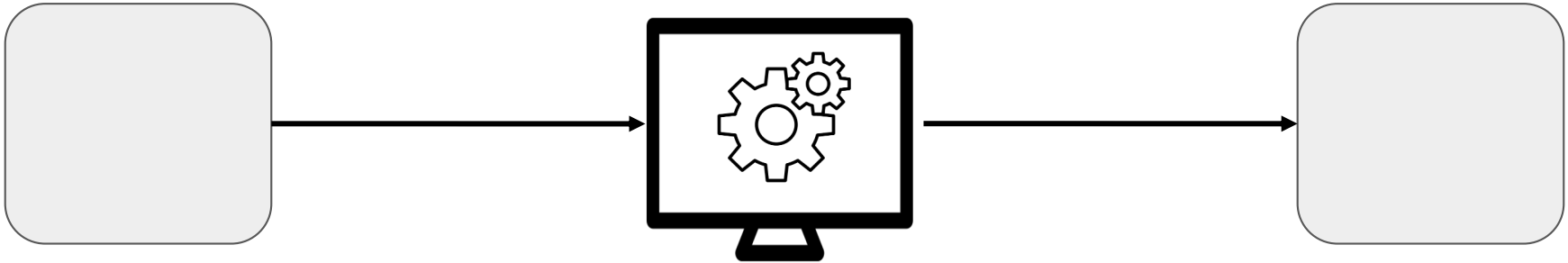
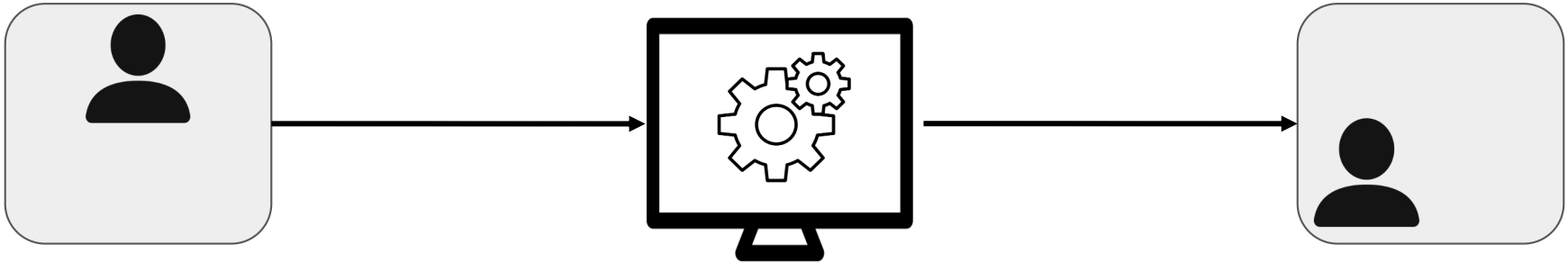
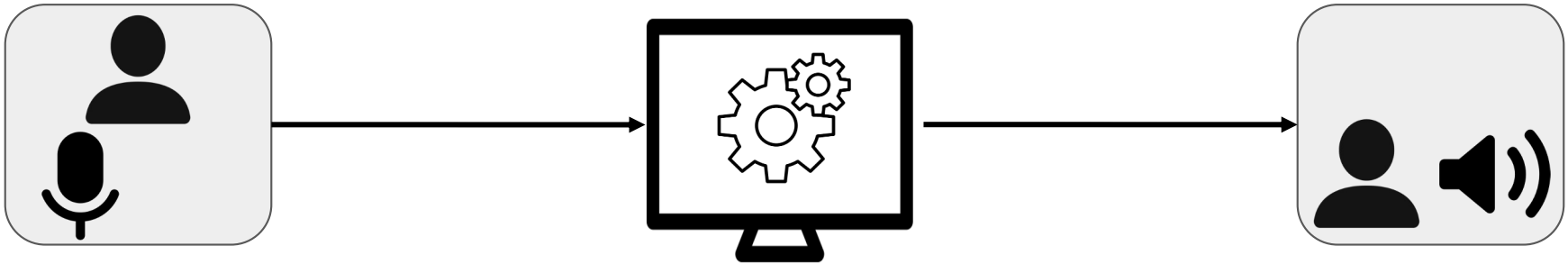
Information Flow–Based Vulnerability Modeling

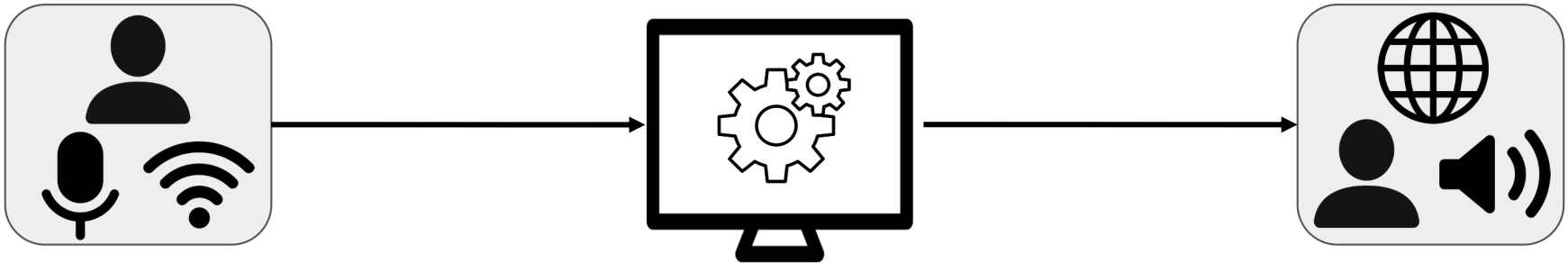
Brian Johannesmeyer

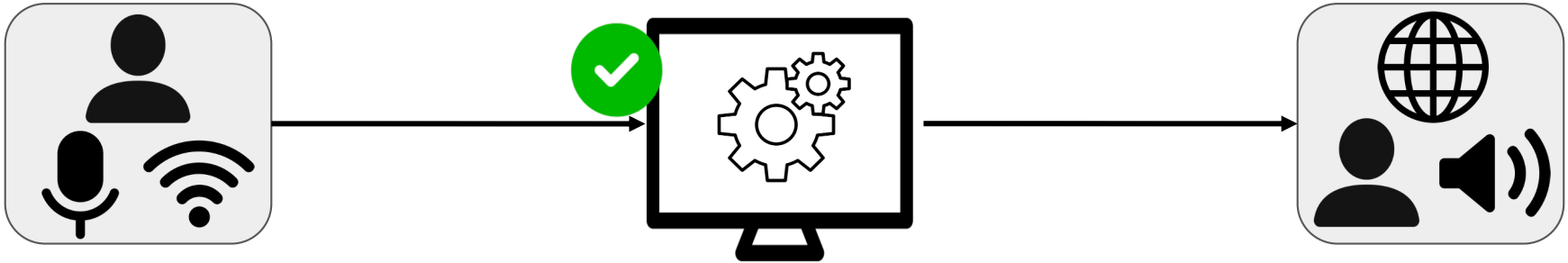
VU VRIJE UNIVERSITEIT AMSTERDAM

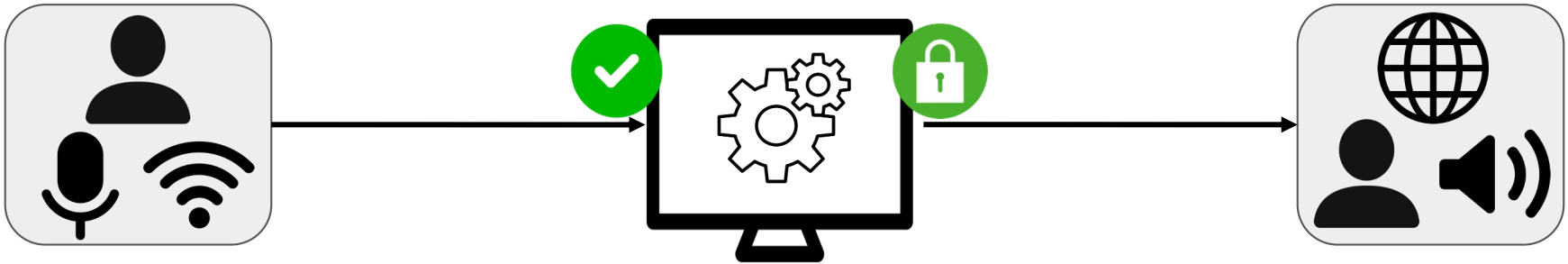


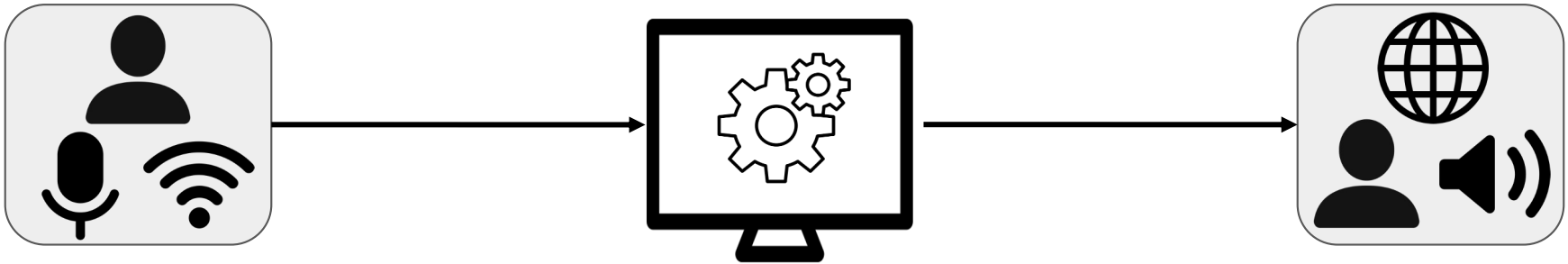


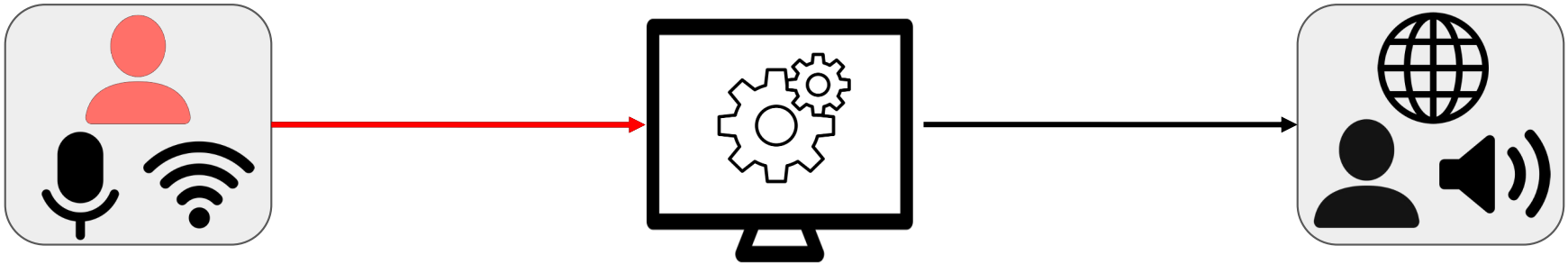


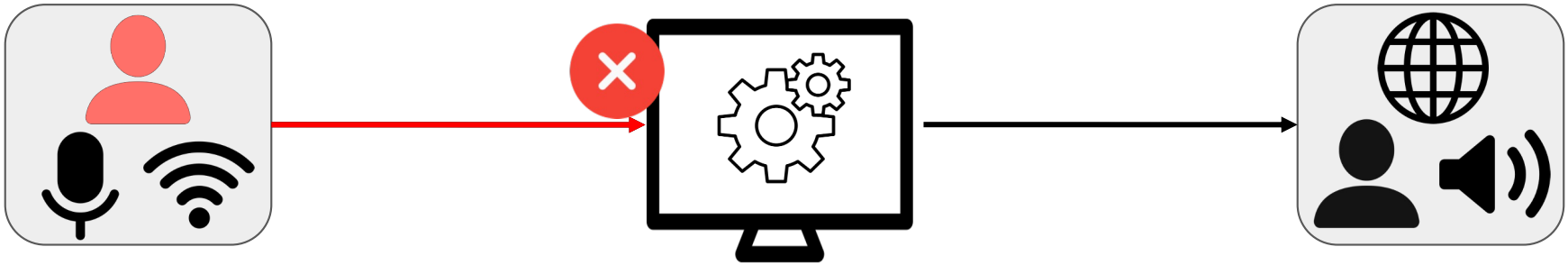


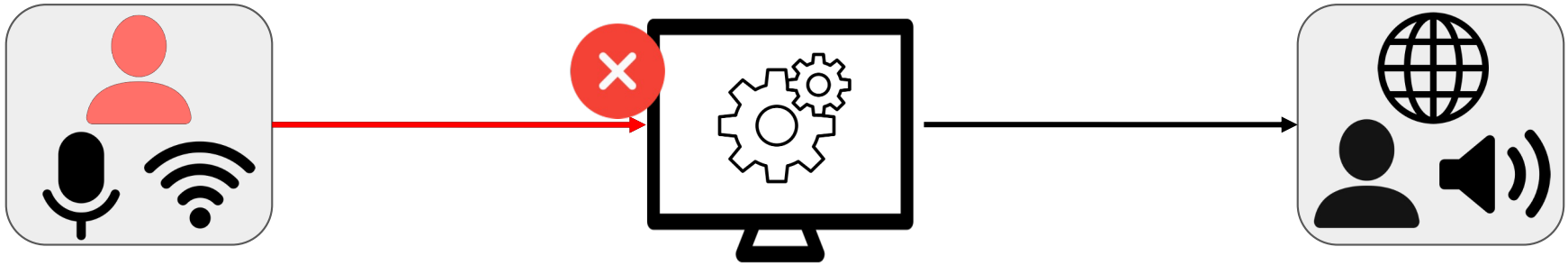










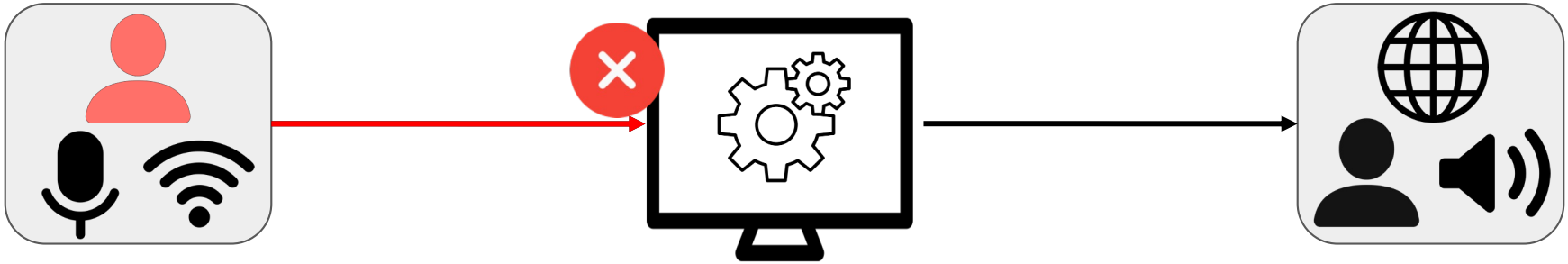


KIM ZETTER SECURITY NOV 3. 2014 6:30 AM

An Unprecedented Look at Stuxnet, the World's First Digital Weapon

In an excerpt from her new book, "Countdown to Zero Day," WIRED's Kim Zetter describes the dark path the world's first digital weapon took to reach its target in Iran.

This recent undated satellite image provided by Space Imaging/Inta SpaceTurk shows the once-secret Natanz nuclear complex in Natanz, Iran, about 150 miles south of Tehran. AP PHOTO/SPACE IMAGING/INTA SPACETURK, HO



KIM ZETTER SECURITY NOV 3. 2014 6:30 AM

An Unprecedented Look at Stuxnet, the World's First Digital Weapon

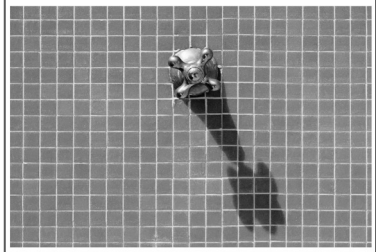
In an excerpt from her new book, "Countdown to Zero Day," WIRED's Kim Zetter describes the dark path the world's first digital weapon took to reach its target in Iran.

This recent undated satellite image provided by Space Imaging/Inta SpaceTurk shows the once-secret Natanz nuclear complex in Natanz, Iran, about 150 miles south of Tehran. AP PHOTO/SPACE IMAGING/INTA SPACETURK, HO

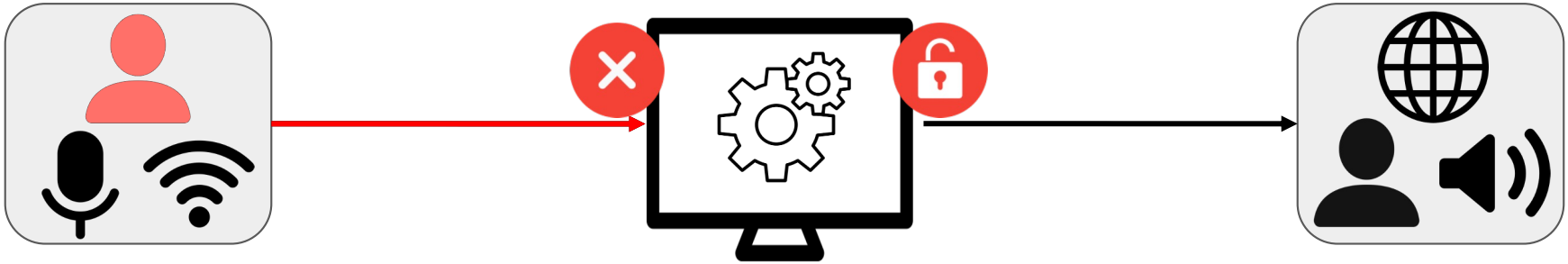
ANDY GREENBERG SECURITY FEB 8. 2021 6:54 PM

A Hacker Tried to Poison a Florida City's Water Supply, Officials Say

The attacker upped sodium hydroxide levels in the Oldsmar, Florida, water supply to extremely dangerous levels.



The cursor began clicking through the water treatment plant's controls. Within seconds, the intruder was attempting to change the water supply's levels of sodium hydroxide. PHOTOGRAPH: GETTY IMAGES



KIM ZETTER SECURITY NOV 3. 2014 6:30 AM

An Unprecedented Look at Stuxnet, the World's First Digital Weapon

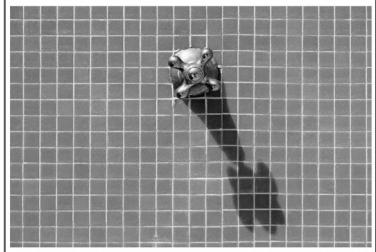
In an excerpt from her new book, "Countdown to Zero Day," WIRED's Kim Zetter describes the dark path the world's first digital weapon took to reach its target in Iran.

This recent undated satellite image provided by Space Imaging/Inta SpaceTurk shows the once-secret Natanz nuclear complex in Natanz, Iran, about 150 miles south of Tehran. AP PHOTO/SPACE IMAGING/INTA SPACETURK, HO

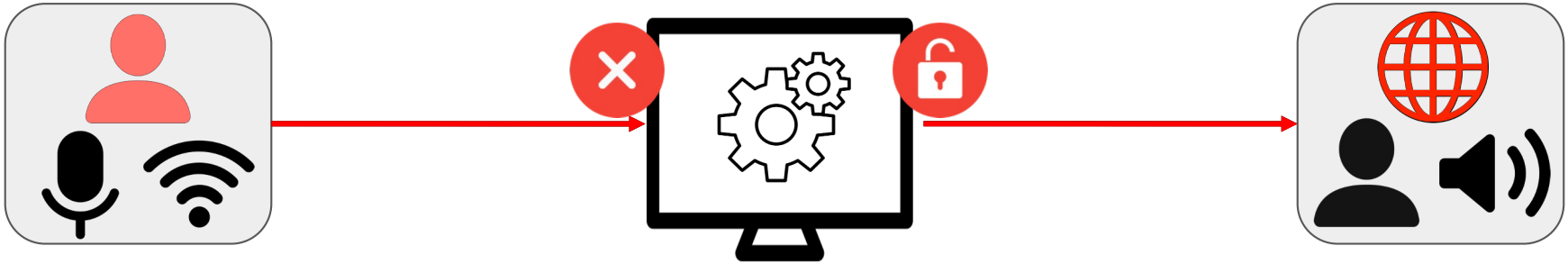
ANDY GREENBERG SECURITY FEB 8. 2021 6:54 PM

A Hacker Tried to Poison a Florida City's Water Supply, Officials Say

The attacker upped sodium hydroxide levels in the Oldsmar, Florida, water supply to extremely dangerous levels.



The cursor began clicking through the water treatment plant's controls. Within seconds, the intruder was attempting to change the water supply's levels of sodium hydroxide. PHOTOGRAPH: GETTY IMAGES



KIM ZETTER SECURITY NOV 3. 2014 6:30 AM

An Unprecedented Look at Stuxnet, the World's First Digital Weapon

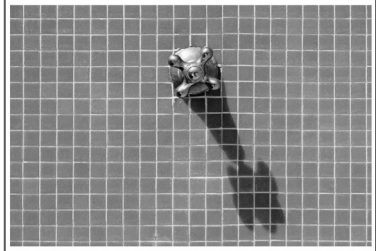
In an excerpt from her new book, "Countdown to Zero Day," WIRED's Kim Zetter describes the dark path the world's first digital weapon took to reach its target in Iran.

This recent undated satellite image provided by Space Imaging/Inta SpaceTurk shows the once-secret Natanz nuclear complex in Natanz, Iran, about 150 miles south of Tehran. AP PHOTO/SPACE IMAGING/INTA SPACETURK, HO

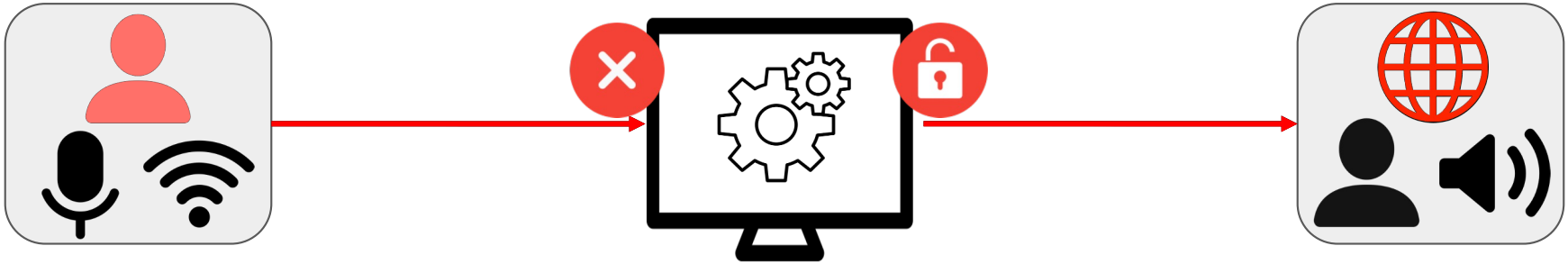
ANDY GREENBERG SECURITY FEB 8. 2021 6:54 PM

A Hacker Tried to Poison a Florida City's Water Supply, Officials Say

The attacker upped sodium hydroxide levels in the Oldsmar, Florida, water supply to extremely dangerous levels.



The cursor began clicking through the water treatment plant's controls. Within seconds, the intruder was attempting to change the water supply's levels of sodium hydroxide. PHOTOGRAPH: GETTY IMAGES



KIM ZETTER SECURITY NOV 3. 2014 6:30 AM

An Unprecedented Look at Stuxnet, the World's First Digital Weapon

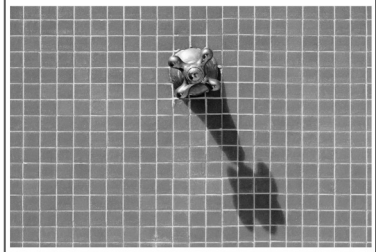
In an excerpt from her new book, "Countdown to Zero Day," WIRED's Kim Zetter describes the dark path the world's first digital weapon took to reach its target in Iran.

This recent undated satellite image provided by Space Imaging/Inta SpaceTurk shows the once-secret Natanz nuclear complex in Natanz, Iran, about 150 miles south of Tehran. AP PHOTO/SPACE IMAGING/INTA SPACETURK, HO

ANDY GREENBERG SECURITY FEB 8. 2021 6:54 PM

A Hacker Tried to Poison a Florida City's Water Supply, Officials Say

The attacker upped sodium hydroxide levels in the Oldsmar, Florida, water supply to extremely dangerous levels.

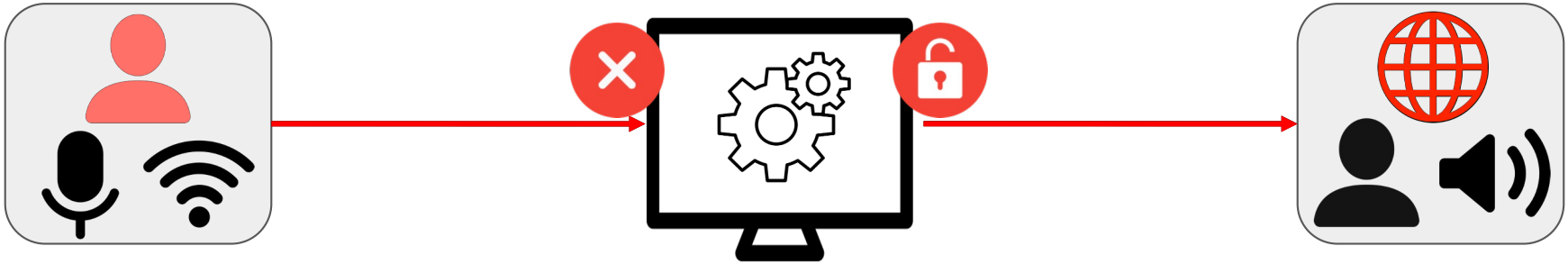


The cursor began clicking through the water treatment plant's controls. Within seconds, the intruder was attempting to change the water supply's levels of sodium hydroxide. PHOTOGRAPH: GETTY IMAGES

KIM ZETTER SECURITY APR 11. 2014 4:57 PM

Report: NSA Exploited Heartbleed to Siphon Passwords for Two Years

The NSA knew about and exploited the Heartbleed vulnerability for two years before it was publicly exposed this week, and used it to steal account passwords and other data, according to a news report.



KIM ZETTER SECURITY NOV 3. 2014 6:30 AM

An Unprecedented Look at Stuxnet, the World's First Digital Weapon

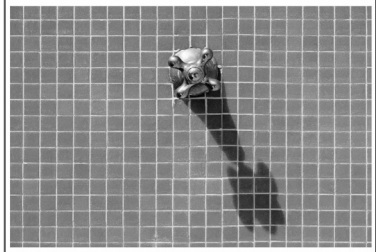
In an excerpt from her new book, "Countdown to Zero Day," WIRED's Kim Zetter describes the dark path the world's first digital weapon took to reach its target in Iran.

This recent undated satellite image provided by Space Imaging/Inta SpaceTurk shows the once-secret Natanz nuclear complex in Natanz, Iran, about 150 miles south of Tehran. AP PHOTO/SPACE IMAGING/INTA SPACETURK, HO

ANDY GREENBERG SECURITY FEB 8. 2021 6:54 PM

A Hacker Tried to Poison a Florida City's Water Supply, Officials Say

The attacker upped sodium hydroxide levels in the Oldsmar, Florida, water supply to extremely dangerous levels.



The cursor began clicking through the water treatment plant's controls. Within seconds, the intruder was attempting to change the water supply's levels of sodium hydroxide. PHOTOGRAPH: GETTY IMAGES

KIM ZETTER SECURITY APR 11. 2014 4:57 PM

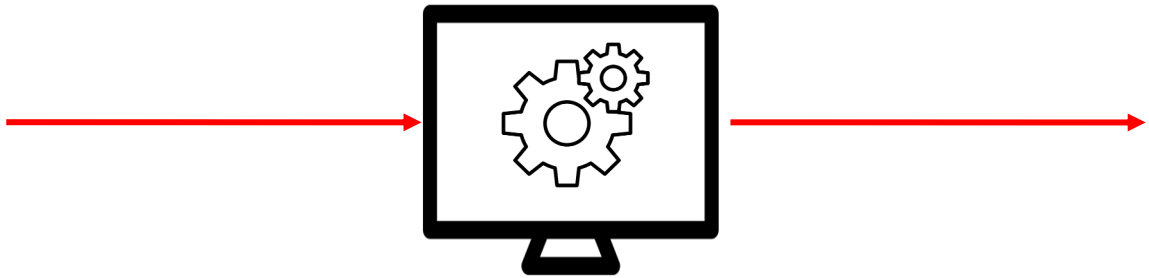
Report: NSA Exploited Heartbleed to Siphon Passwords for Two Years

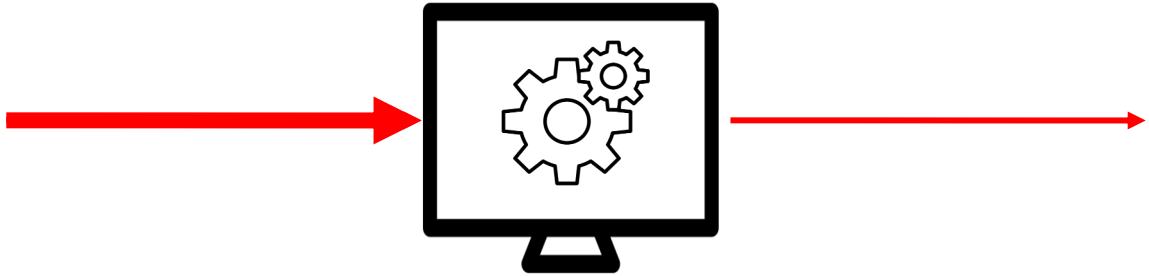
The NSA knew about and exploited the Heartbleed vulnerability for two years before it was publicly exposed this week, and used it to steal account passwords and other data, according to a news report.

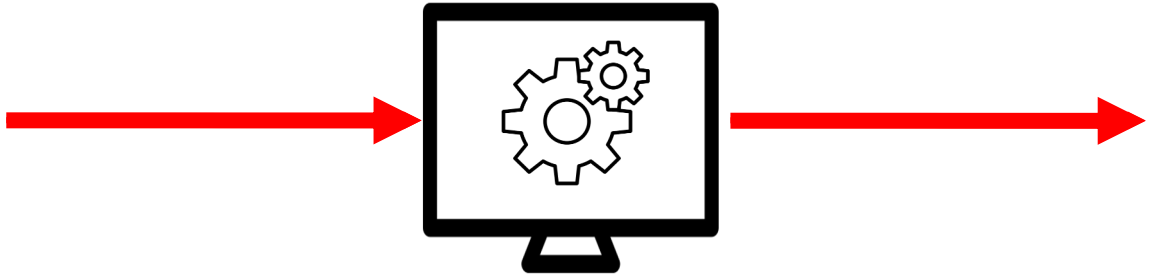
BRIAN BARRETT SECURITY DEC 19. 2020 9:00 AM

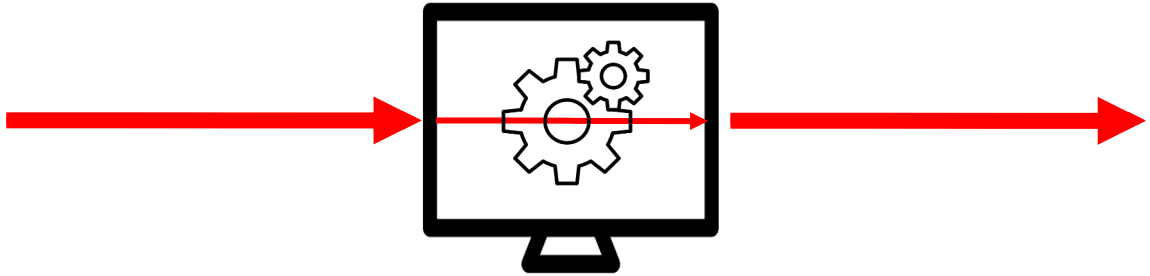
Security News This Week: Russia's SolarWinds Hack Is a Historic Mess

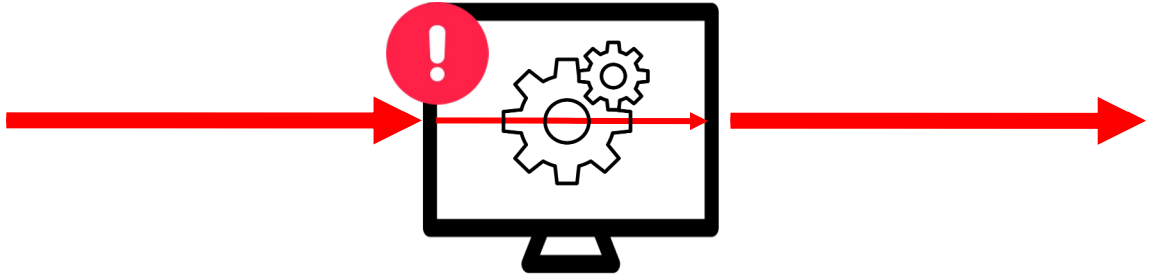
All the most important stories about the biggest hack in years.

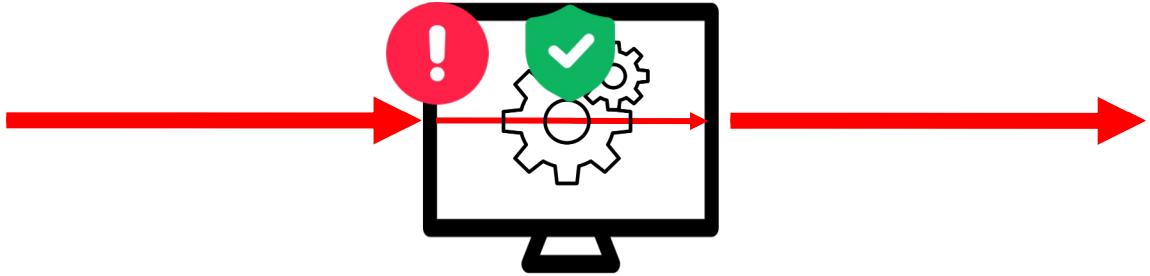


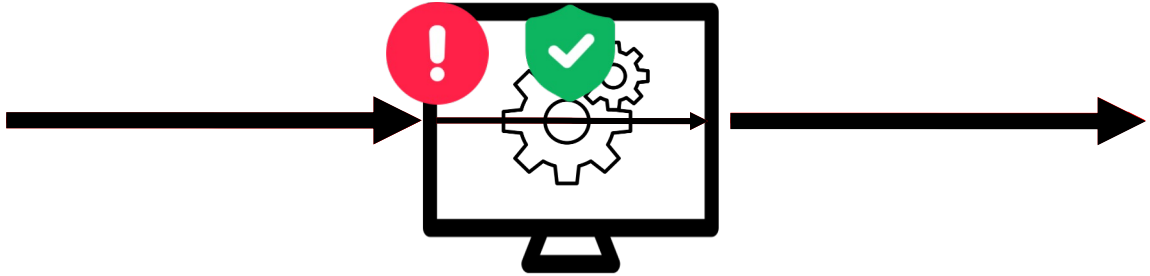


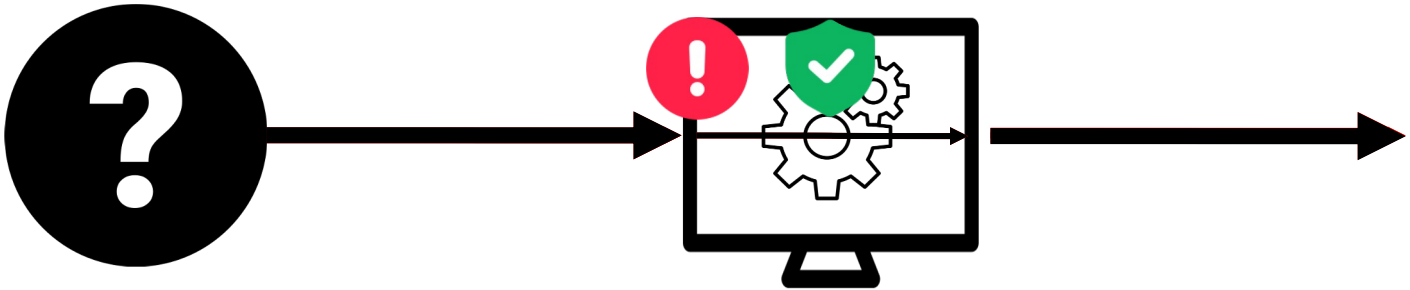


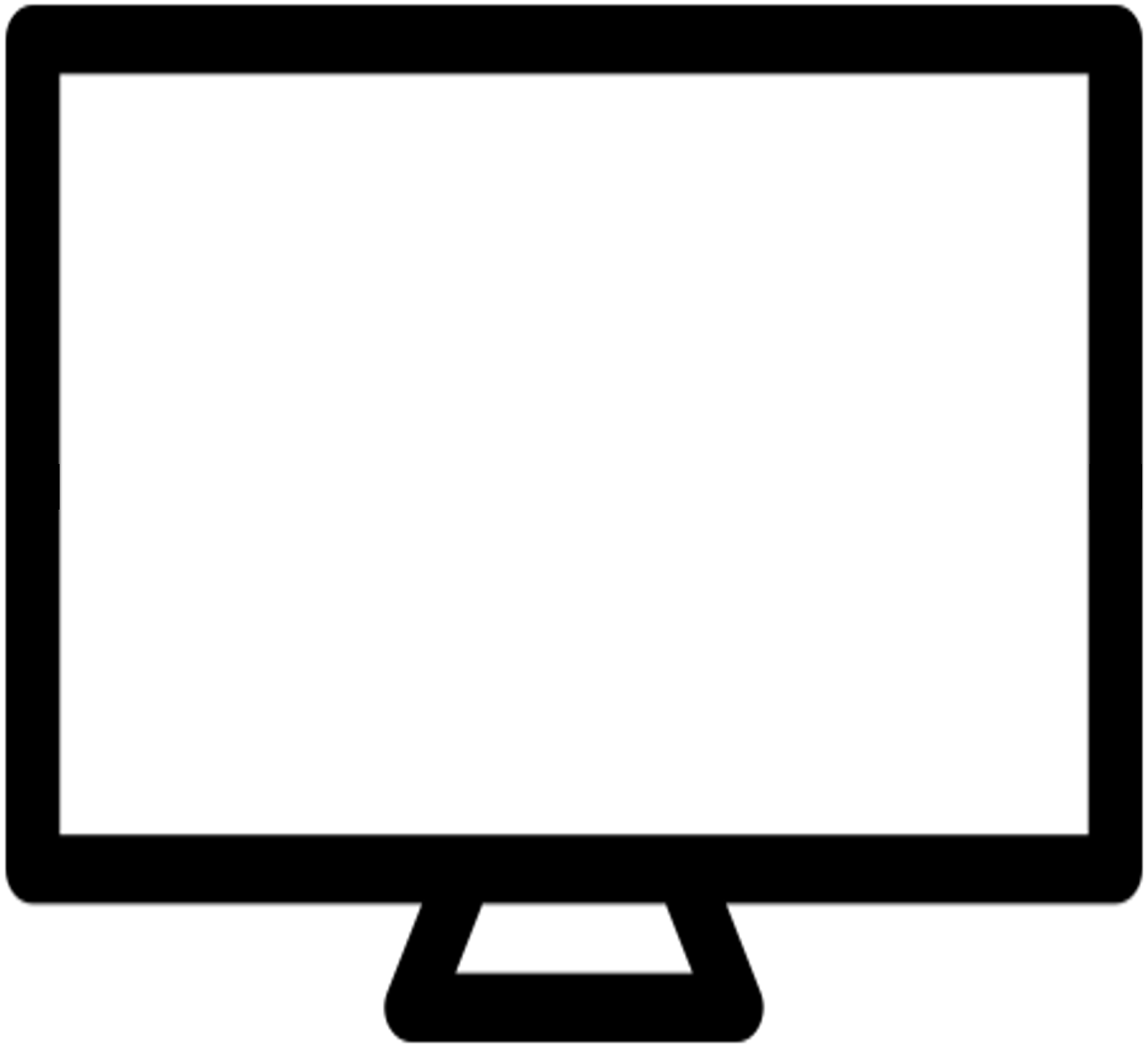


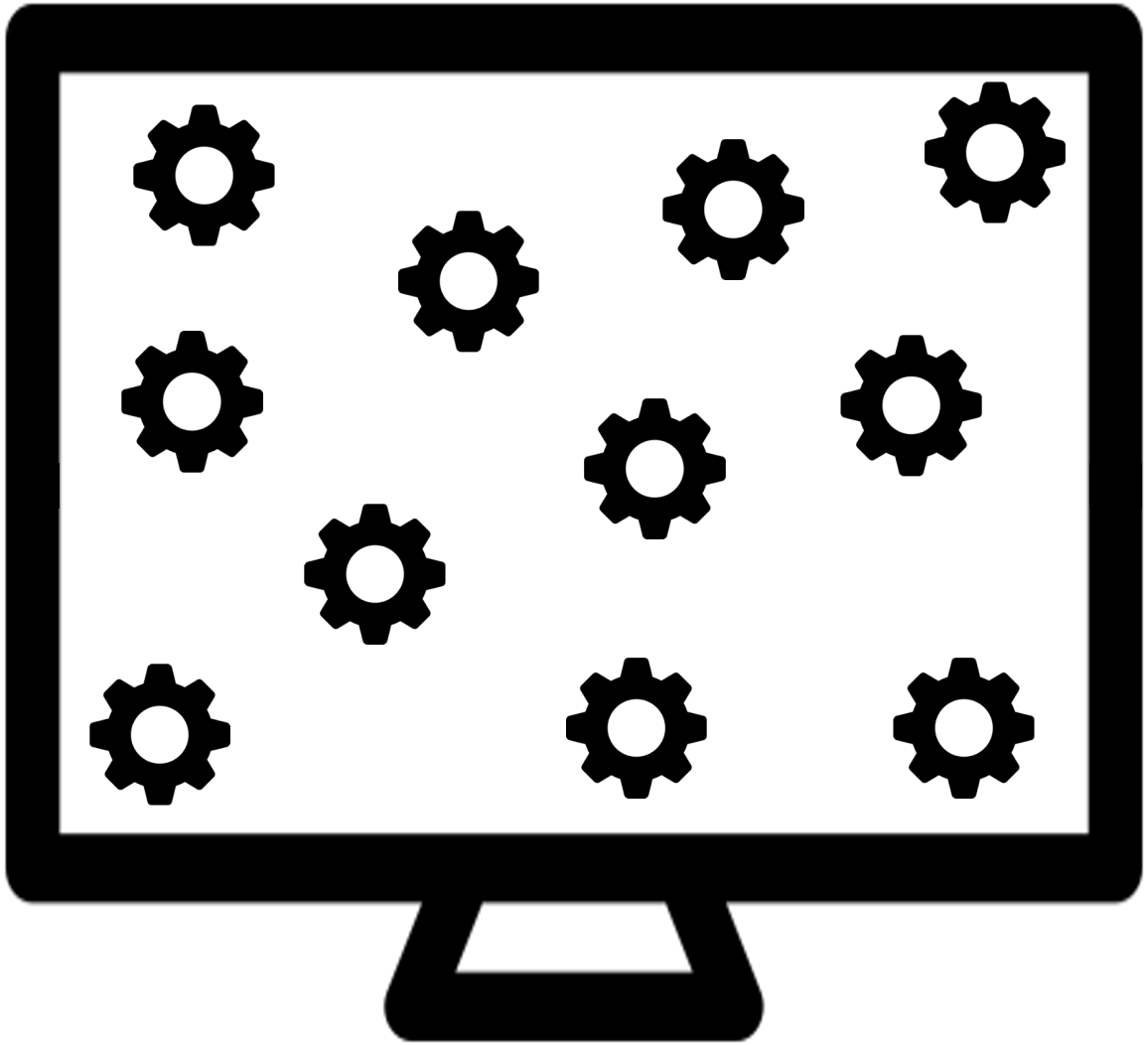


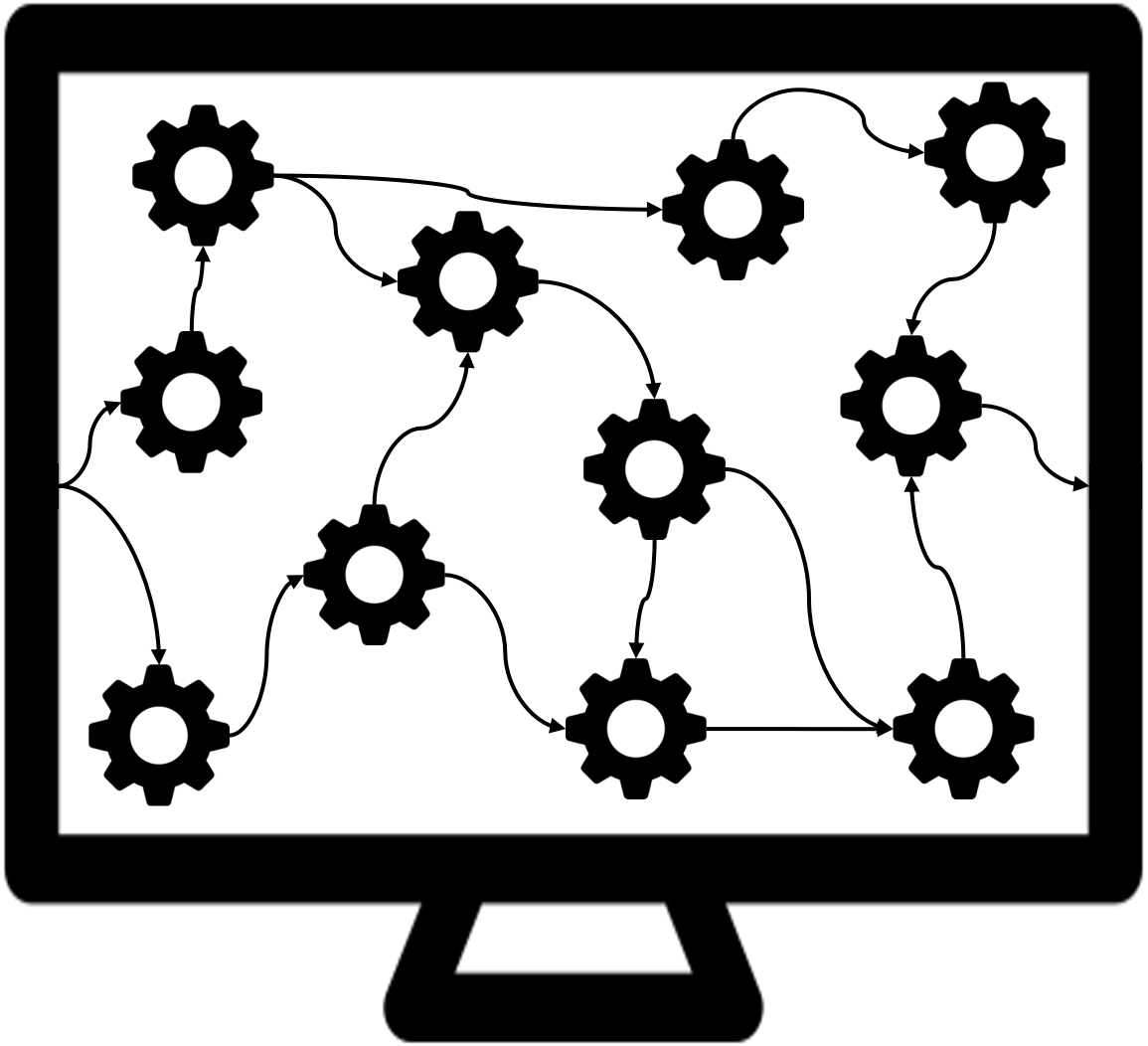


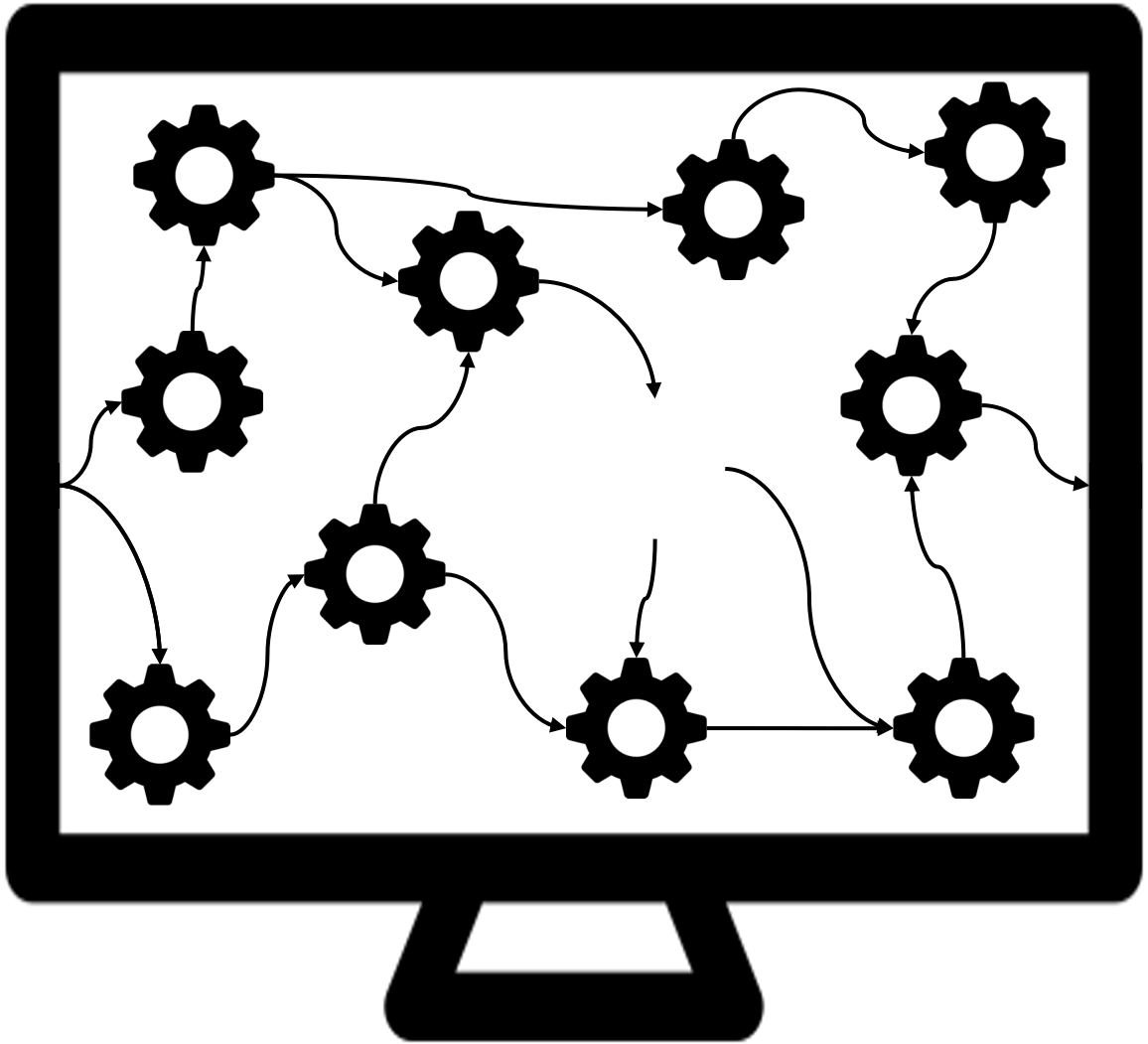


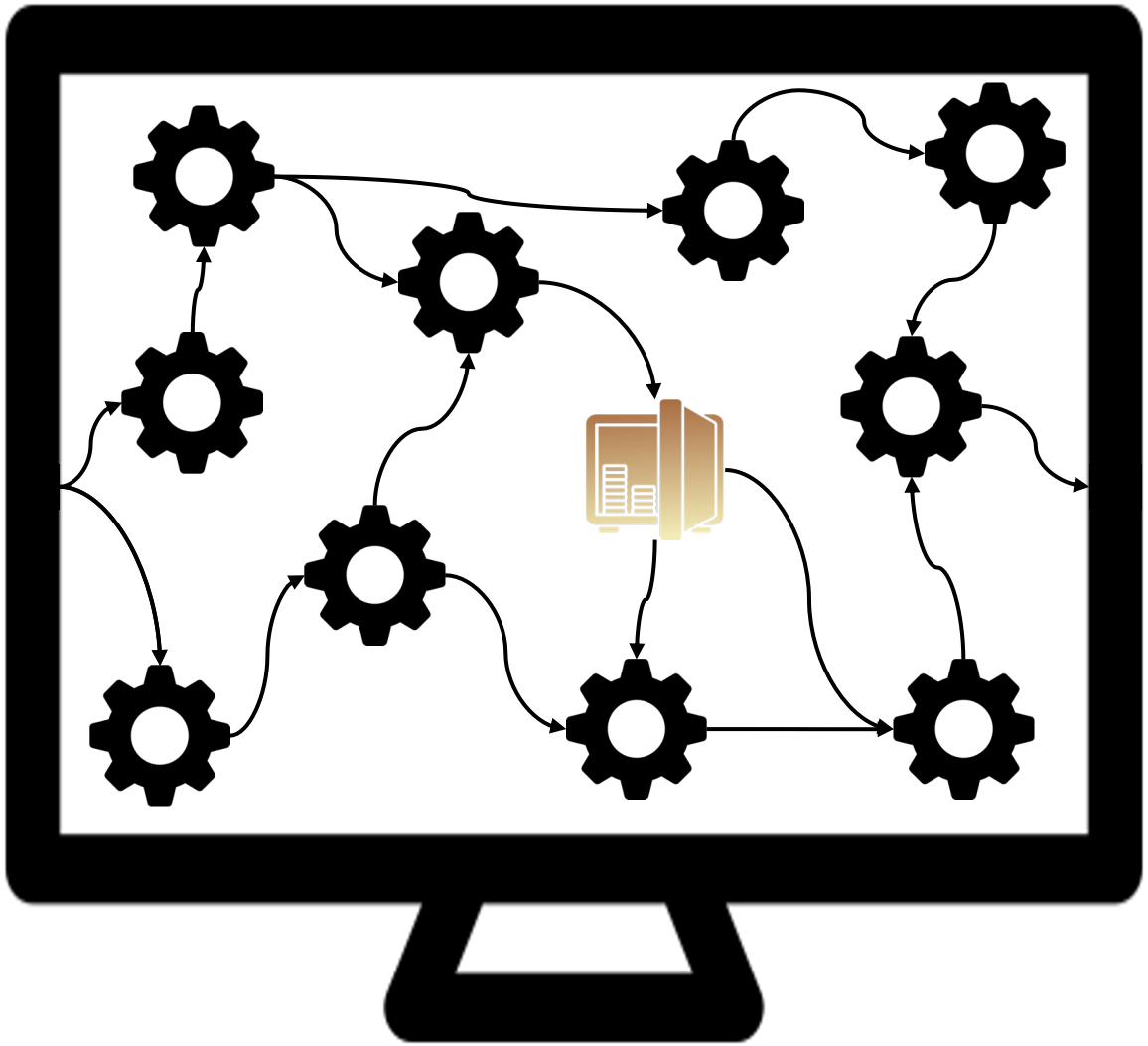






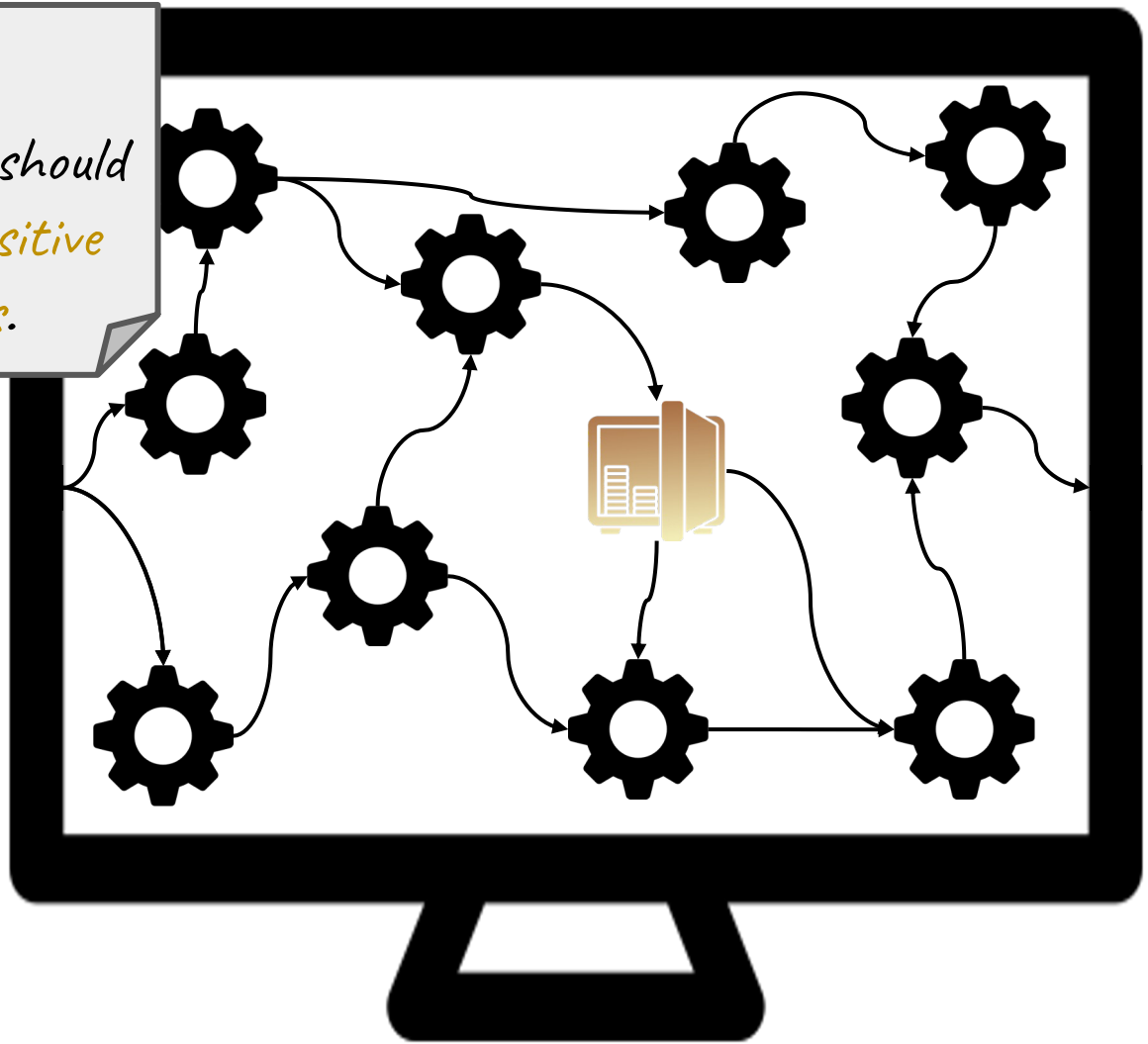






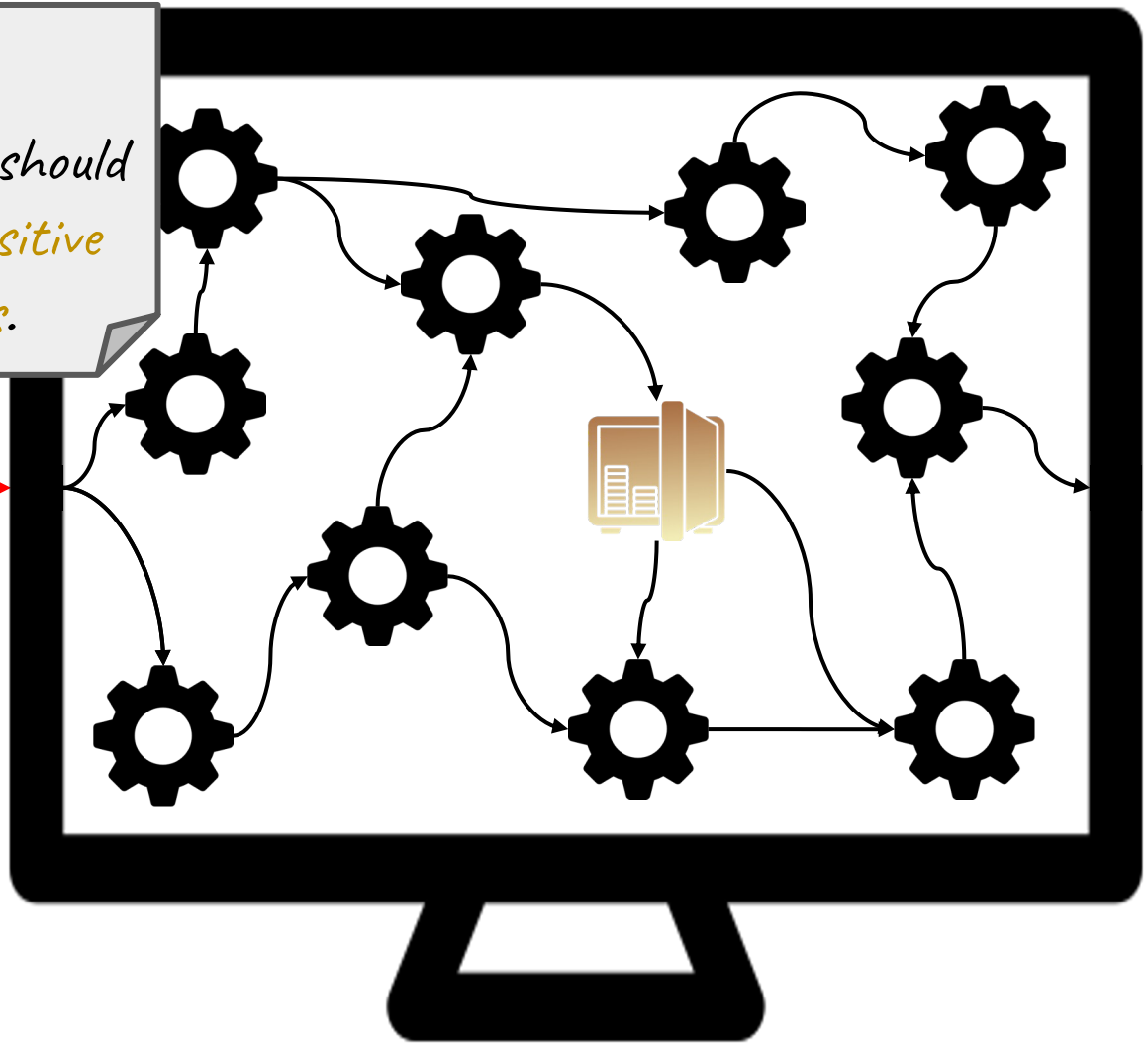
Policy

Attacker data should not reach sensitive operations.



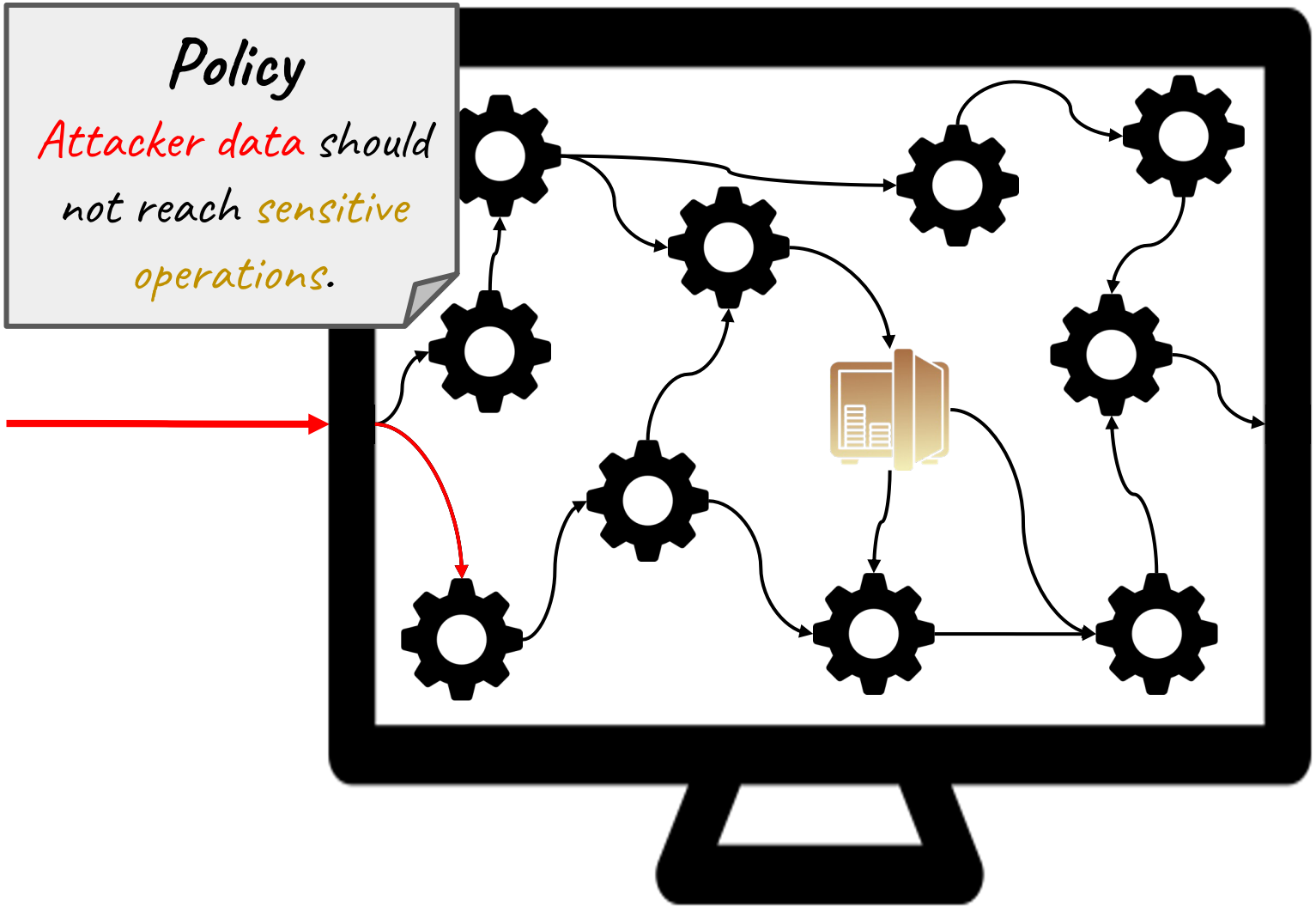
Policy

Attacker data should not reach sensitive operations.



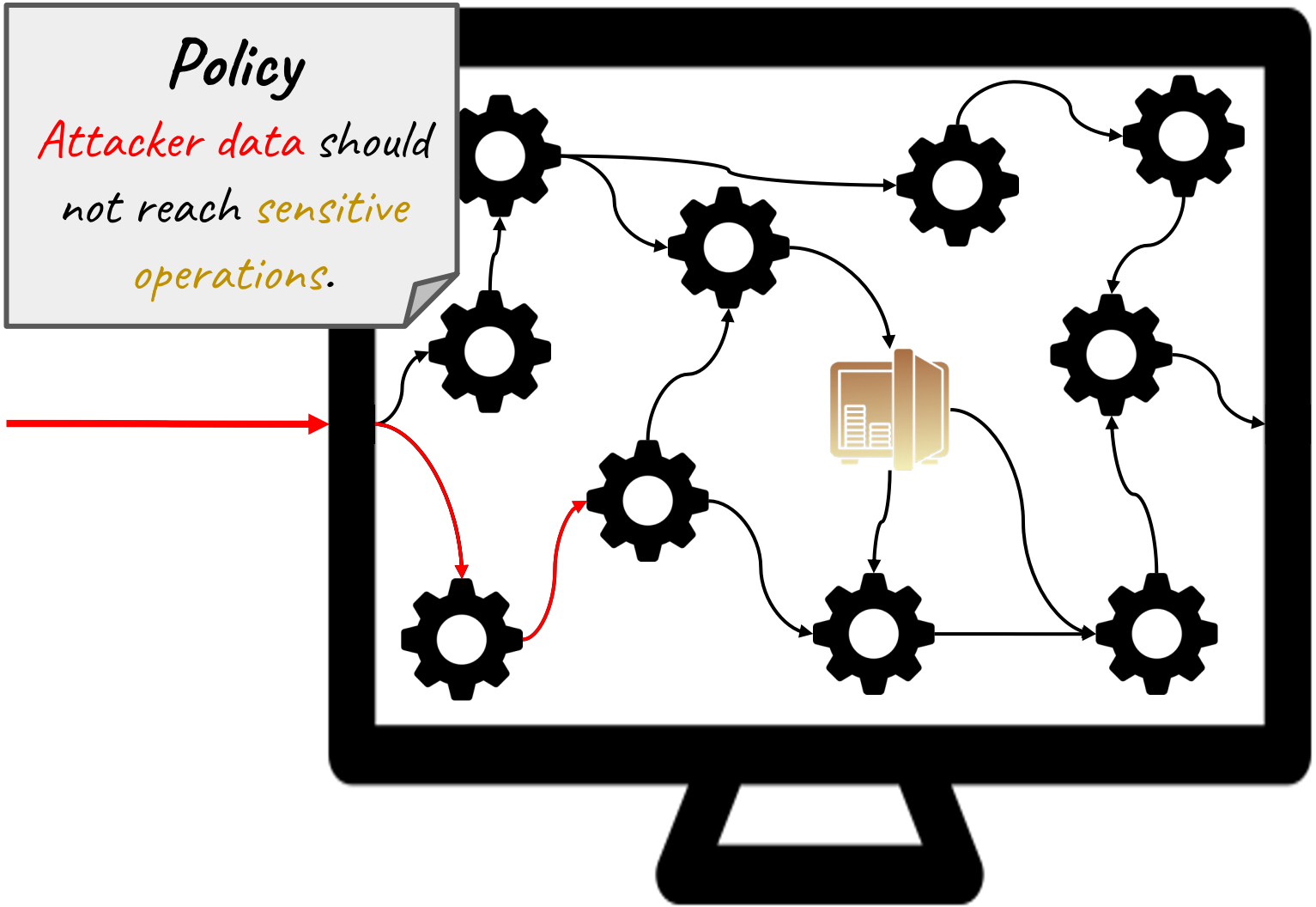
Policy

Attacker data should not reach sensitive operations.



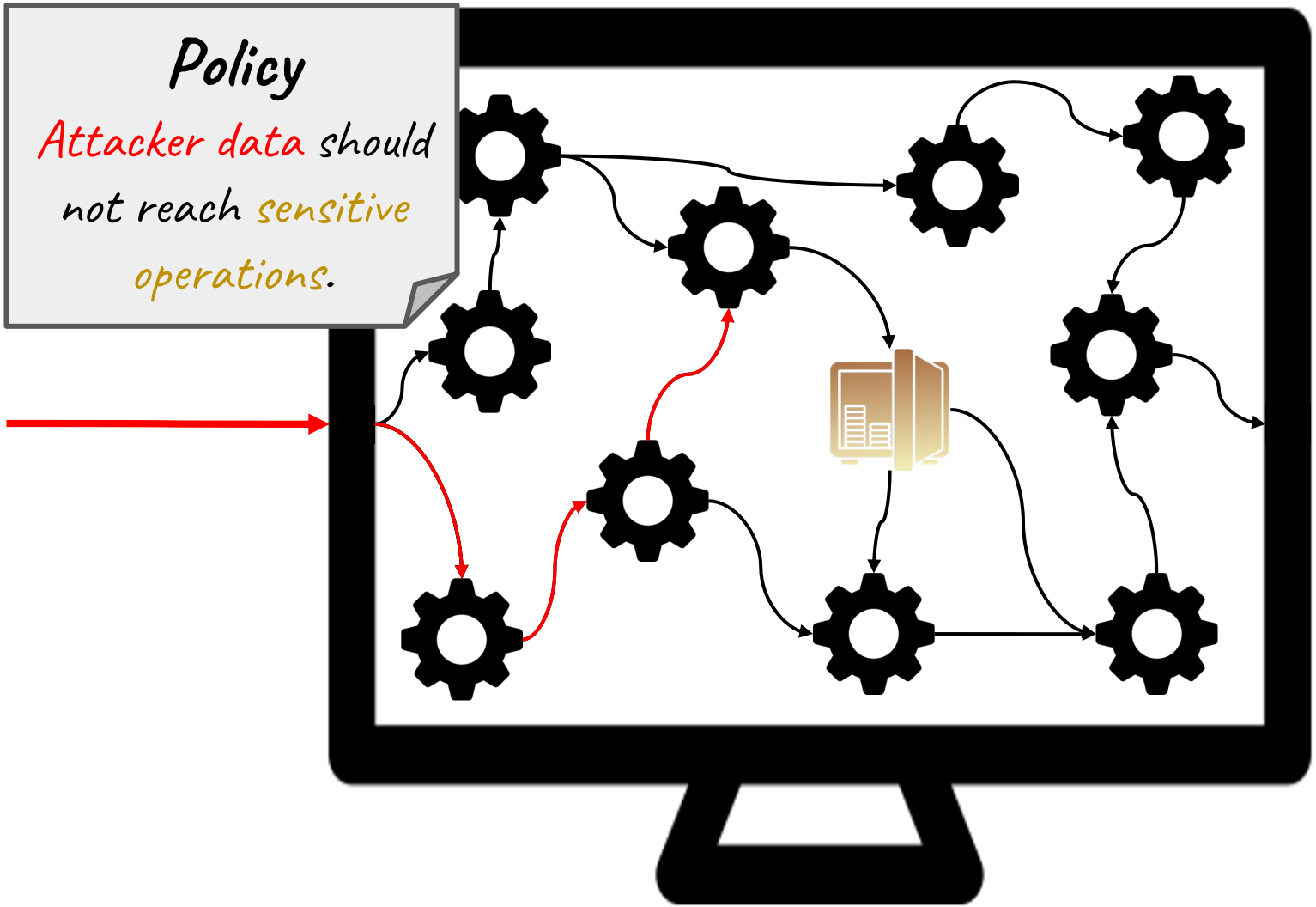
Policy

Attacker data should not reach sensitive operations.



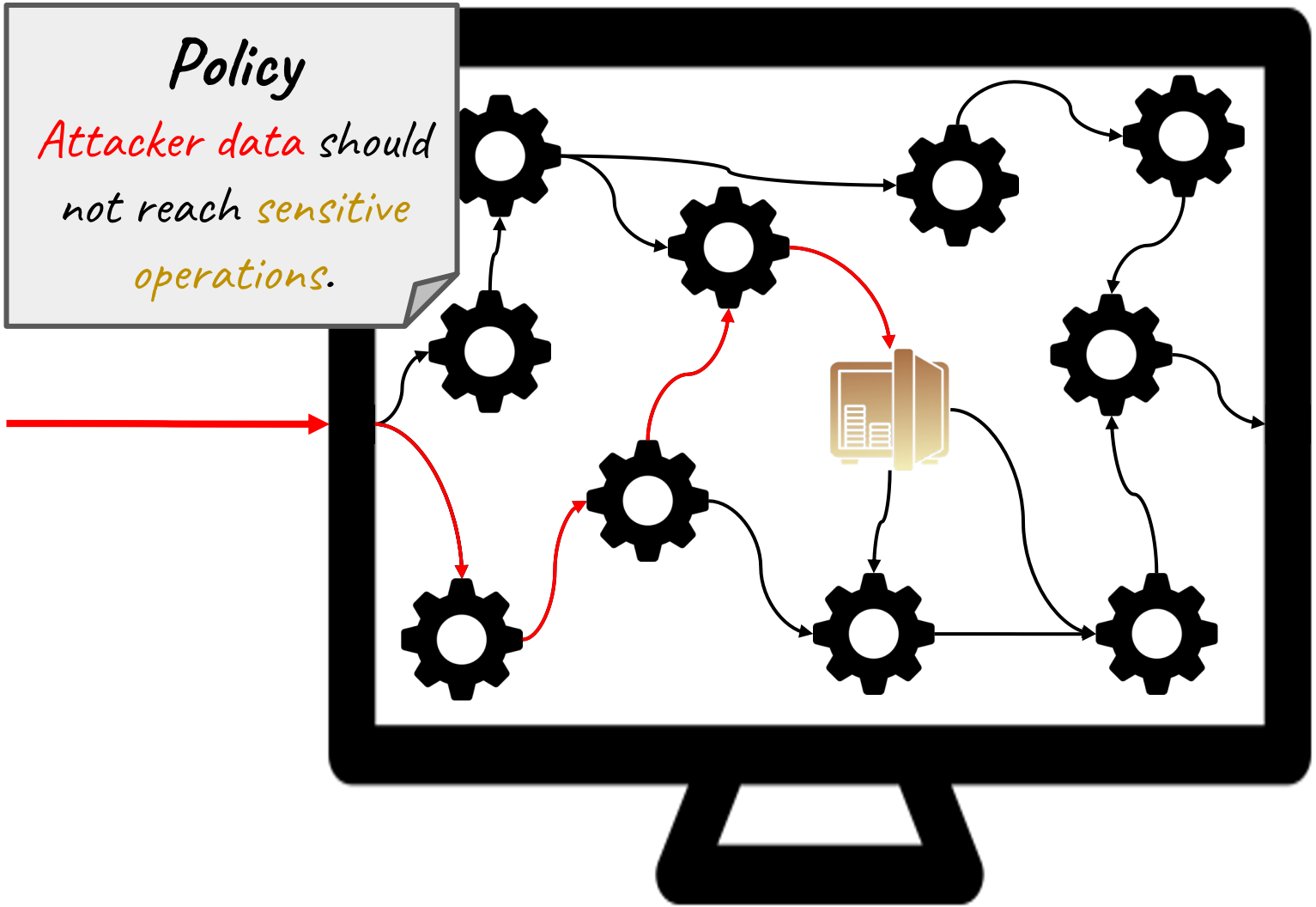
Policy

Attacker data should not reach sensitive operations.



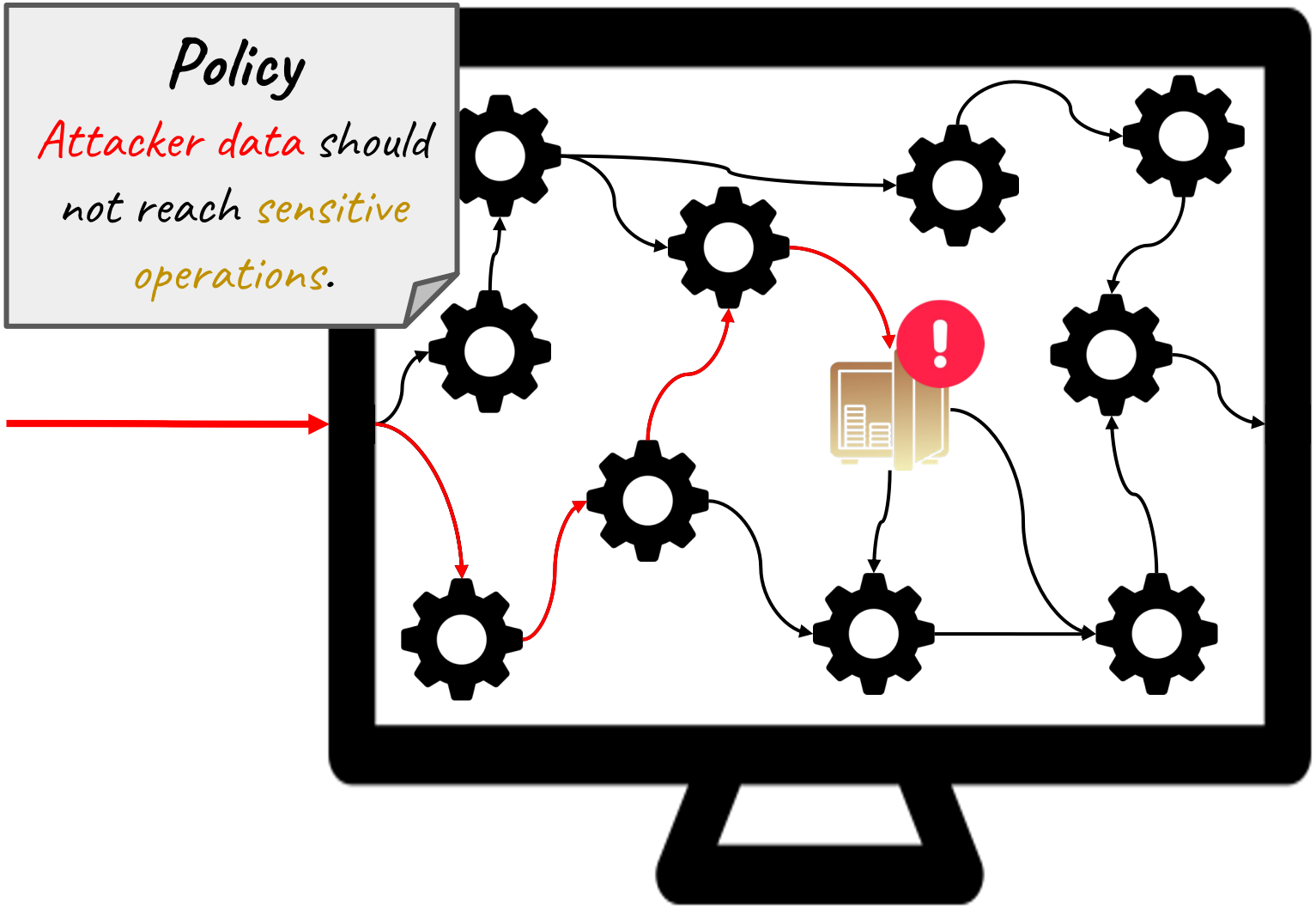
Policy

Attacker data should not reach sensitive operations.



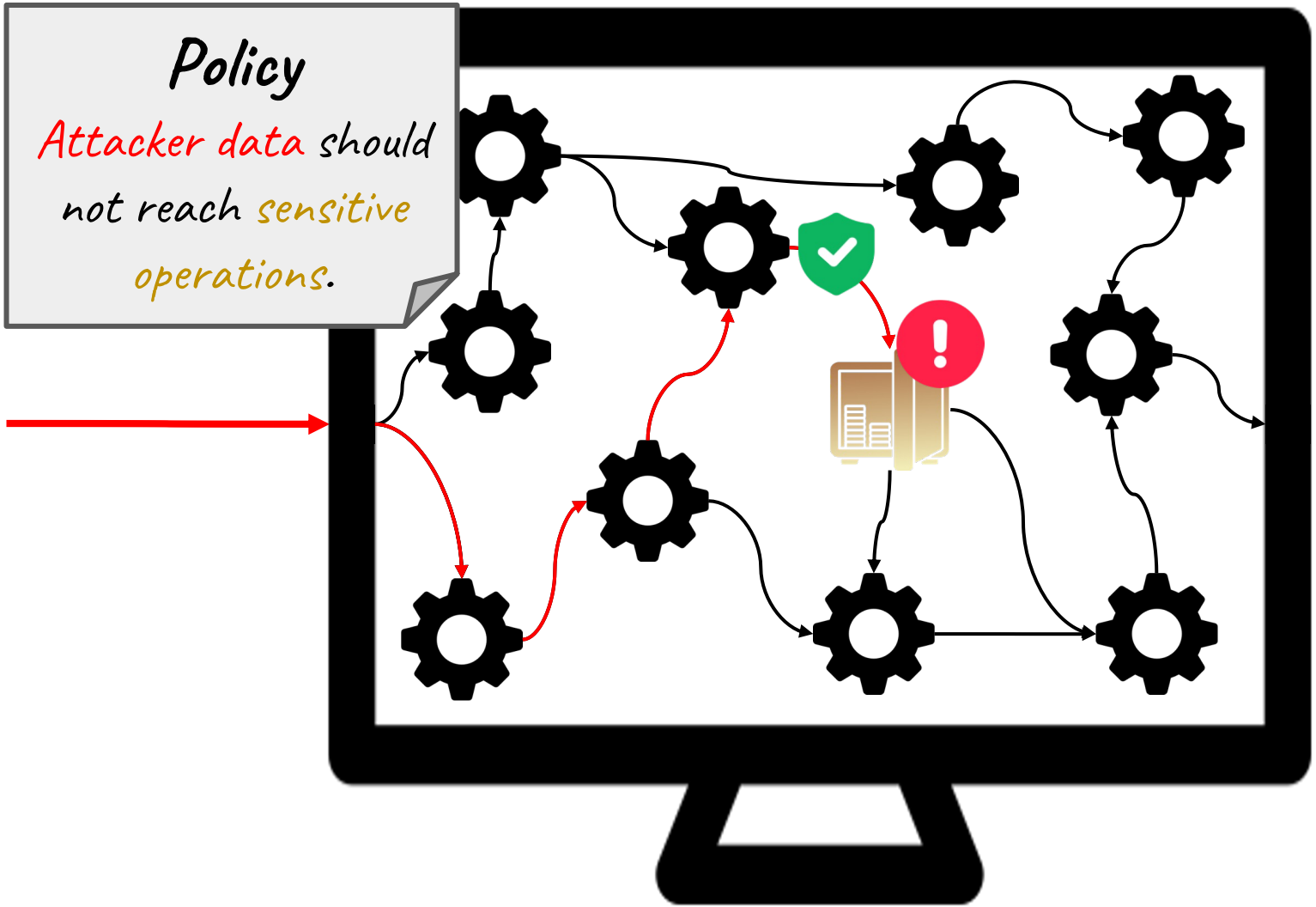
Policy

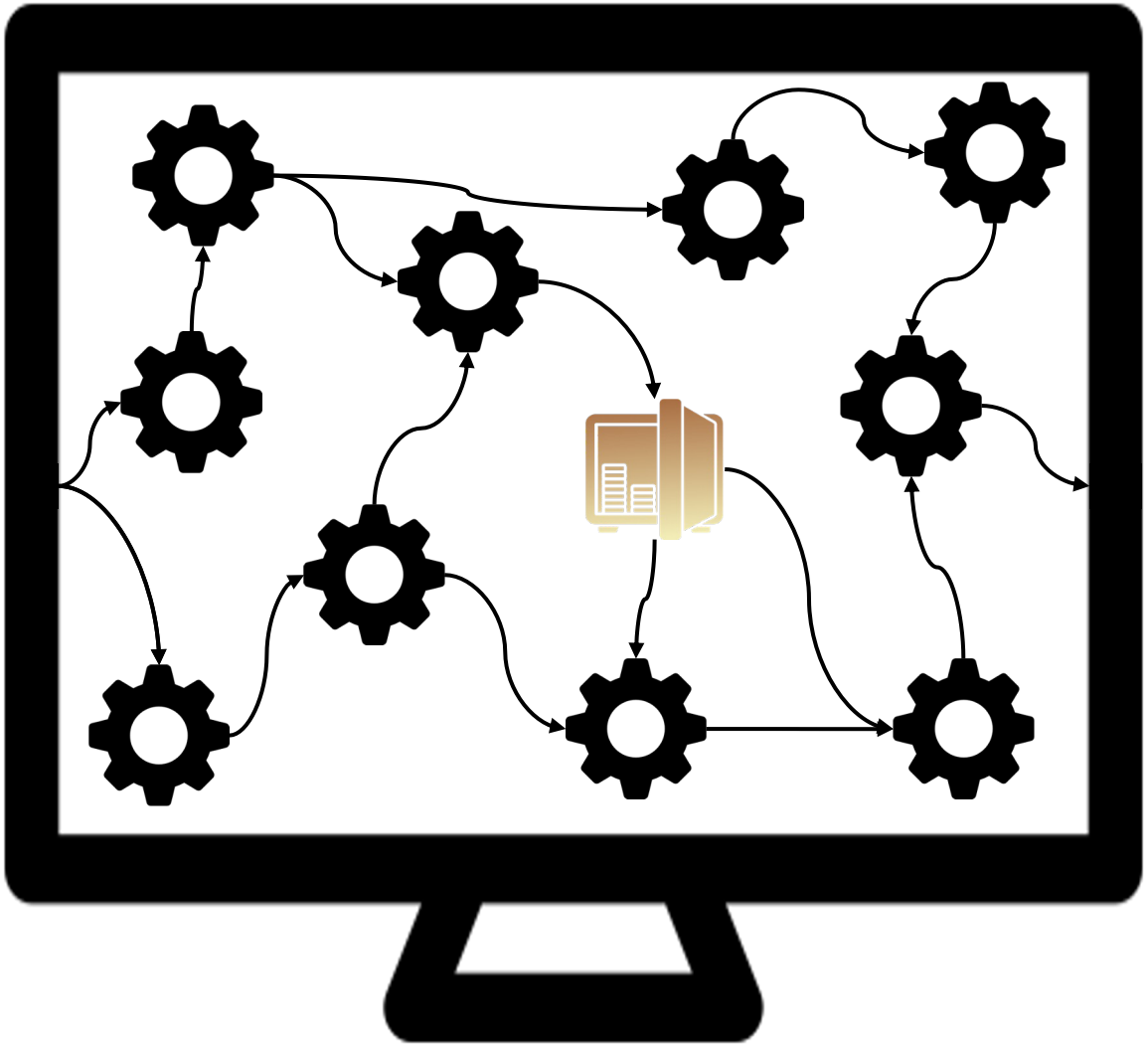
Attacker data should not reach sensitive operations.



Policy

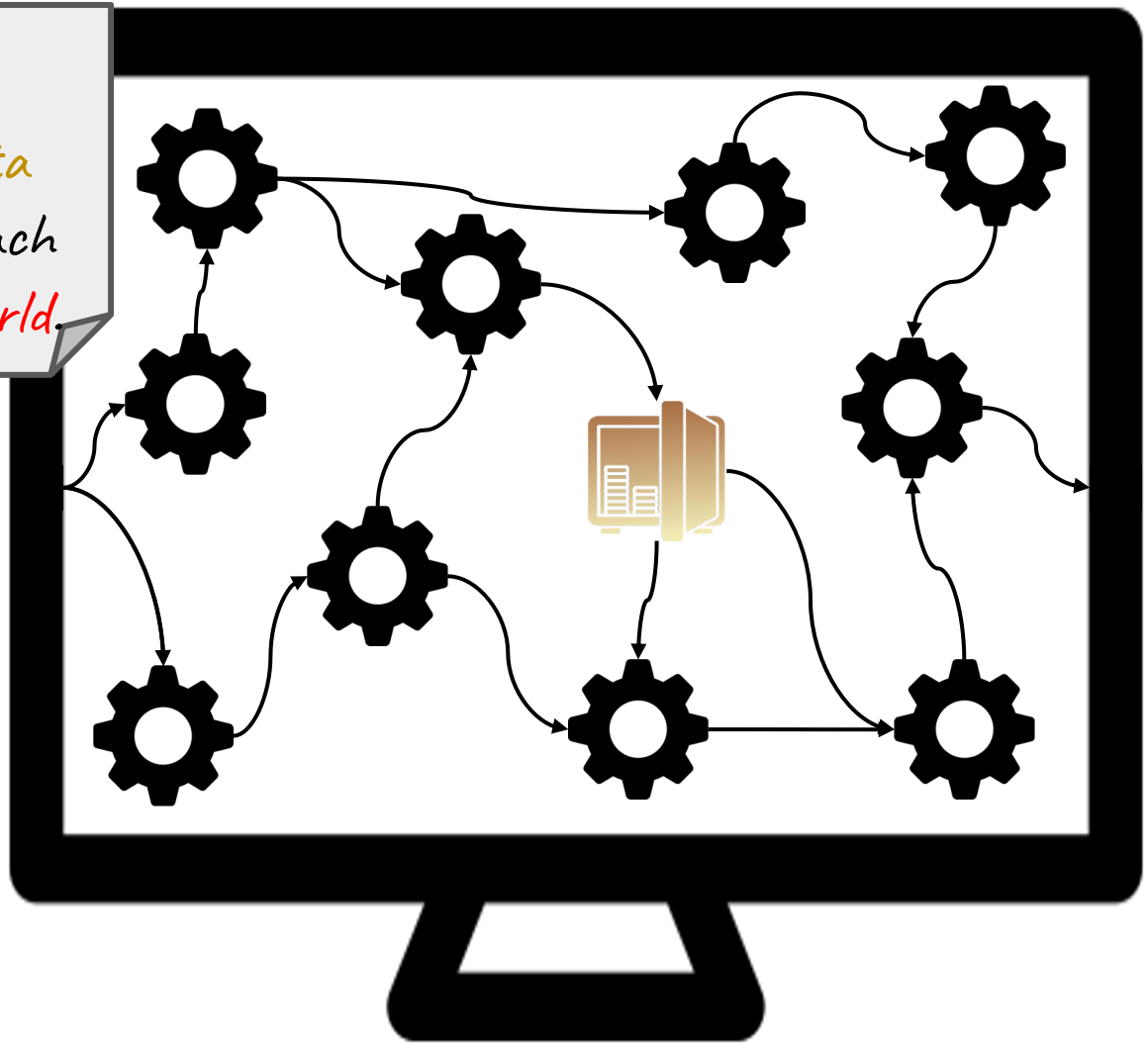
Attacker data should not reach sensitive operations.





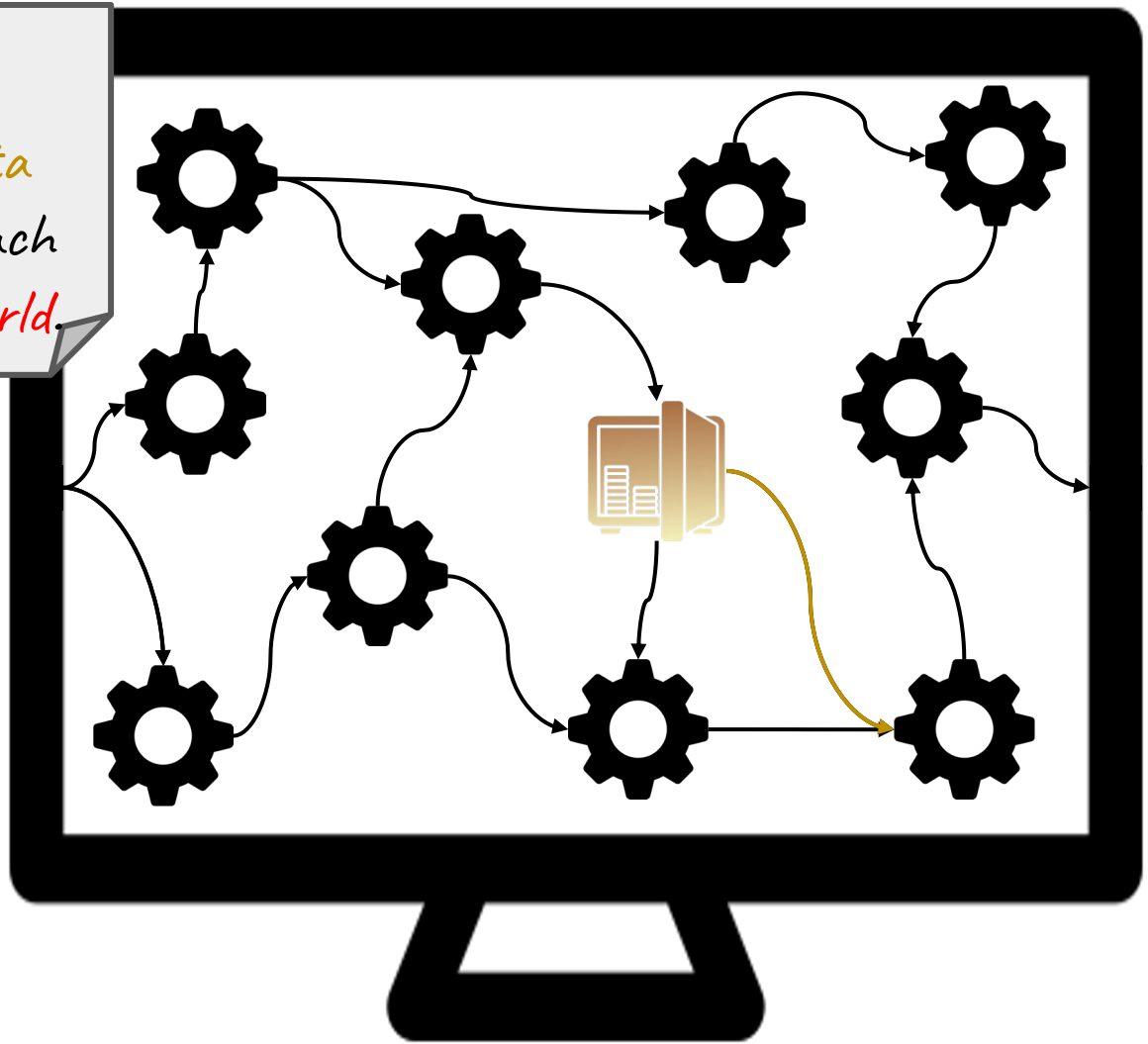
Policy

Sensitive data should not reach the outside world.



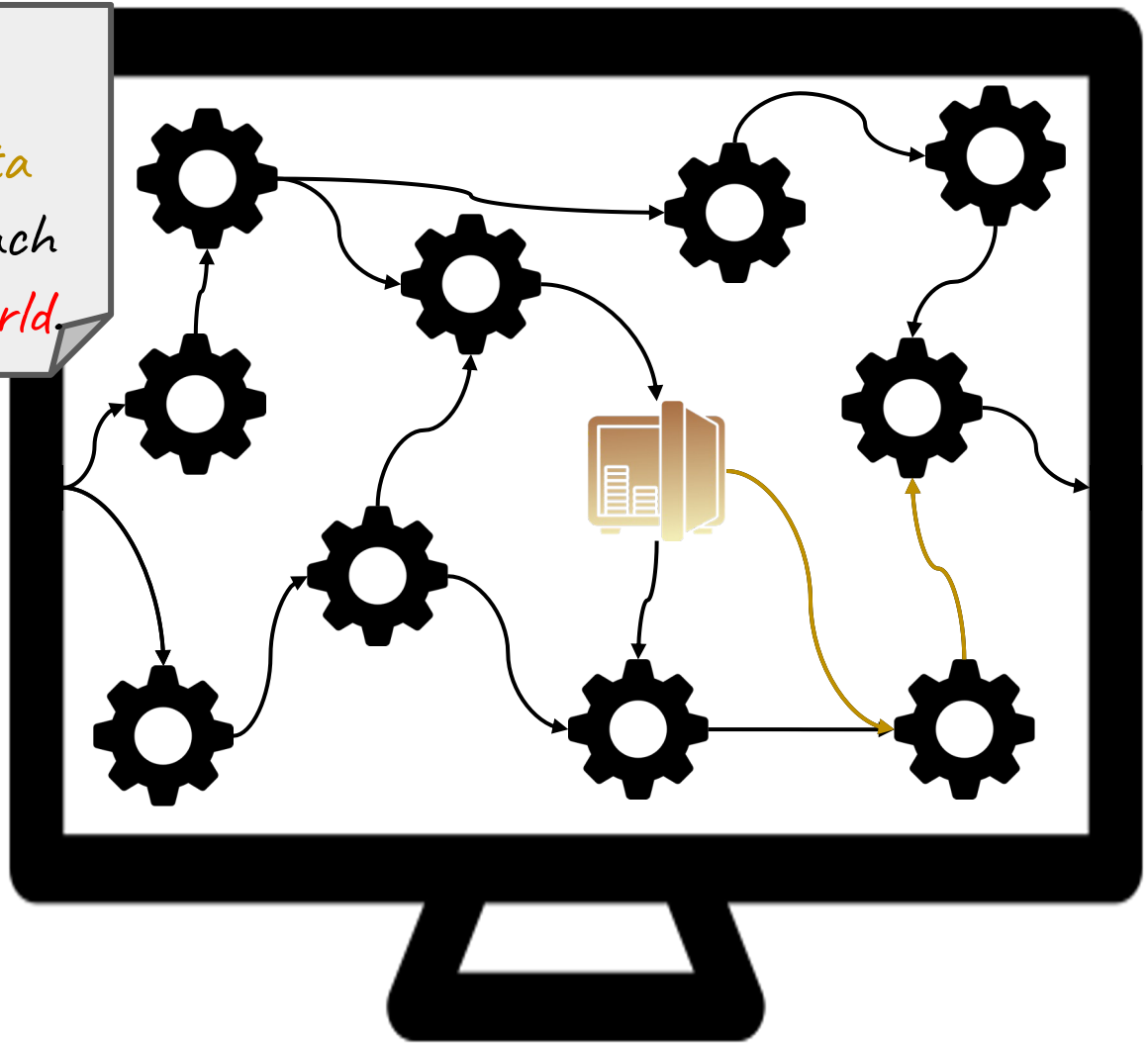
Policy

Sensitive data should not reach the outside world.



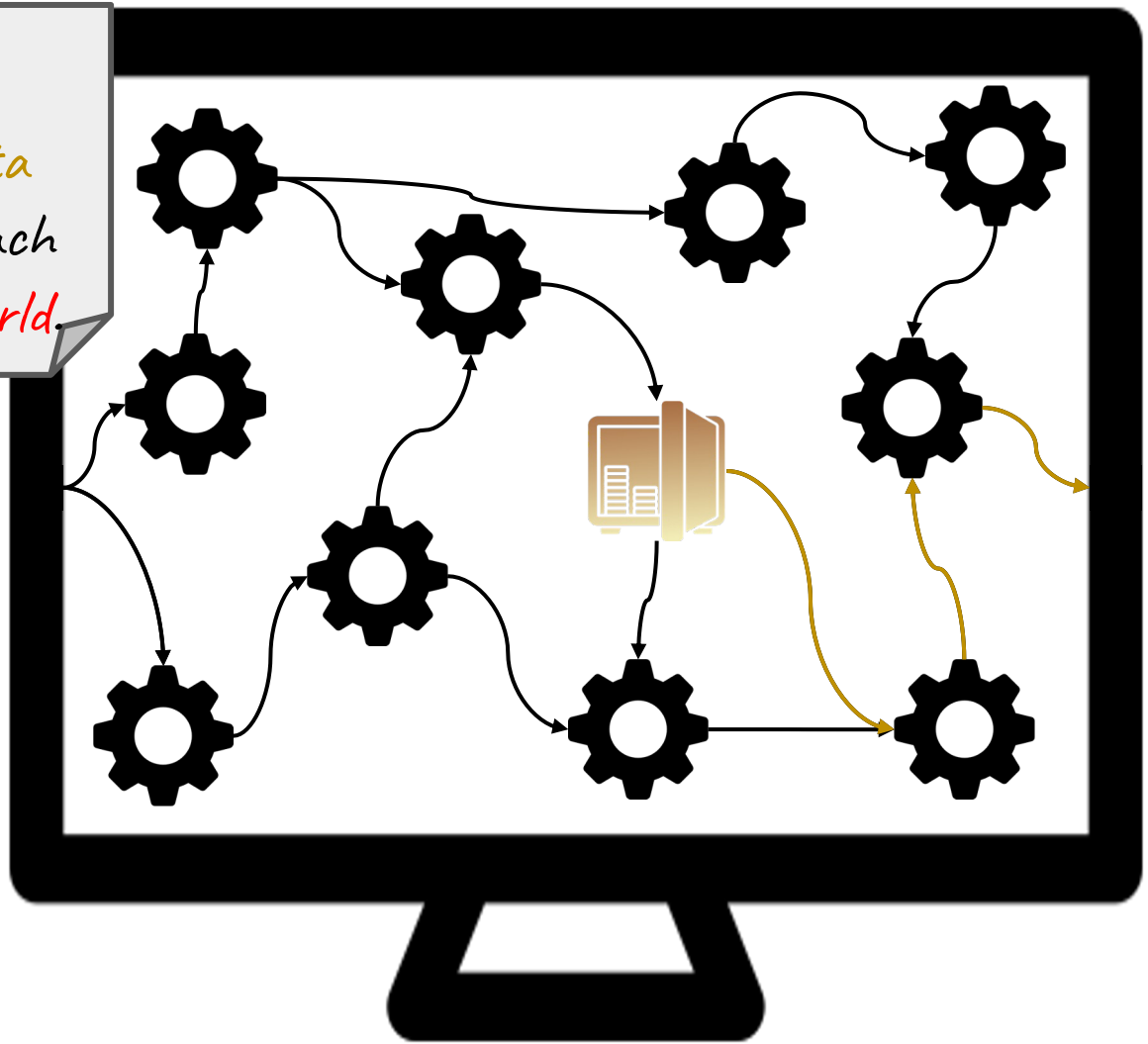
Policy

Sensitive data should not reach the outside world.



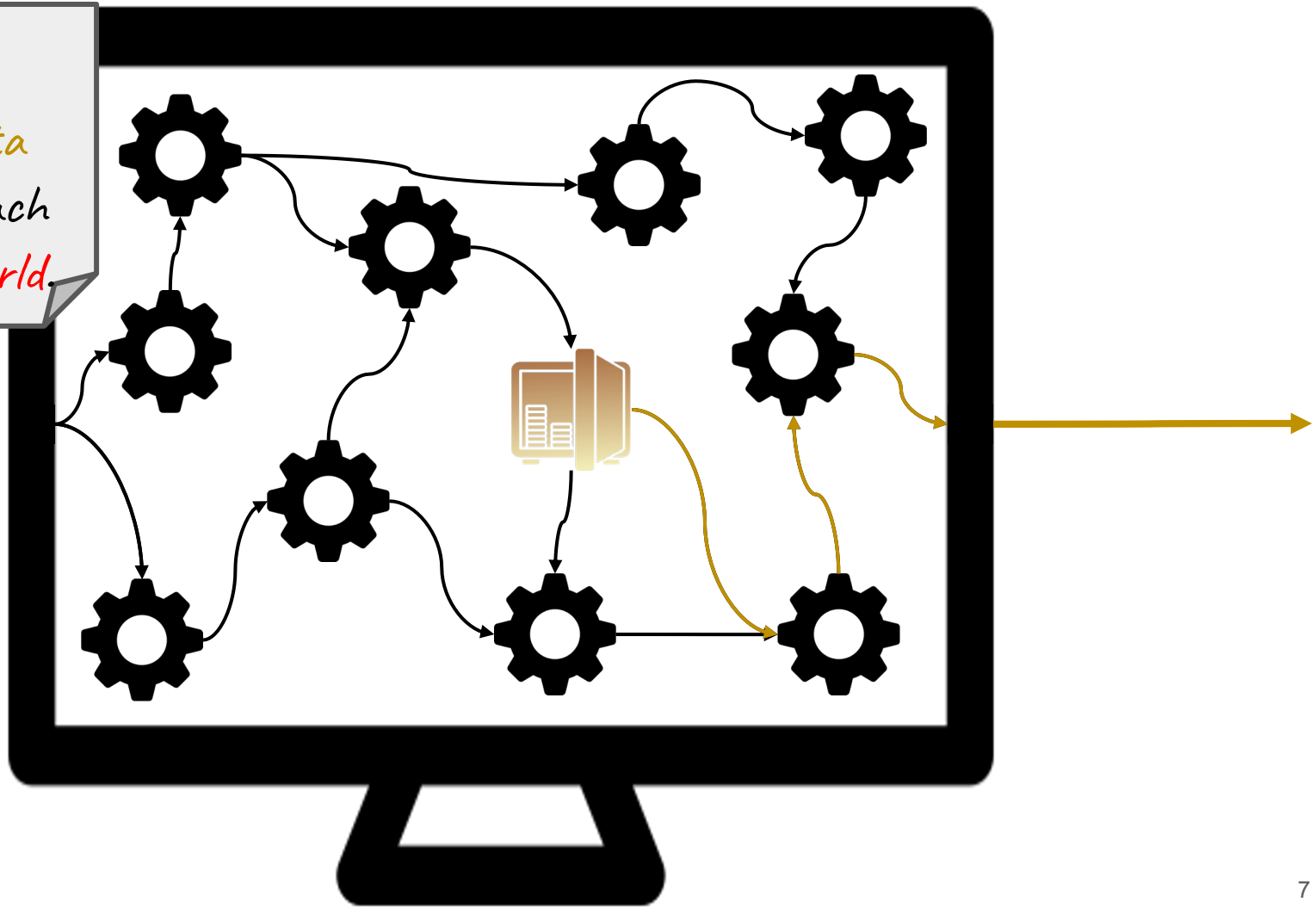
Policy

Sensitive data should not reach the outside world.



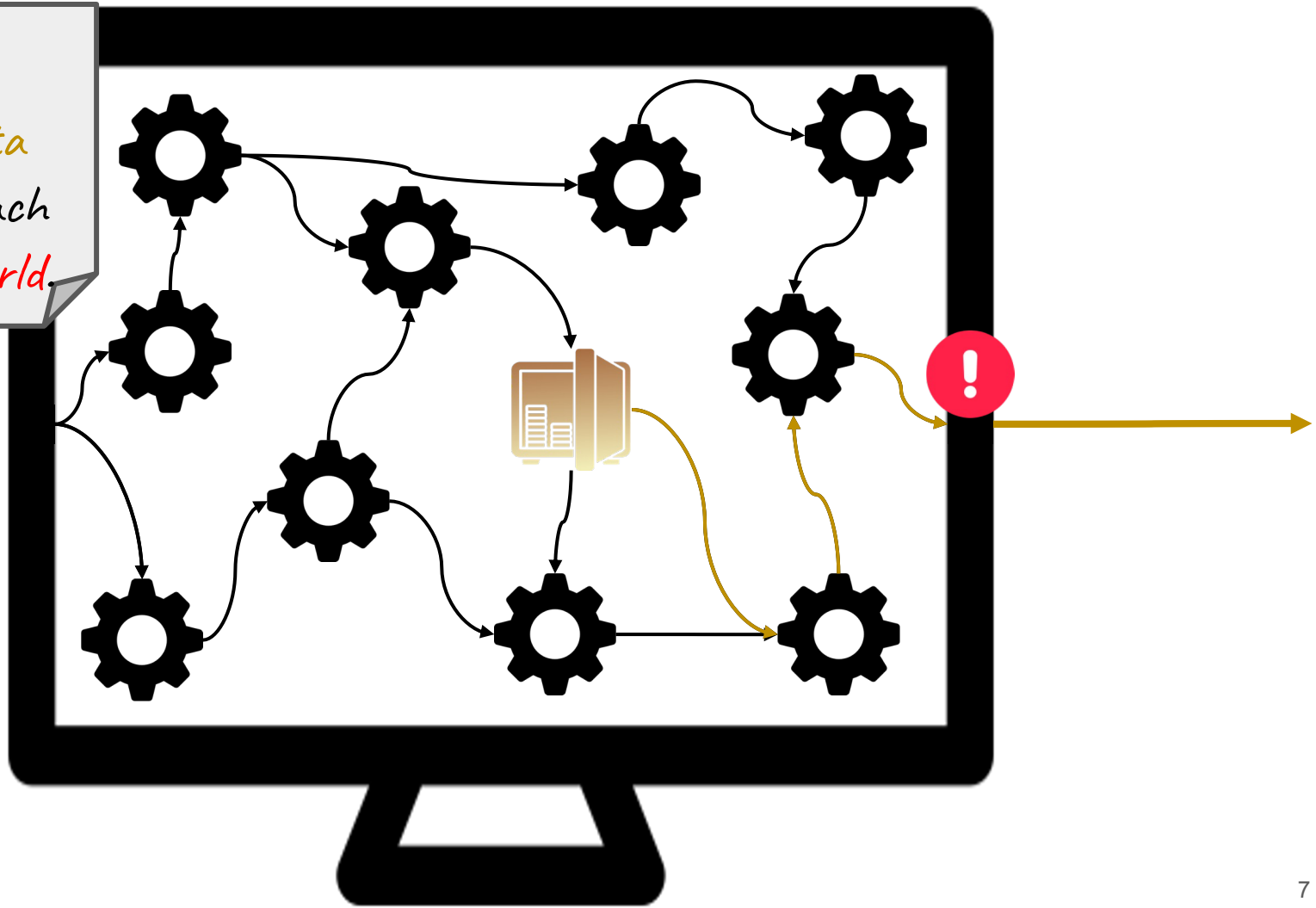
Policy

Sensitive data should not reach the outside world.



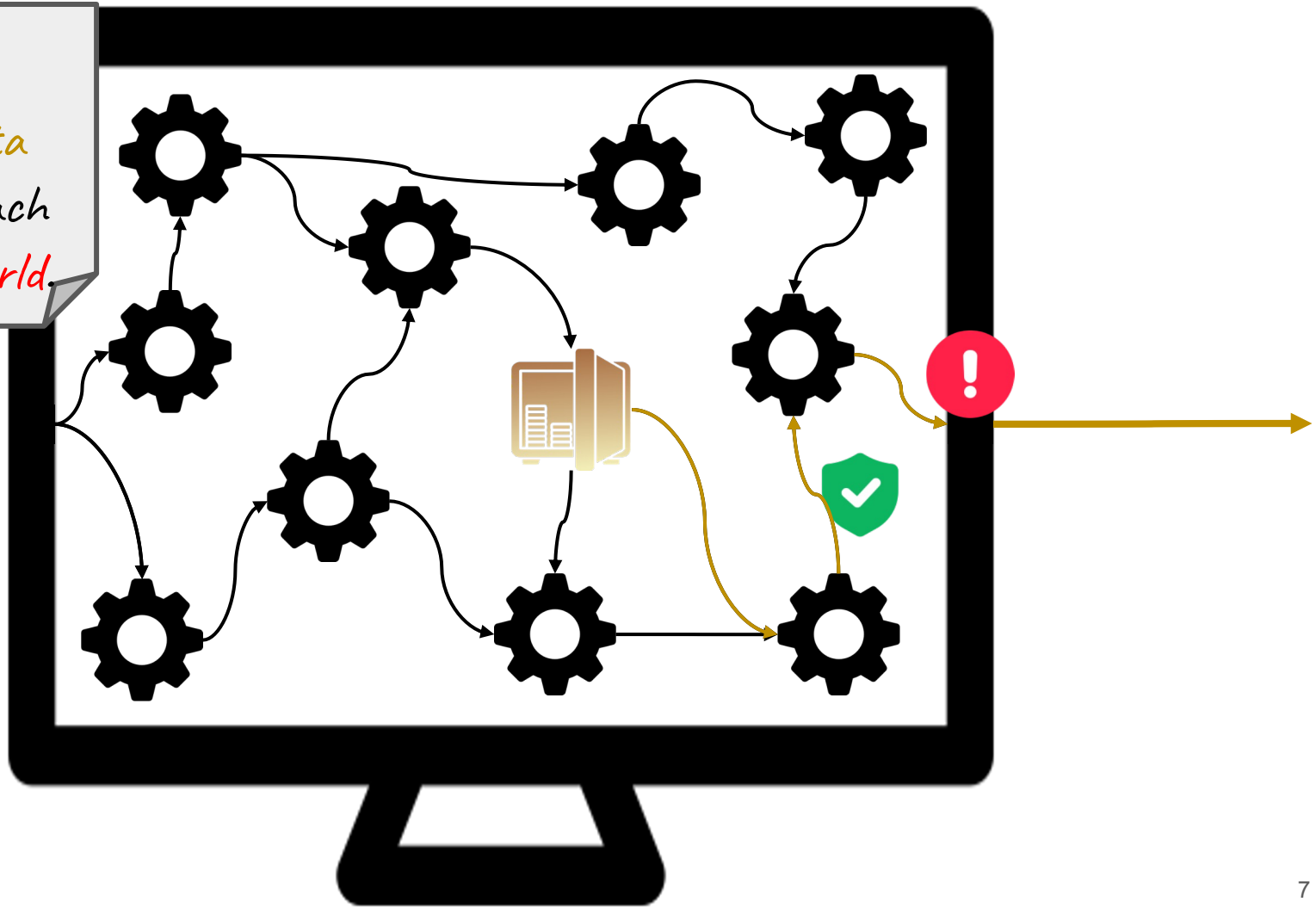
Policy

Sensitive data should not reach the outside world.



Policy

Sensitive data should not reach the outside world.



Policy (NDSS 2005)

Standard input should not reach a return address.

Policy (NDSS 2005)

Standard input should not reach a return address.

Policy (FSE 2006)

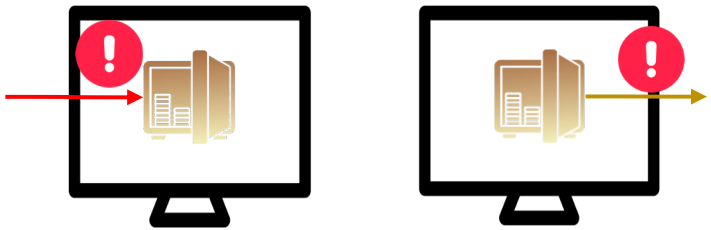
Network data should not reach a SQL query.

Policy (NDSS 2005)

Standard input should not reach a return address.

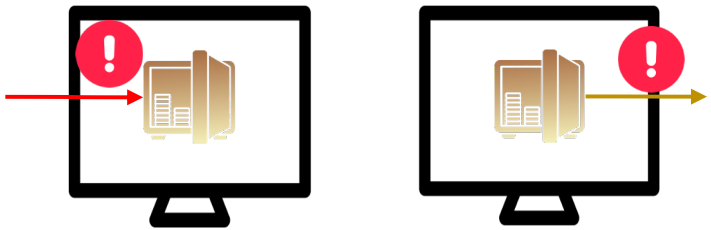
Policy (FSE 2006)

Network data should not reach a SQL query.



Policy (NDSS 2005)
Standard input should not reach a return address.

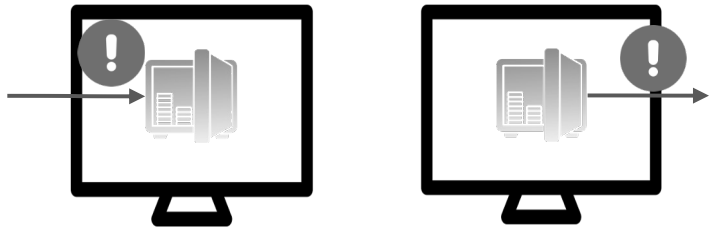
Policy (FSE 2006)
Network data should not reach a SQL query.



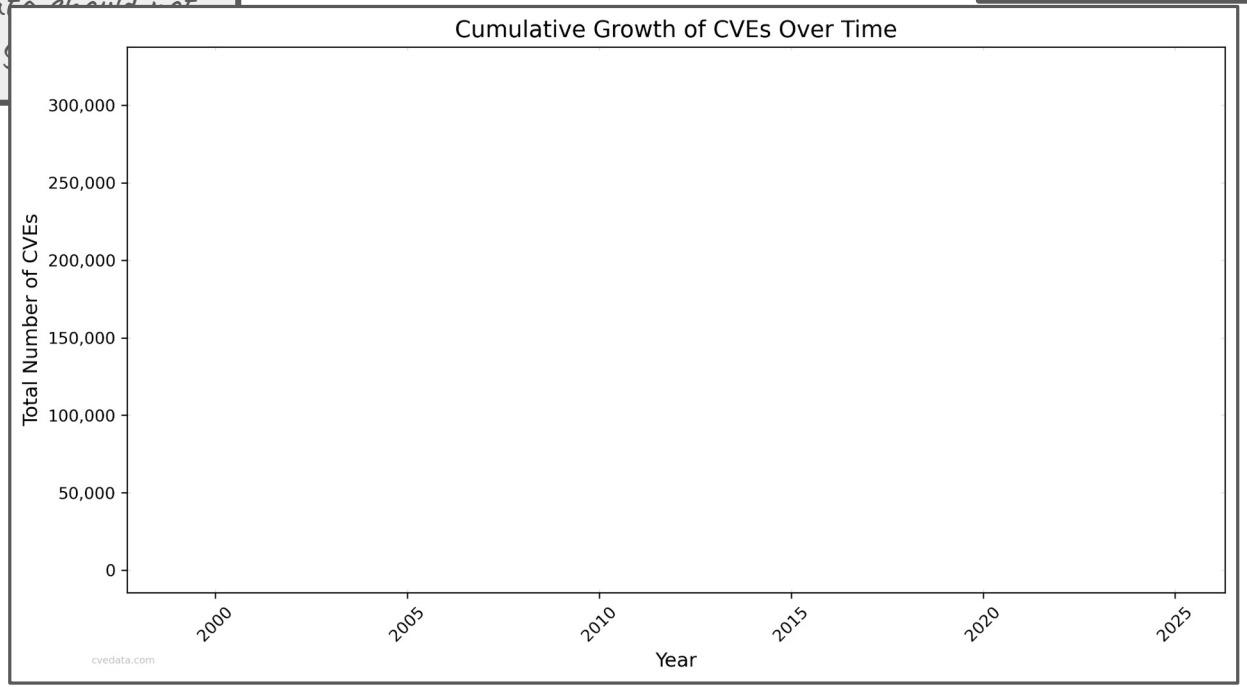
Policy (OSDI 2010)
Smartphone sensor data should not reach third-party applications.

Policy (NDSS 2005)
Standard input should not reach a return address.

Policy (FSE 2006)
Network data should not reach a

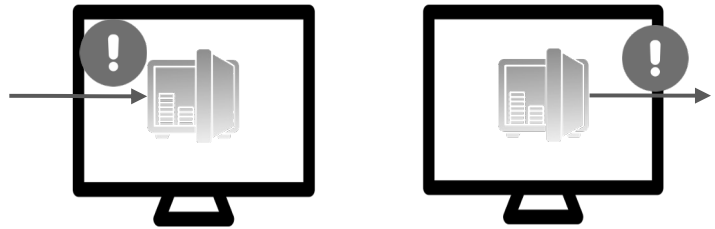


Policy (OSDI 2010)
Smartphone sensor data should not reach third-party applications.

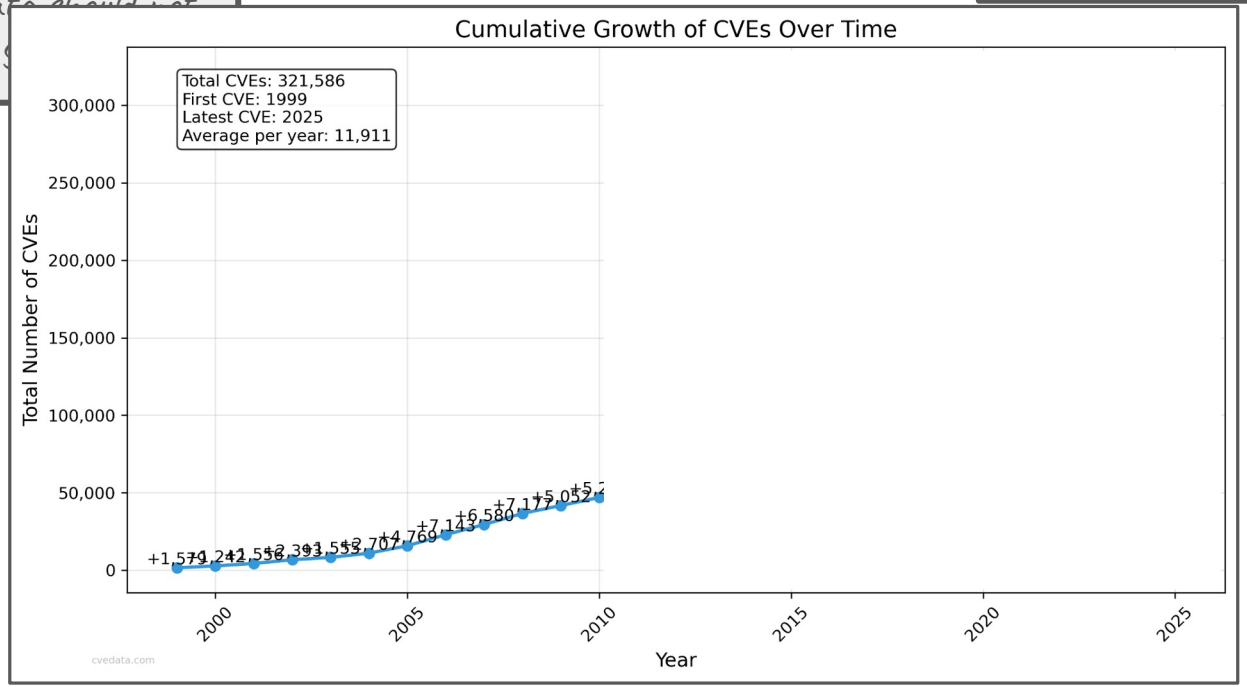


Policy (NDSS 2005)
Standard input should not reach a return address.

Policy (FSE 2006)
Network data should not reach a

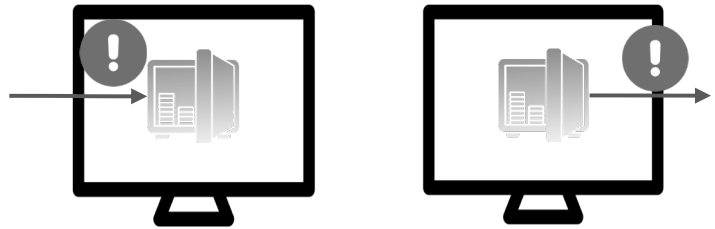


Policy (OSDI 2010)
Smartphone sensor data should not reach third-party applications.

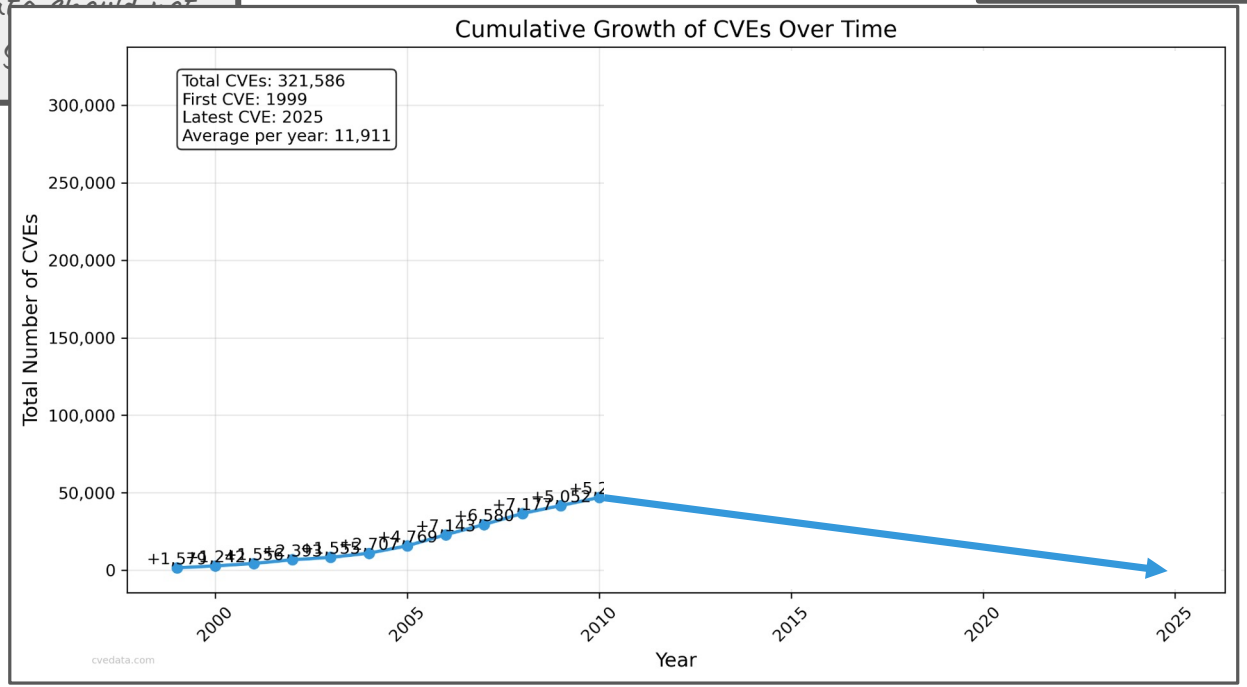


Policy (NDSS 2005)
Standard input should not reach a return address.

Policy (FSE 2006)
Network data should not reach a



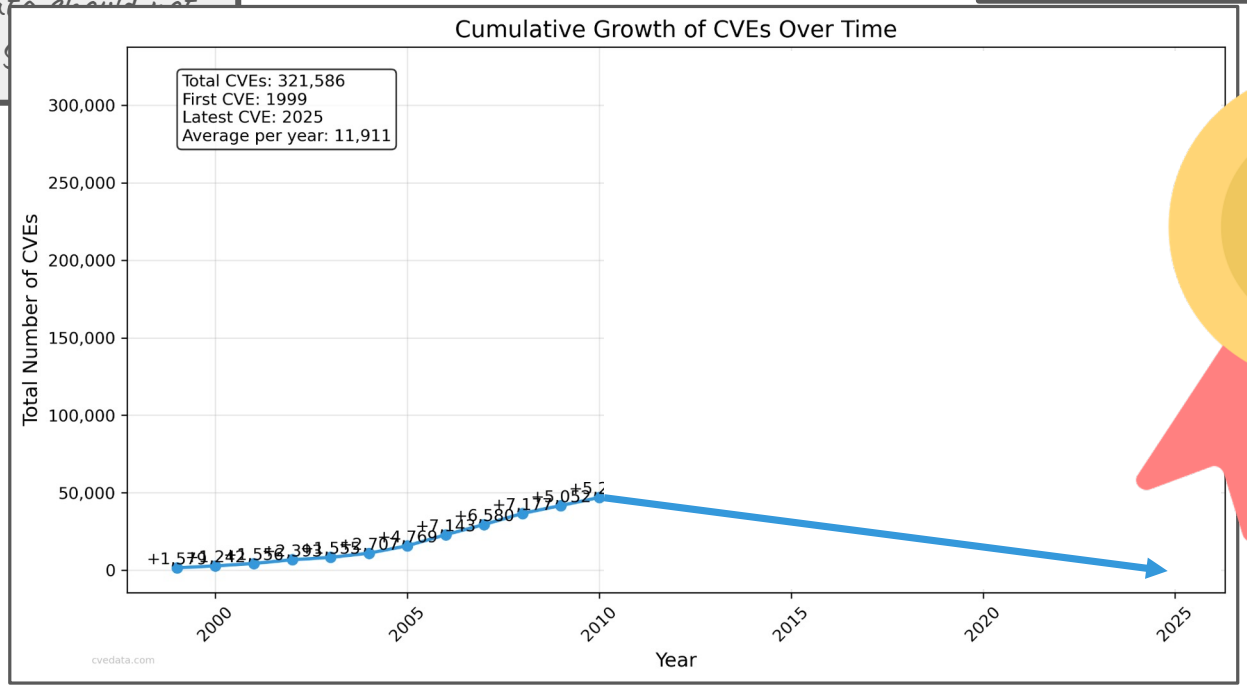
Policy (OSDI 2010)
Smartphone sensor data should not reach third-party applications.



Policy (NDSS 2005)
Standard input should not reach a return address.

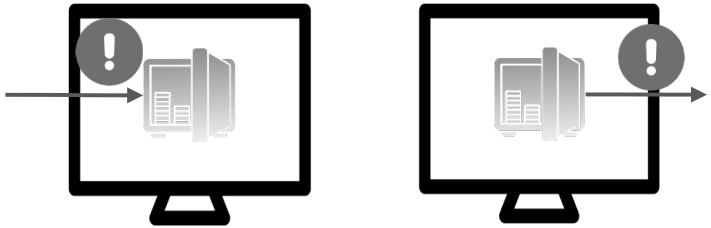
Policy (FSE 2006)
Network data should not reach a

Policy (OSDI 2010)
Smartphone sensor data should not reach third-party applications.

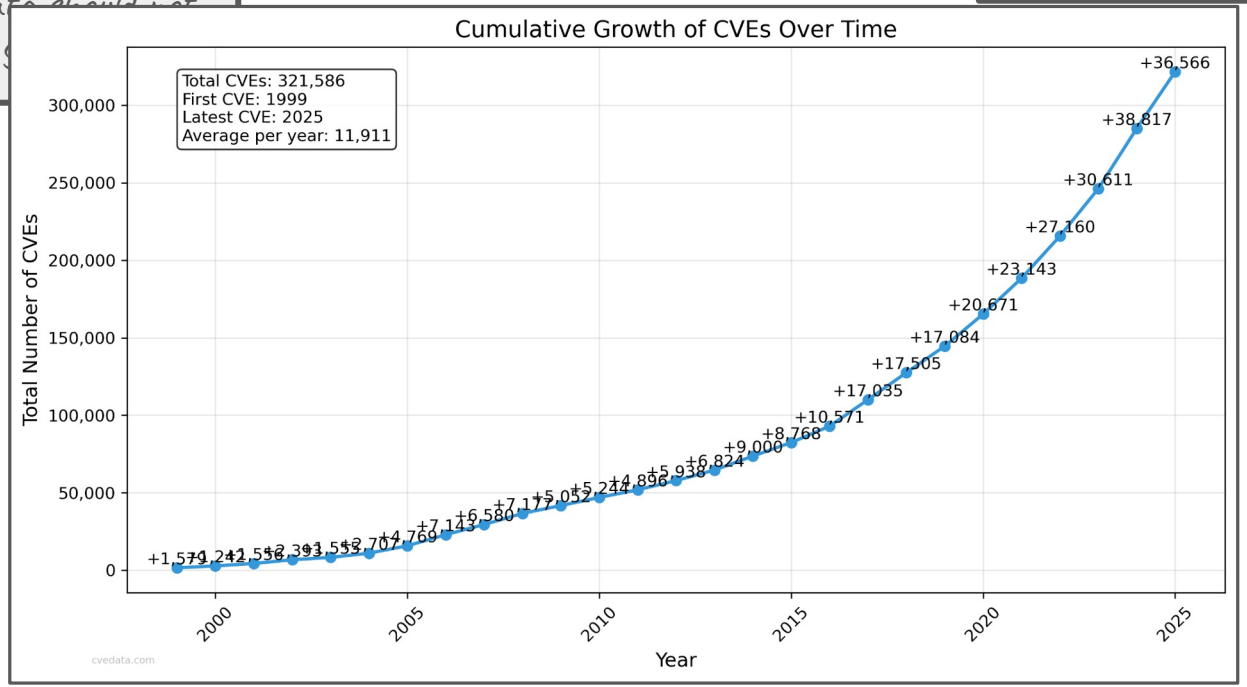


Policy (NDSS 2005)
Standard input should not reach a return address.

Policy (FSE 2006)
Network data should not reach a



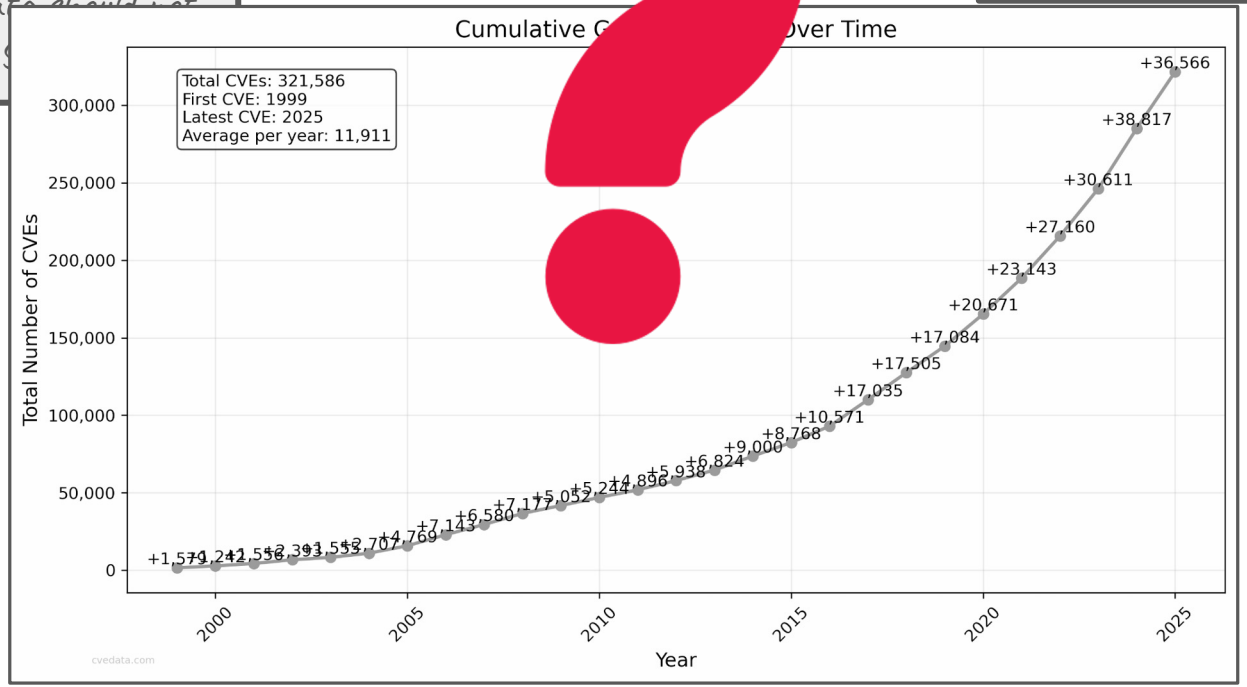
Policy (OSDI 2010)
Smartphone sensor data should not reach third-party applications.



Policy (NDSS 2005)
Standard input should not reach a return address.

Policy (FSE 2006)
Network data should not reach a

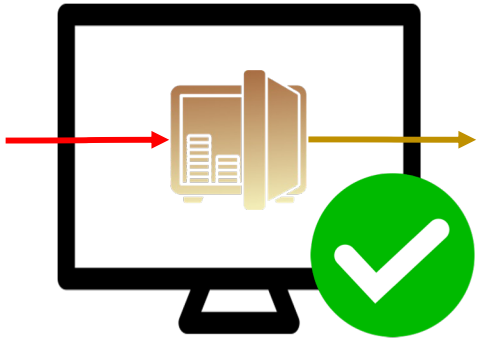
Policy (OSDI 2010)
Smartphone sensor data should not reach third-party applications.



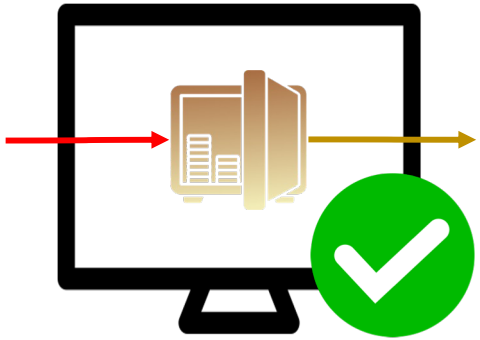
*Previous approaches: Modeled specific **exploit techniques**.*

*Previous approaches: Modeled specific **exploit techniques**.*

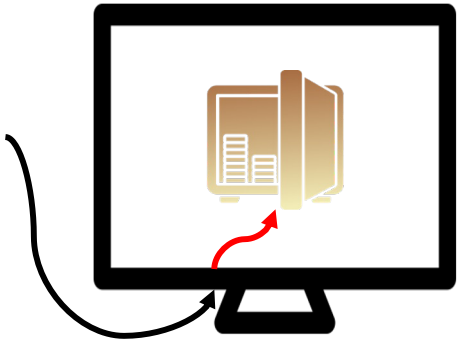
*Previous approaches: Modeled specific **exploit techniques**.*



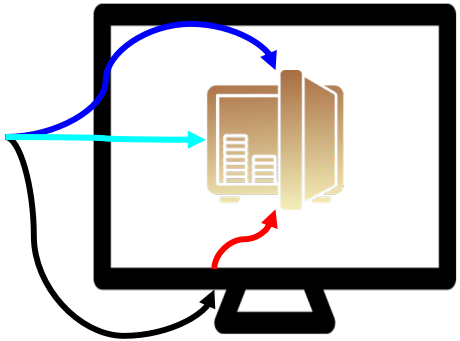
*Previous approaches: Modeled specific **exploit techniques**.*



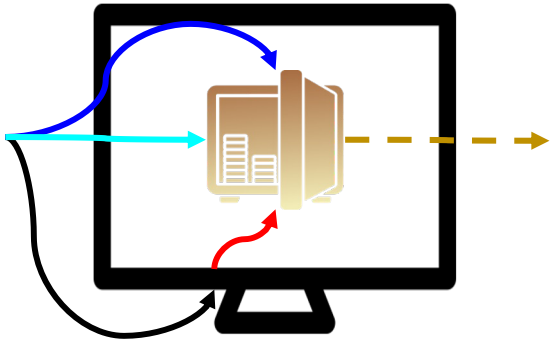
*Previous approaches: Modeled specific **exploit techniques**.*



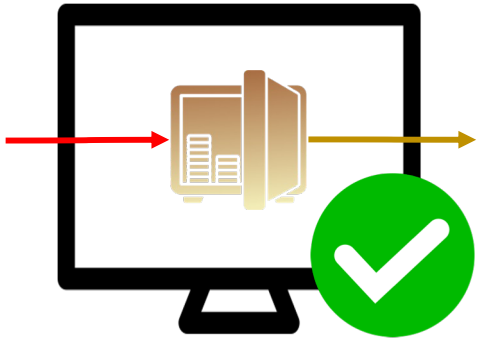
*Previous approaches: Modeled specific **exploit techniques**.*

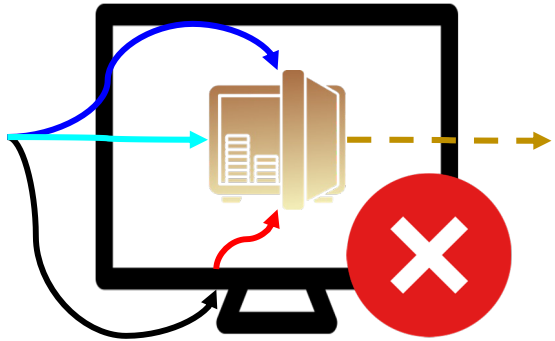


*Previous approaches: Modeled specific **exploit techniques**.*

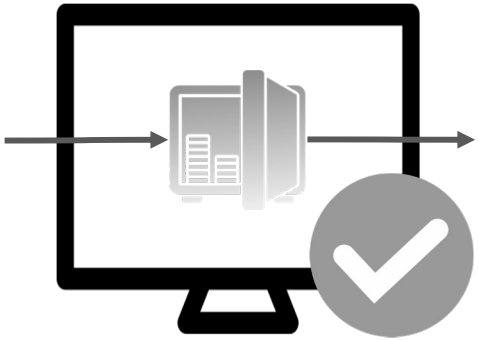


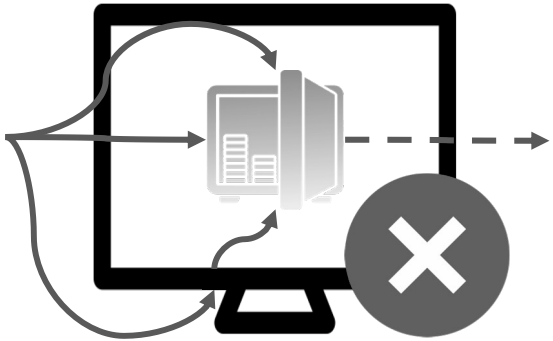
*Previous approaches: Modeled specific **exploit techniques**.*



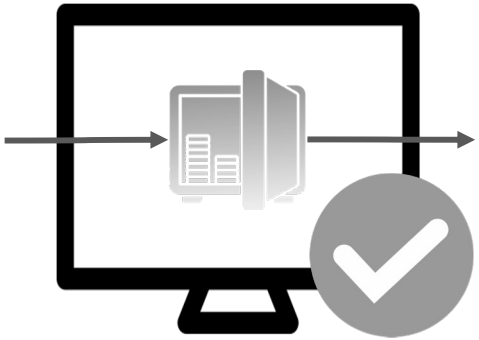


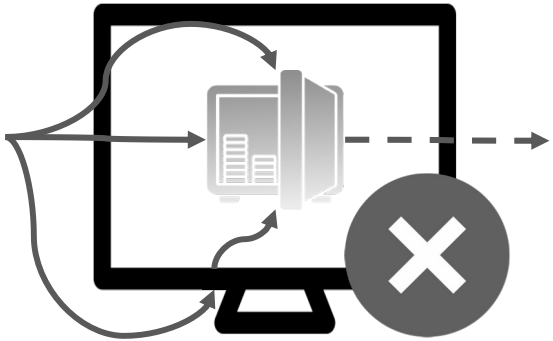
*Previous approaches: Modeled specific **exploit techniques**.*





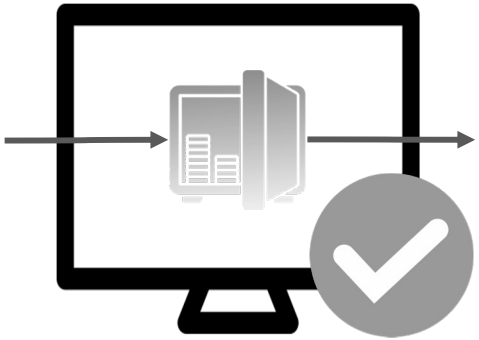
*Previous approaches: Modeled specific **exploit techniques**.*

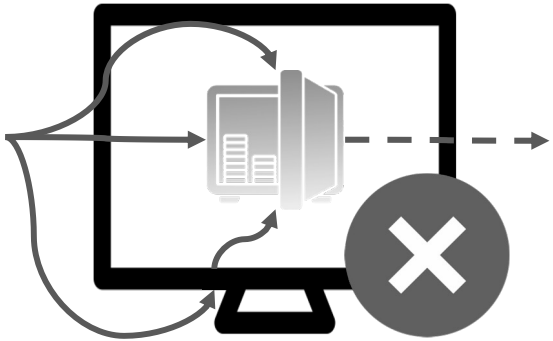




*Our approach: Model the **essential steps of a vulnerability**.*

*Previous approaches: Modeled specific **exploit techniques**.*

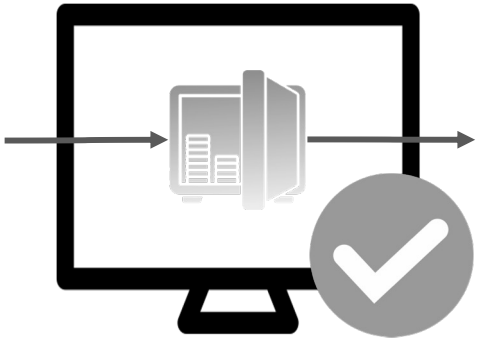


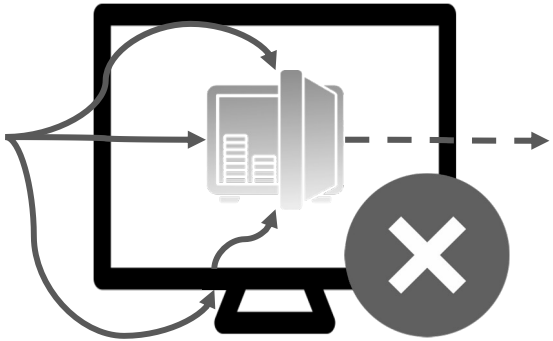


*Our approach: Model the **essential steps of a vulnerability**.*

- *Identifies modern vulnerabilities*

*Previous approaches: Modeled specific **exploit techniques**.*



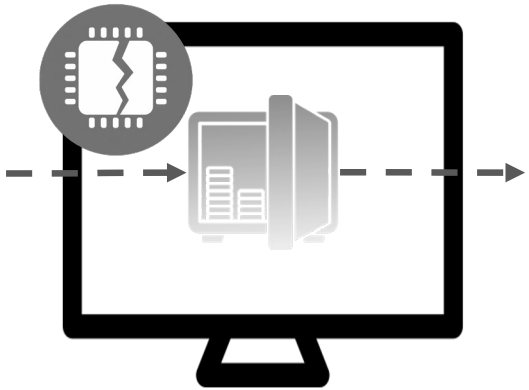


*Our approach: Model the **essential steps of a vulnerability**.*

- *Identifies modern vulnerabilities*
- *Reduce false alarms.*

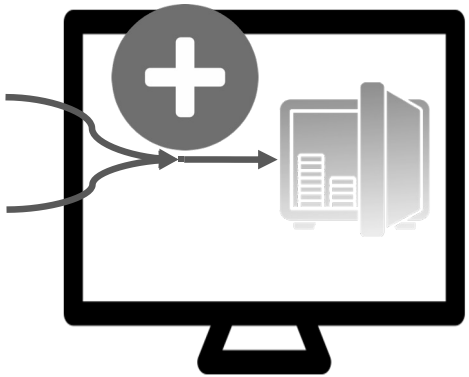
Explicit vulnerability modeling: ***Case studies***

Explicit vulnerability modeling: ***Case studies***



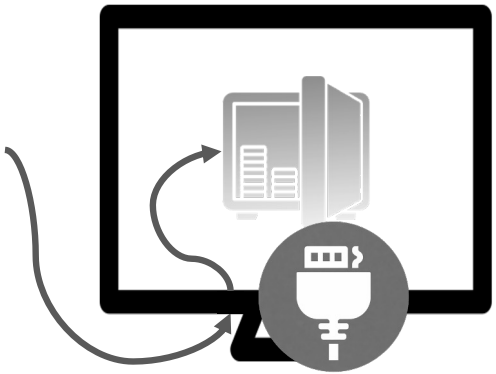
Kasper

(NDSS 2022)



Einstein

(USENIX Sec. 2024)



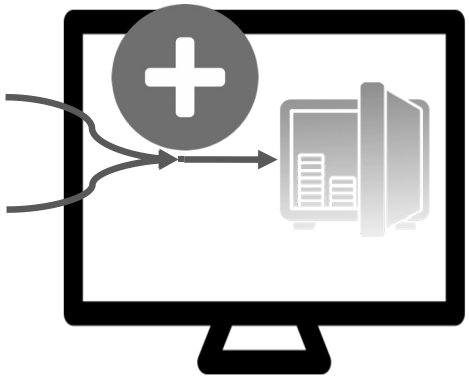
DMARacer

(CCS 2025)

Explicit vulnerability modeling: ***Case studies***

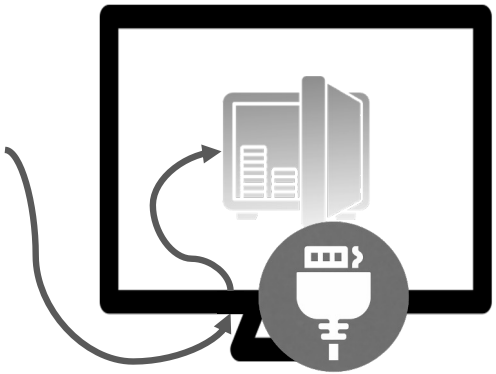
Kasper

(NDSS 2022)



Einstein

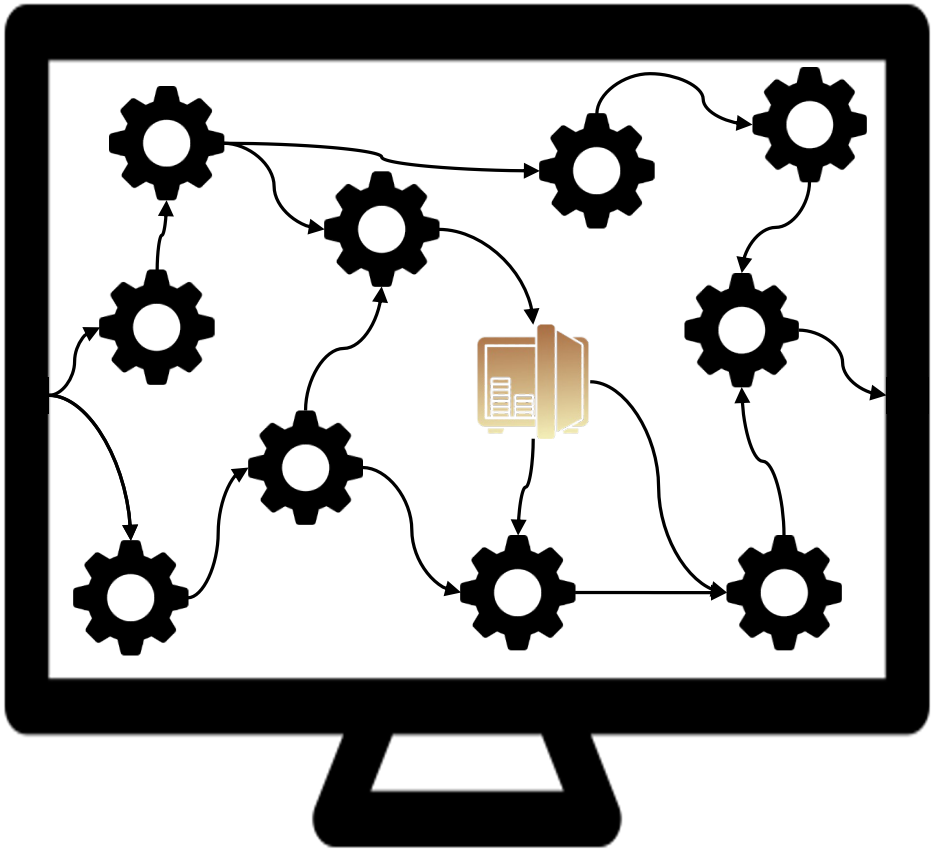
(USENIX Sec. 2024)



DMARacer

(CCS 2025)

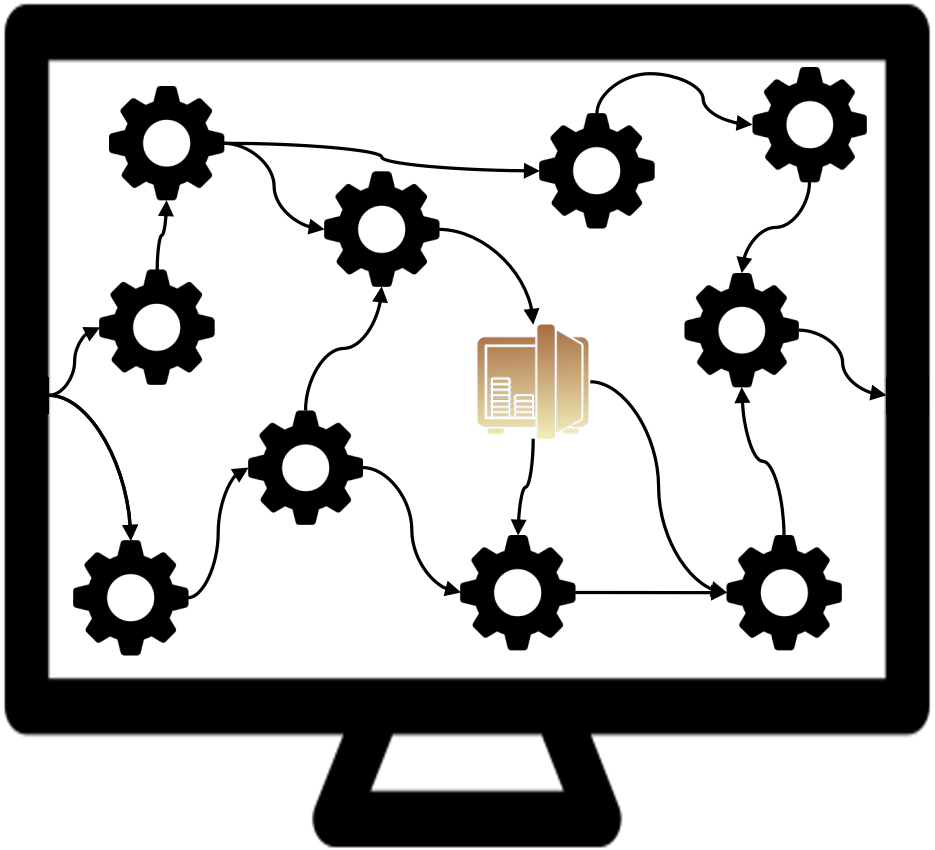
Kasper



Kasper

Branch Misprediction

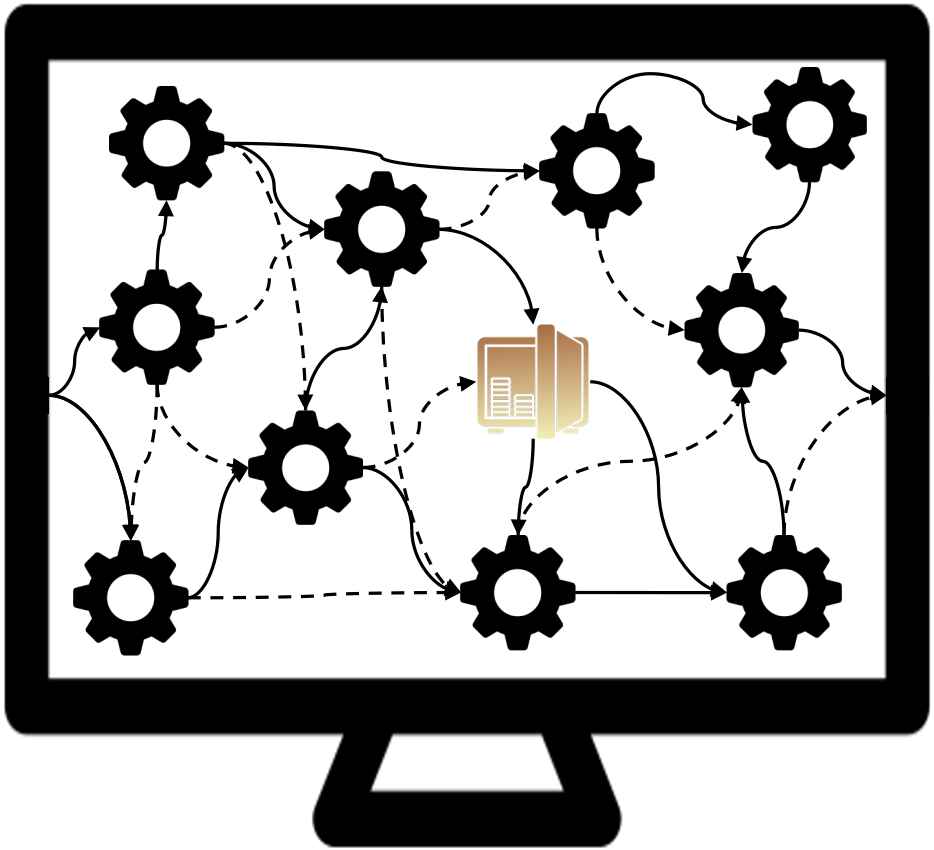
Divert conditional branches.



Kasper

Branch Misprediction

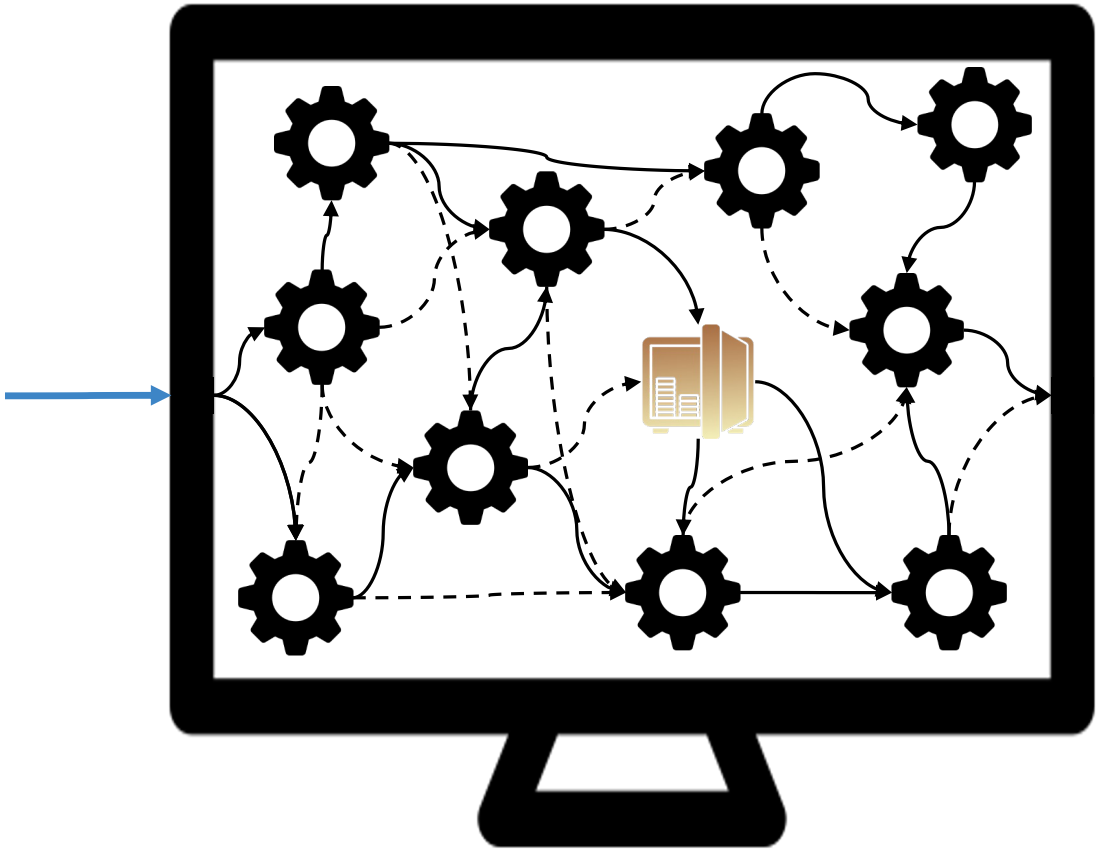
Divert conditional branches.



Kasper

Branch Misprediction

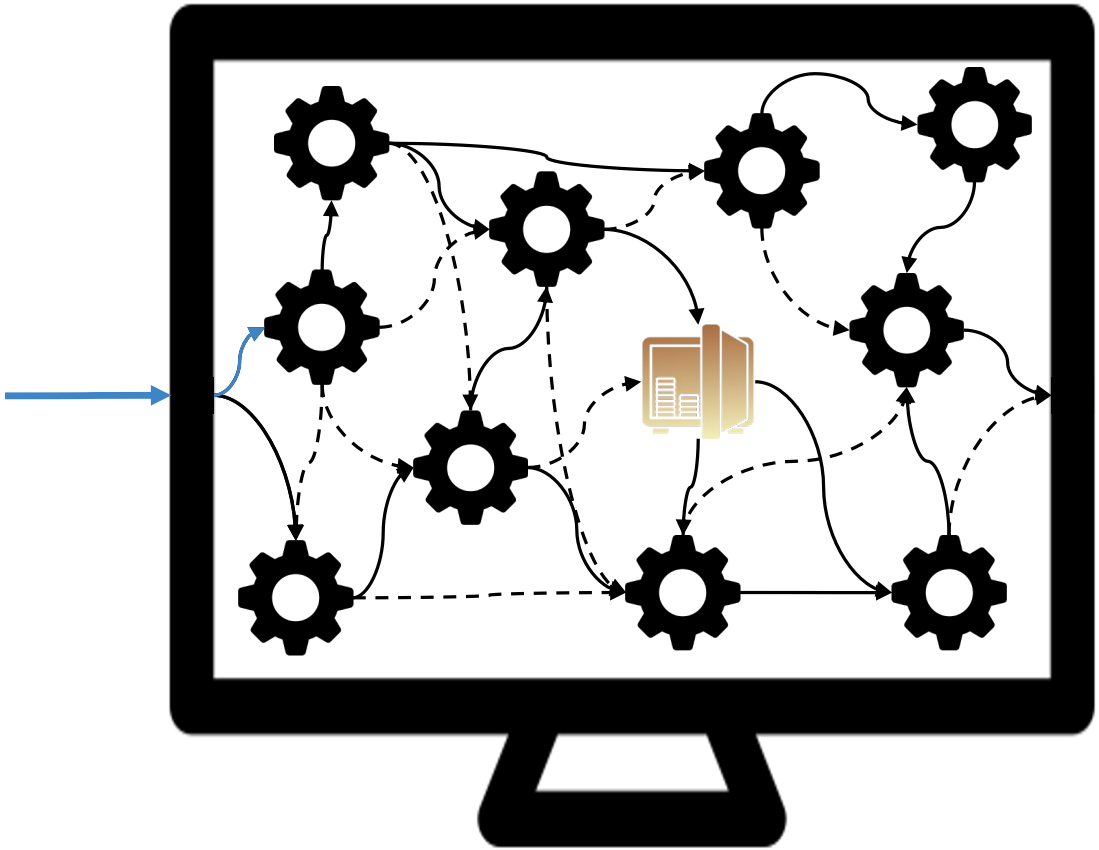
Divert conditional branches.



Kasper

Branch Misprediction

Divert conditional branches.



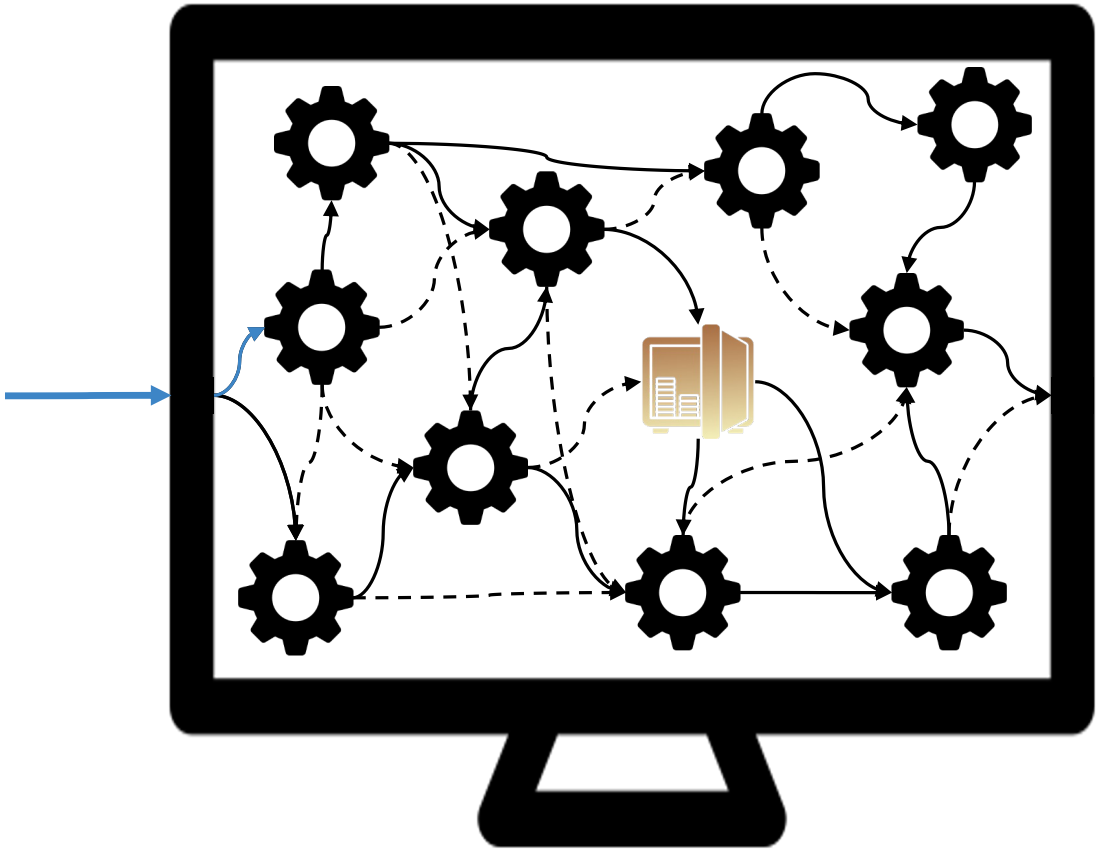
Kasper

Branch Misprediction

Divert conditional branches.

LVI

Invalid transient loads inject attacker data.



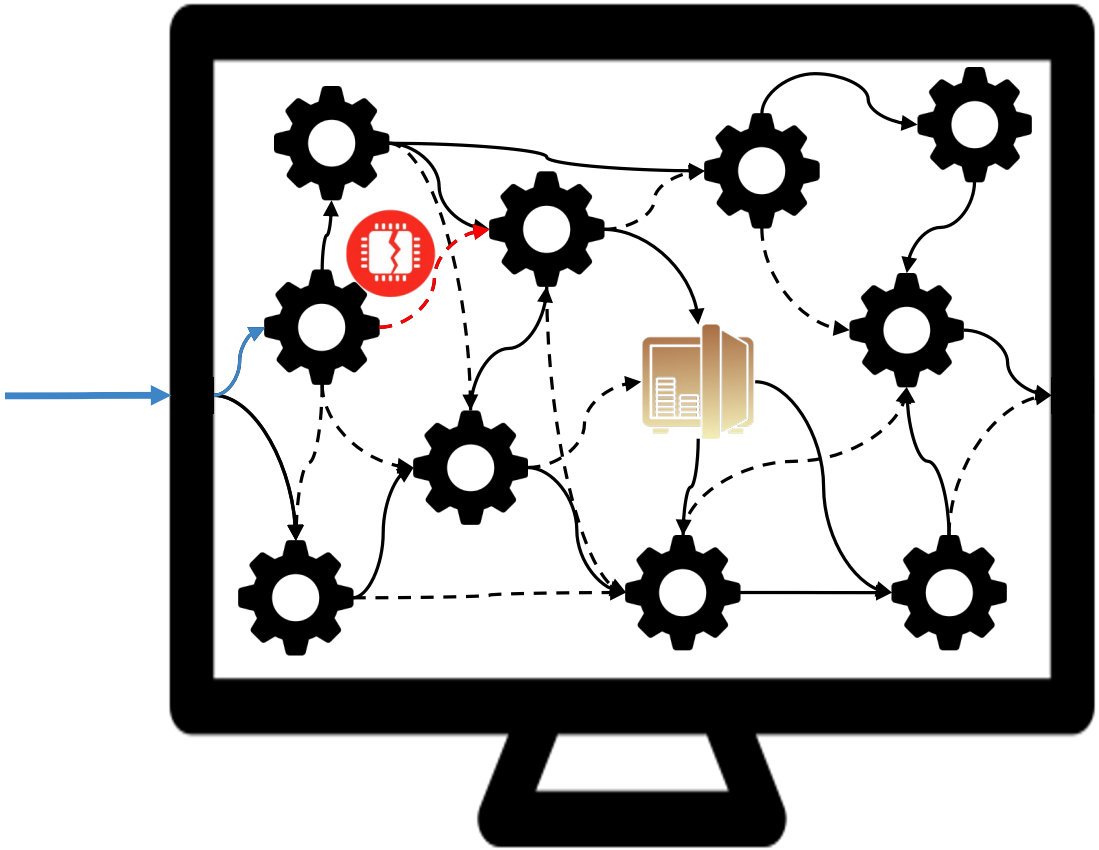
Kasper

Branch Misprediction

Divert conditional branches.

LVI

Invalid transient loads inject attacker data.



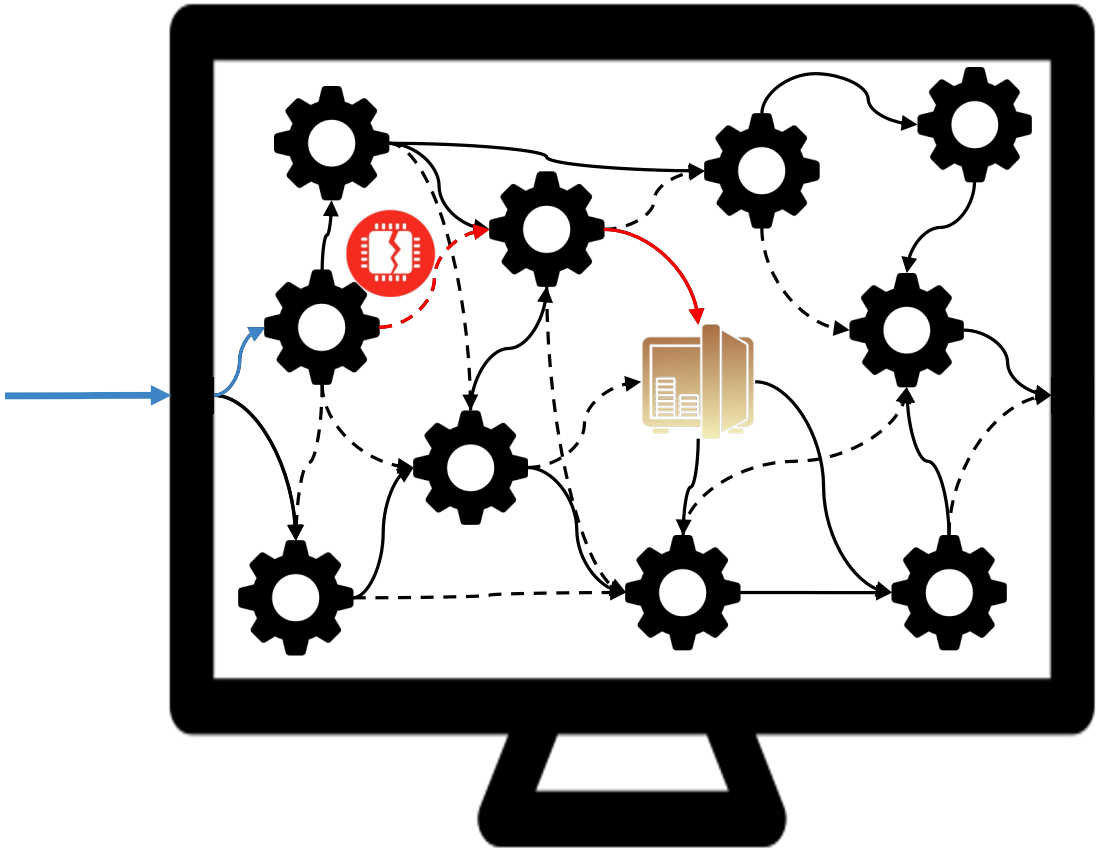
Kasper

Branch Misprediction

Divert conditional branches.

LVI

Invalid transient loads inject attacker data.



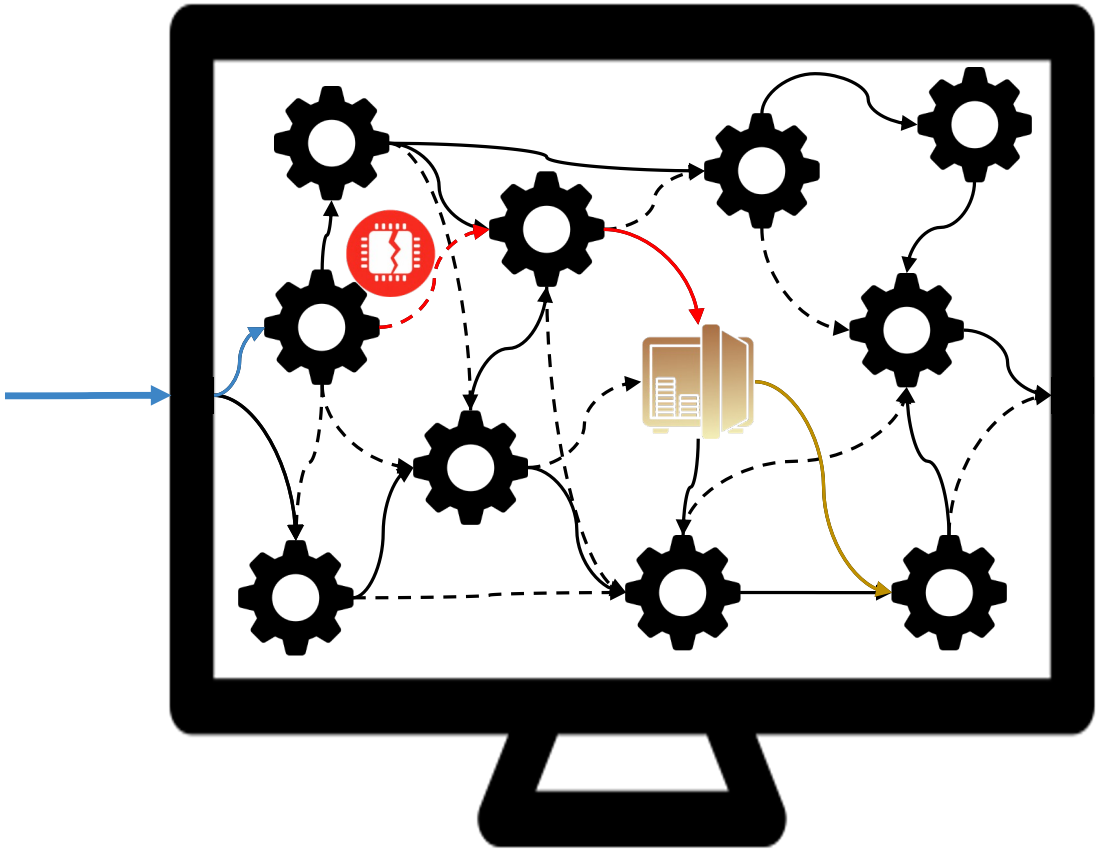
Kasper

Branch Misprediction

Divert conditional branches.

LVI

Invalid transient loads inject attacker data.



Kasper

Branch Misprediction

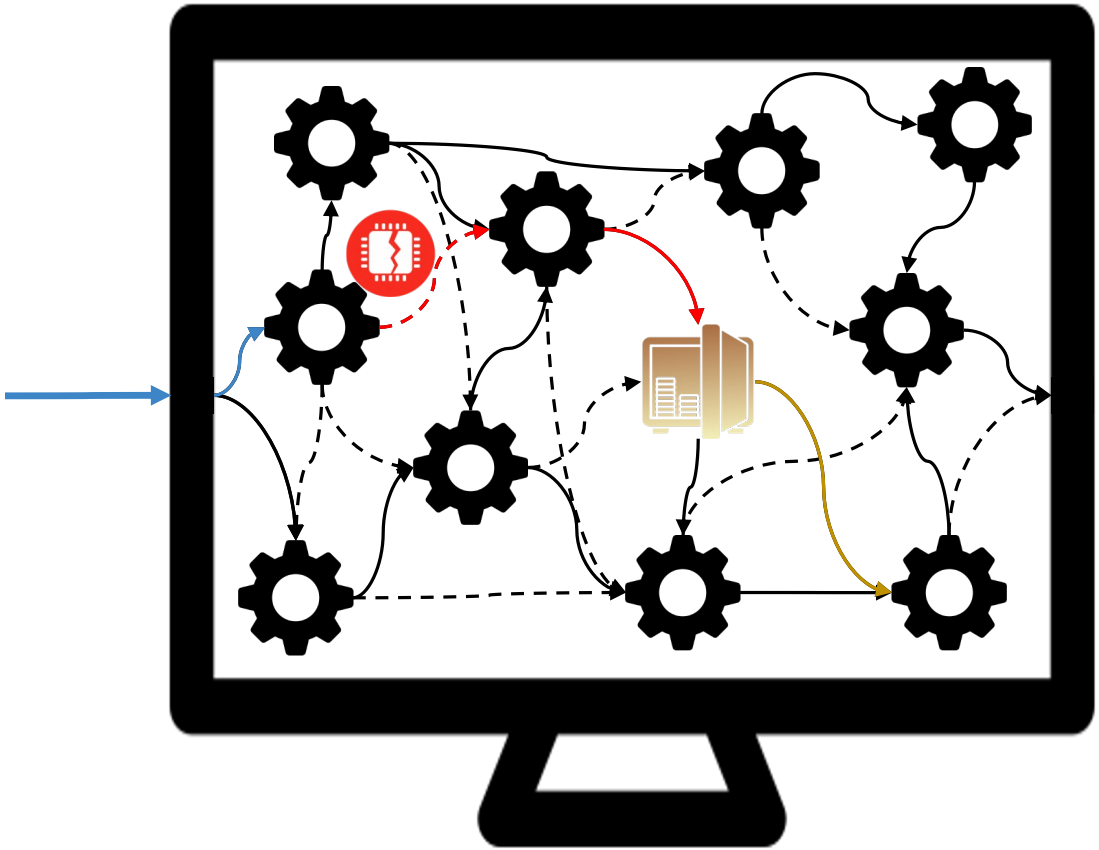
Divert conditional branches.

LVI

Invalid transient loads inject attacker data.

Cache Contention

Dereferencing an secret pointer leaks it.



Kasper

Branch Misprediction

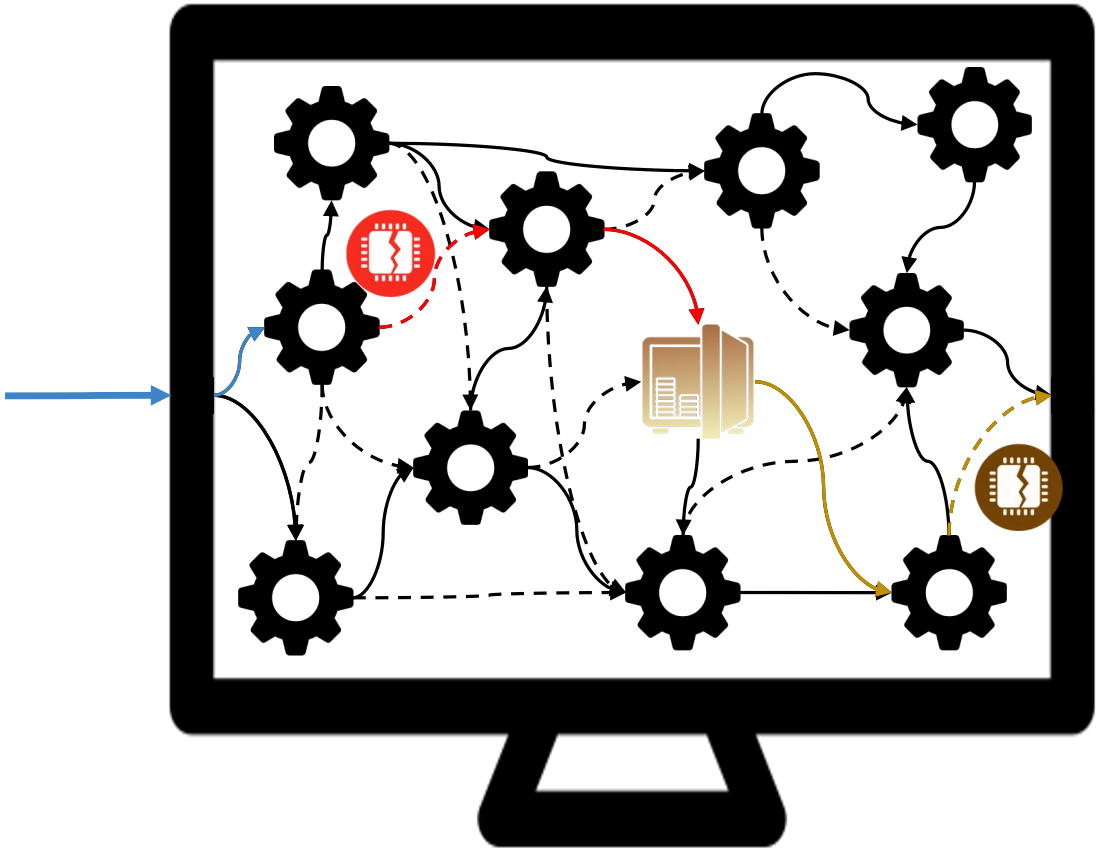
Divert conditional branches.

LVI

Invalid transient loads inject attacker data.

Cache Contention

Dereferencing an secret pointer leaks it.



Kasper

Branch Misprediction

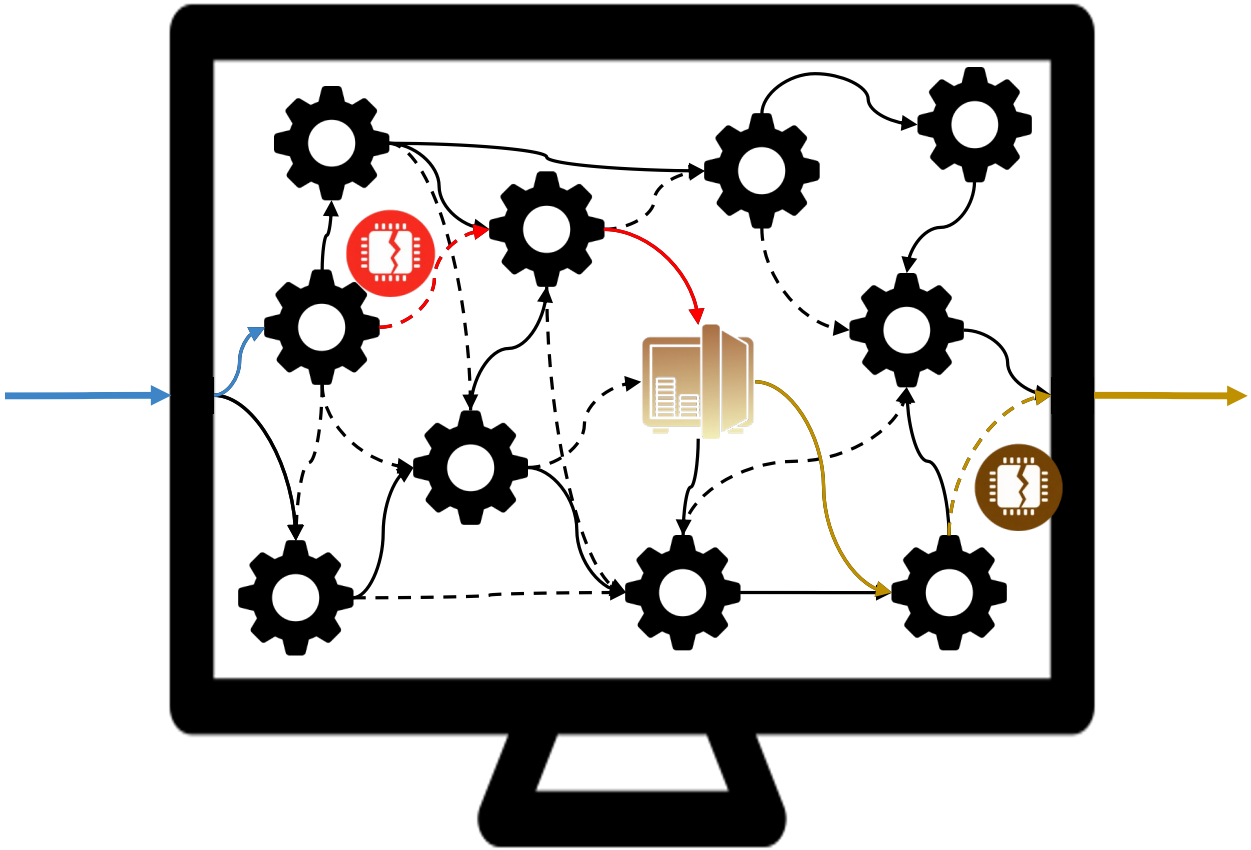
Divert conditional branches.

LVI

Invalid transient loads inject attacker data.

Cache Contention

Dereferencing an secret pointer leaks it.



Kasper

Branch Misprediction

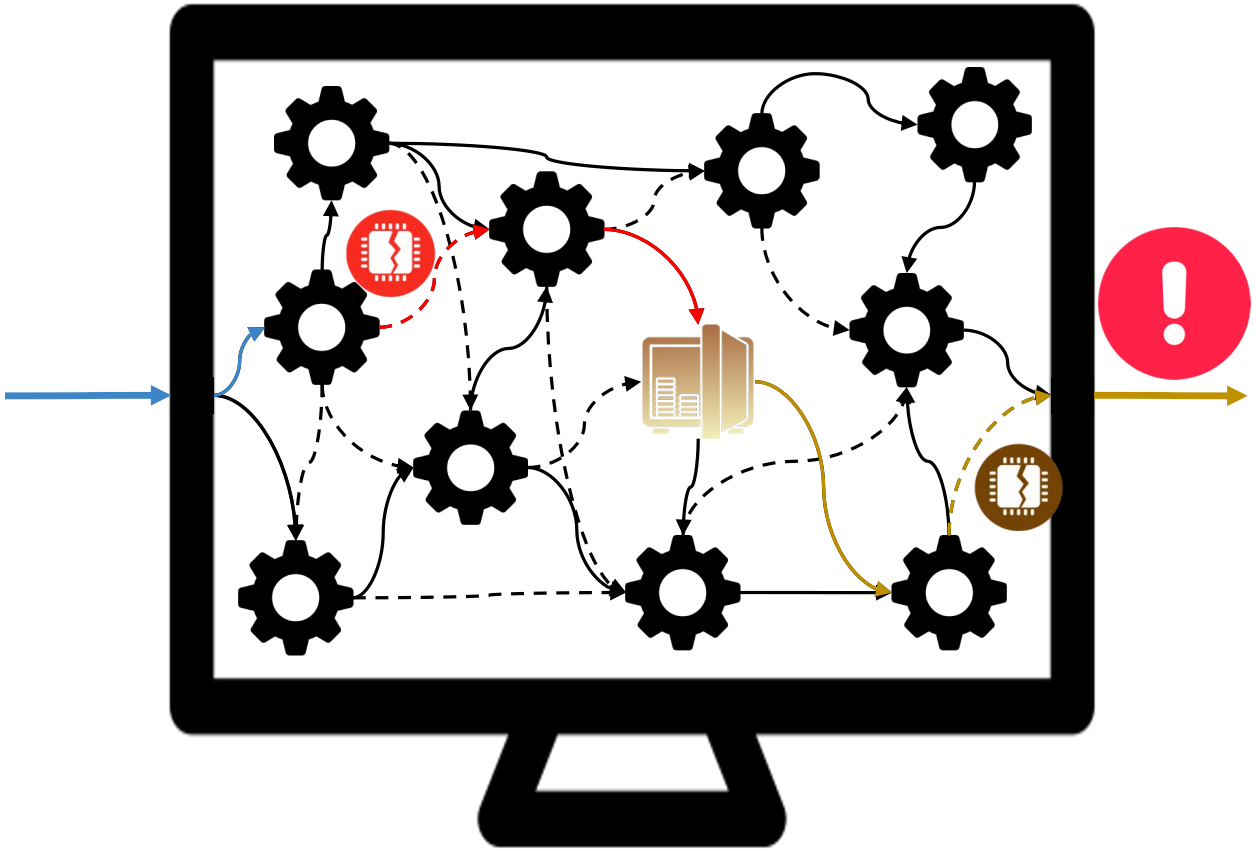
Divert conditional branches.

LVI

Invalid transient loads inject attacker data.

Cache Contention

Dereferencing an secret pointer leaks it.



Kasper

Branch Misprediction
Divert conditional branches.

Memory Massaging
Unsafe transient

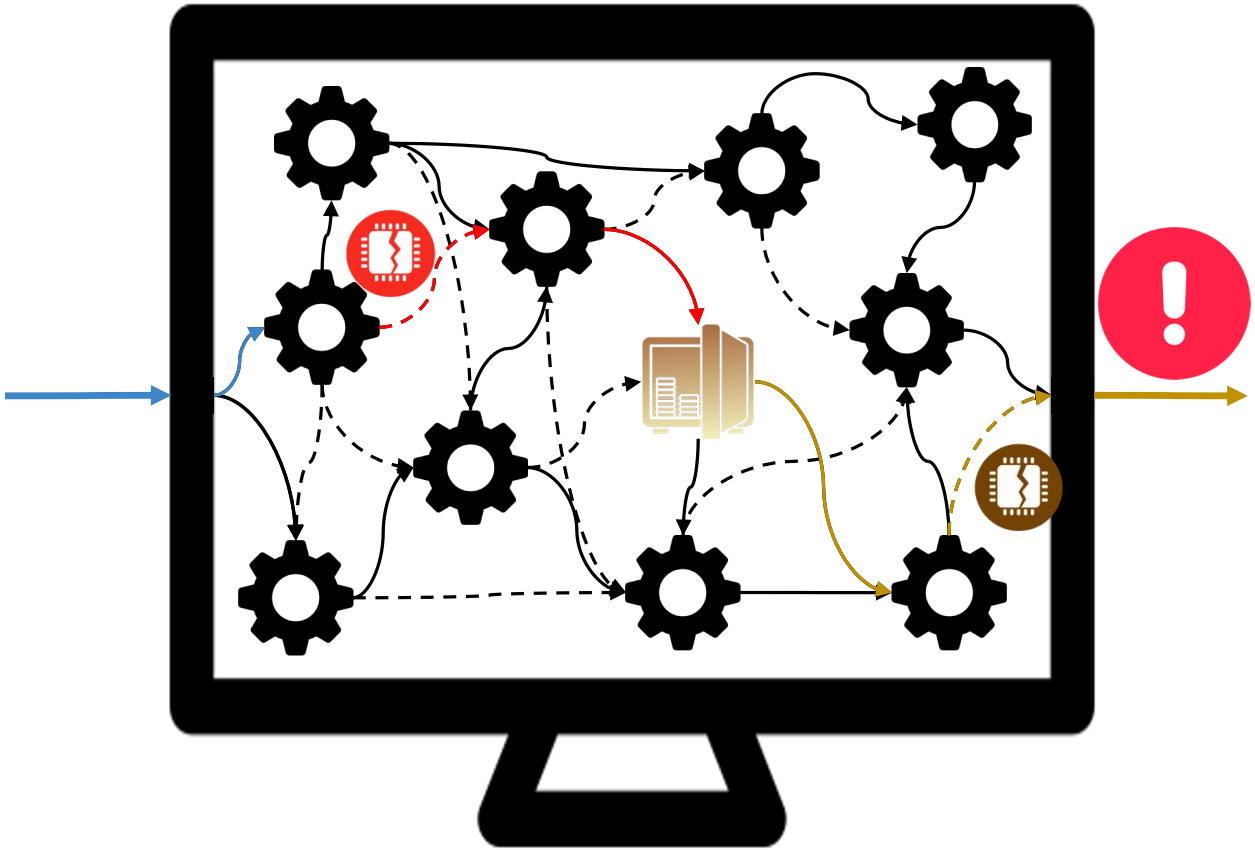
LVI
Invalid transient loads inject attacker data.

User Data
Syscall arguments and
cercopies inject attacker data.

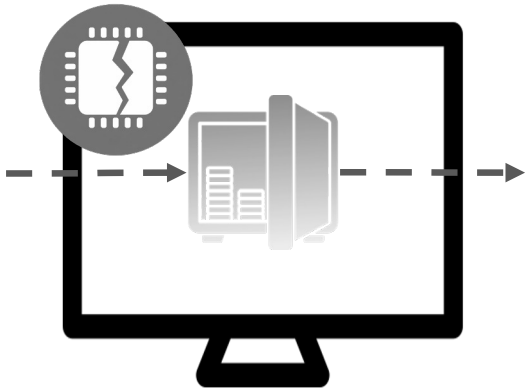
Port Contention
Branching on a
leak

MDS
acker
et it

Cache Contention
Dereferencing an secret pointer leaks it.

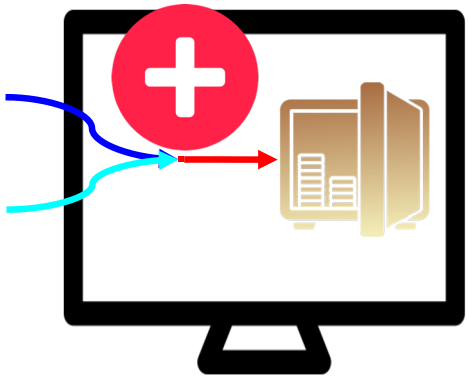


Explicit vulnerability modeling: ***Case studies***



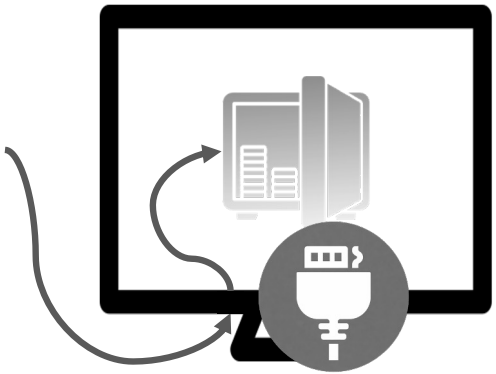
Kasper

(NDSS 2022)



Einstein

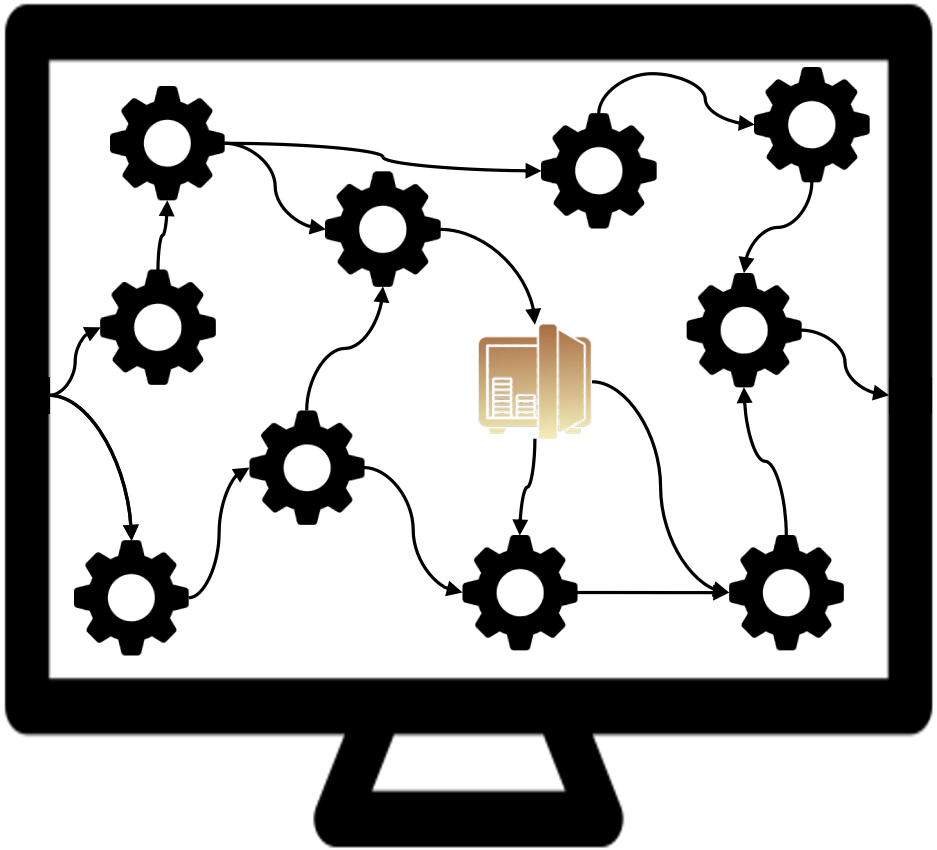
(USENIX Sec. 2024)



DMARacer

(CCS 2025)

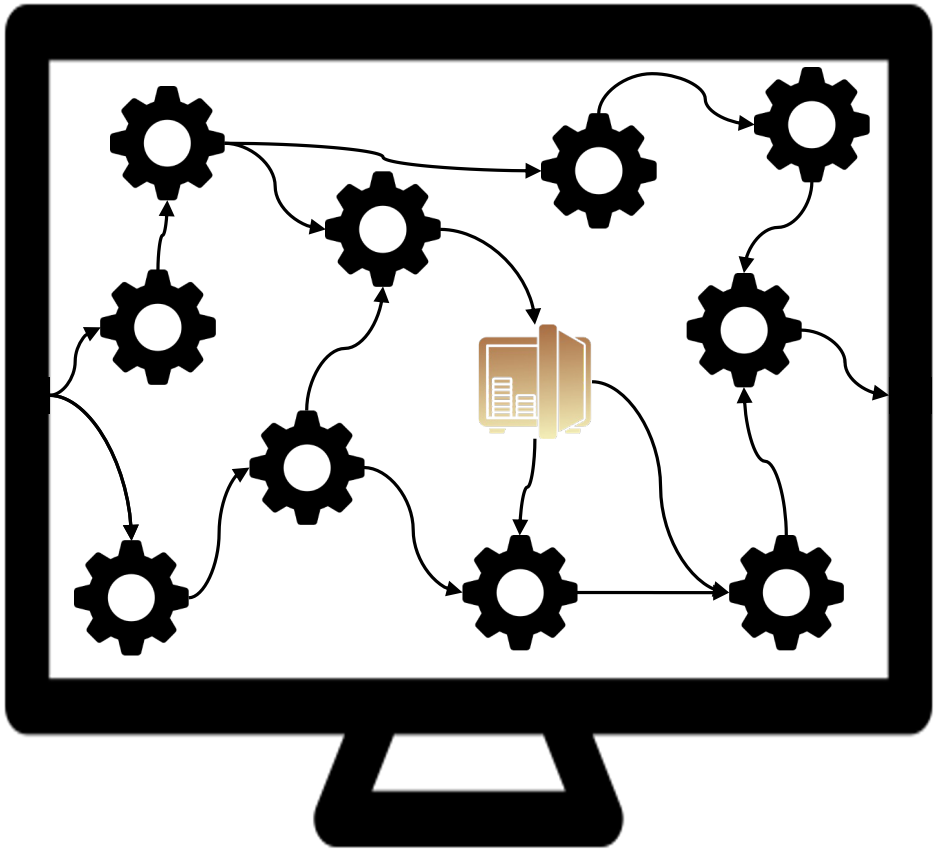
Einstein



Einstein

Memory Write Primitive

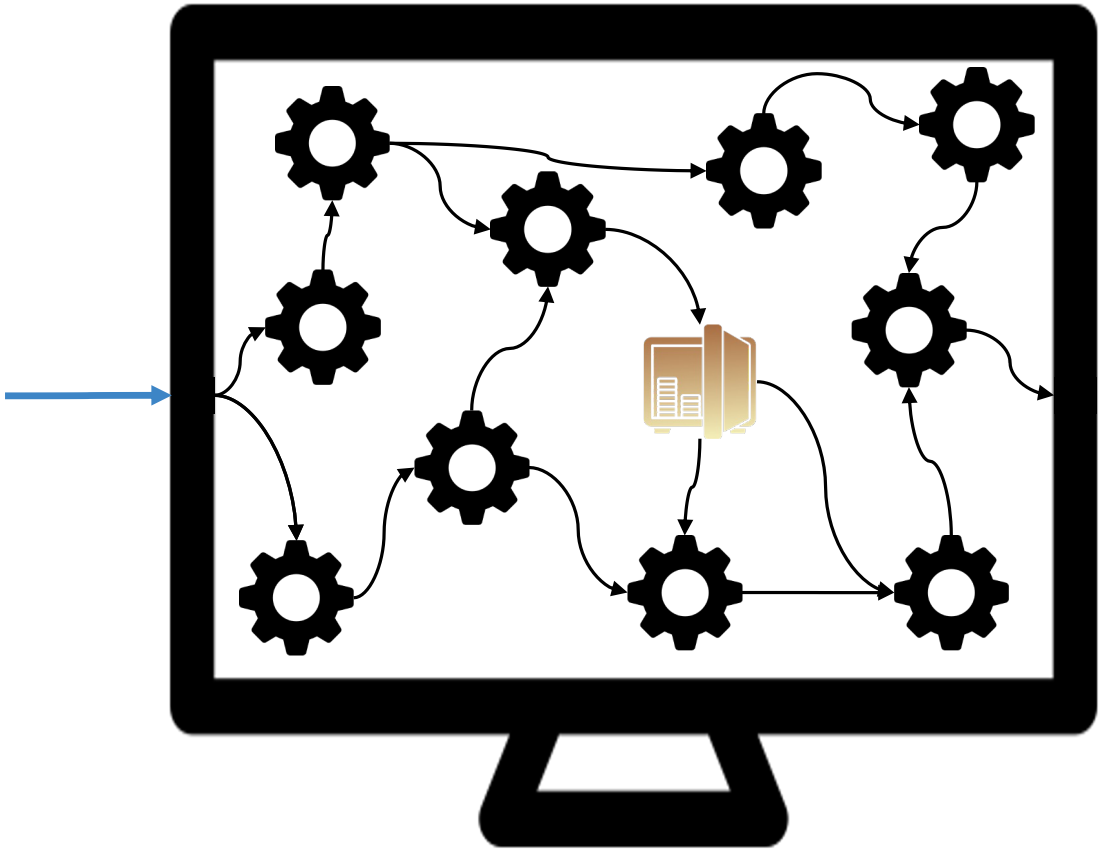
Any corruptible data is attacker data.



Einstein

Memory Write Primitive

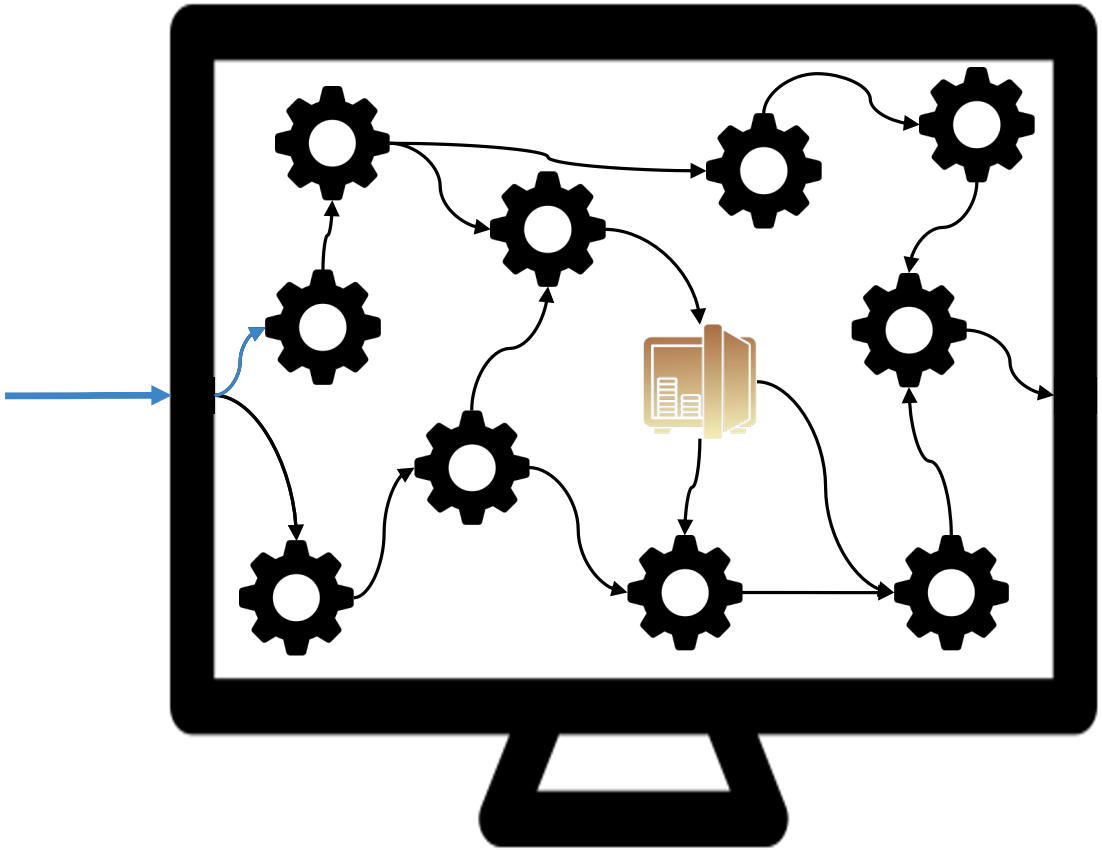
Any corruptible data is attacker data.



Einstein

Memory Write Primitive

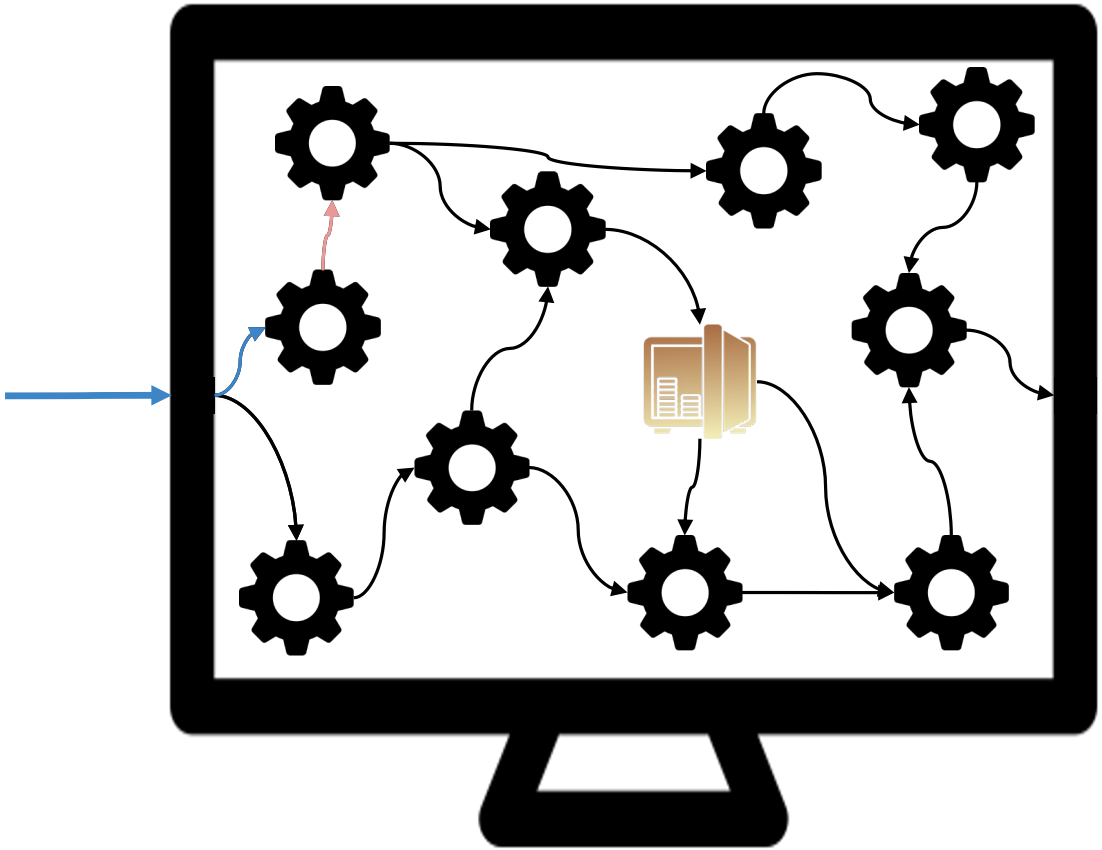
Any corruptible data is attacker data.



Einstein

Memory Write Primitive

Any corruptible data is attacker data.



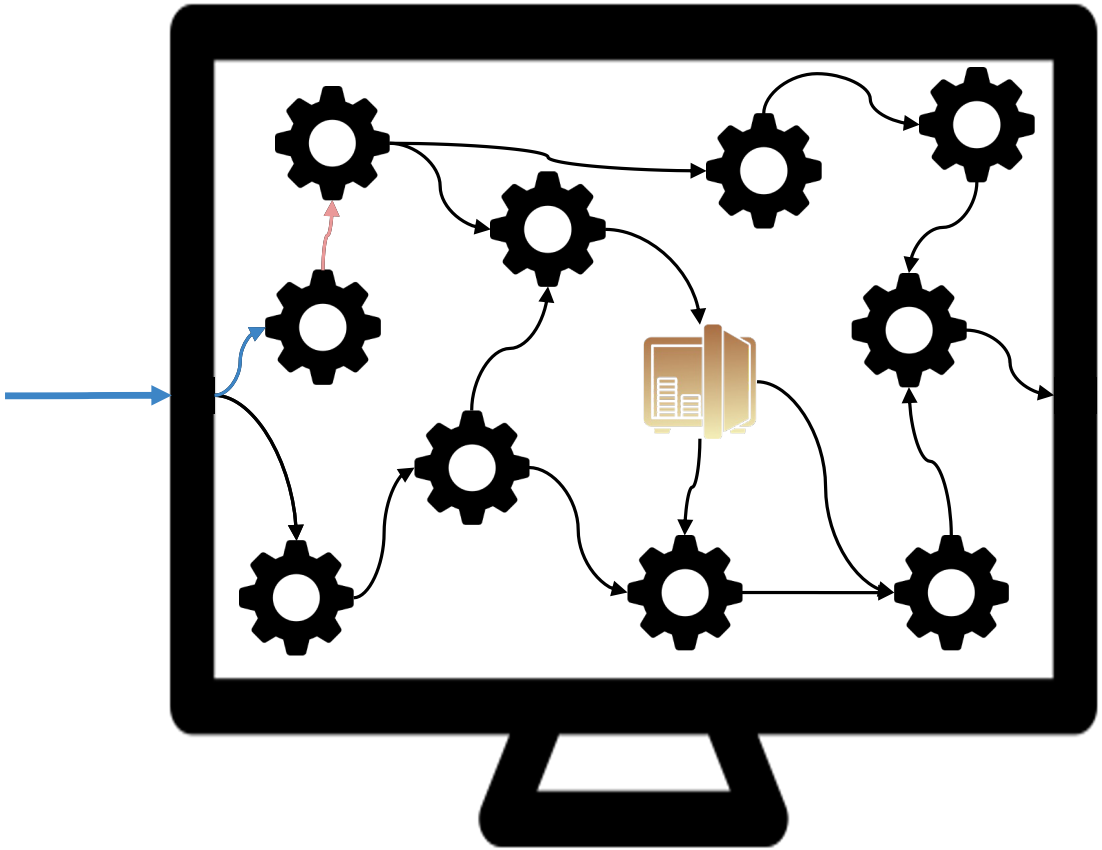
Einstein

Memory Write Primitive

Any corruptible data is attacker data.

openat

Attacker argument generates an attacker file.



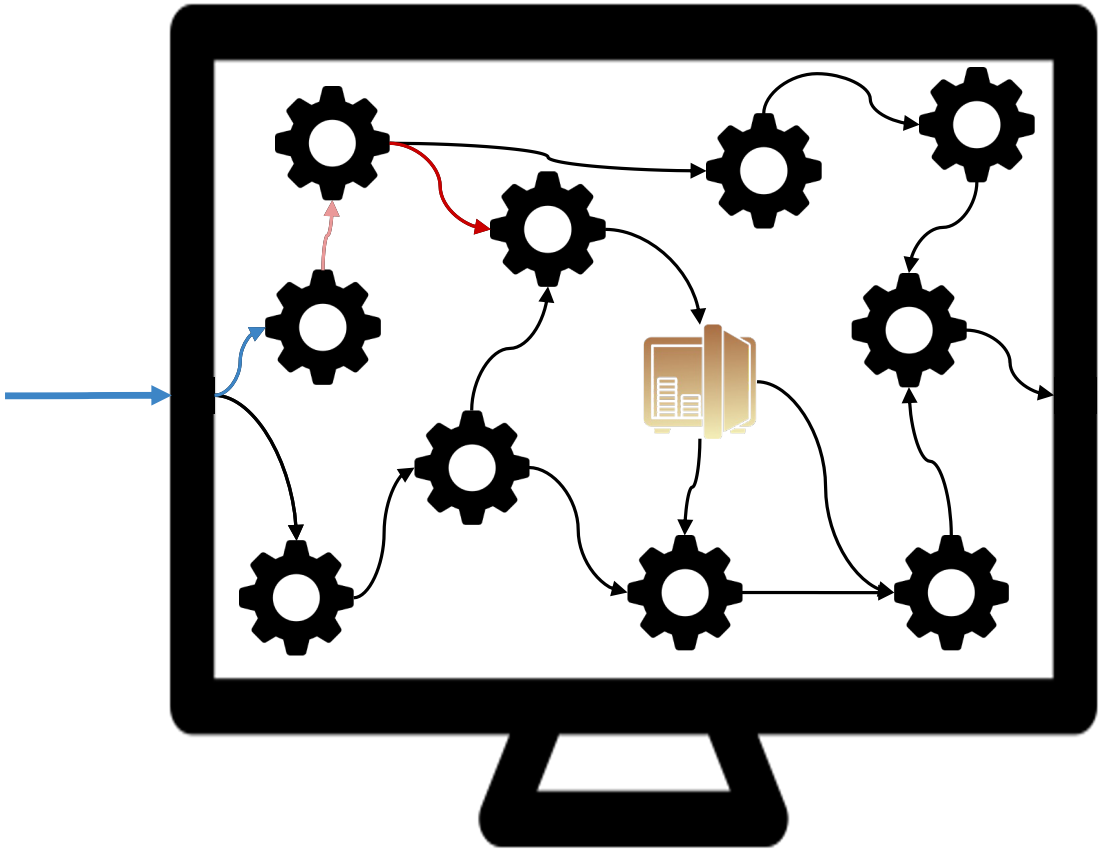
Einstein

Memory Write Primitive

Any corruptible data is attacker data.

openat

Attacker argument generates an attacker file.



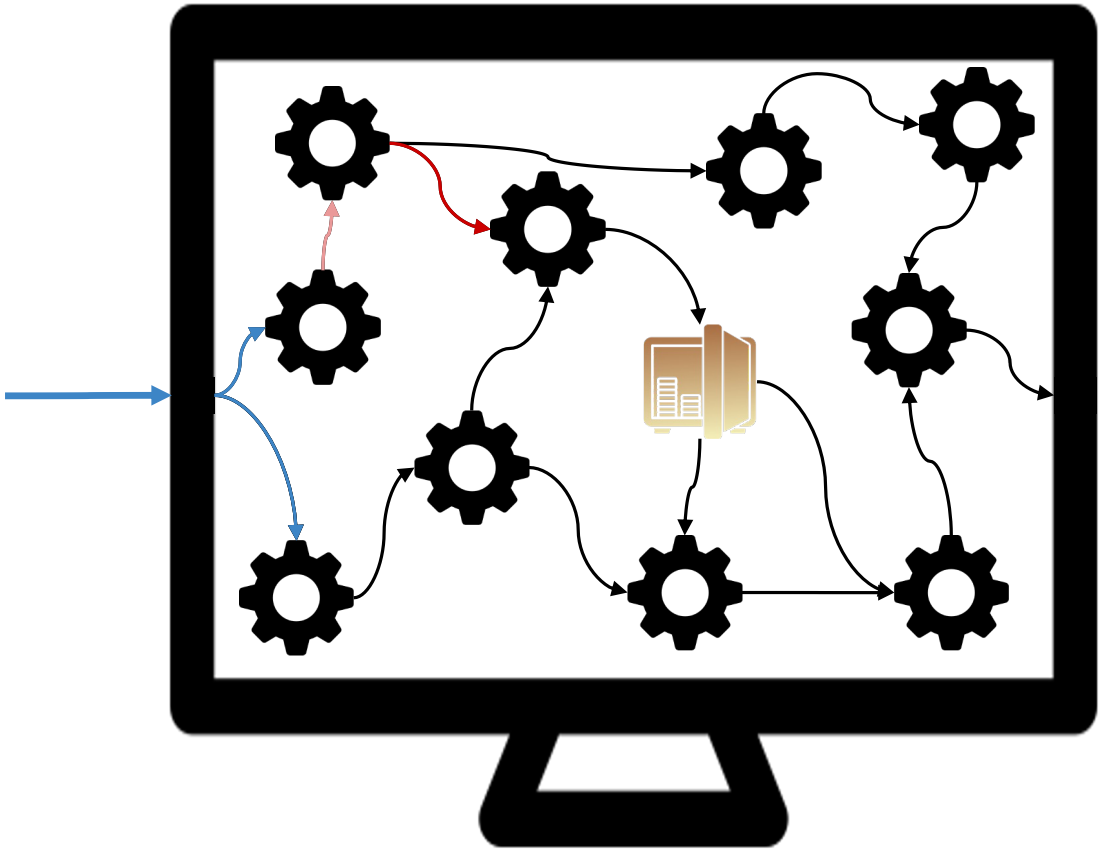
Einstein

Memory Write Primitive

Any corruptible data is attacker data.

openat

Attacker argument generates an attacker file.



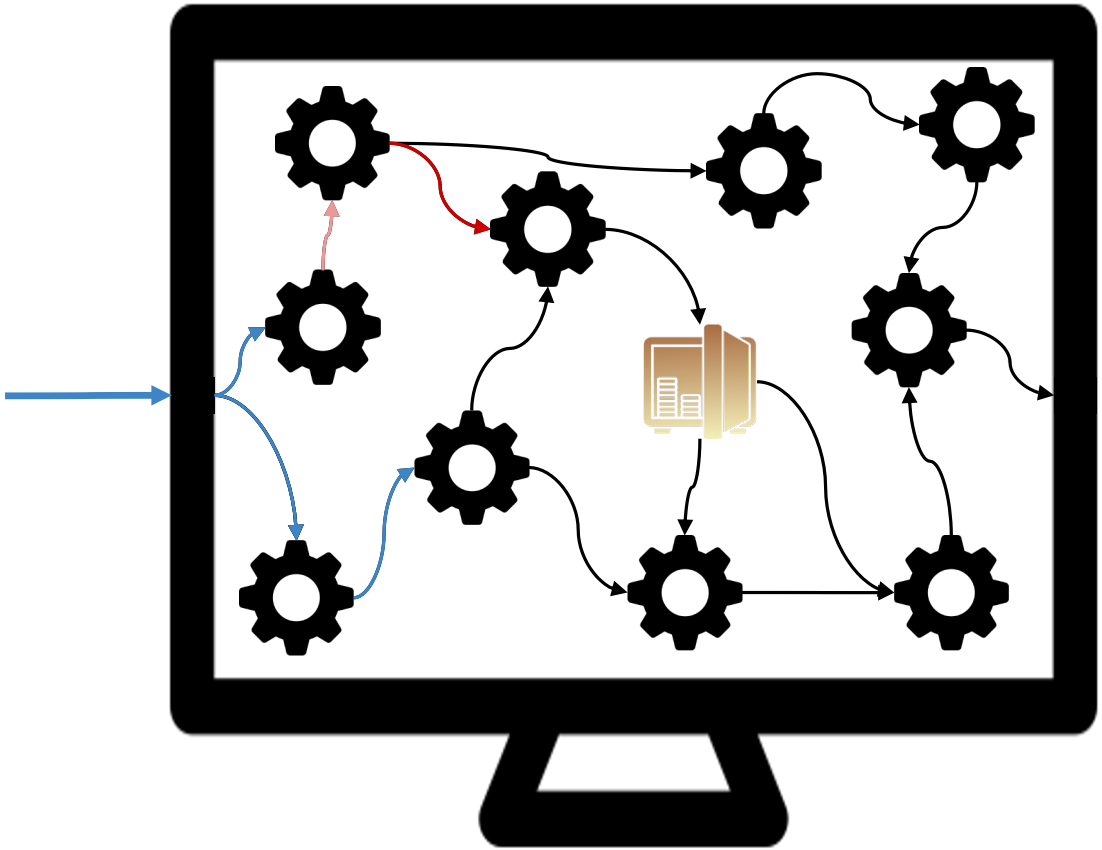
Einstein

Memory Write Primitive

Any corruptible data is attacker data.

openat

Attacker argument generates an attacker file.



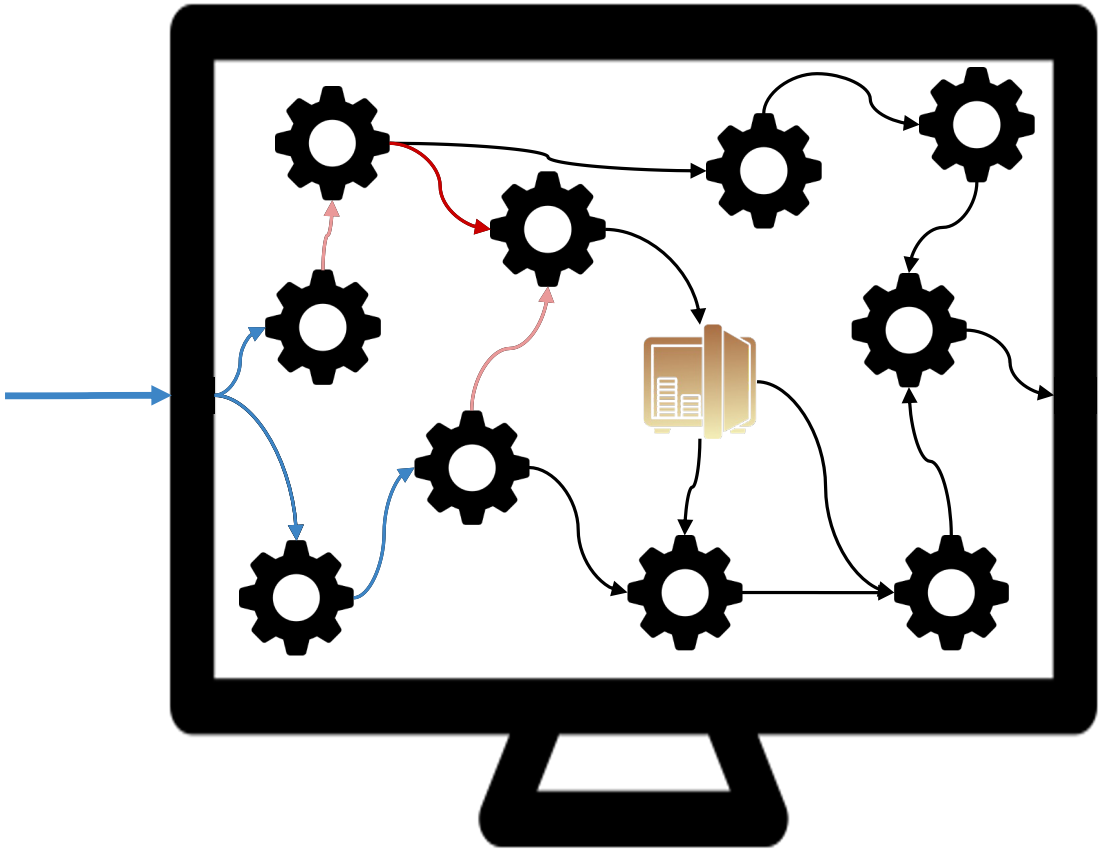
Einstein

Memory Write Primitive

Any corruptible data is attacker data.

openat

Attacker argument generates an attacker file.



Einstein

Memory Write Primitive

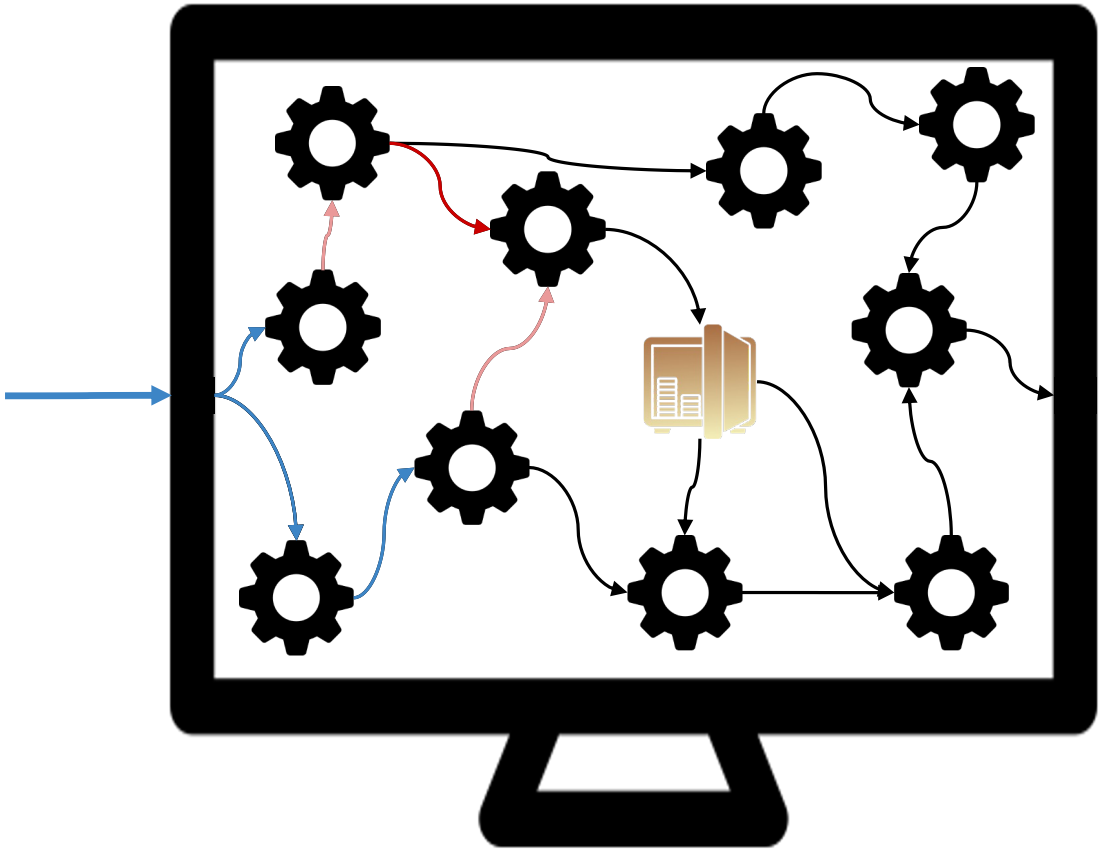
Any corruptible data is attacker data.

openat

Attacker argument generates an attacker file.

write

Attacker argument yields a write-what-where attack.



Einstein

Memory Write Primitive

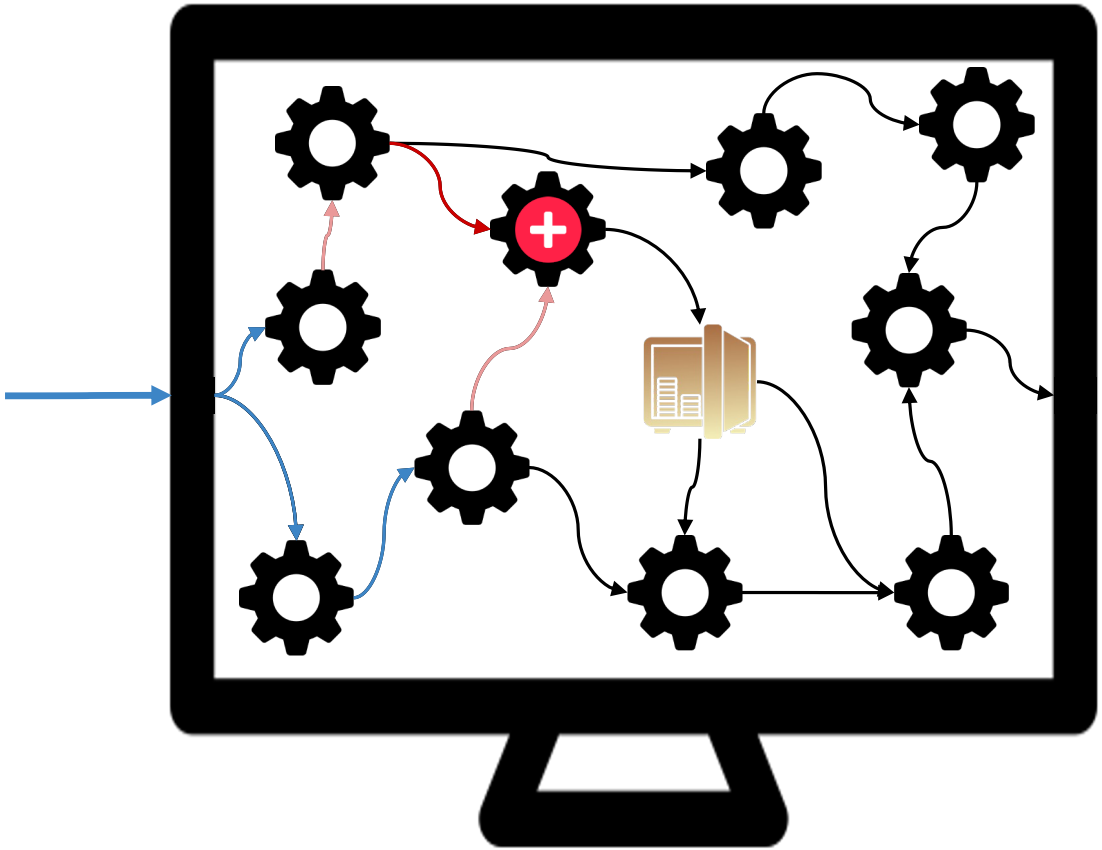
Any corruptible data is attacker data.

openat

Attacker argument generates an attacker file.

write

Attacker argument yields a write-what-where attack.



Einstein

Memory Write Primitive

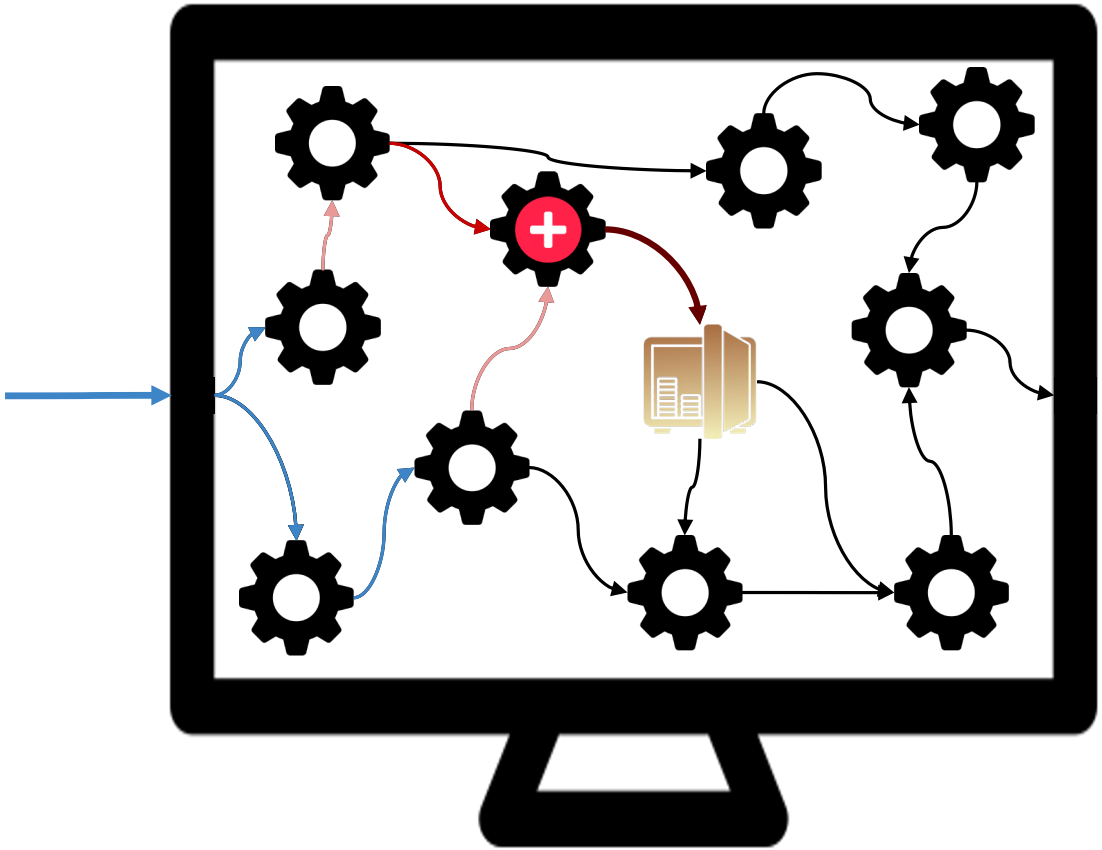
Any corruptible data is attacker data.

openat

Attacker argument generates an attacker file.

write

Attacker argument yields a write-what-where attack.



Einstein

Memory Write Primitive

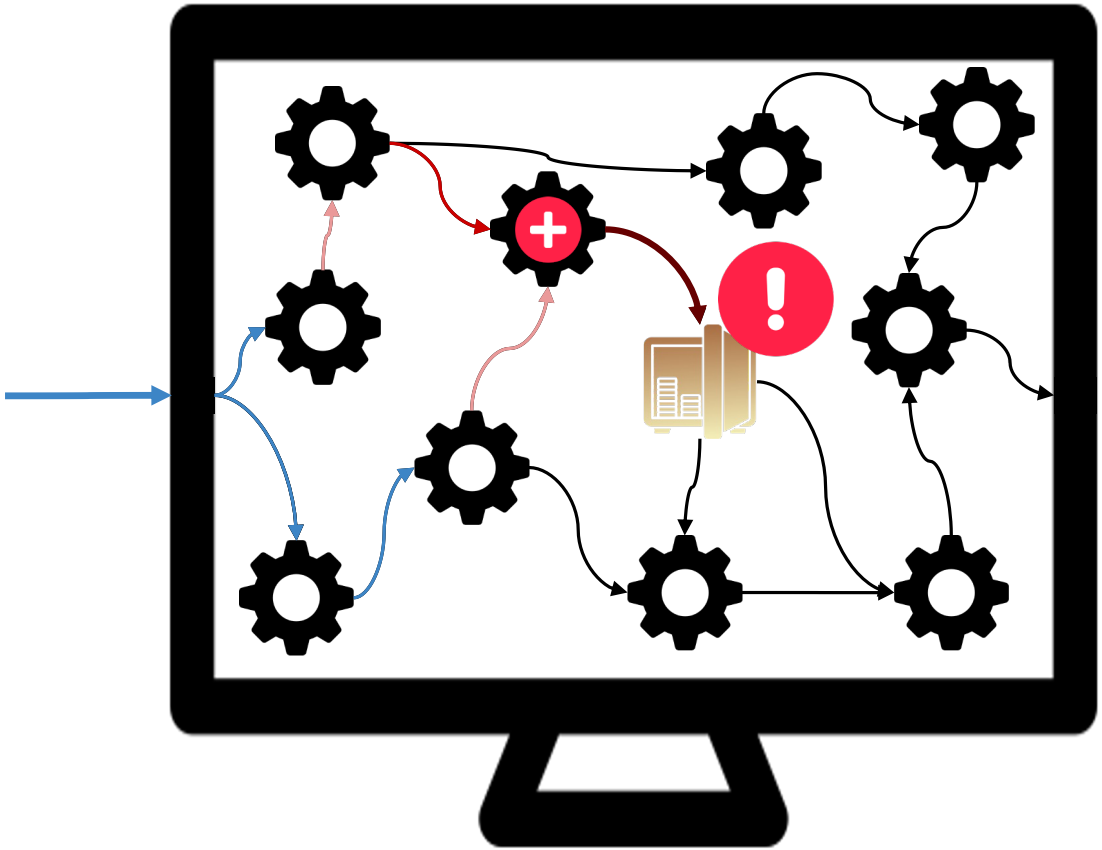
Any corruptible data is attacker data.

openat

Attacker argument generates an attacker file.

write

Attacker argument yields a write-what-where attack.



Einstein

Memory Write Primitive

Any corruptible data is attacker data.

openat

Attacker argument generates an attacker file.

connect

ttacker argument enerates an attacker socket.

execve

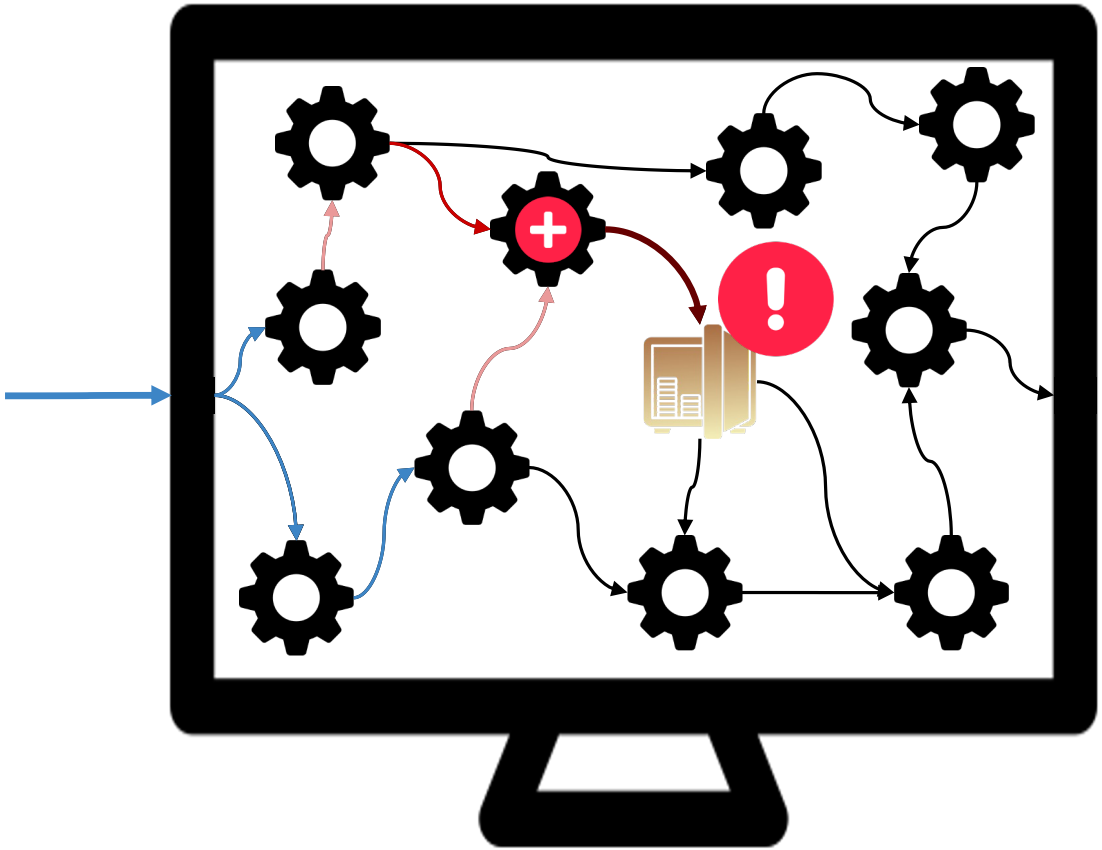
Attacker argument yields a code-execution attack.

endto

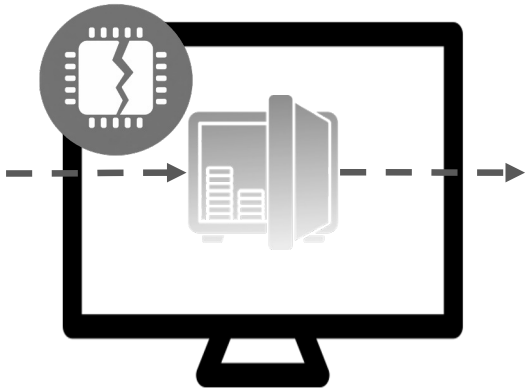
t yields a send- e attack.

write

Attacker argument yields a write-what-where attack.

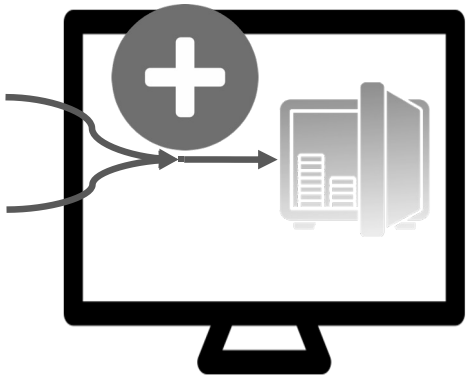


Explicit vulnerability modeling: ***Case studies***



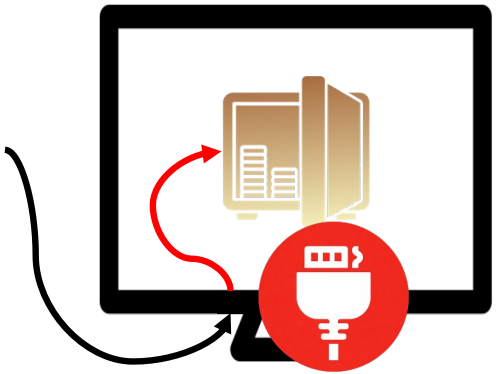
Kasper

(NDSS 2022)



Einstein

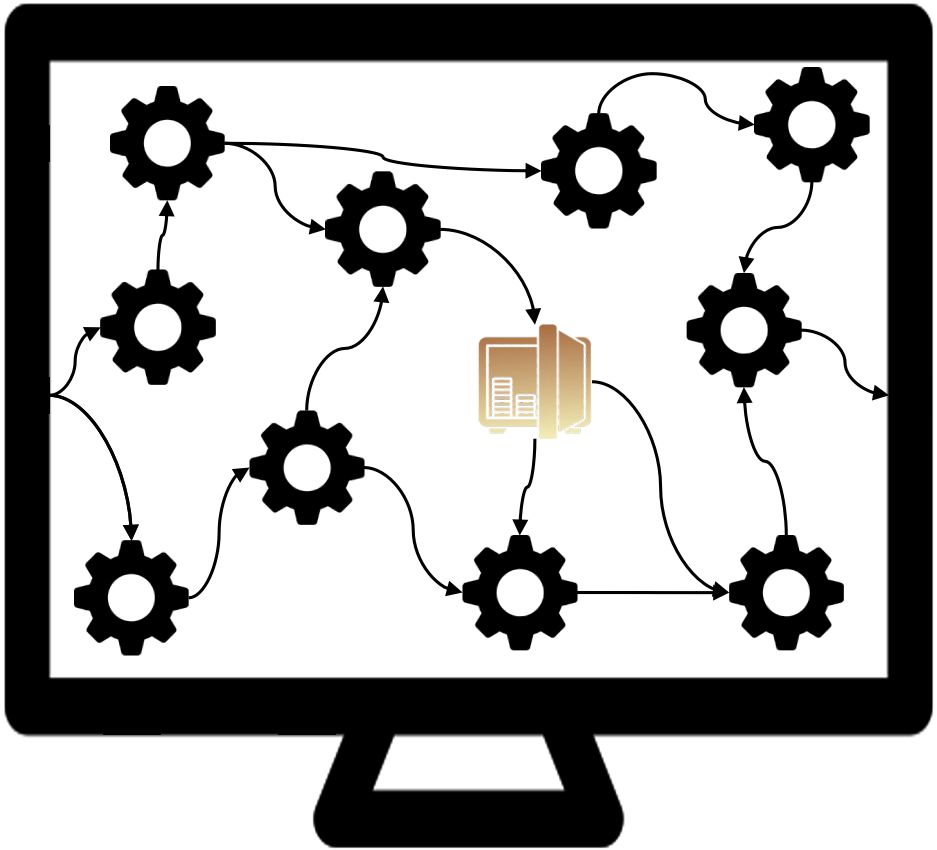
(USENIX Sec. 2024)



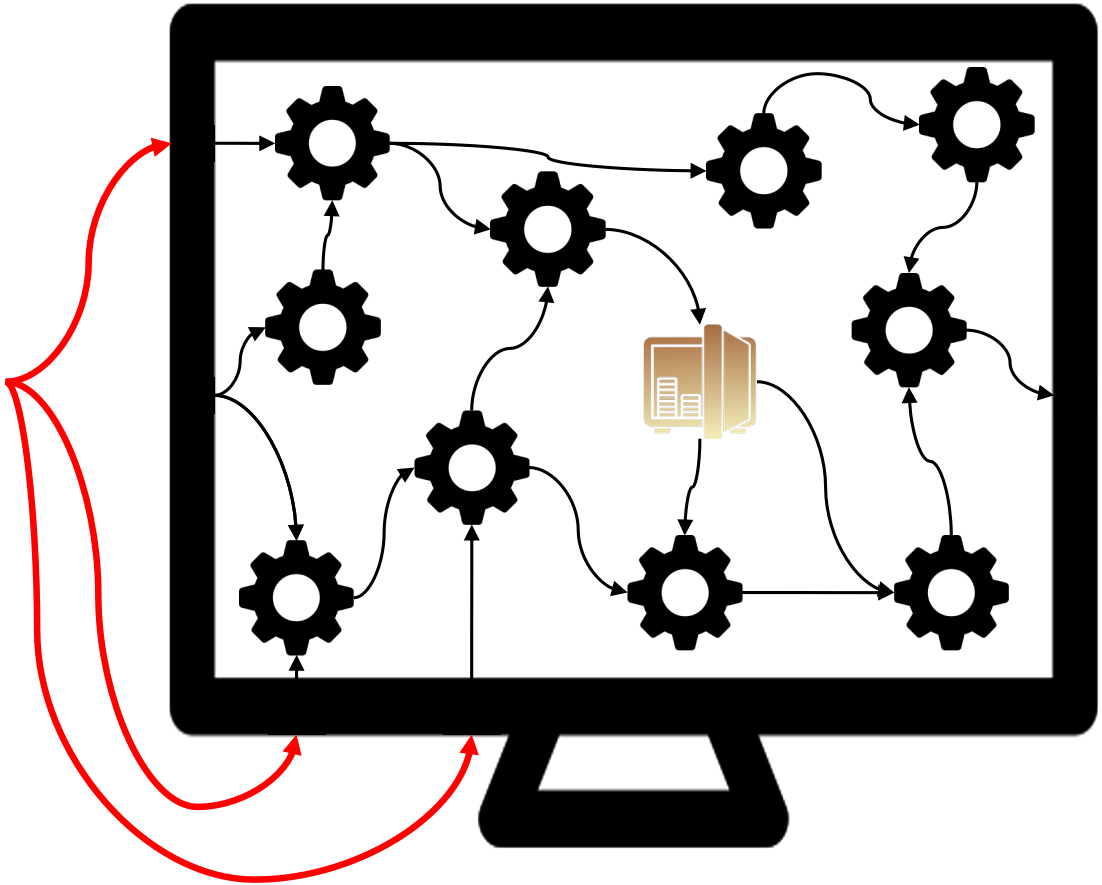
DMARacer

(CCS 2025)

DMARacer



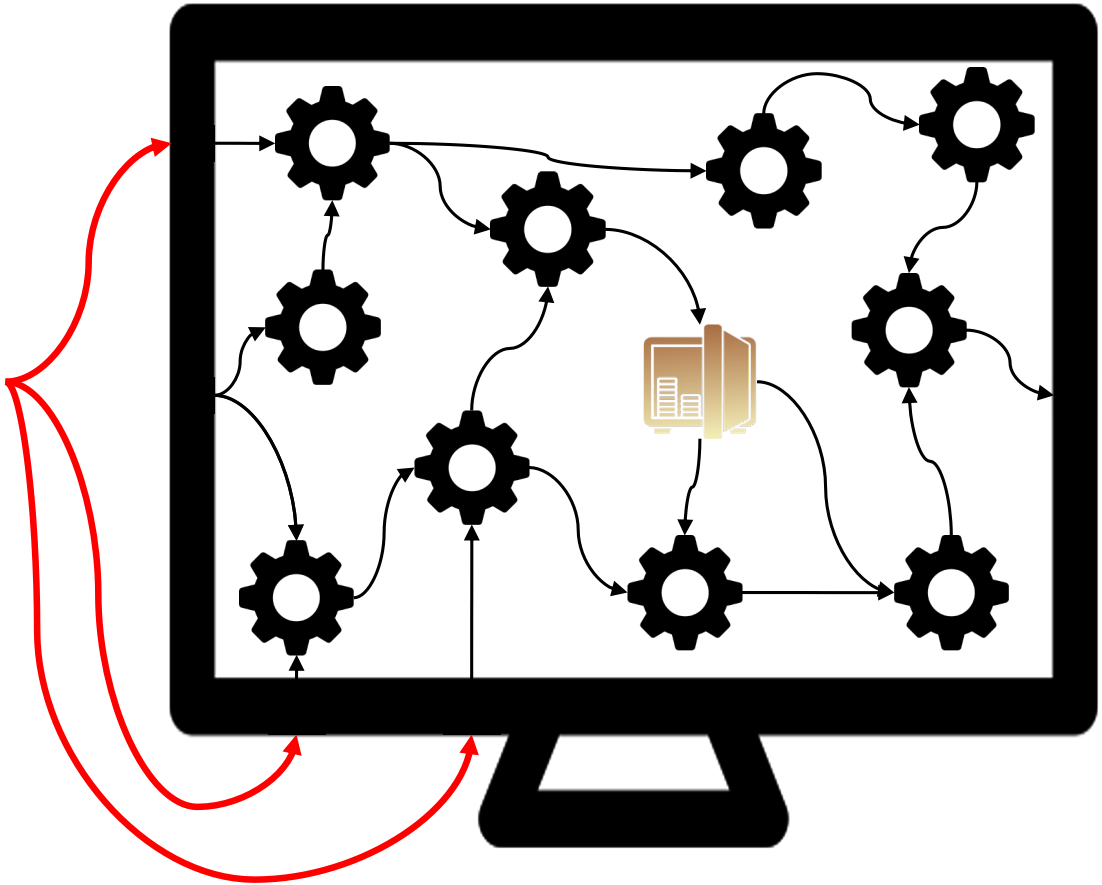
DMARacer



DMARacer

Time-of-Check to Time-of-Use

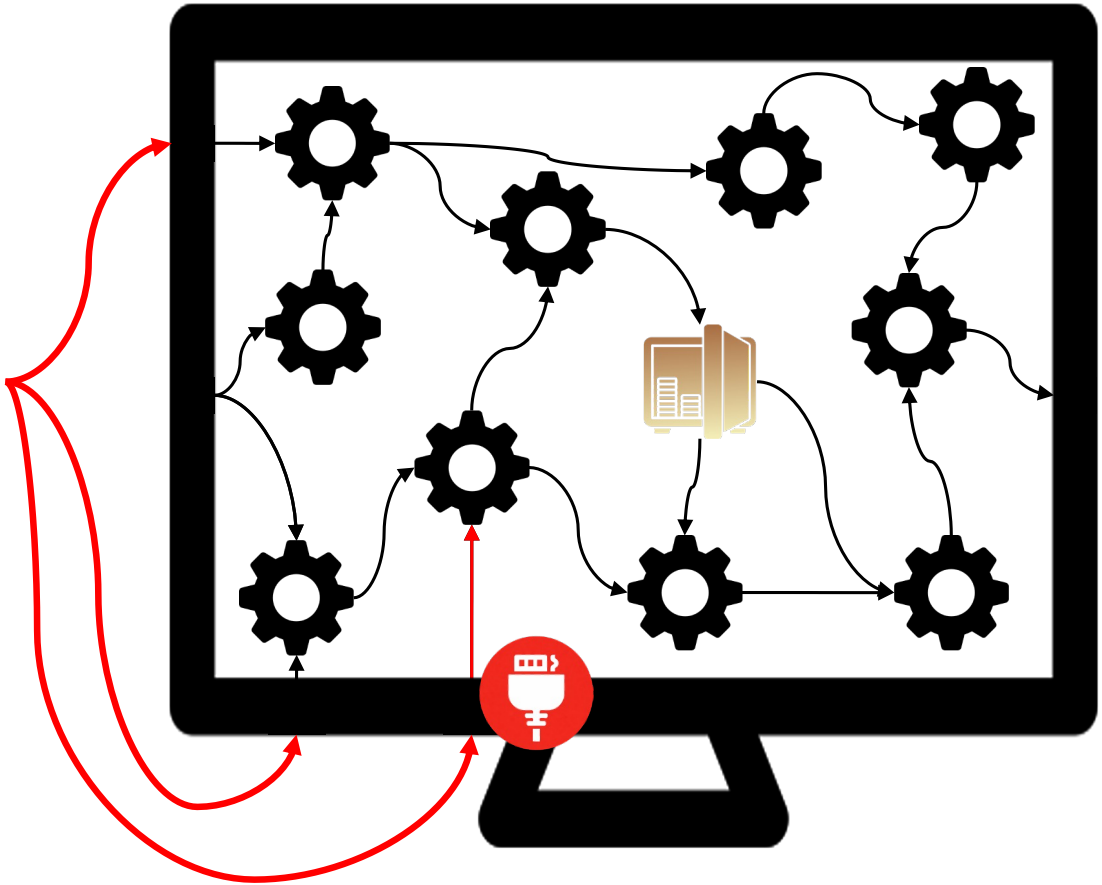
Multiple DMA loads generate attacker data.



DMARacer

Time-of-Check to Time-of-Use

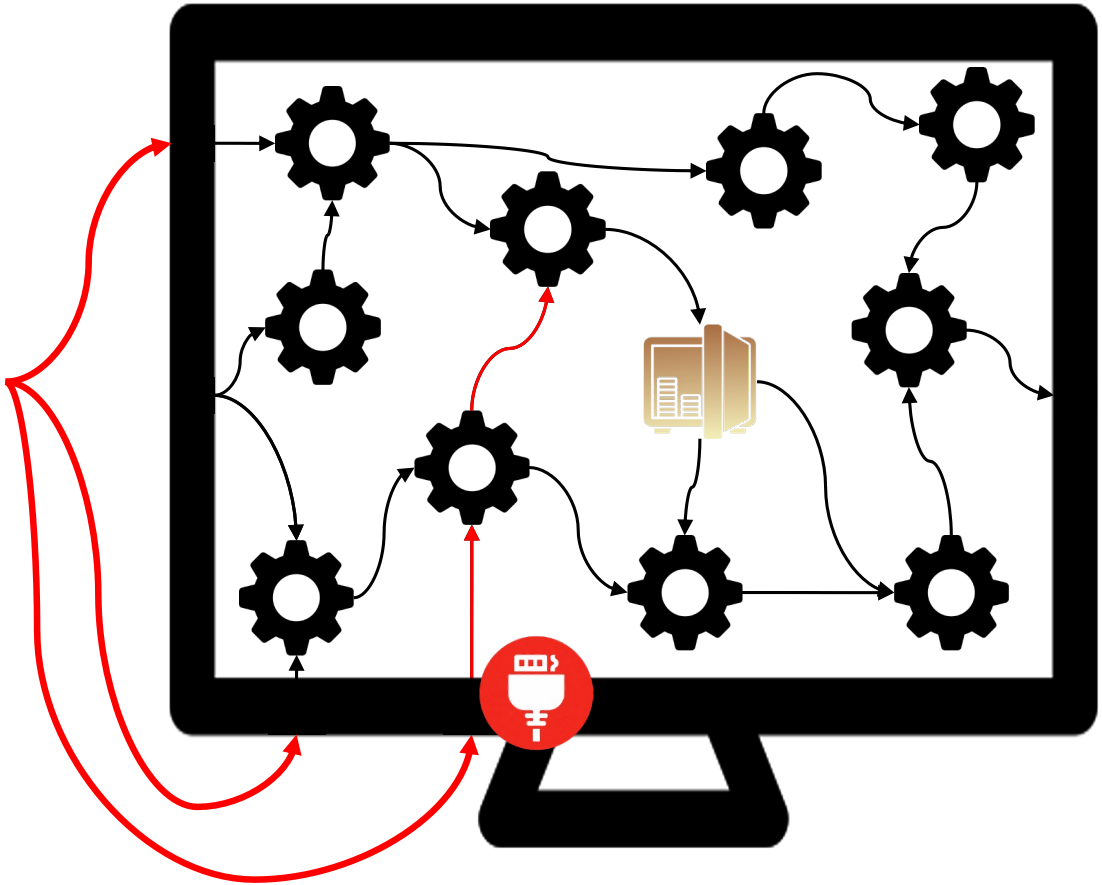
Multiple DMA loads generate attacker data.



DMARacer

Time-of-Check to Time-of-Use

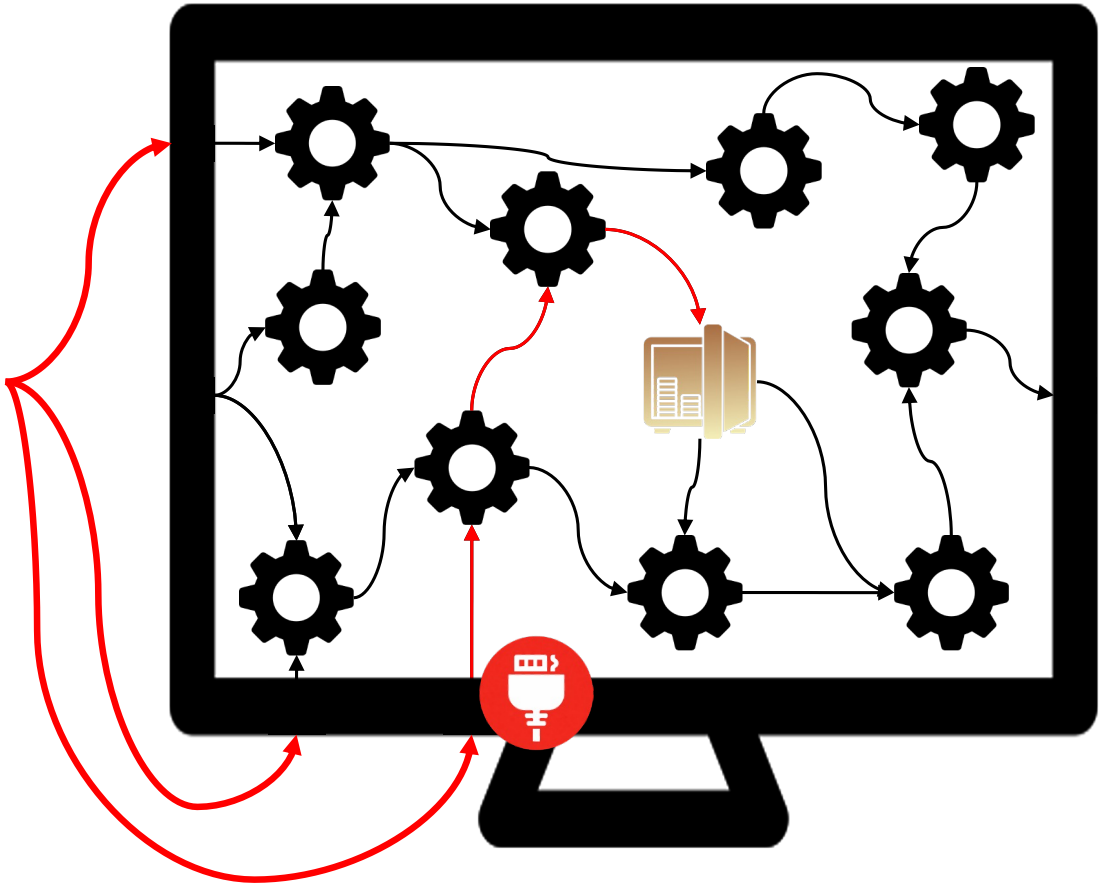
Multiple DMA loads generate attacker data.



DMARacer

Time-of-Check to Time-of-Use

Multiple DMA loads generate attacker data.



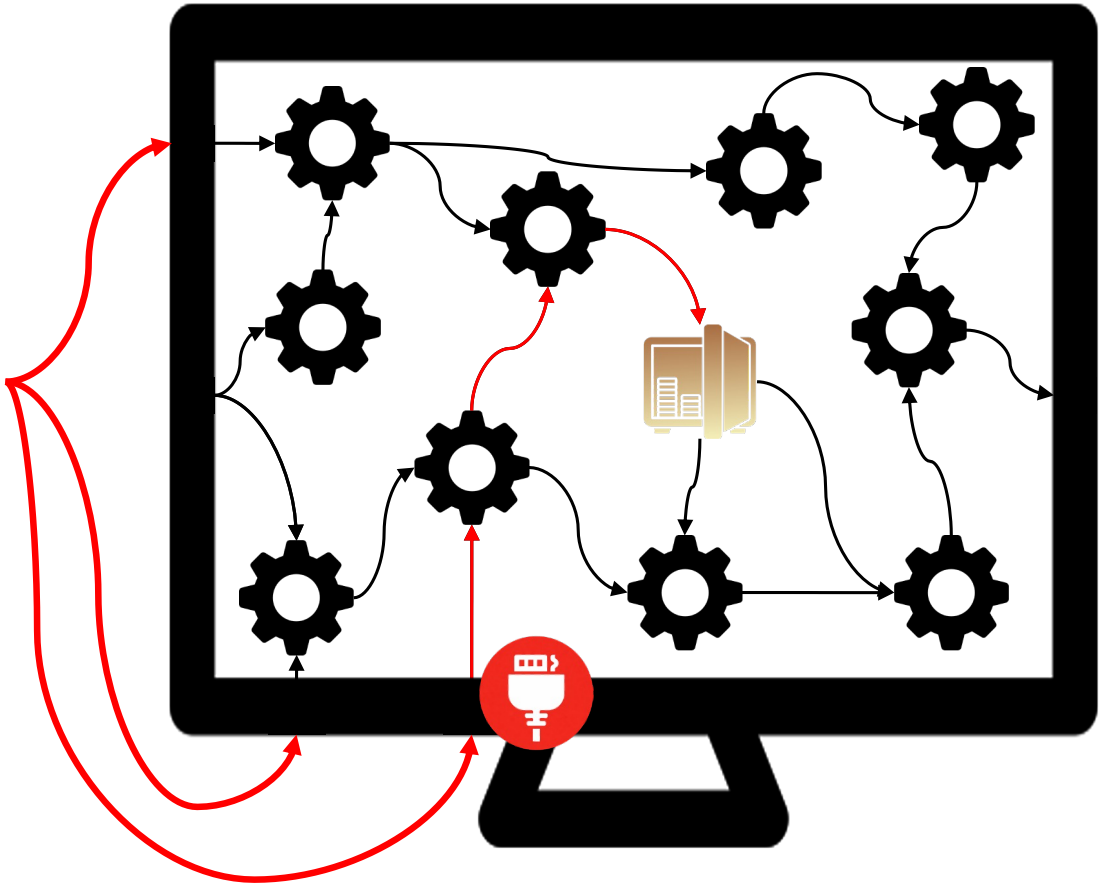
DMARacer

Time-of-Check to Time-of-Use

Multiple DMA loads generate attacker data.

Denial of Service

Asserting an attacker condition yields a DoS attack.



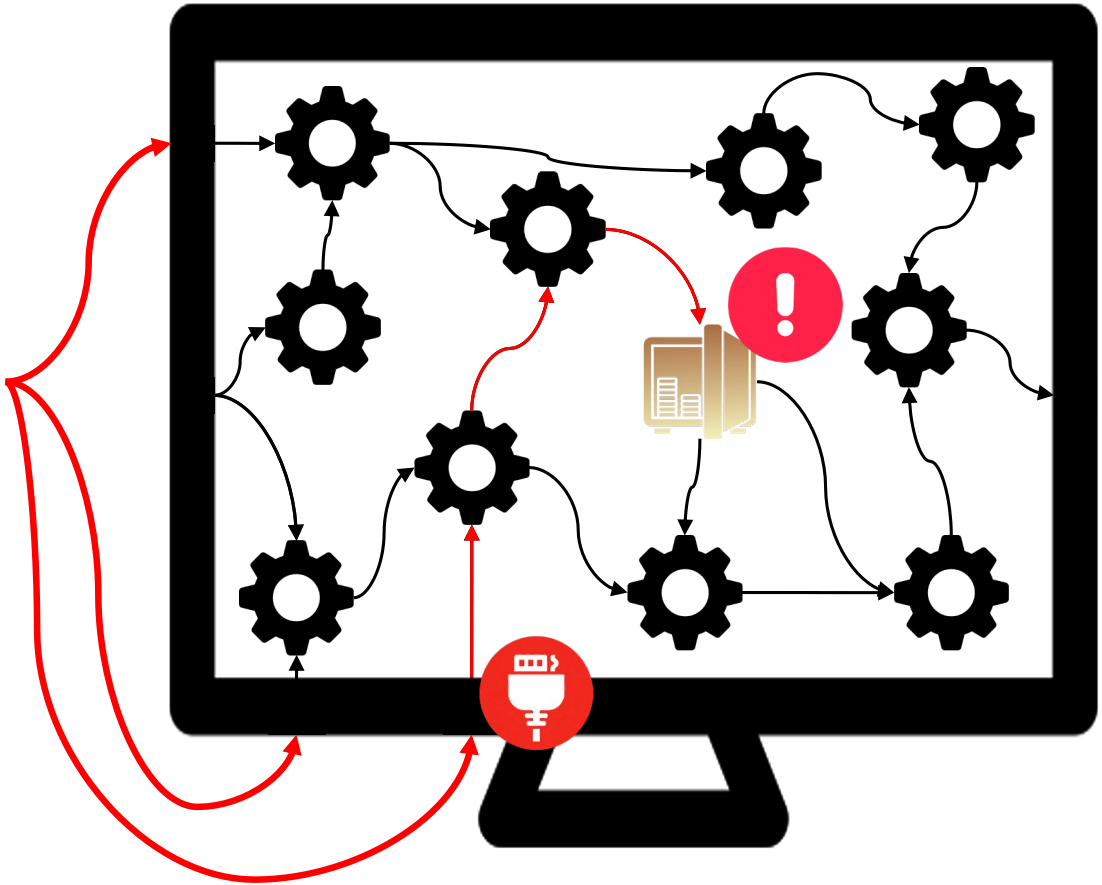
DMARacer

Time-of-Check to Time-of-Use

Multiple DMA loads generate attacker data.

Denial of Service

Asserting an attacker condition yields a DoS attack



DMARacer

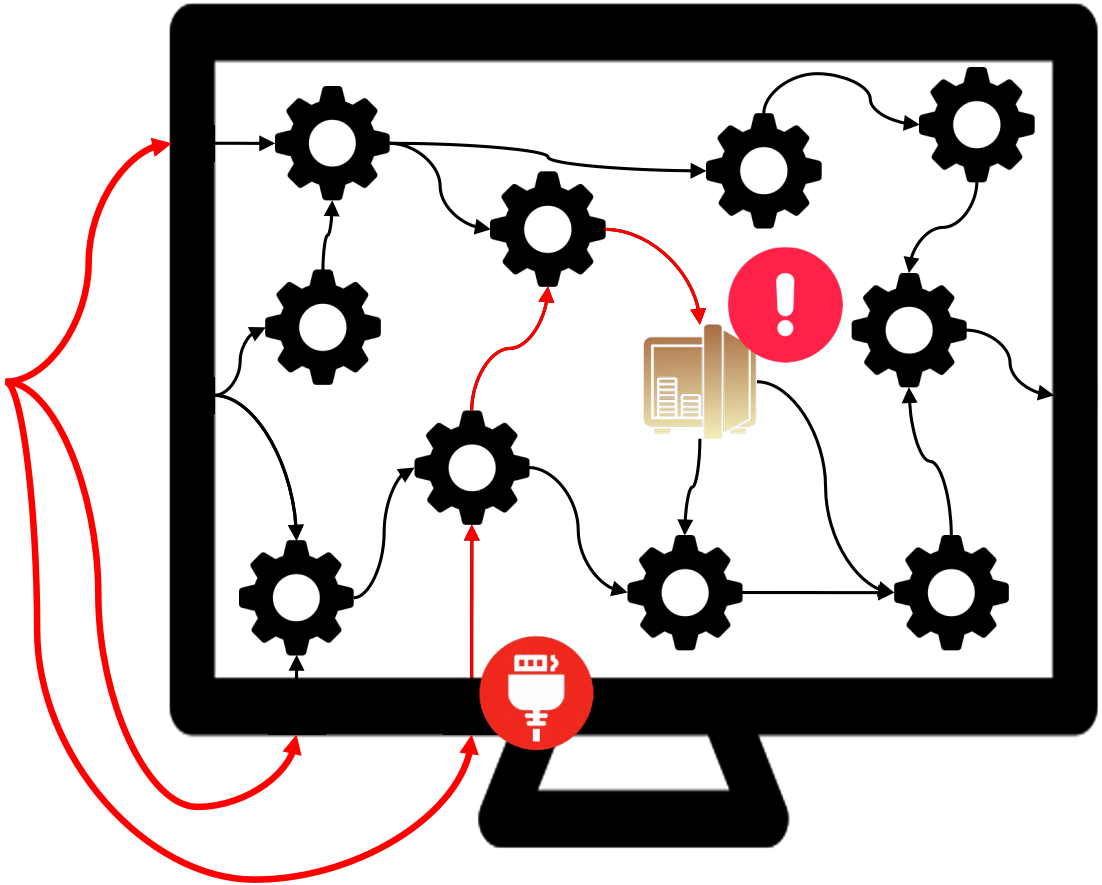
Time-of-Check to Time-of-Use
Multiple DMA loads generate attacker data.

Inconsiste
Unsynchronized stre
generates in

Time-of-Initialization to Time-of-Use
DMA load following a store generates attacker data.

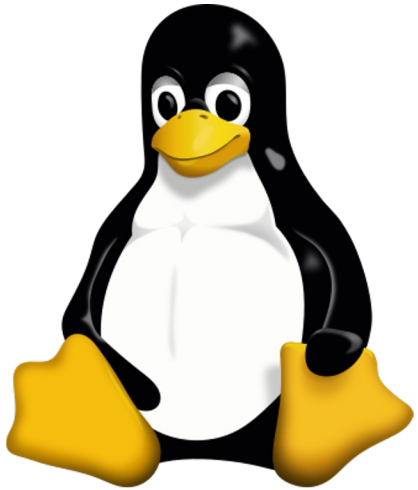
Memory Corruption
g an attacker pointer yields
ory corruption attack.

Denial of Service
Asserting an attacker condition yields a DoS attack.

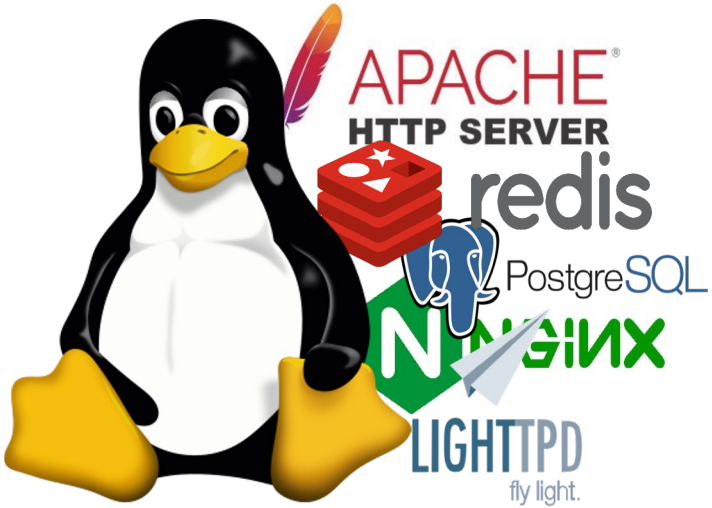


Explicit vulnerability modeling: ***Results***

Explicit vulnerability modeling: ***Results***

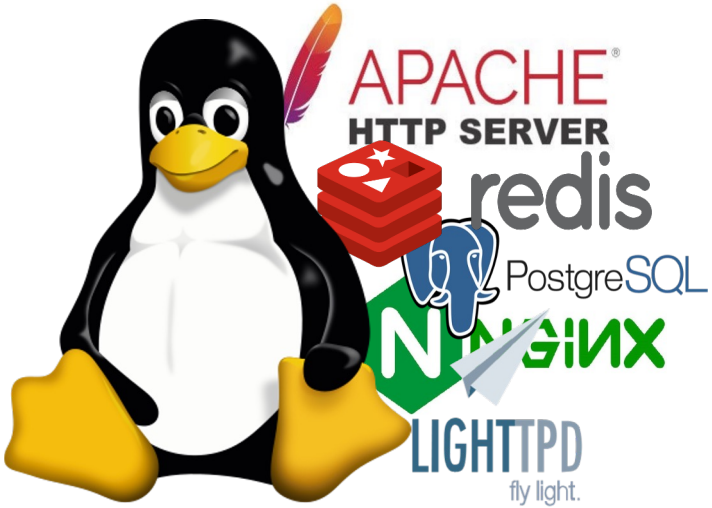


Explicit vulnerability modeling: ***Results***



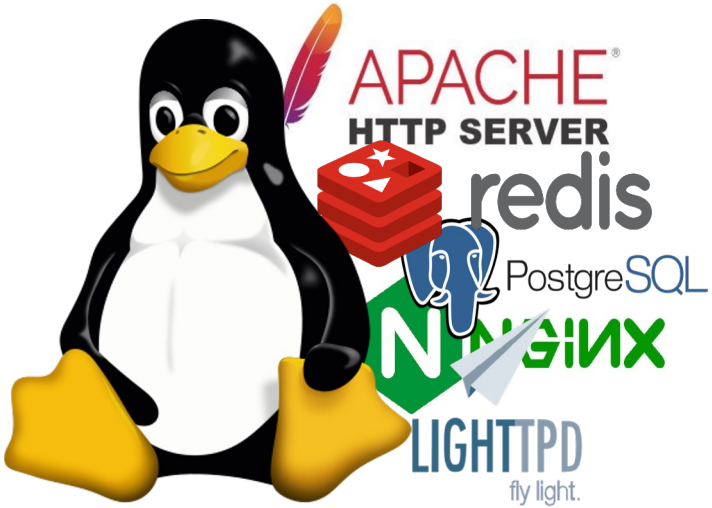
Explicit vulnerability modeling: ***Results***

- *Found vulnerabilities*



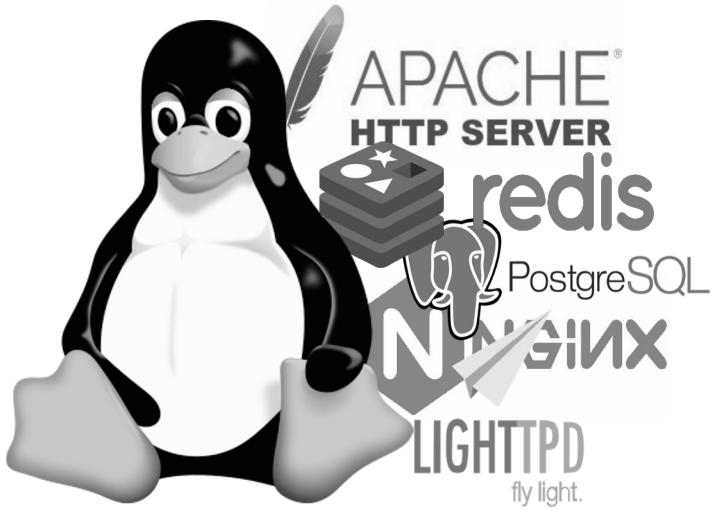
Explicit vulnerability modeling: ***Results***

- *Found vulnerabilities*
- *Built exploits*



Explicit vulnerability modeling: ***Results***

- *Found vulnerabilities*
- *Built exploits*
- ***Applied fixes***



*Introduce **explicit vulnerability modeling** for information-flow tracking*

*Introduce **explicit vulnerability modeling** for information-flow tracking*

*Discover new vulnerabilities in real-world software **efficiently***

*Introduce **explicit vulnerability modeling** for information-flow tracking*

*Discover new vulnerabilities in real-world software **efficiently***

*Provide an extensible, future-resilient foundation for **vulnerability detection***