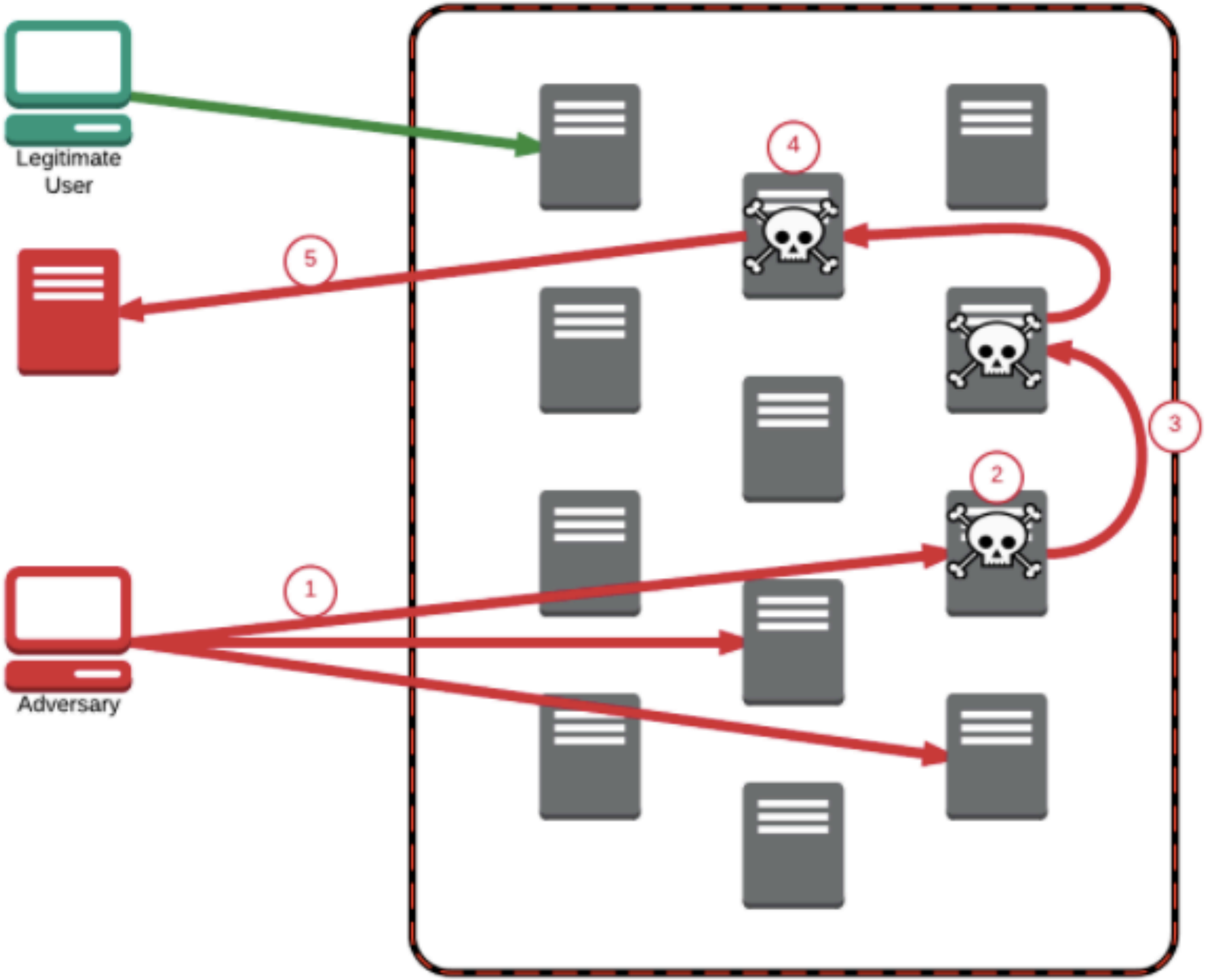
Establish Foothold



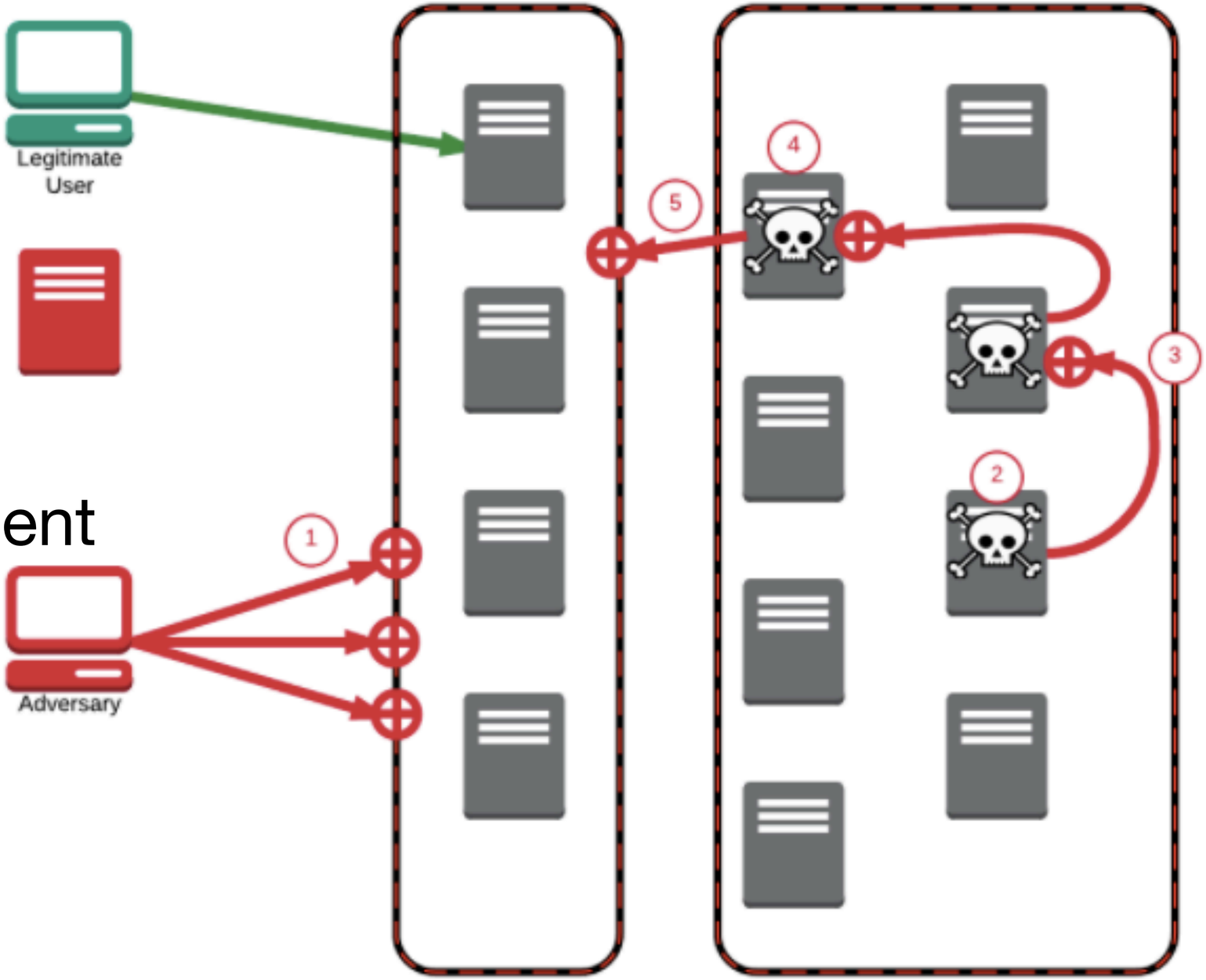
Escalate Privileges

Complete Mission

1. Initial Recon
2. Initial Compromise
3. Lateral Movement
4. Complete Mission
5. Exfiltration



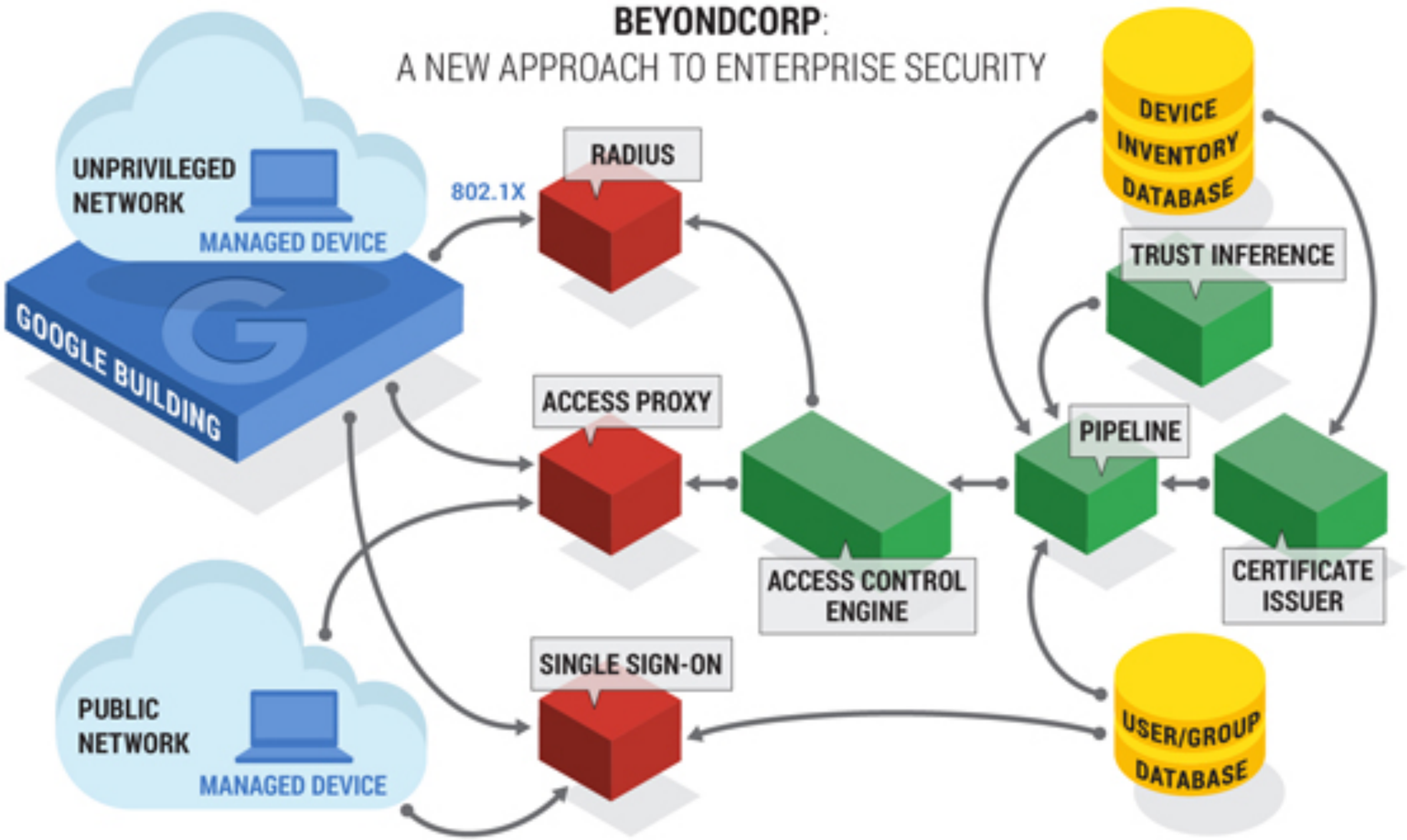
1. Reduced Attack-Surface
2. Hardened Systems
3. Limit Lateral Movement
4. Protected Access
5. Restrict Egress



Zero Trust

https://unsplash.com/photos/reWrNwCzIUU
Photo by Lisa McIntyre on Unsplash

Zero Trust

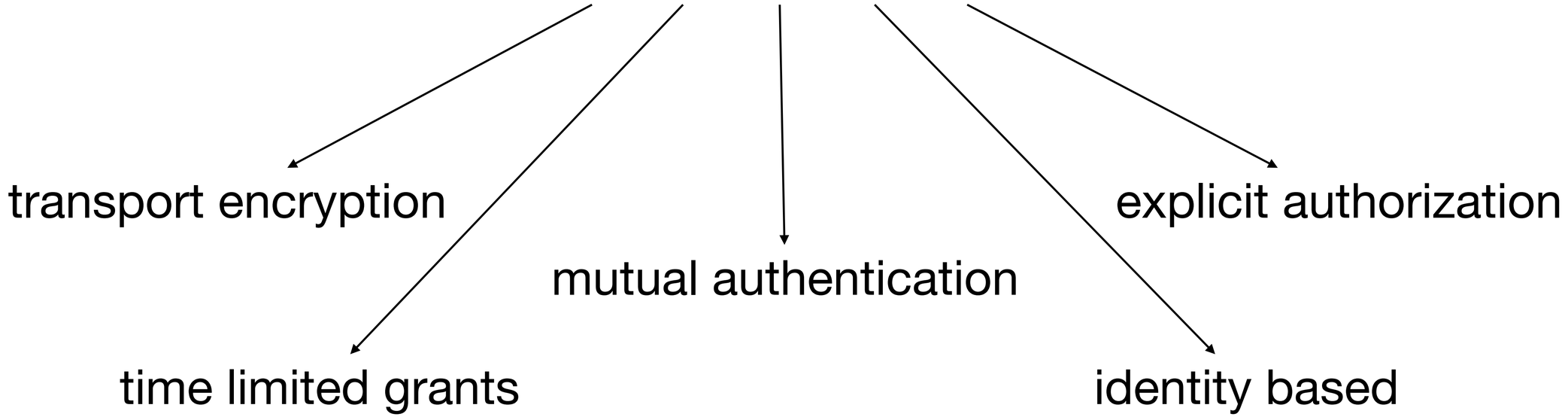


https://www.beyondcorp.com/

Zero Trust

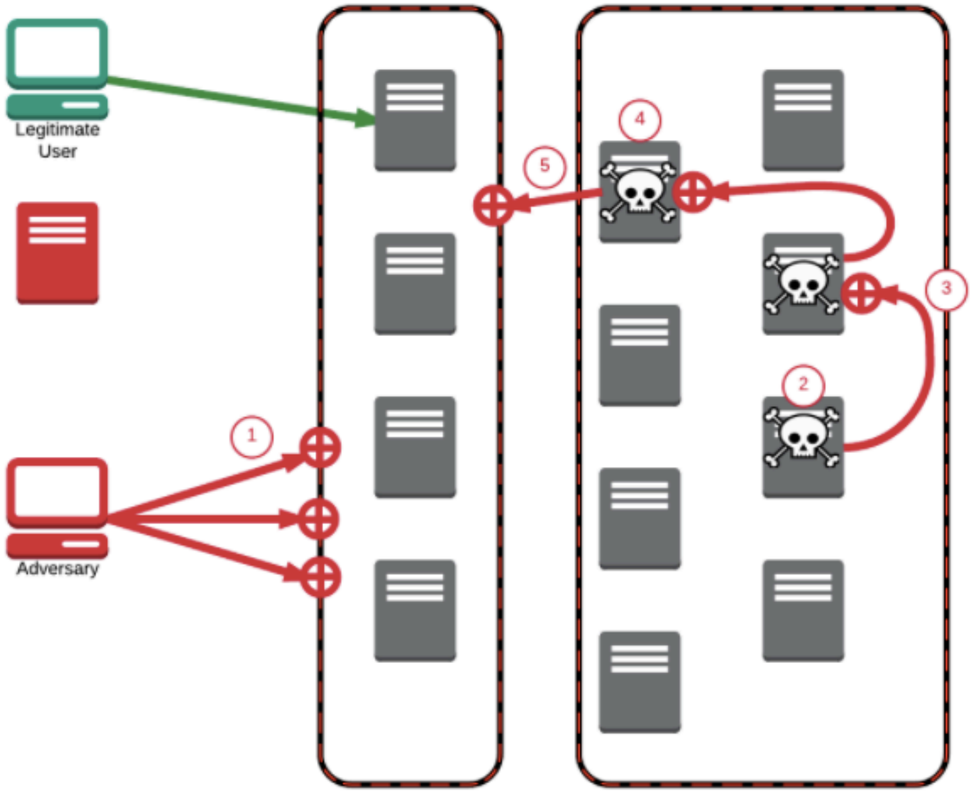
Zero Trust

Core concept: the simple assumption of a *compromised* or *hostile* environment.



Zero Trust

- not a product, but a *model:* **no inherent or assumed trust**
- assume all networks are hostile
- encrypt all traffic in transit
- users and clients are mutually authenticated
- actions are explicitly authorized
- authorizations are tightly scoped
- privileges are identity based and time limited



Reading Assignment:
“Reflections on Trusting Trust”

Links

- https://www.fireeye.com/blog/executive-perspective/2014/04/zero-day-attacks-are-not-the-same-as-zero-day-vulnerabilities.html
- https://www.netmeister.org/blog/attack-life-cycle.html
- https://www.beyondcorp.com/
- https://twitter.com/jschauma/status/1324462203215499266
- https://dl.acm.org/doi/10.1145/358198.358210