System-level Support for Intrusion Recovery

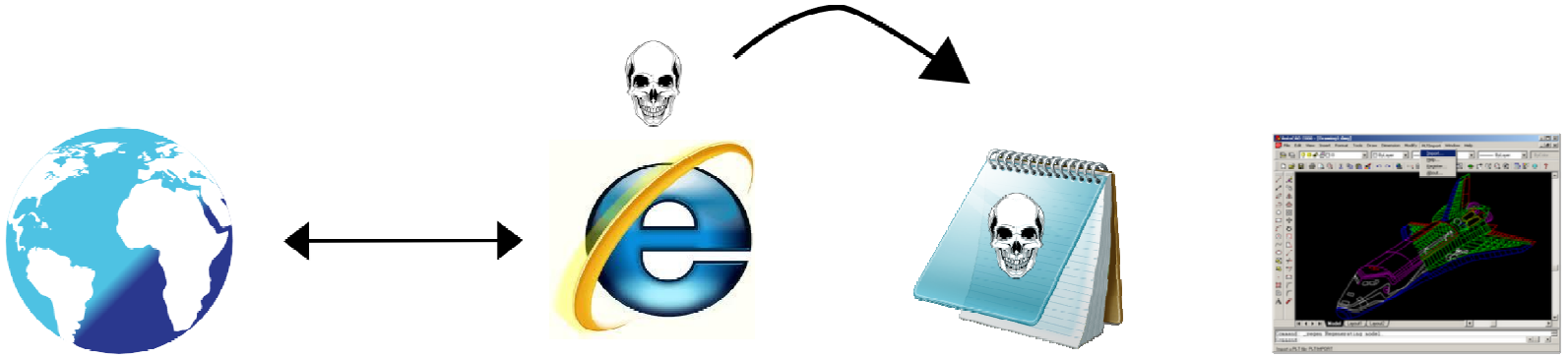
Andrei Bacs, Remco Vermeulen,
Asia Slowinska, Herbert Bos

Introduction

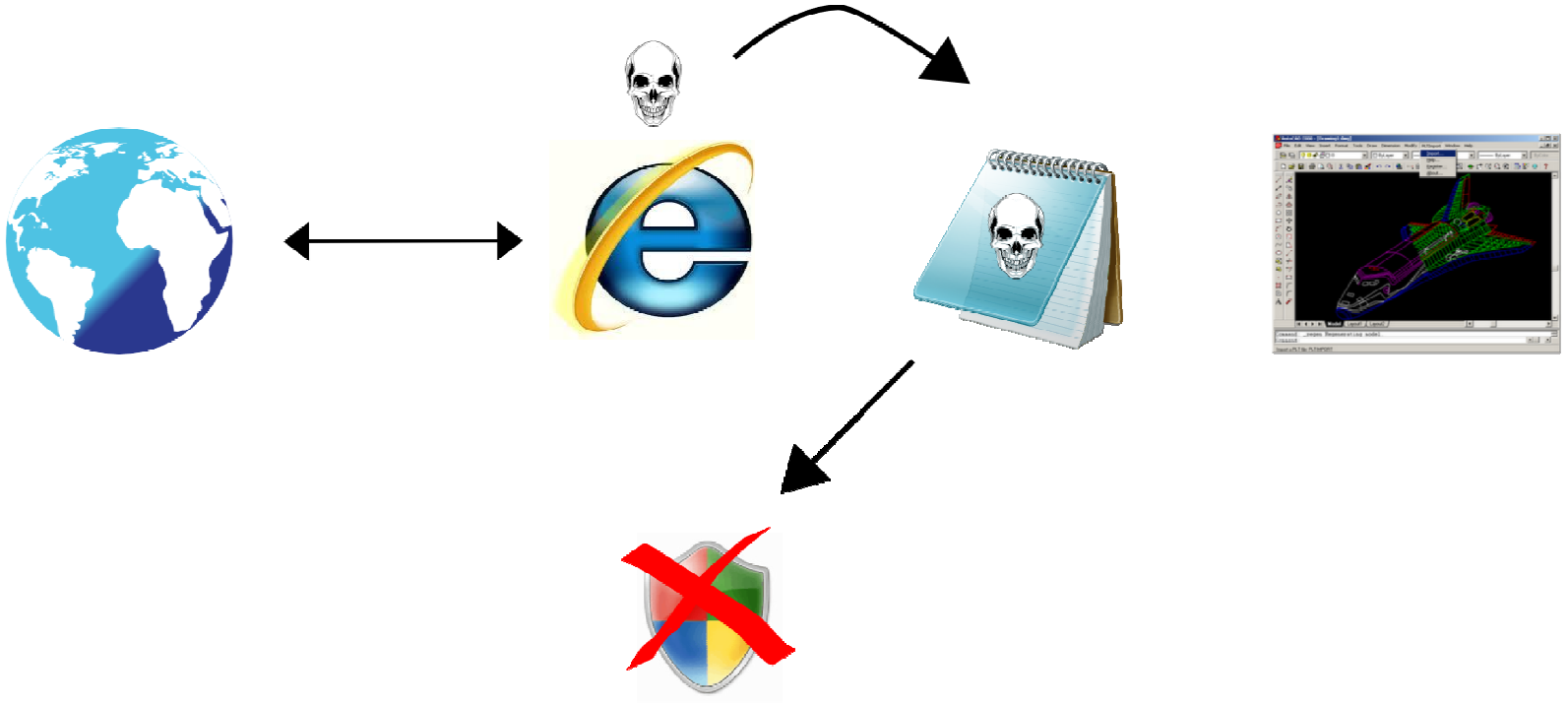
- System compromise is common
- Typically the attack is detected later
- Can the user still trust the user data created after the attack?

Attack example

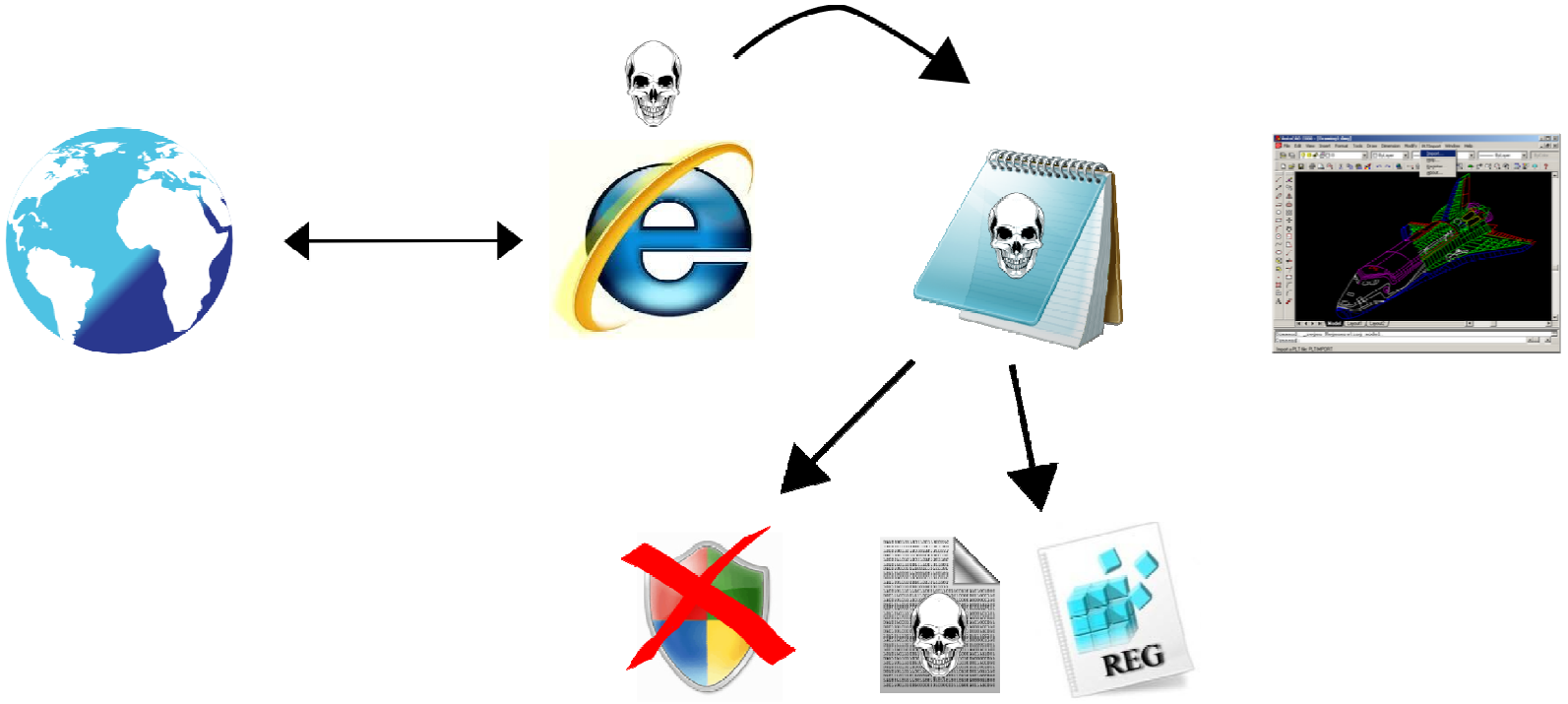
Attack example



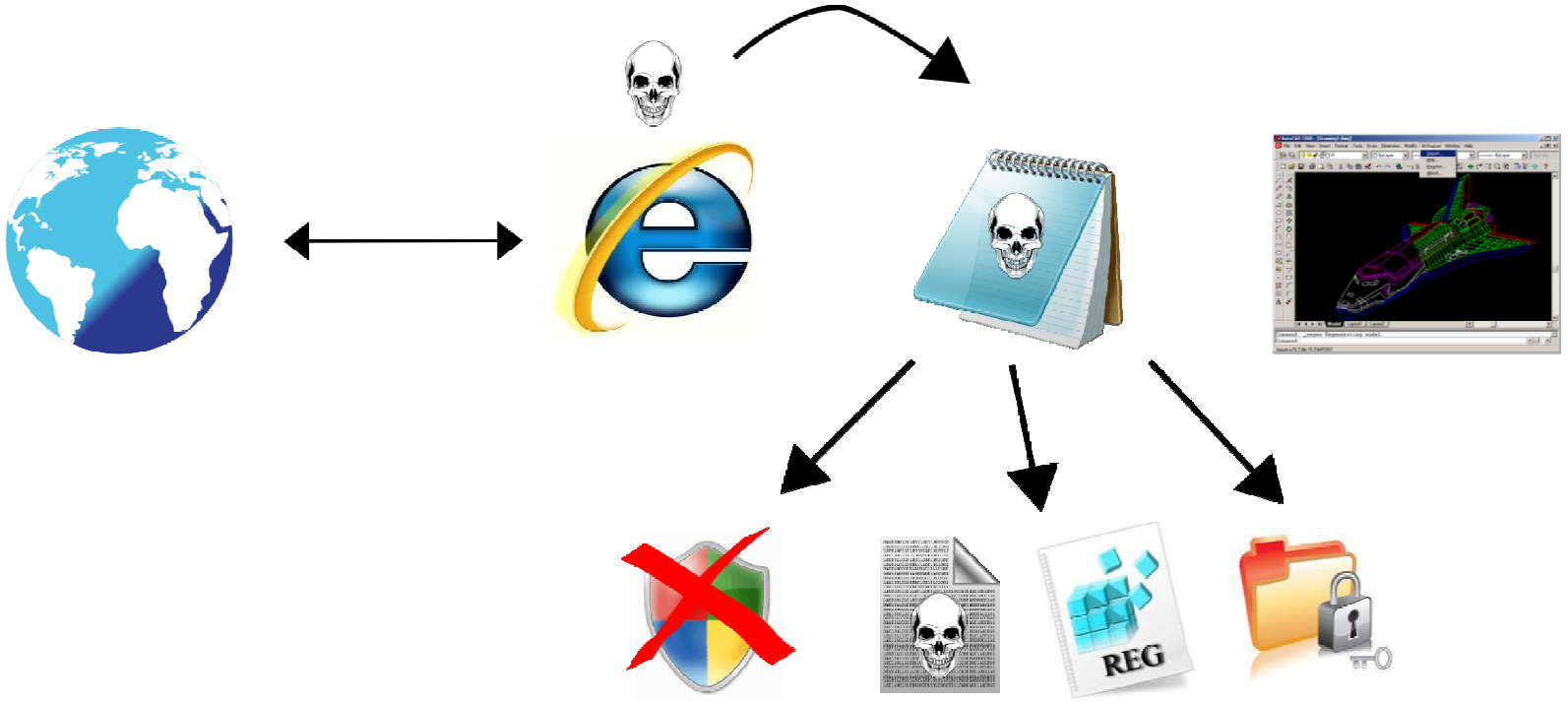
Attack example



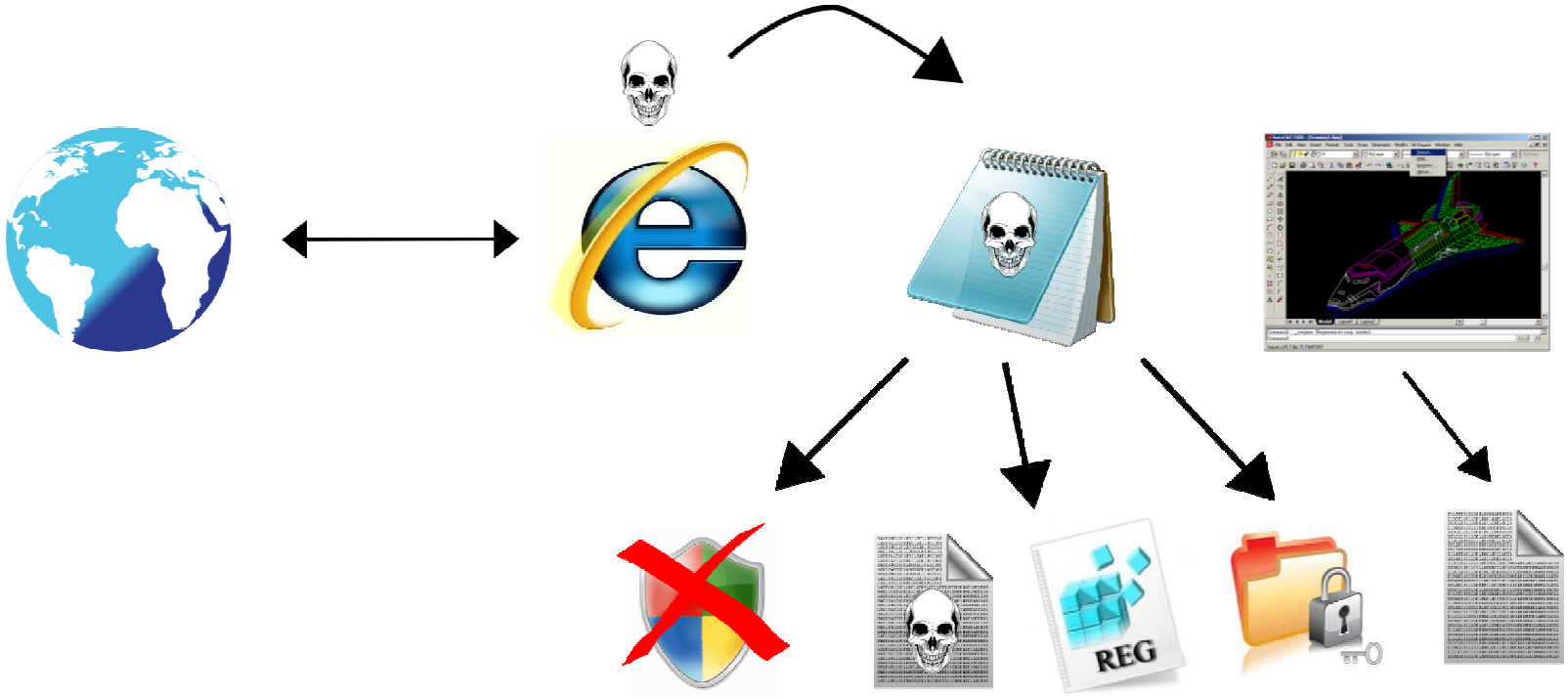
Attack example



Attack example



Attack example



Recovering from attacks

- AV scanners
  - signatures are always late
  - may not clean all infected data

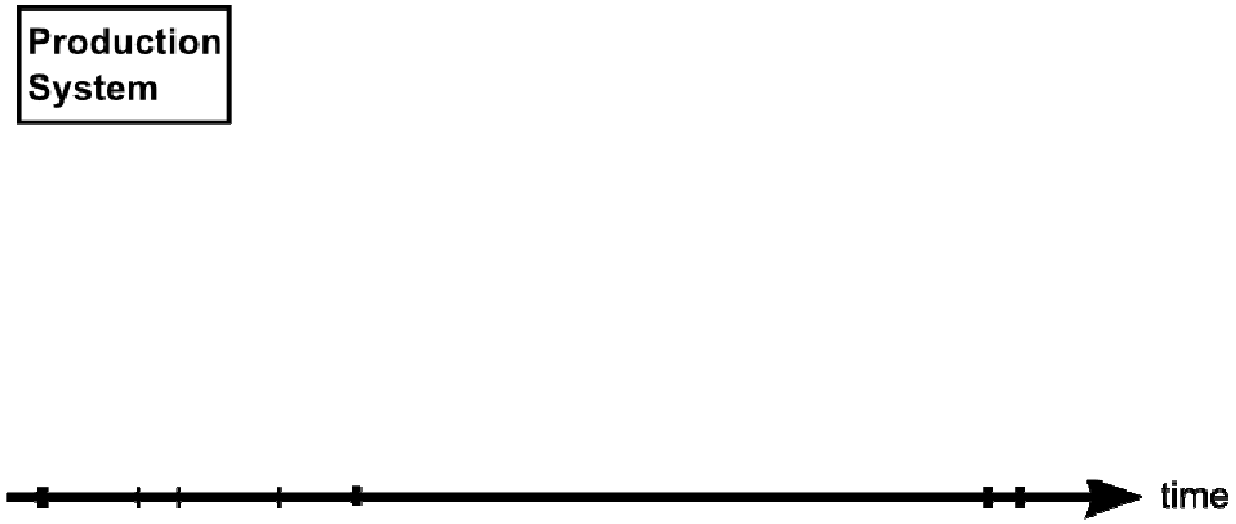
- Restore from backups
  - recent changes are lost

DiskDuster

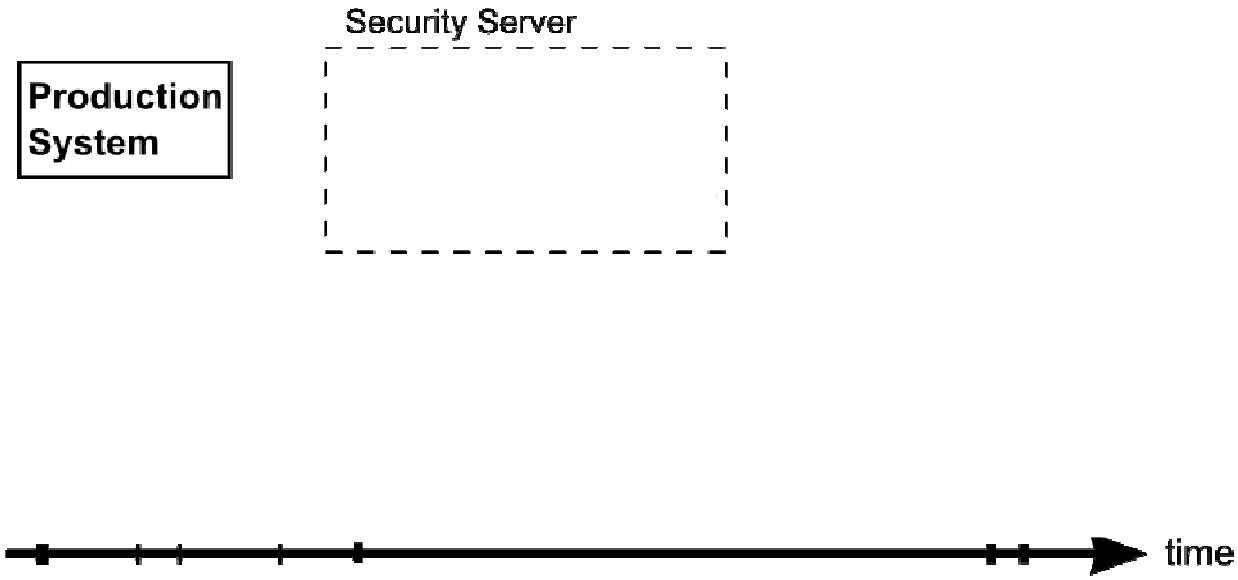
- Recover user data produced after the attack.

- Recover even if the malware was active for a longer time period.

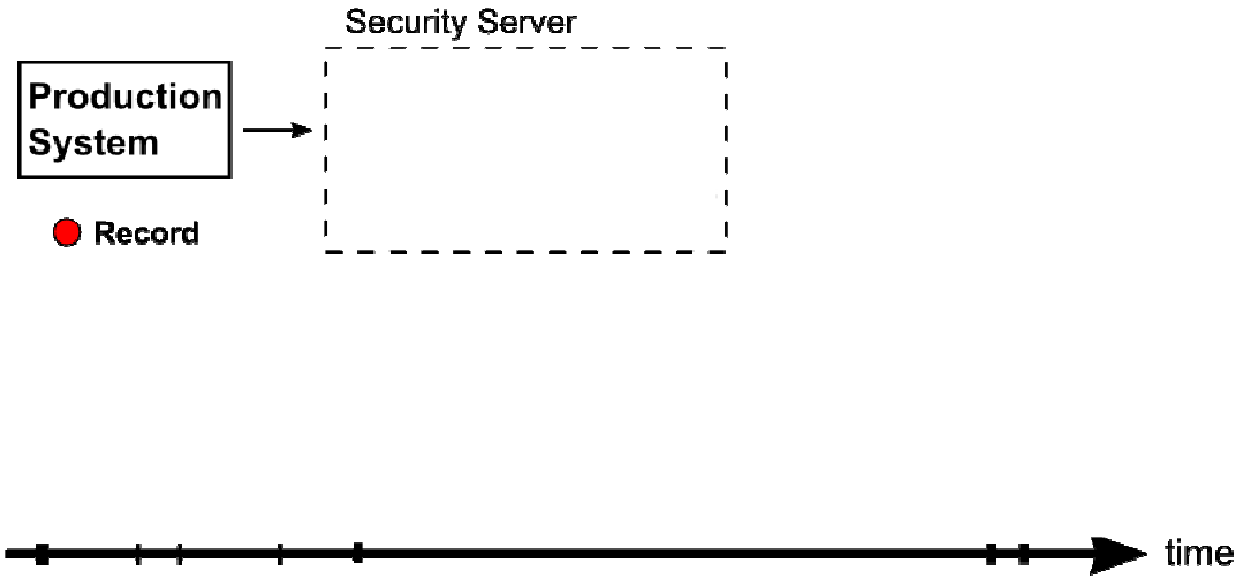
Recovery in decoupled security



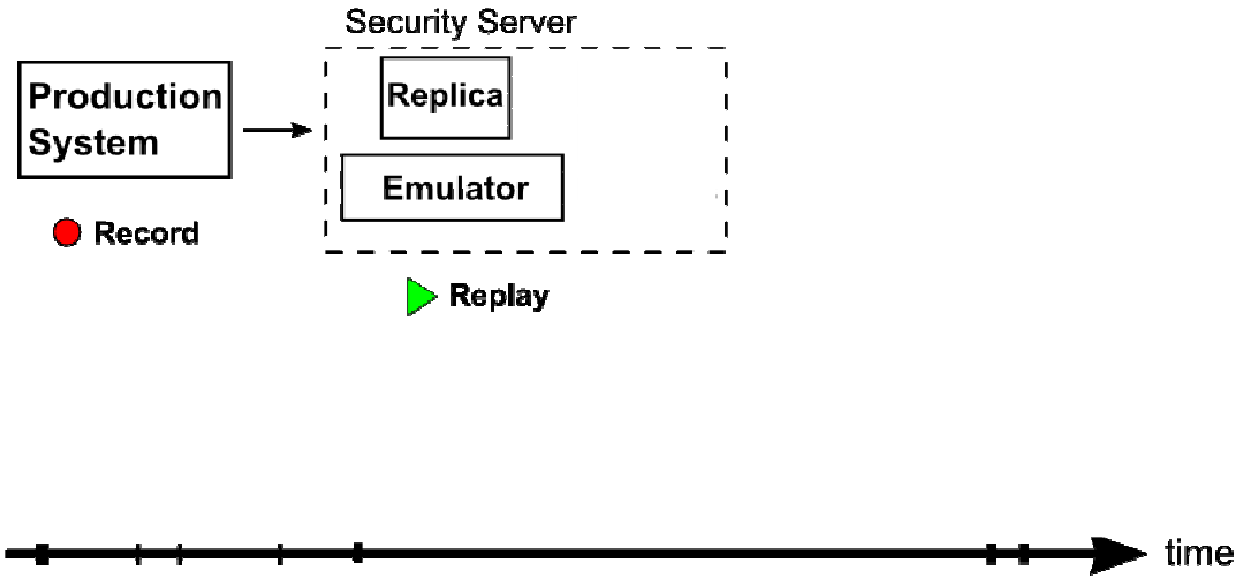
Recovery in decoupled security



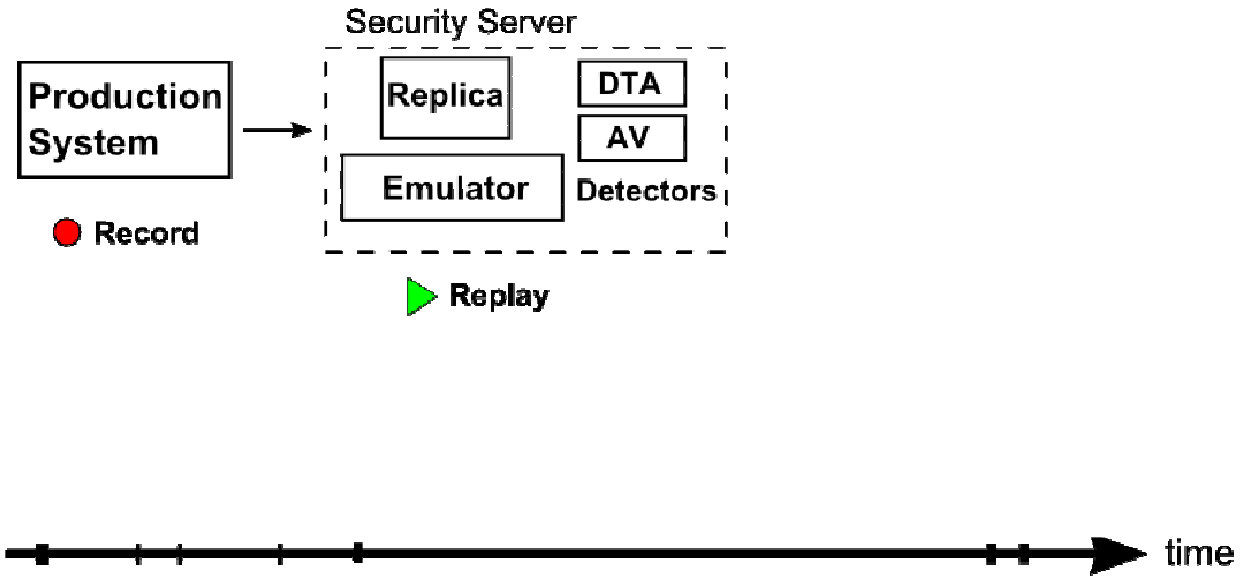
Recovery in decoupled security



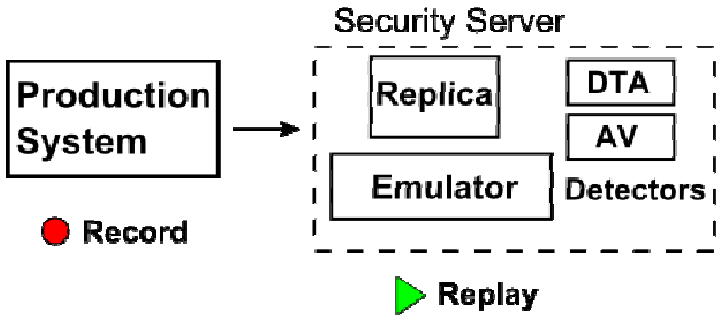
Recovery in decoupled security



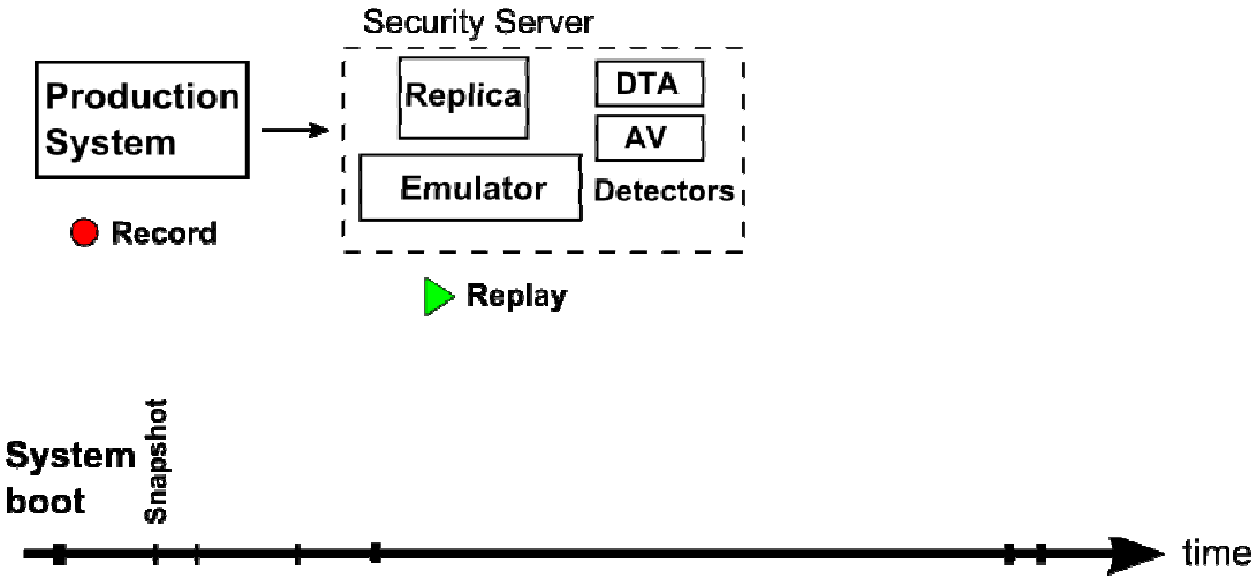
Recovery in decoupled security



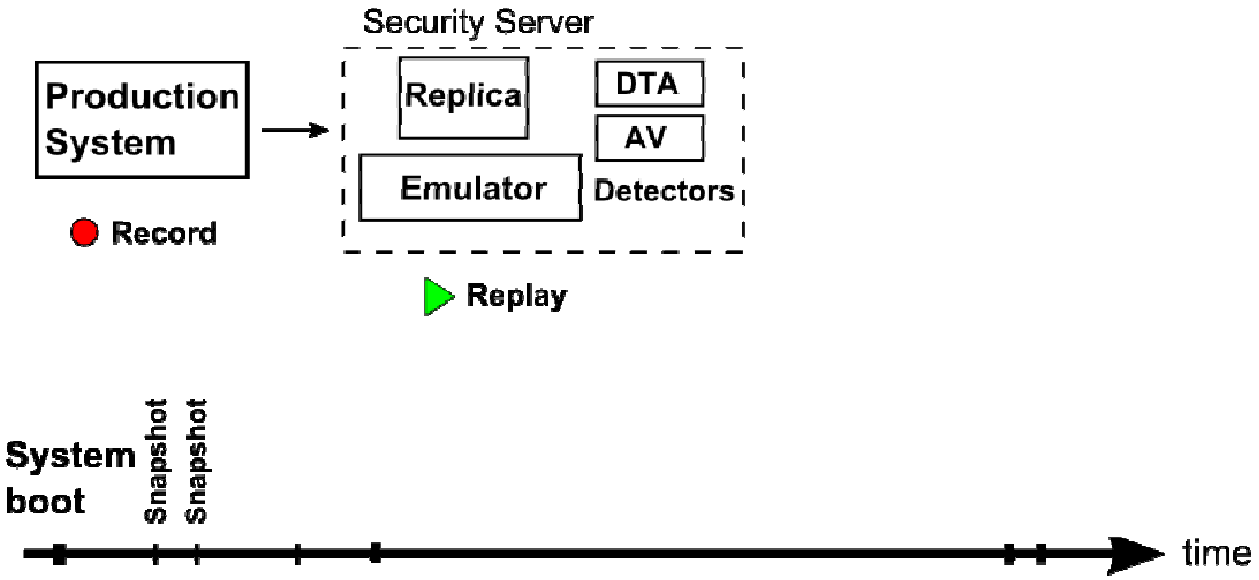
Recovery in decoupled security



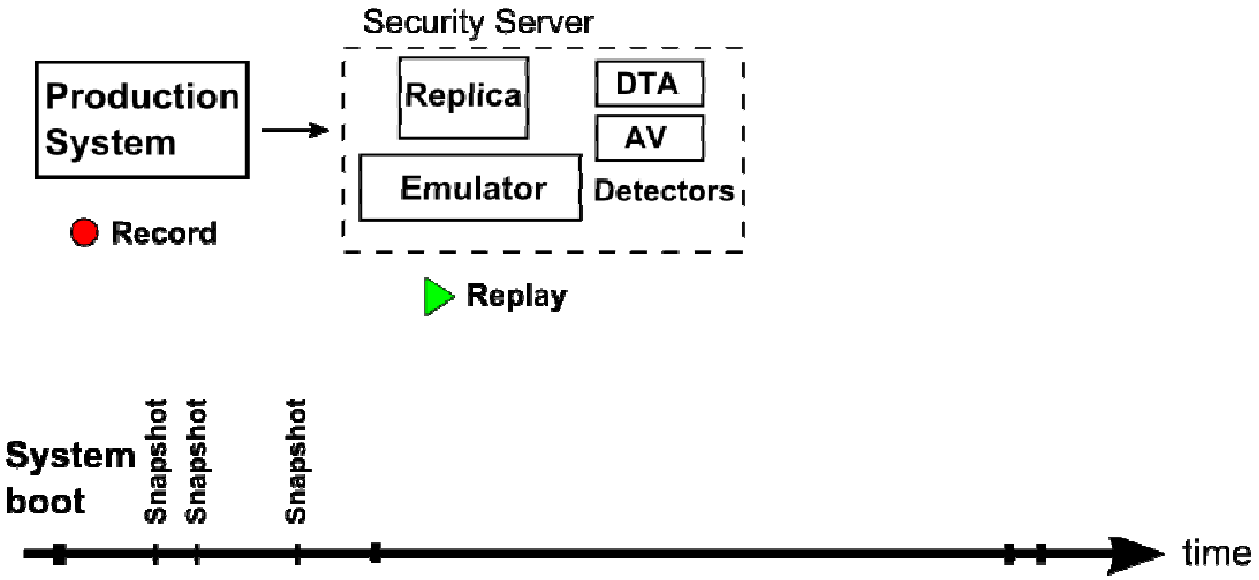
Recovery in decoupled security



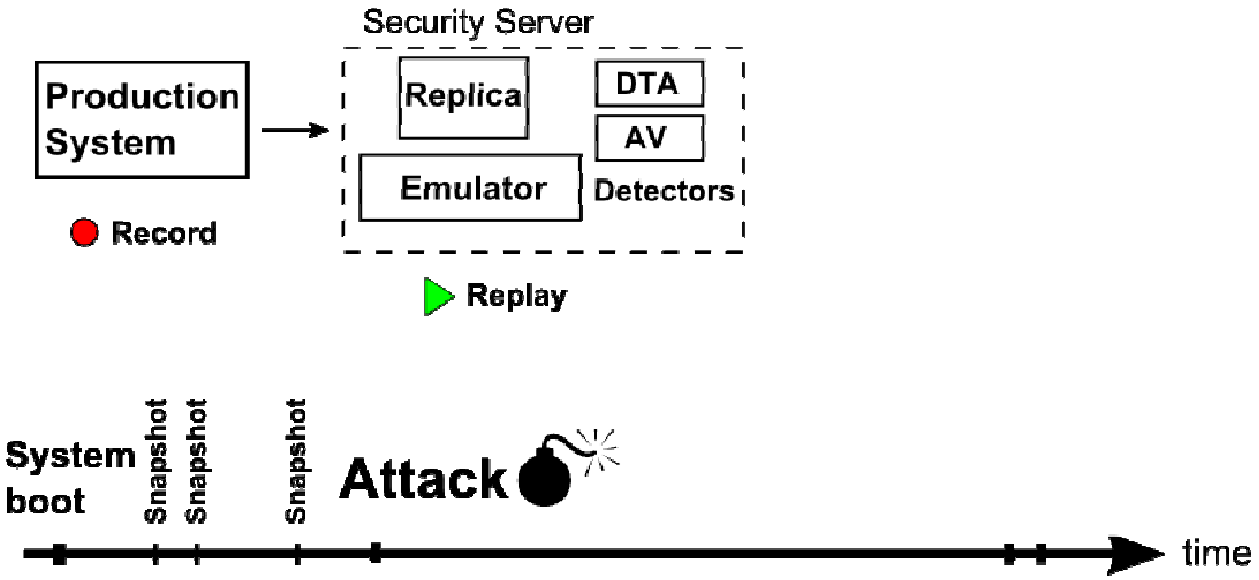
Recovery in decoupled security



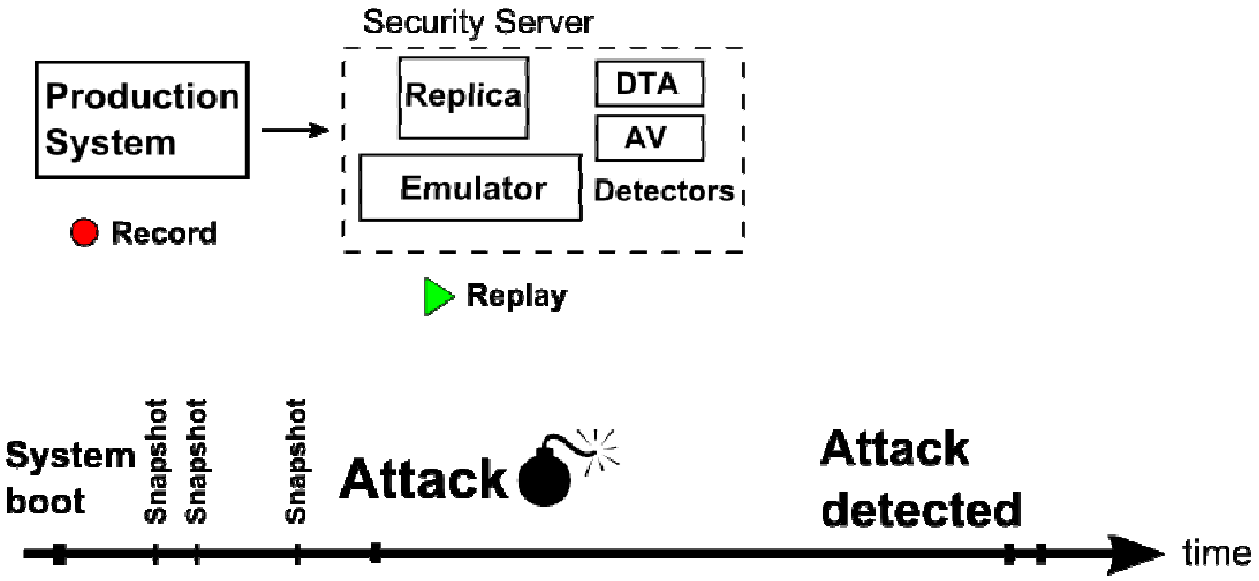
Recovery in decoupled security



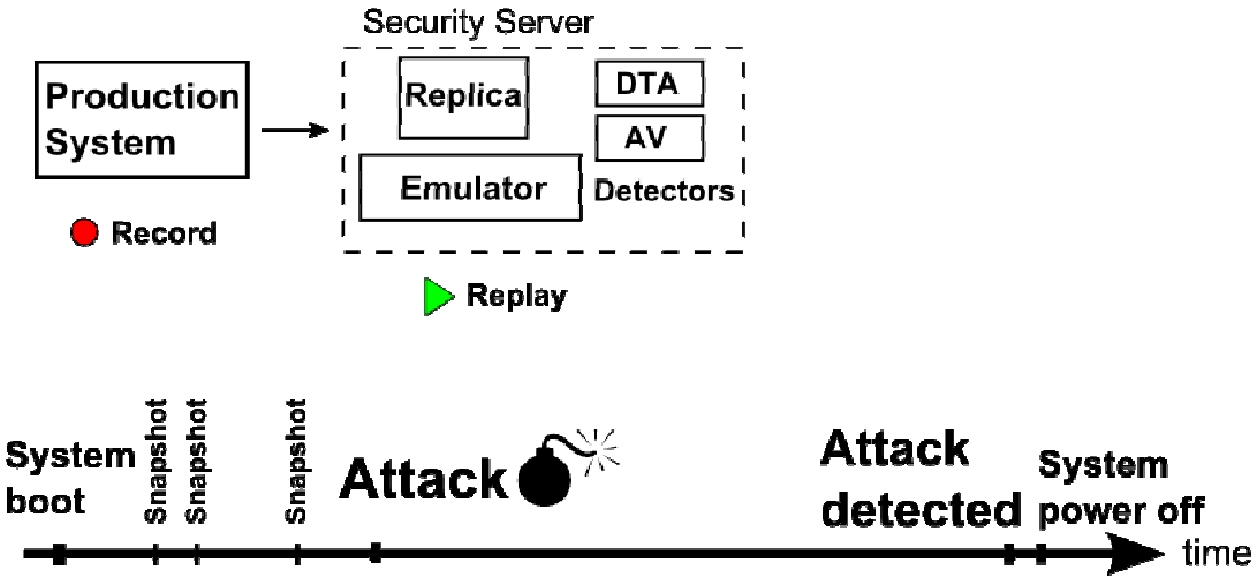
Recovery in decoupled security



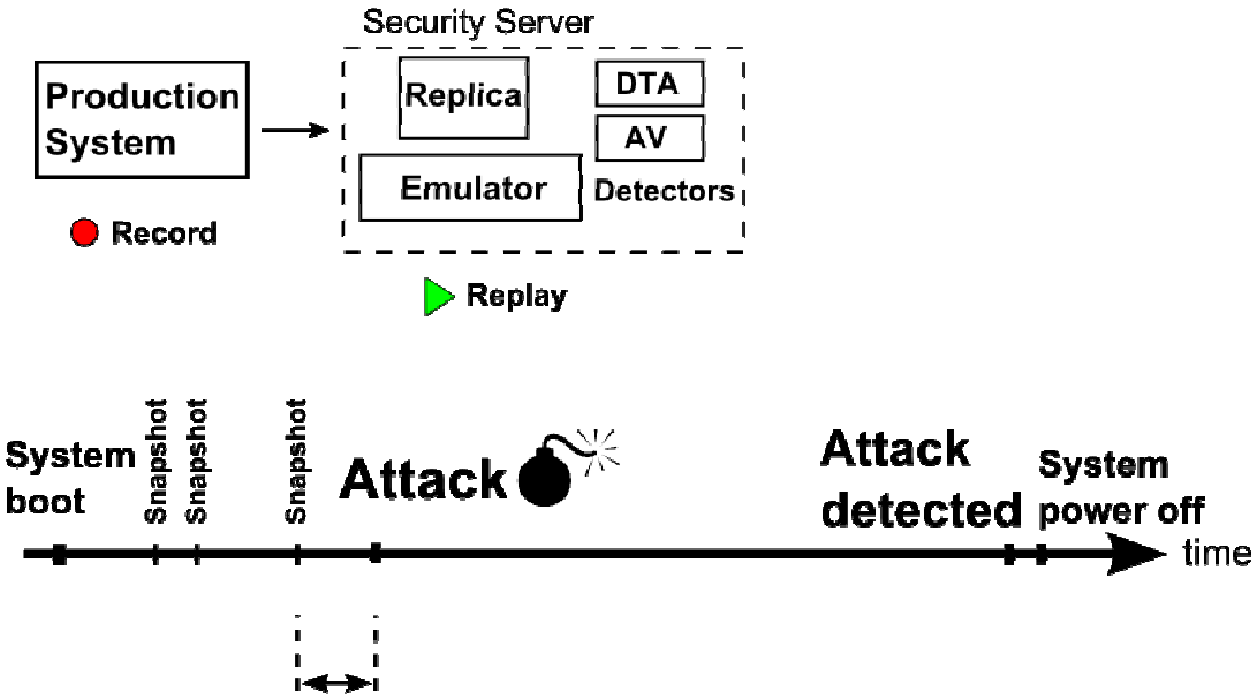
Recovery in decoupled security



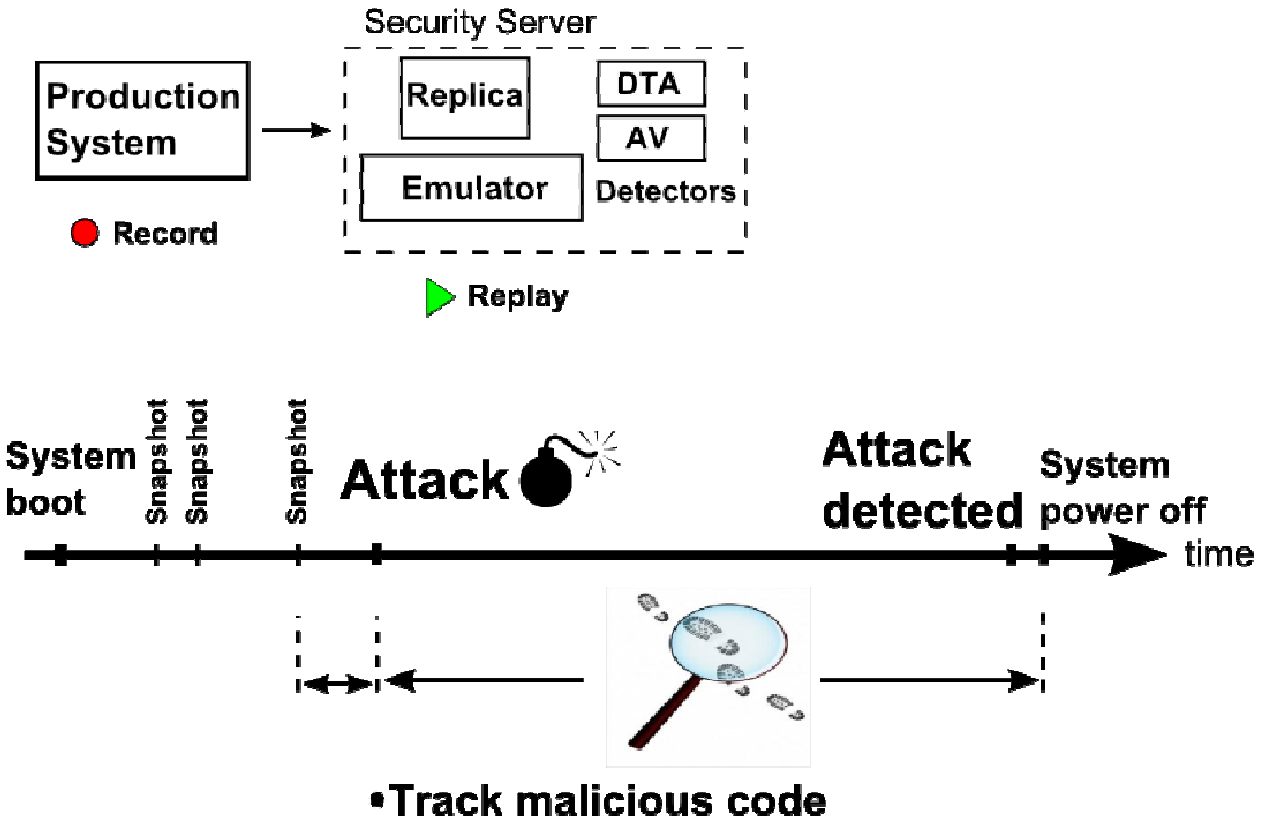
Recovery in decoupled security



Recovery in decoupled security

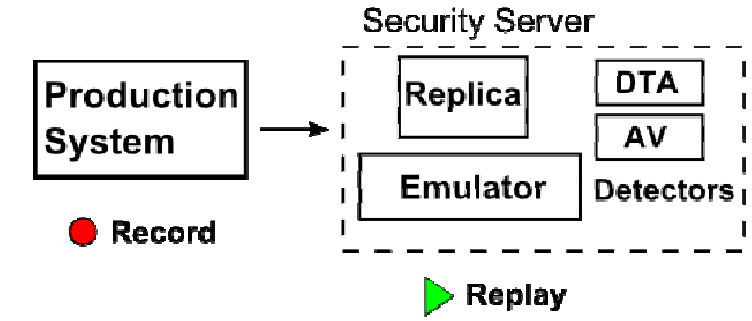


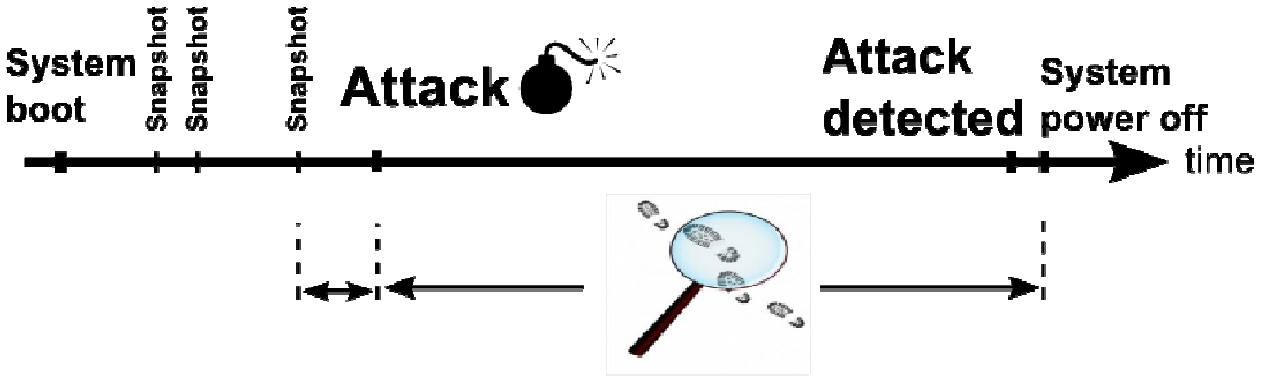
Recovery in decoupled security



- Track malicious code

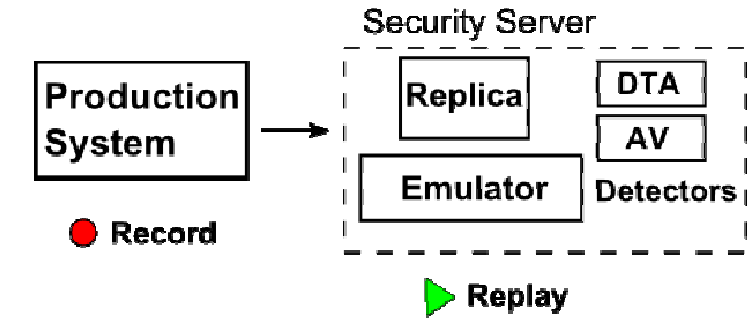
Recovery in decoupled security

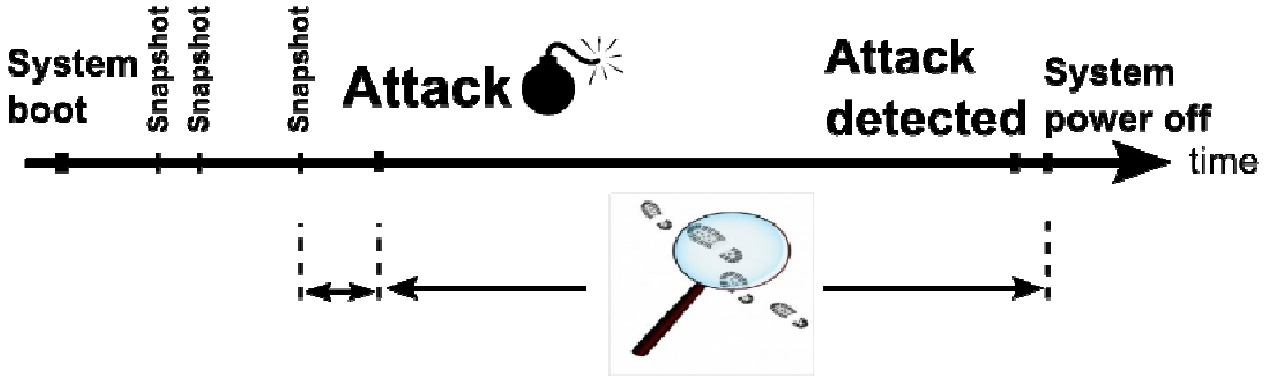




- Track malicious code
- Classify data: malicious, suspicious, clean

Recovery in decoupled security



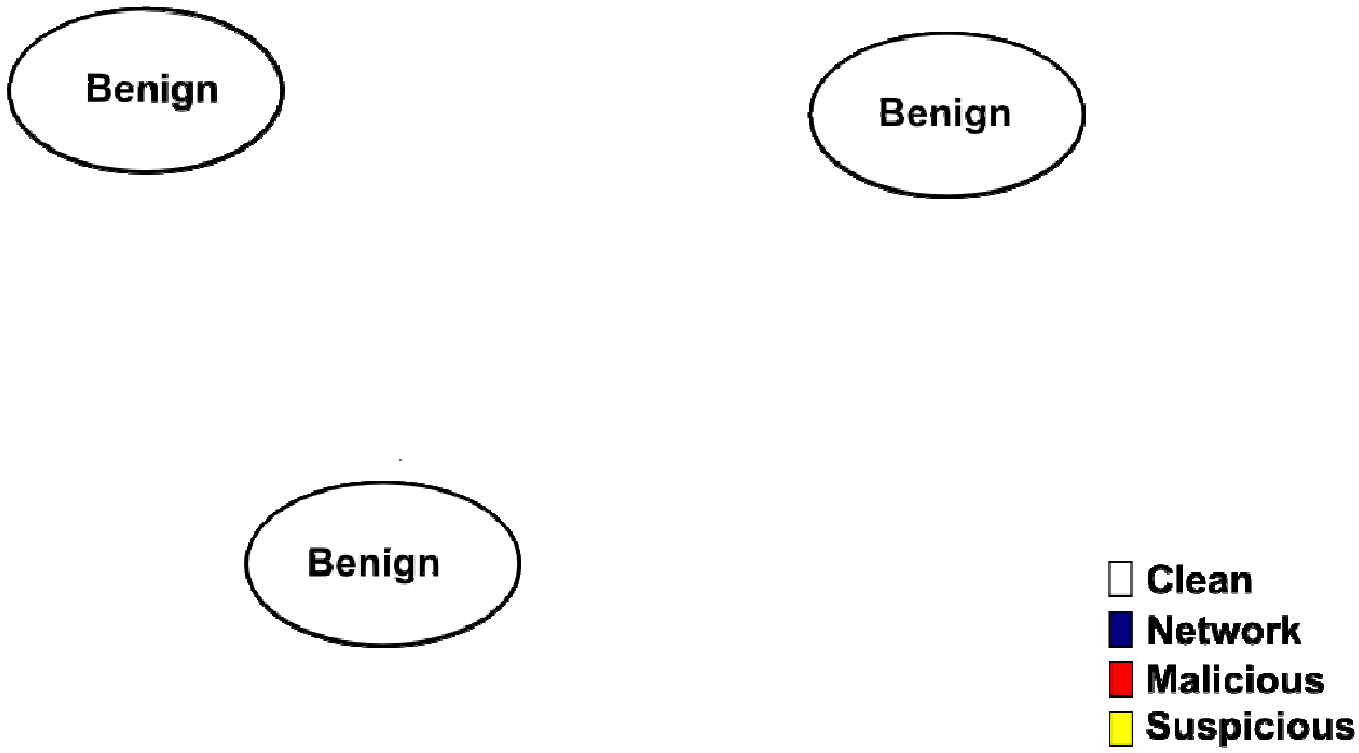


- Track malicious code
- Classify data: malicious, suspicious, clean
- Recover

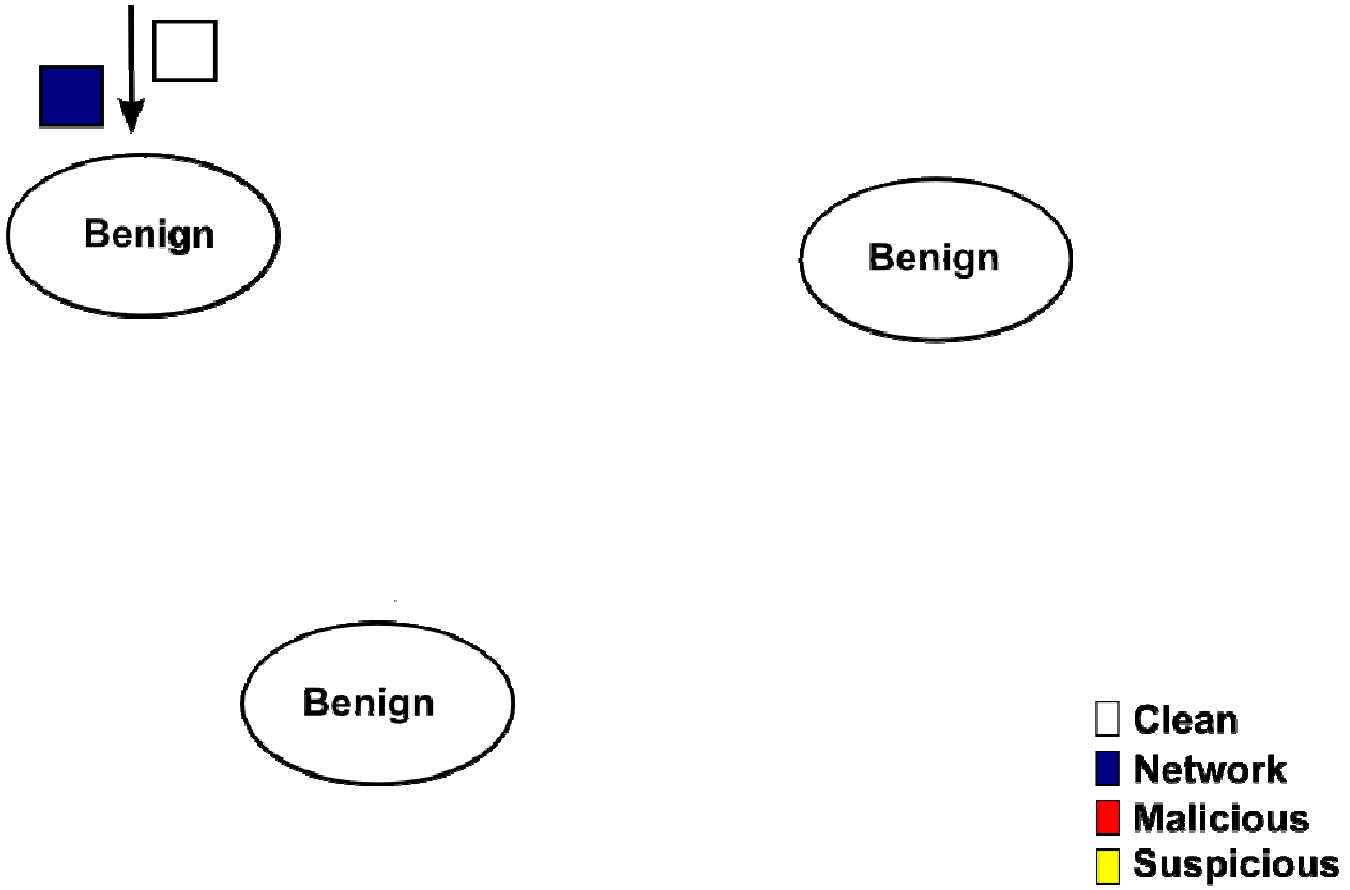
Attack detection

- Dynamic taint analysis (DTA):
  - Taint data from the network
  - Propagate taint on data copy, arithmetic operations.
  - Raise an alarm when network bytes modify the control flow of an application.
- AV:
  - Raise an alarm when a signature is detected in an application

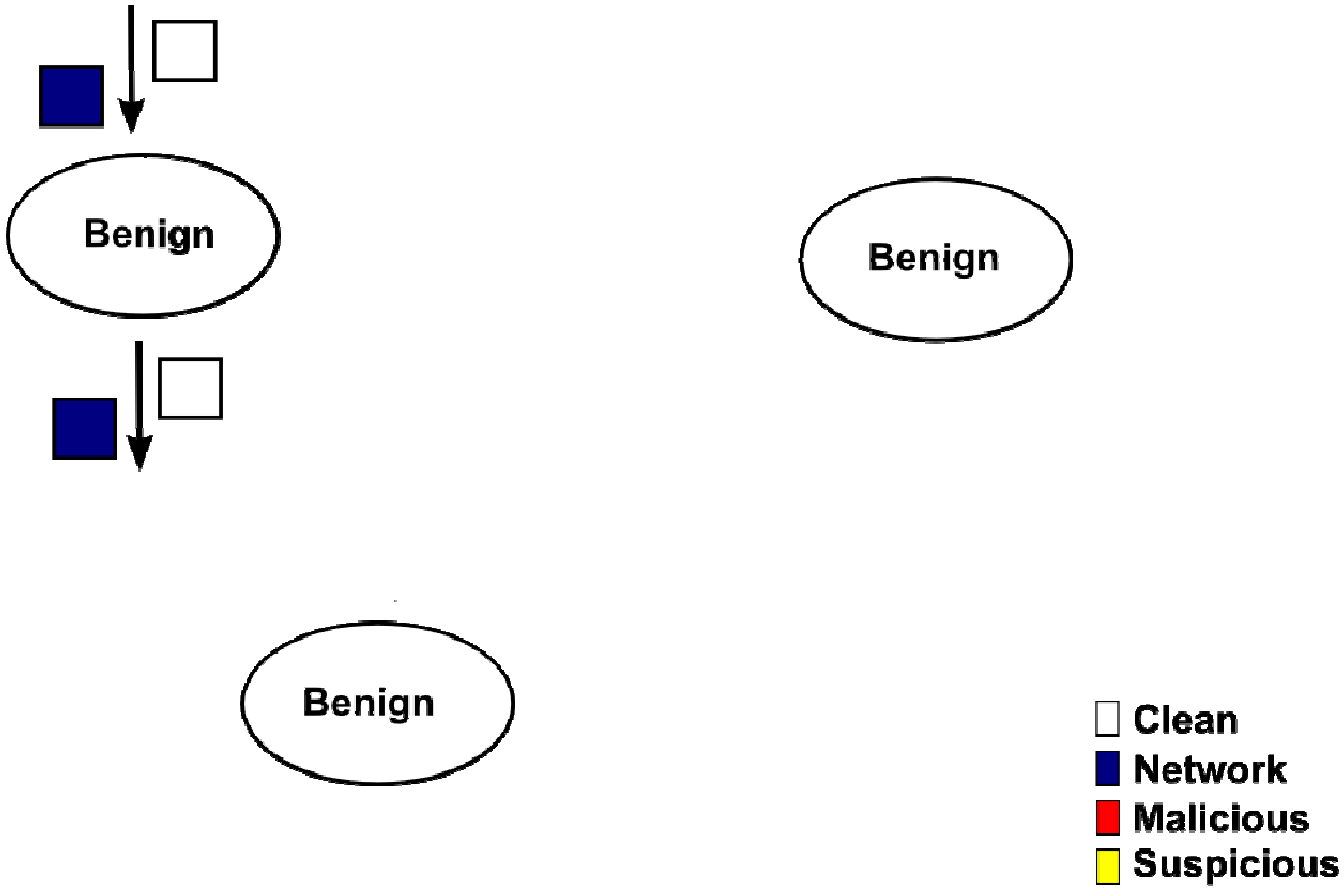
Taint Analysis – process tracking



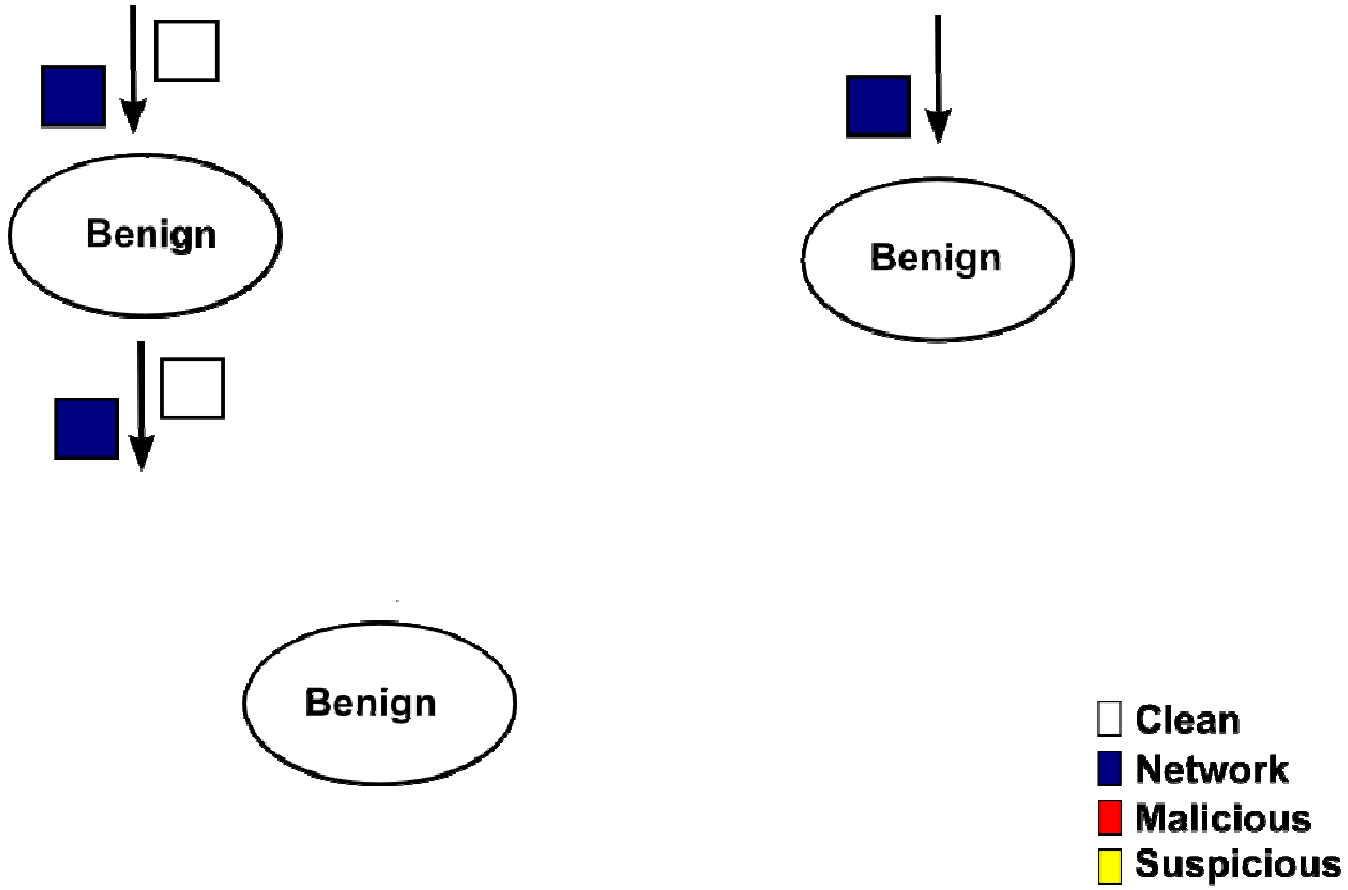
Taint Analysis – process tracking



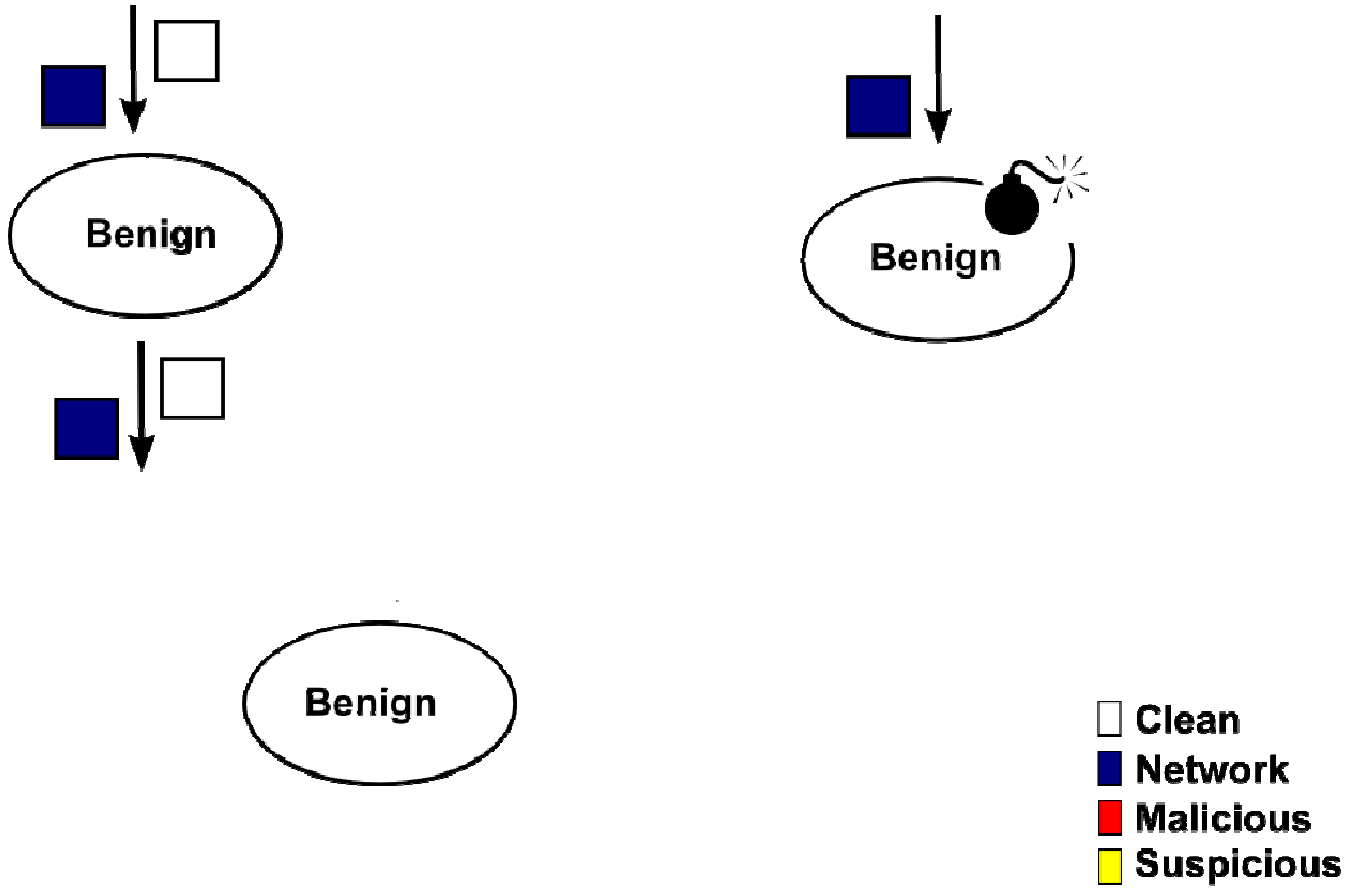
Taint Analysis – process tracking



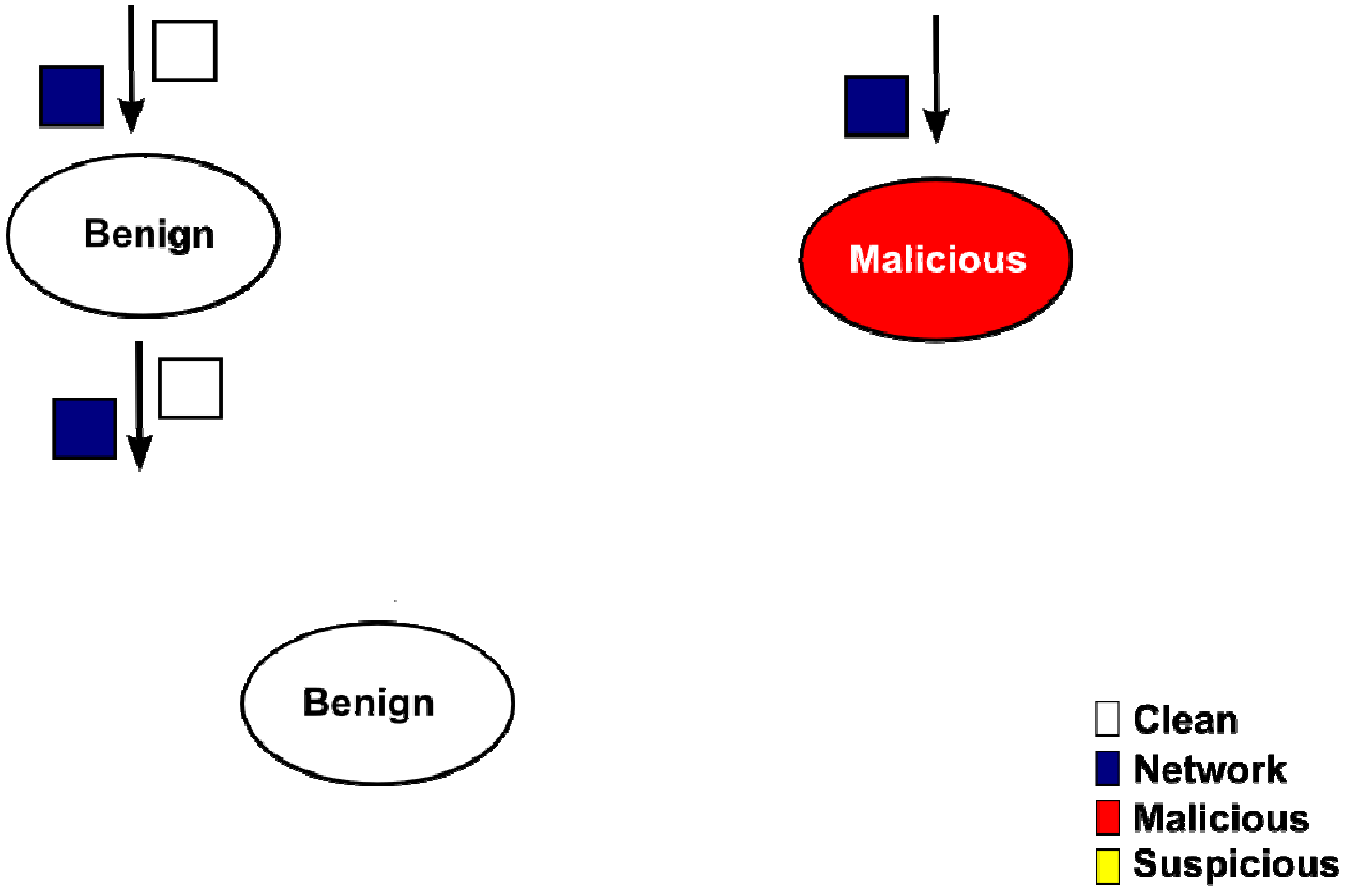
Taint Analysis – process tracking



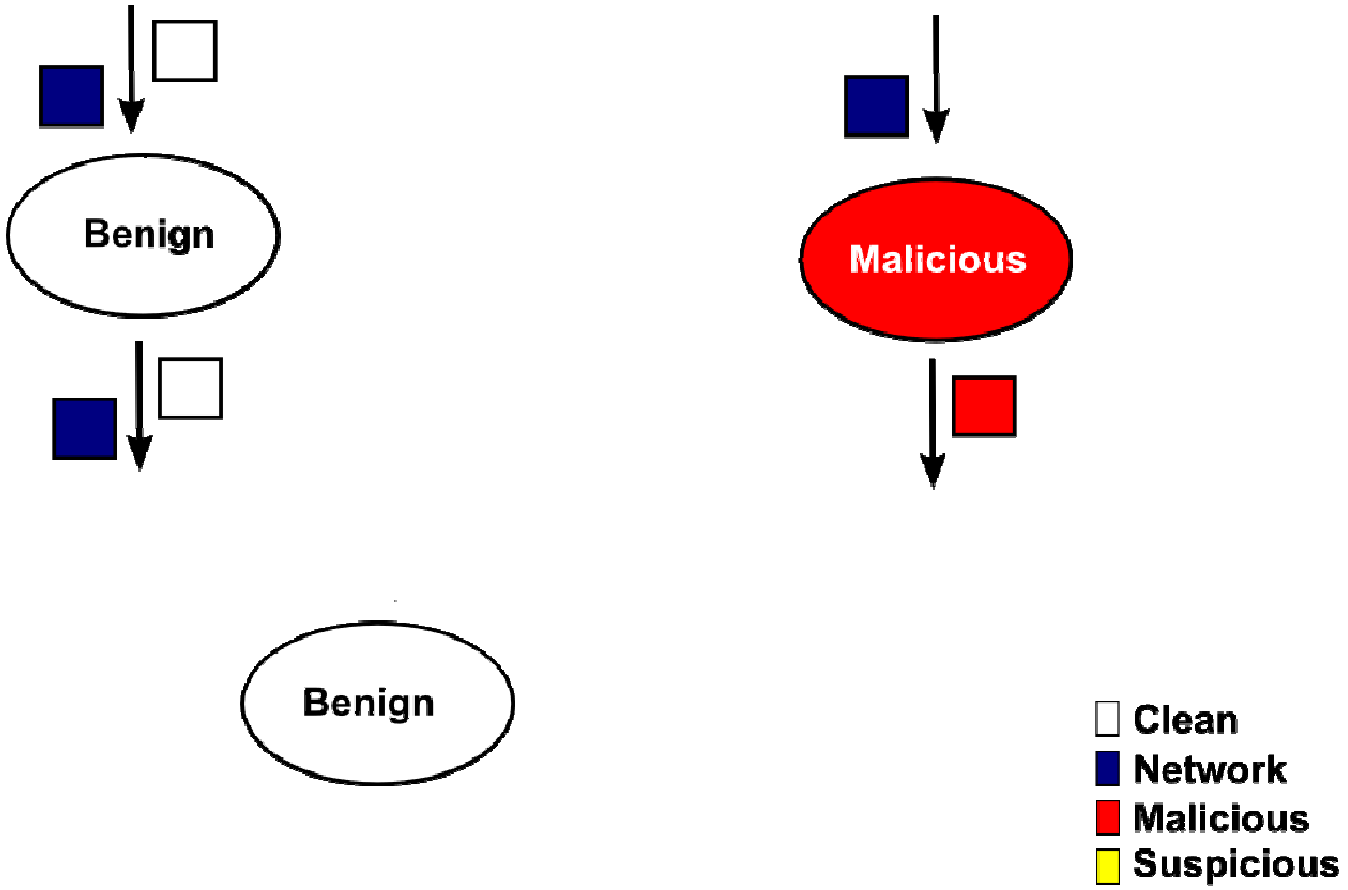
Taint Analysis – process tracking



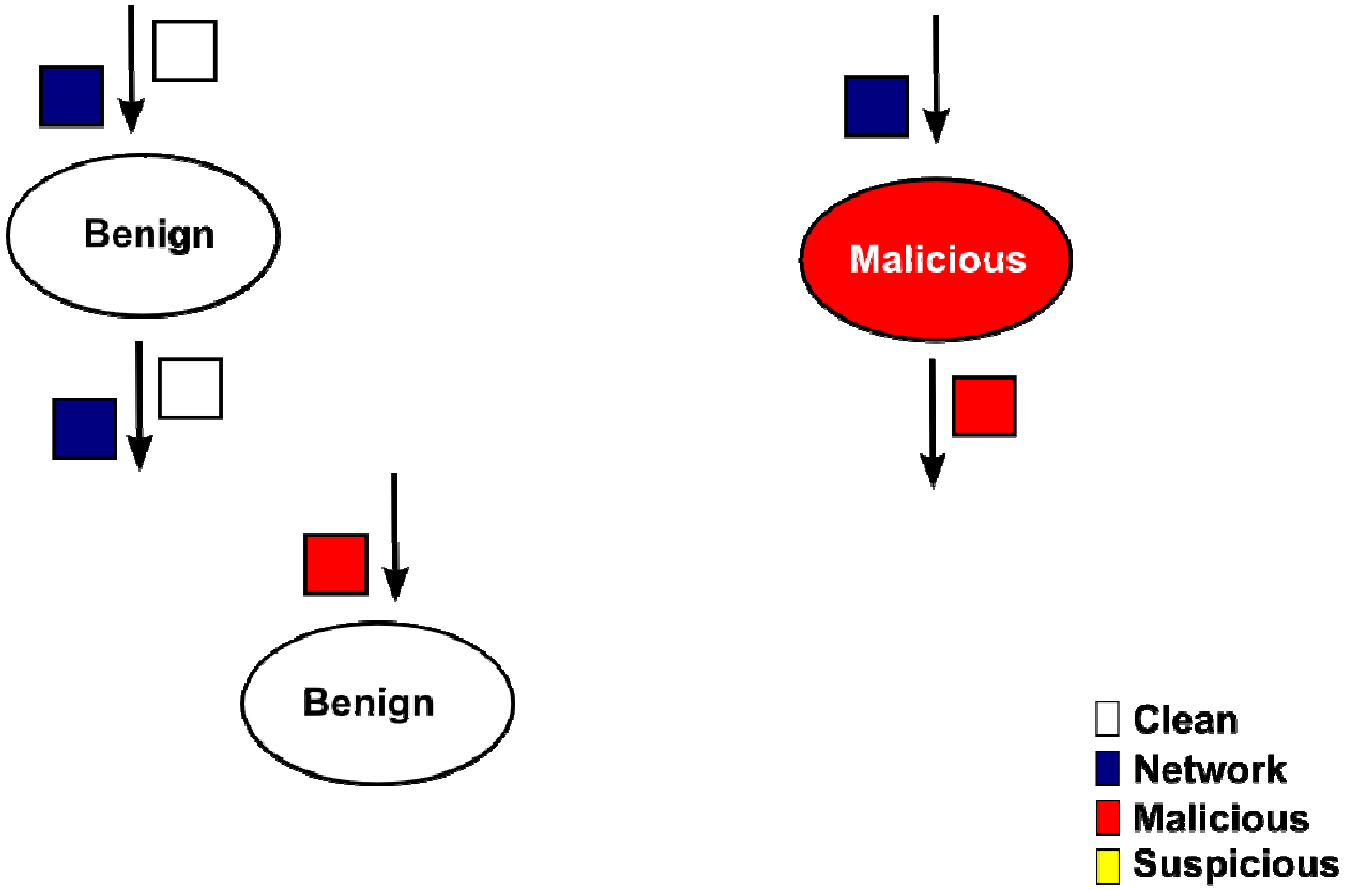
Taint Analysis – process tracking



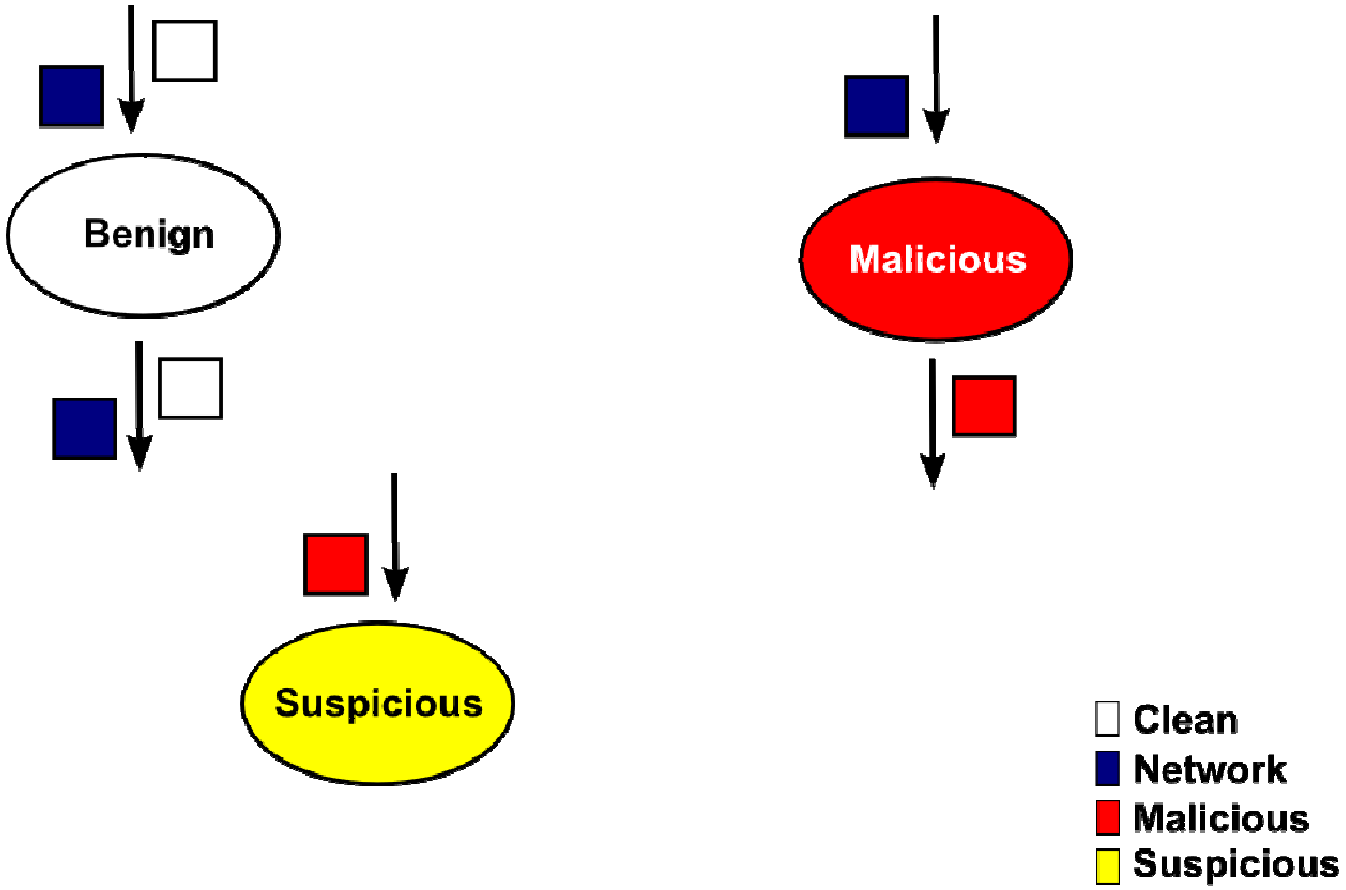
Taint Analysis – process tracking



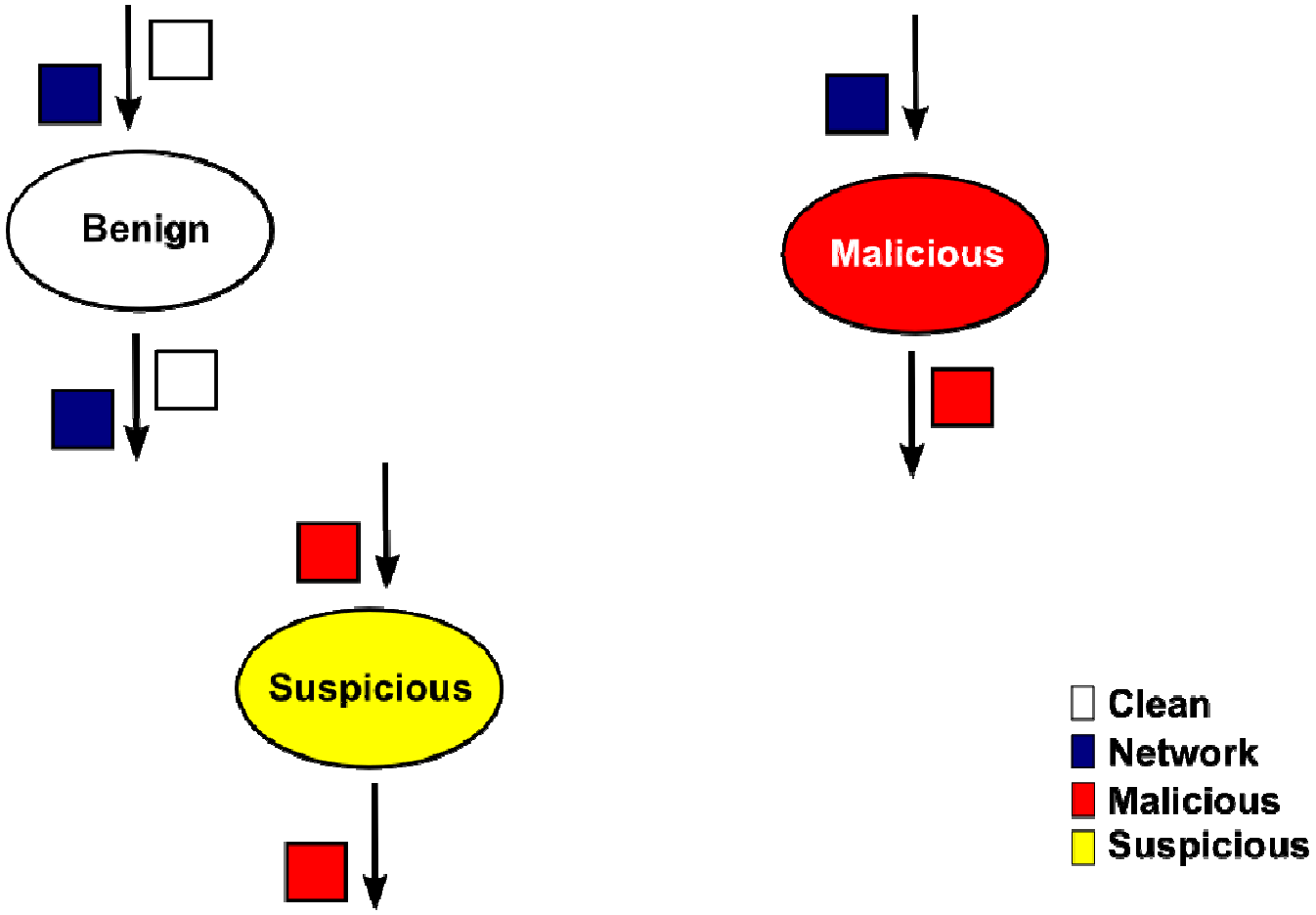
Taint Analysis – process tracking



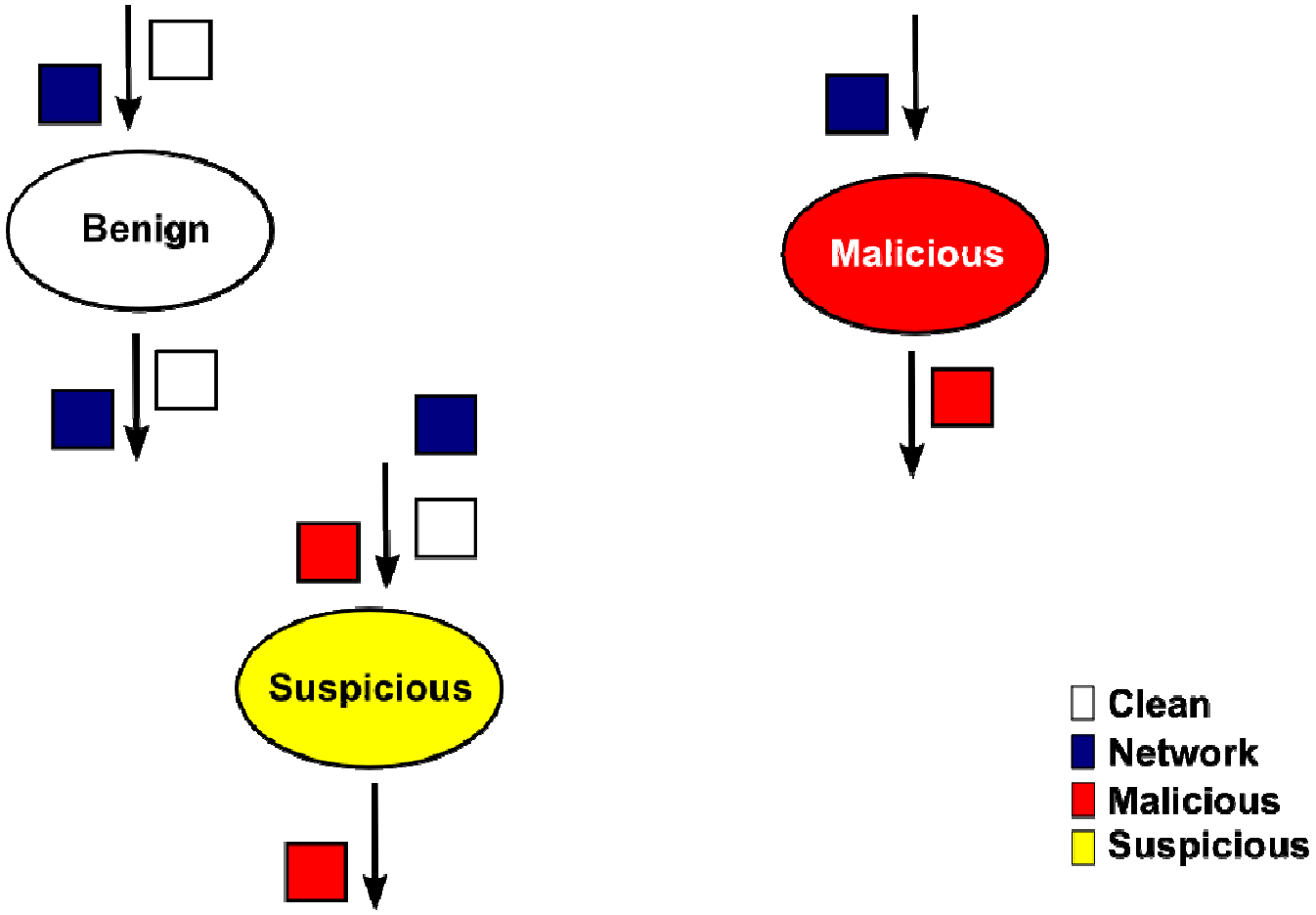
Taint Analysis – process tracking



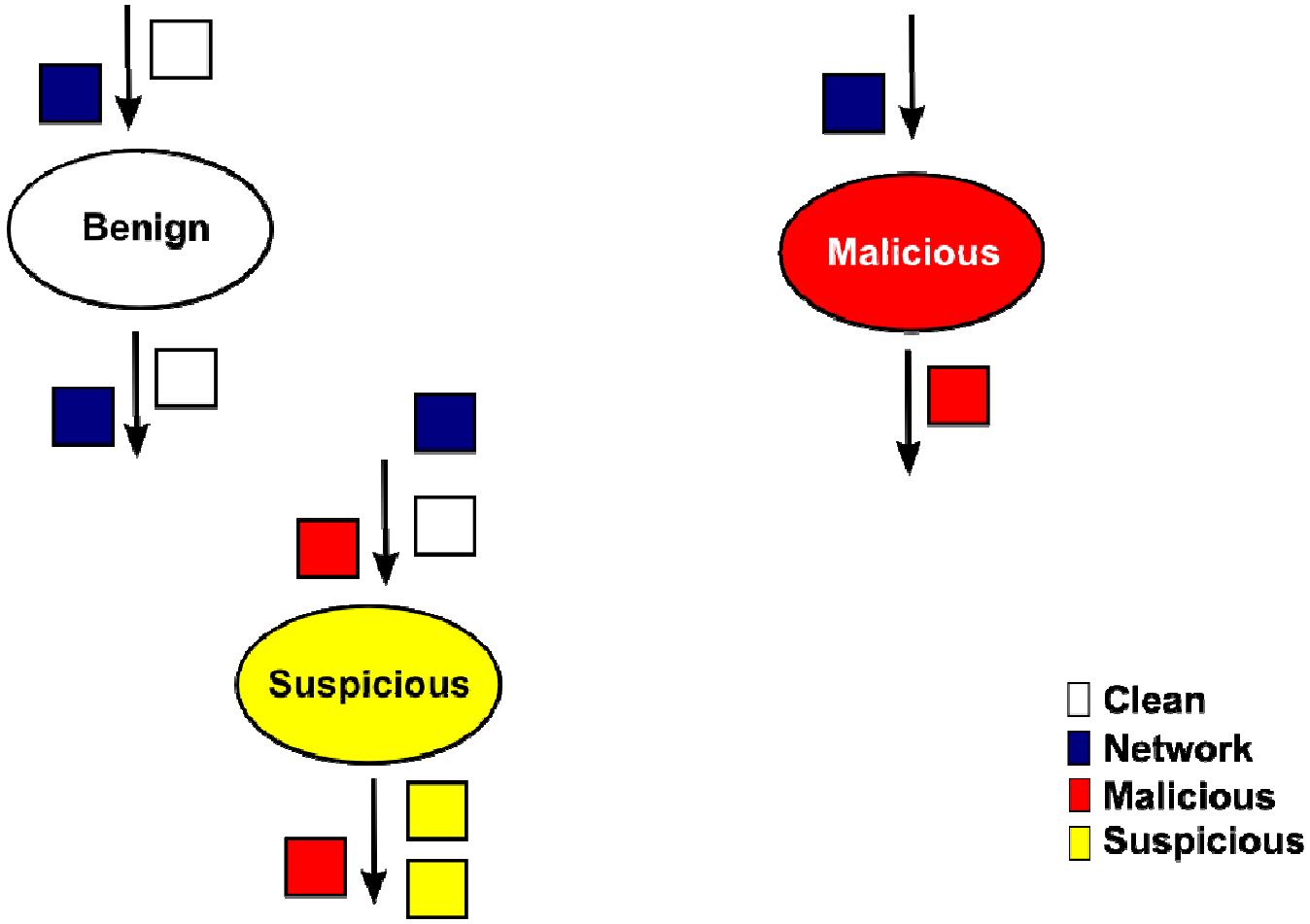
Taint Analysis – process tracking



Taint Analysis – process tracking



Taint Analysis – process tracking



Recovery

- Rollback to the initial intrusion moment.

  - DTA: a process control flow is modified.

  - AV: first write operation which contains a signature.

- Using the analysis logs recover only the benign data.

Evaluation

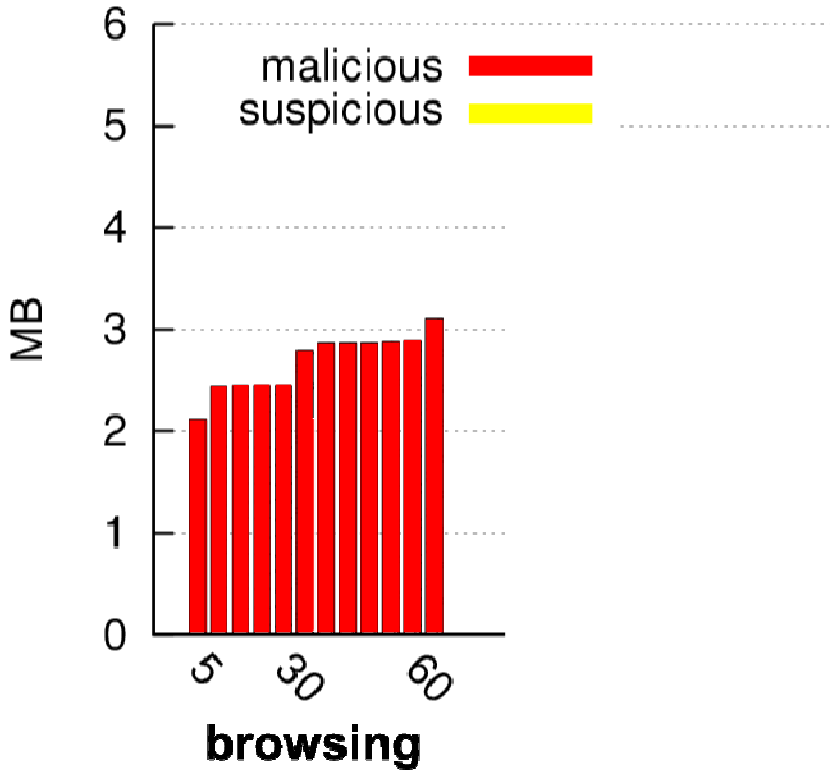
- Simple attack

  - replaced binaries: IE, FoxIT PDF Reader, Paint
  - detected after 1 hour

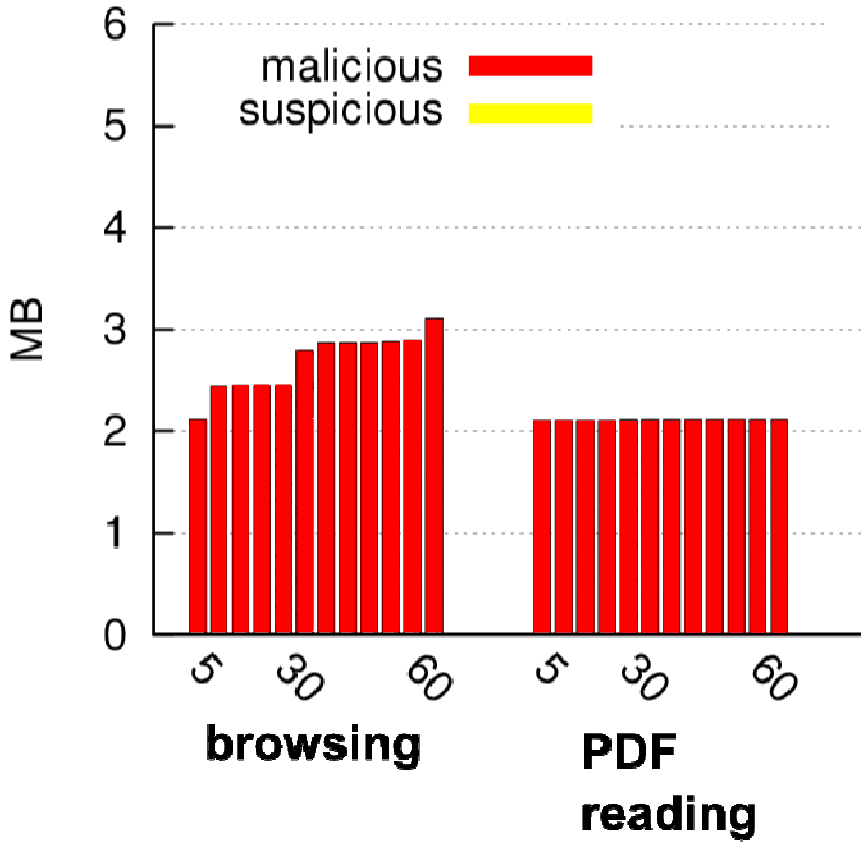
- Real world attack

  - Sality
  - detected after 3 days

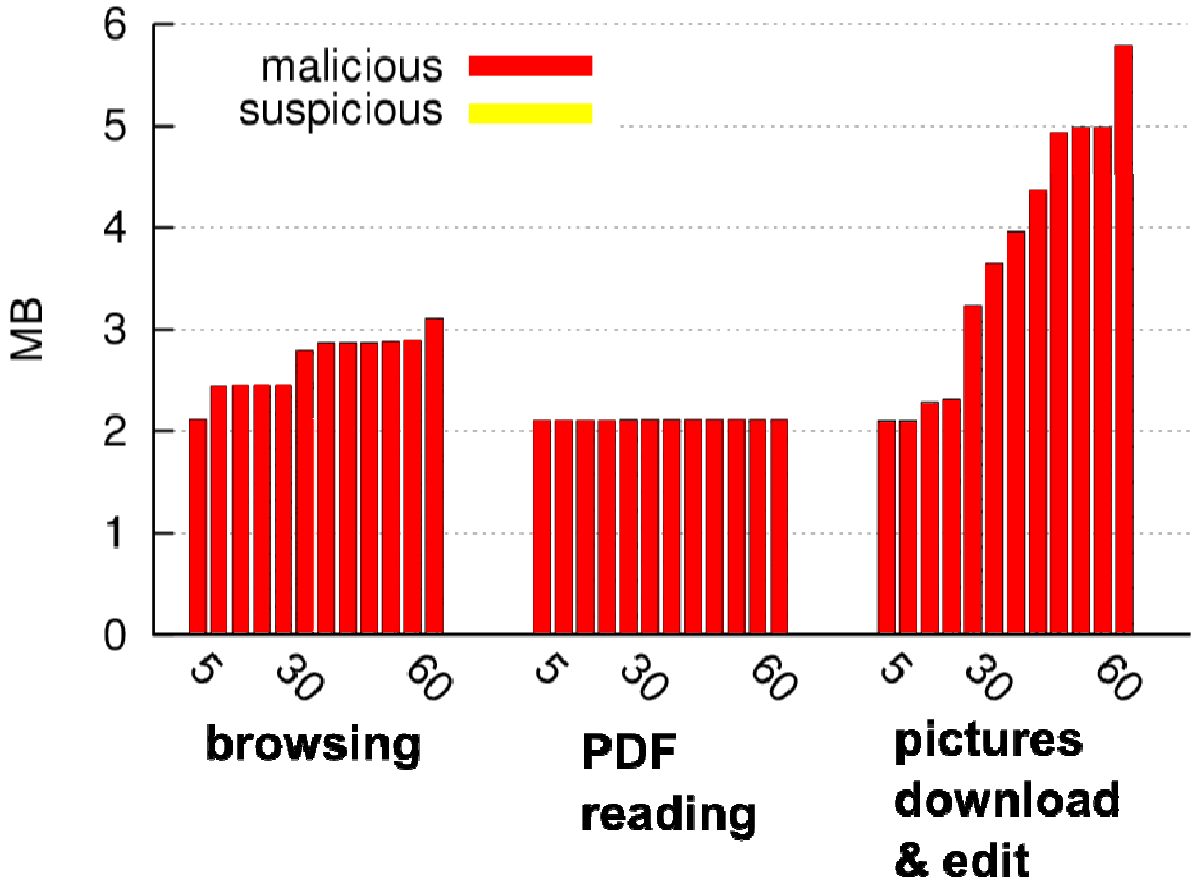
Simple attack taint spread



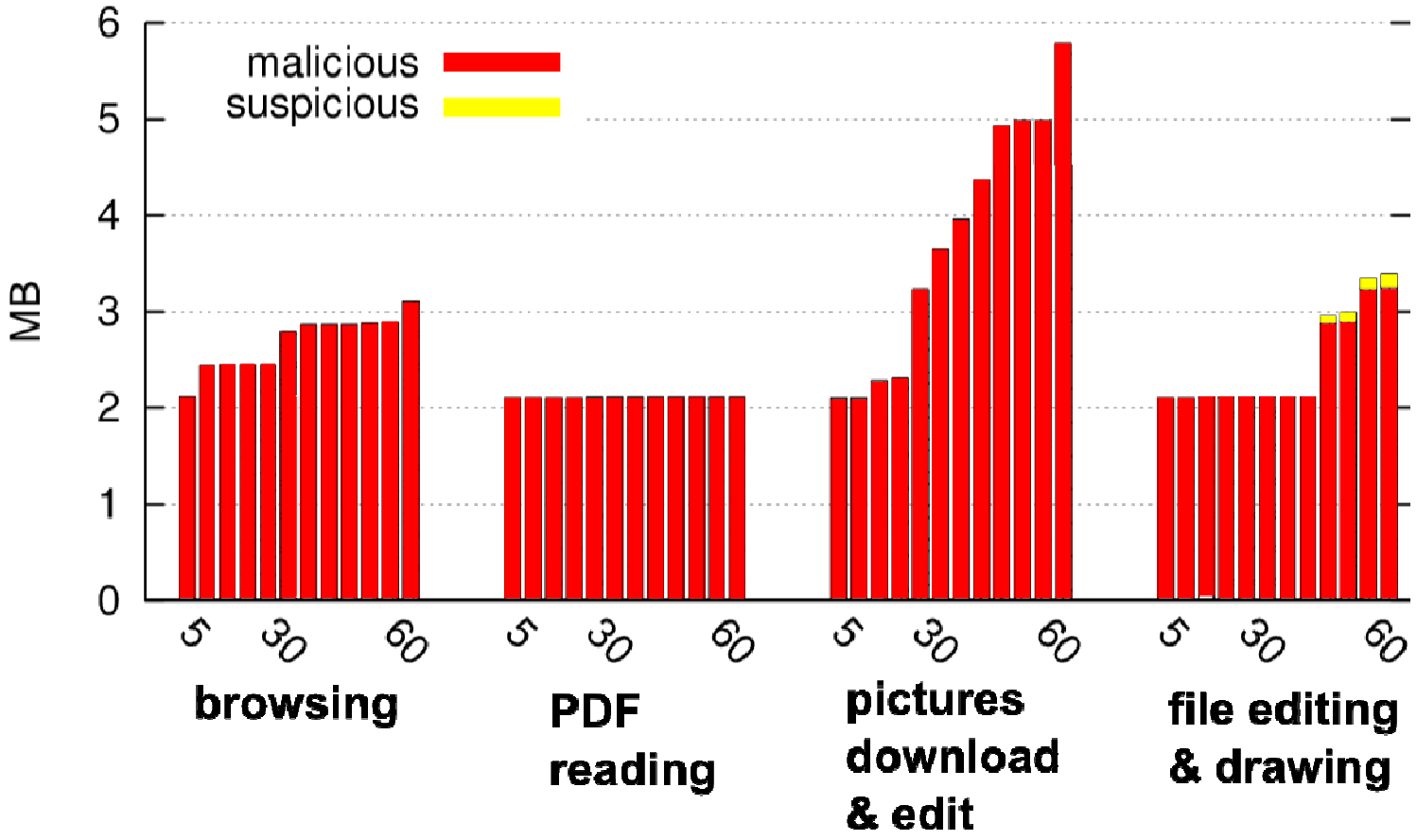
Simple attack taint spread



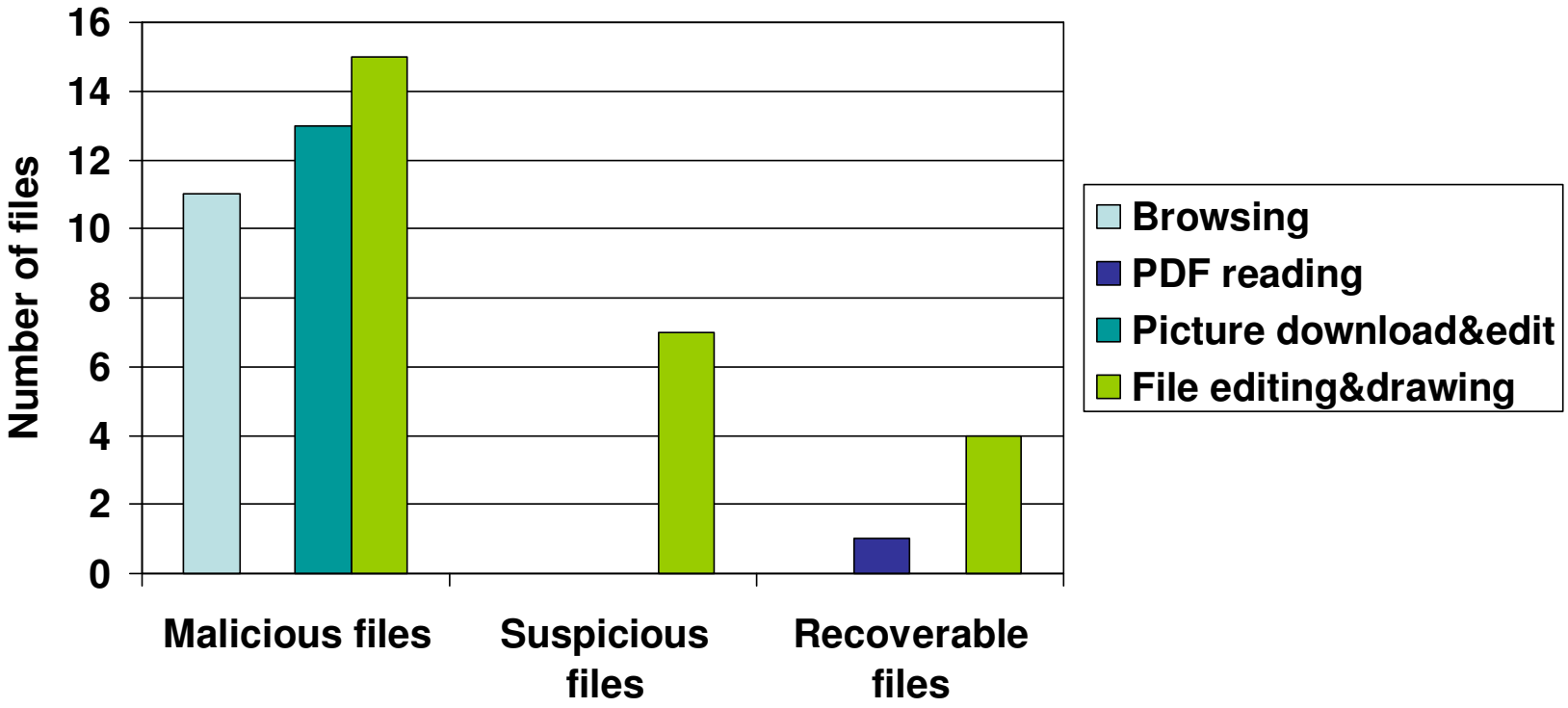
Simple attack taint spread



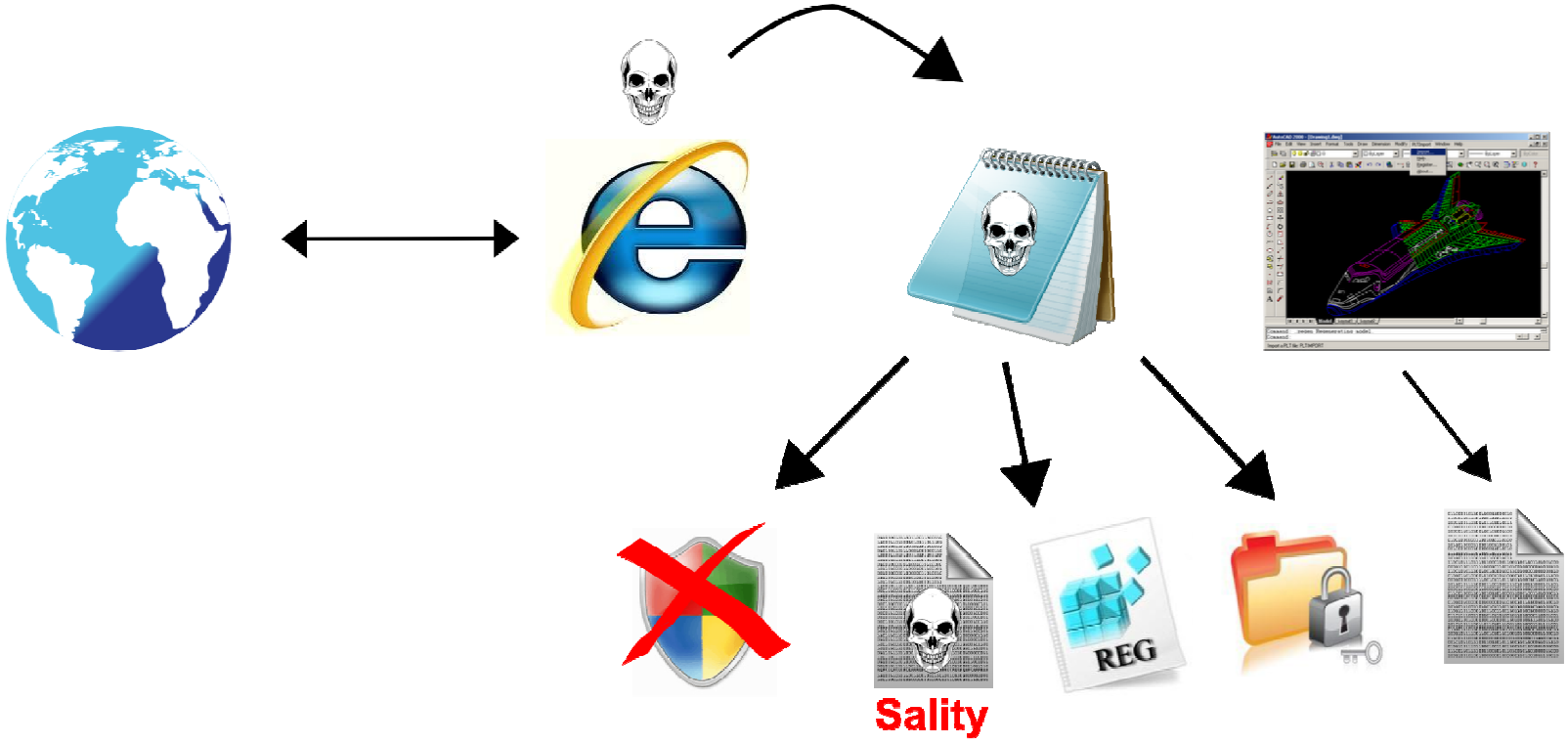
Simple attack taint spread on disk



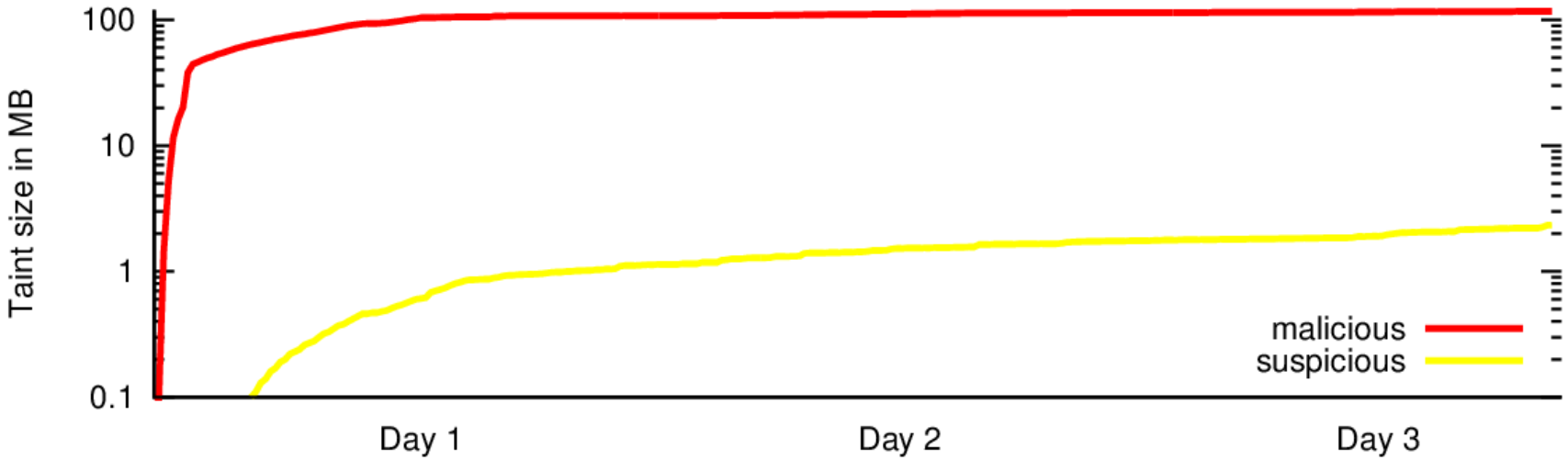
Simple attack recovery



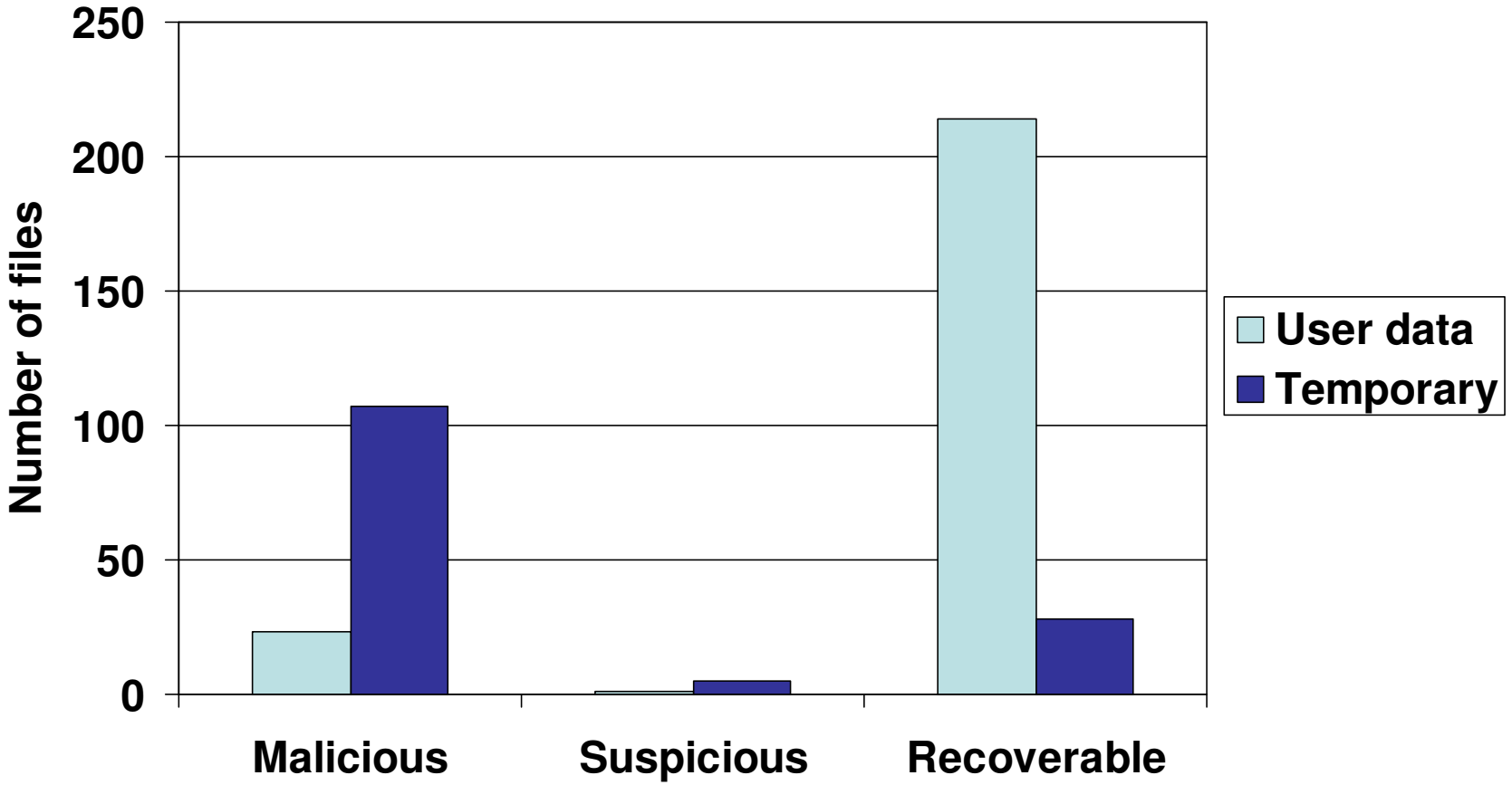
Attack: Sality/Win32



Sality/Win32 taint spread on disk



Sality/Win32 recovery



Conclusions

- Recover from complicated attacks to the state before the attack.
- Analyze the actions of malicious code and classify the bytes on the physical drive.
- Restore files up to the attack and recover the benign files edited or created after the attack.

Sality/Win32