Survivability Analysis of a Computer System under an Advanced Persistent Threat Attack

Ricardo J. Rodríguez[†], Xiaolin Chang[‡], Xiaodan Li[§], Kishor S. Trivedi[§]

rjrodriguez@unizar.es, xlchang@bjtu.edu.cn, {xiaodan.li,ktrivedi}@duke.edu

Universidad Zaragoza

Duke UNIVERSITY

[†]University of Zaragoza
[†]Second University of Naples

[‡]Beijing Jiaotong University

[§]Duke University

June 27, 2016

3rd International Workshop on Graphical Models for Security
Lisbon, Portugal

Introduction (I)

- Cyberattacks are rapidly increasing
  - $+38\%$ in 2015[a]
  - Cybercrime is a growing (and quite wealthy) industry
- High cost for companies (estimated cost of $\$575B$)
  - Service downtime and cleanup of compromised systems
  - Loss of customer confidence, even data theft

[a] https://news.sap.com/pwc-study-biggest-increase-in-cyberattacks-in-over-10-years/

Universidad Zaragoza 1542

Introduction (I)

- Cyberattacks are rapidly increasing
  - $+38\%$ in 2015[a]
  - Cybercrime is a growing (and quite wealthy) industry
- High cost for companies (estimated cost of $\$575B$)
  - Service downtime and cleanup of compromised systems
  - Loss of customer confidence, even data theft

[a] https://news.sap.com/pwc-study-biggest-increase-in-cyberattacks-in-over-10-years/

Just a little bit scared...

- Critical infrastructures: provide essential services to the society
  - Examples: power distribution, water treatment, financial services...
  - Discontinuity of service may lead to fatalities or injuries
    - Different nature, from unintended acts of nature to intentional attacks (e.g., sabotage, terrorism)
  - Cyberattacks to these systems have an increasing trend

Introduction (II)

Malware

- Specially crafted software with one goal: achieve malicious activities
- Different types of malware, depending on their behaviour
  - Viruses, worms, keyloggers, ransomware, etc.

Universidad Zaragoza
1542

Introduction (II)

Malware

- Specially crafted software with one goal: achieve malicious activities
- Different types of malware, depending on their behaviour
  - Viruses, worms, keyloggers, ransomware, etc.

Advanced Persistent Threat (APT)

- **Advanced**: sophisticated attack
  - Involves a previous reconnaissance of the target
- **Persistent**: long-term staying
  - The longer they stay in the system, the more data are exfiltrated

Universidad Zaragoza 1542

Introduction (II)

Malware

- Specially crafted software with one goal: achieve malicious activities
- Different types of malware, depending on their behaviour
  - Viruses, worms, keyloggers, ransomware, etc.

Advanced Persistent Threat (APT)

- **Advanced**: sophisticated attack
  - Involves a previous reconnaissance of the target
- **Persistent**: long-term staying
  - The longer they stay in the system, the more data are exfiltrated

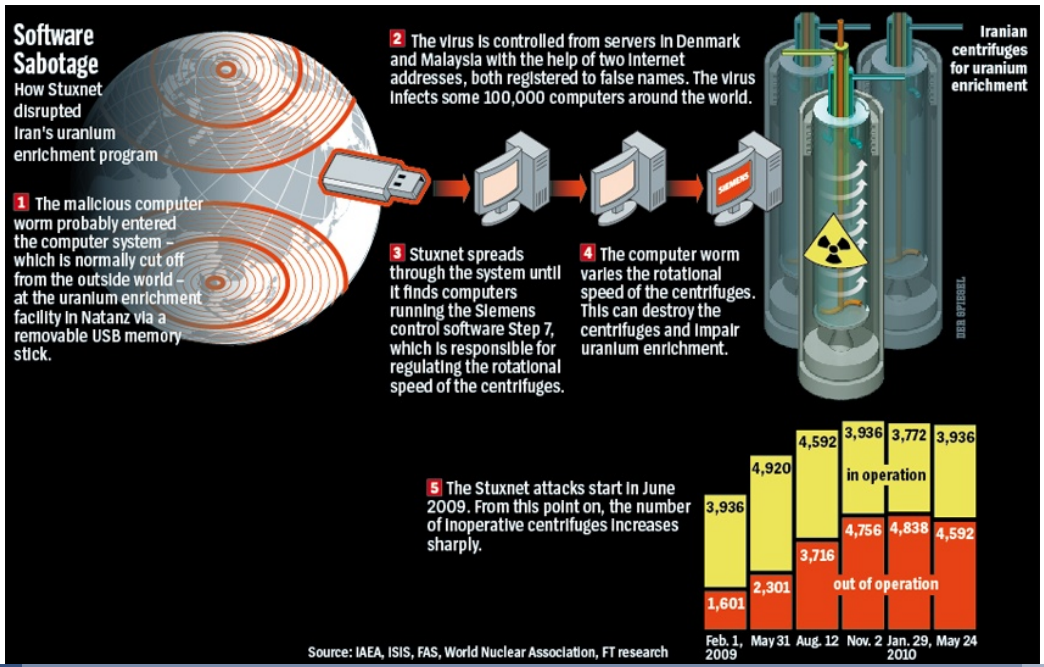
Knowledge is power

Universidad Zaragoza 1542

Introduction (III)

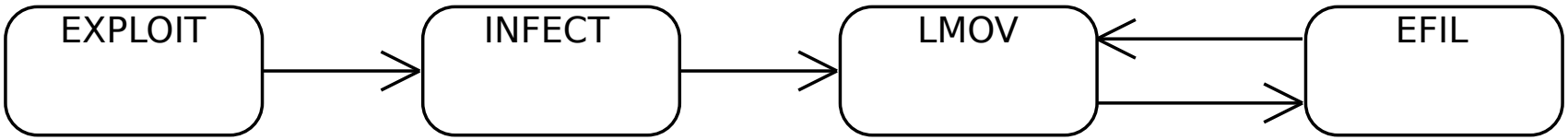
APT examples

- `Operation Aurora`: attributed to China, in 2010 a lot of companies from different domains (such as Google, Yahoo, Morgan Stanley, or Dow Chemicals) were attacked
- `Stuxnet`: attributed to US-Israel and discovered in 2010, affected to Siemens PLCs of SCADA networks in Iran nuclear facilities
- Others: `GhostNet`, `Duqu`, `Flame`, `...`



Introduction (IV)

APT life-cycle

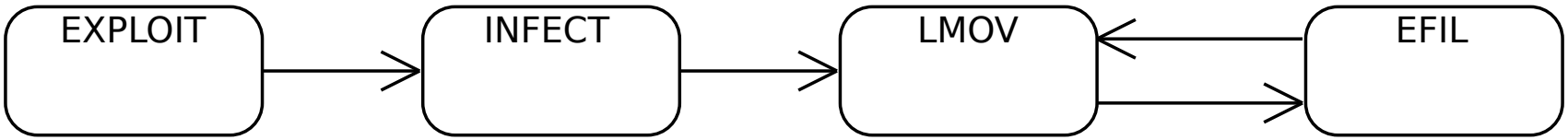


1. Entry point/exploitation: 0-days or known but not fixed vulnerabilities
2. Infection: make persistence. Normally, also installs RAT tools
3. Lateral movement: move through the network, looking data of interest and other hosts to compromise
4. Exfiltration: modify or send out network boundaries sensitive data

Universidad Zaragoza 1542

Introduction (IV)

APT life-cycle



1. Entry point/exploitation: 0-days or known but not fixed vulnerabilities
2. Infection: make persistence. Normally, also installs RAT tools
3. Lateral movement: move through the network, looking data of interest and other hosts to compromise
4. Exfiltration: modify or send out network boundaries sensitive data

Survivability

- *System's ability to withstand malicious attacks and support the system's mission even when parts of the system are damaged*
- Assessing the impact of an APT allows to characterize a system against those intended failures and evaluate mitigation techniques

Introduction (V)

Contribution

- Survivability assessment of a computer system under an APT attack
- Security model (as a Stochastic Reward Net)
  - Integrates defender + attacker actions
- Assumptions made: event times are exponentially distributed
- Four survivability metrics
  1. System recovery
  2. System availability
  3. Data confidentiality loss
  4. Data integrity loss
- . . . after a vulnerability is announced, and during vulnerability mitigation strategy is being deployed

Universidad Zaragoza 1542

Related Work

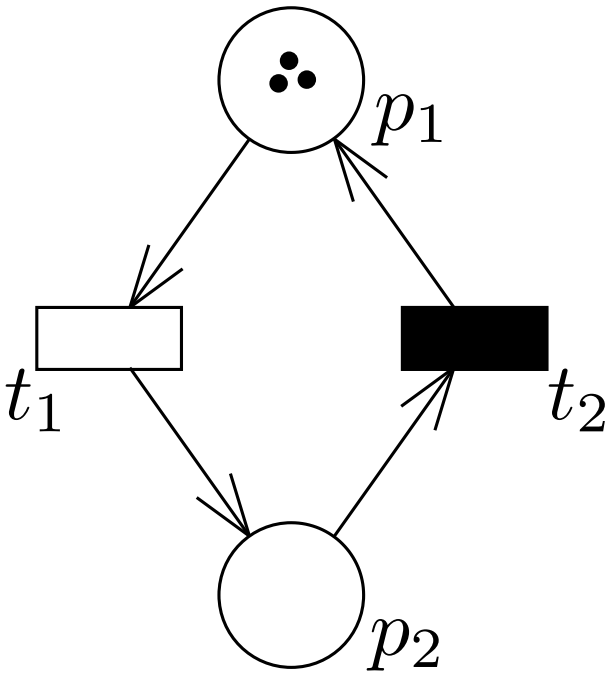
Survivability metrics

- Little research on quantitative evaluation metrics
  - Survivability of a resilient database system against intrusions, modeled with CTMC. Later, extended to semi-Markov processes (Wang et al., 2006, 2010)
  - General approach for survivability quantification of networked systems using SRNs (Trivedi and Xia, 2015)
  - Survivability assessment of Saudi Arabia crude-oil pipeline network (Rodríguez et al., 2015)

Our model allows us. . .

- Not only availability analysis, also confidentiality and integrity (loss)
- Investigate security attributes during the transient period that:
  - Starts after a vulnerability is publicly announced
  - Ends when the vulnerability is fully removed
- Quantitative assessment of these attributes
- Insights on cost/benefit trade-offs of investments

Background

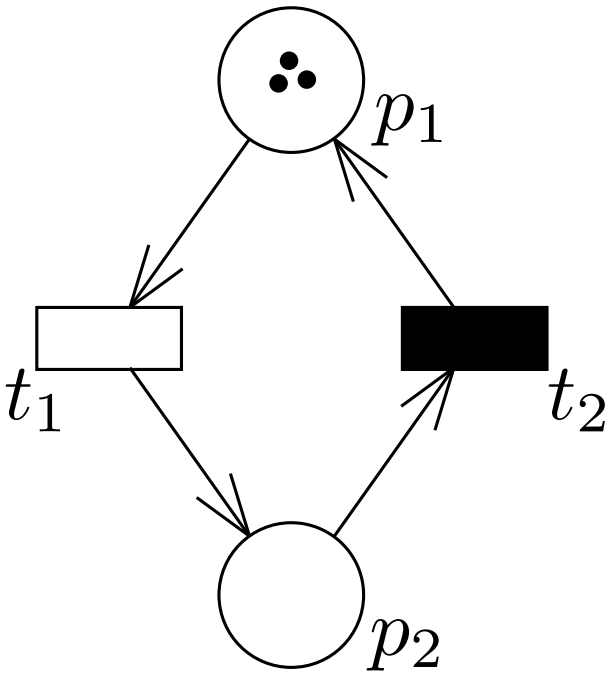


Petri nets – explanation simplified

- Underlying Markov-chain
- Places (circles, p_X)
- Transitions (bars, t_X)
- Time interpretation
- Tokens (black dots)

Universidad Zaragoza
1542

Background



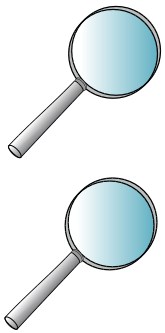
Petri nets – explanation simplified

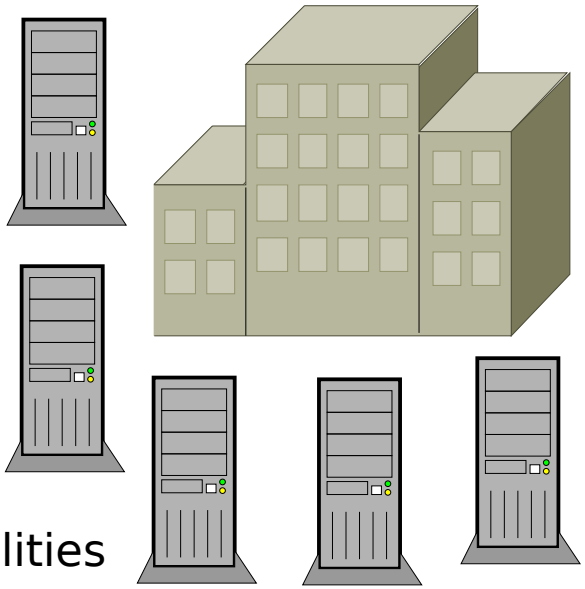
- Underlying Markov-chain
- Places (circles, p_X)
- Transitions (bars, t_X)
- Time interpretation
- Tokens (black dots)

Extensions

- Stochastic PNs: exponentially distributed firing time in transitions
- Generalized SPNs: immediate + timed transitions (any distribution)
  - Also inhibitor arcs
- **Stochastic Reward Nets**: GSPN + reward functions at net level

System Description and Model (I)

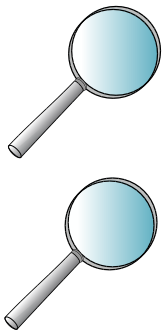


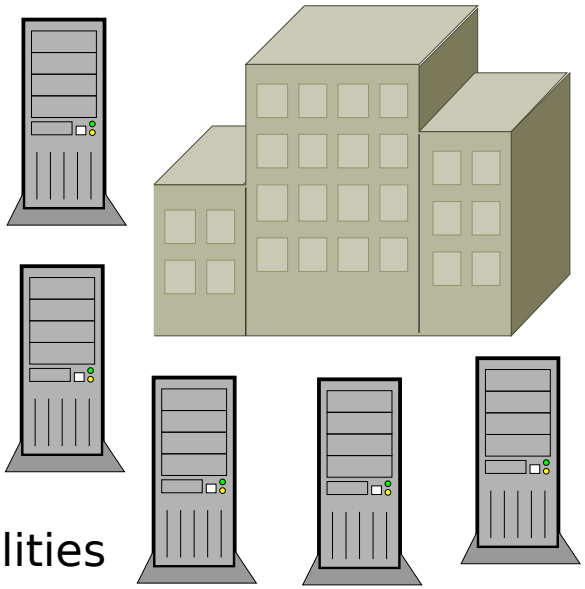


* Not known vulnerabilities
* Not skill enough to find 0-day vulnerabilities

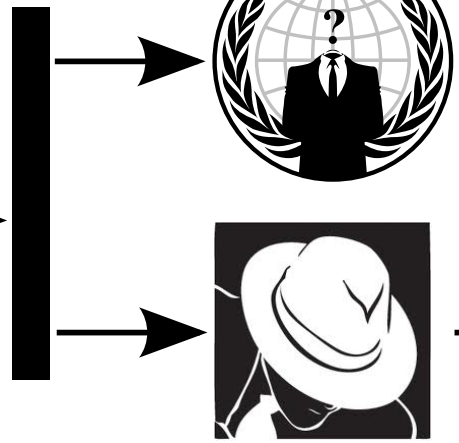
Universidad Zaragoza
1542

System Description and Model (I)





* Not known vulnerabilities
* Not skill enough to find 0-day vulnerabilities

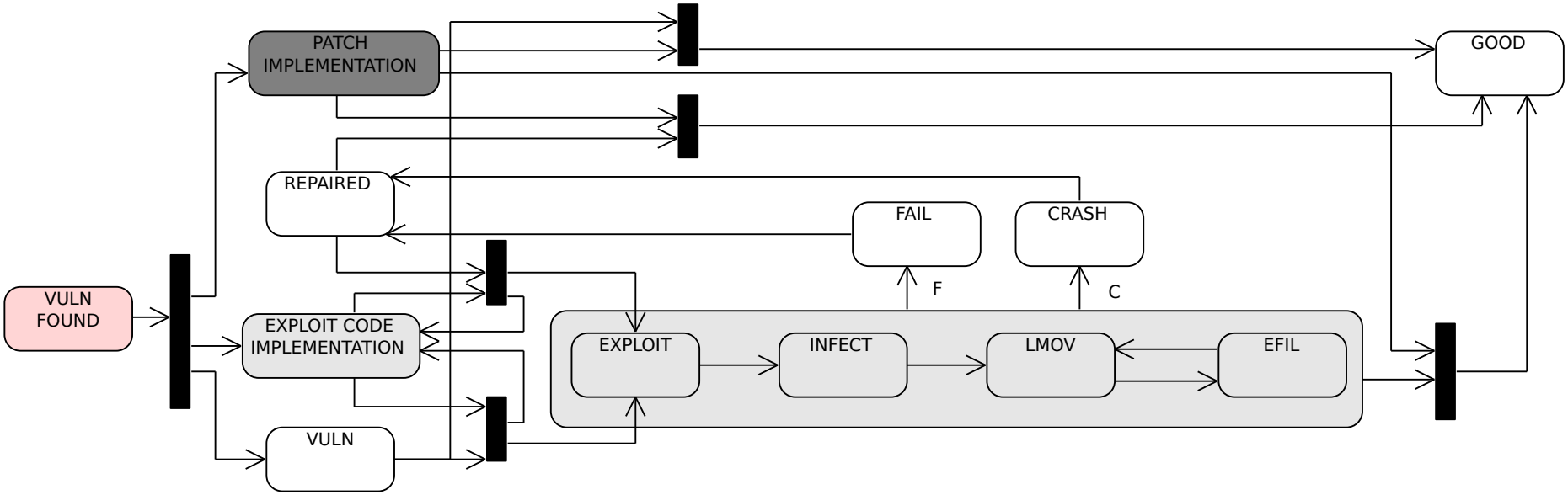


Starts
exploit implementation

Starts
vulnerability mitigation
deployment

Universidad Zaragoza

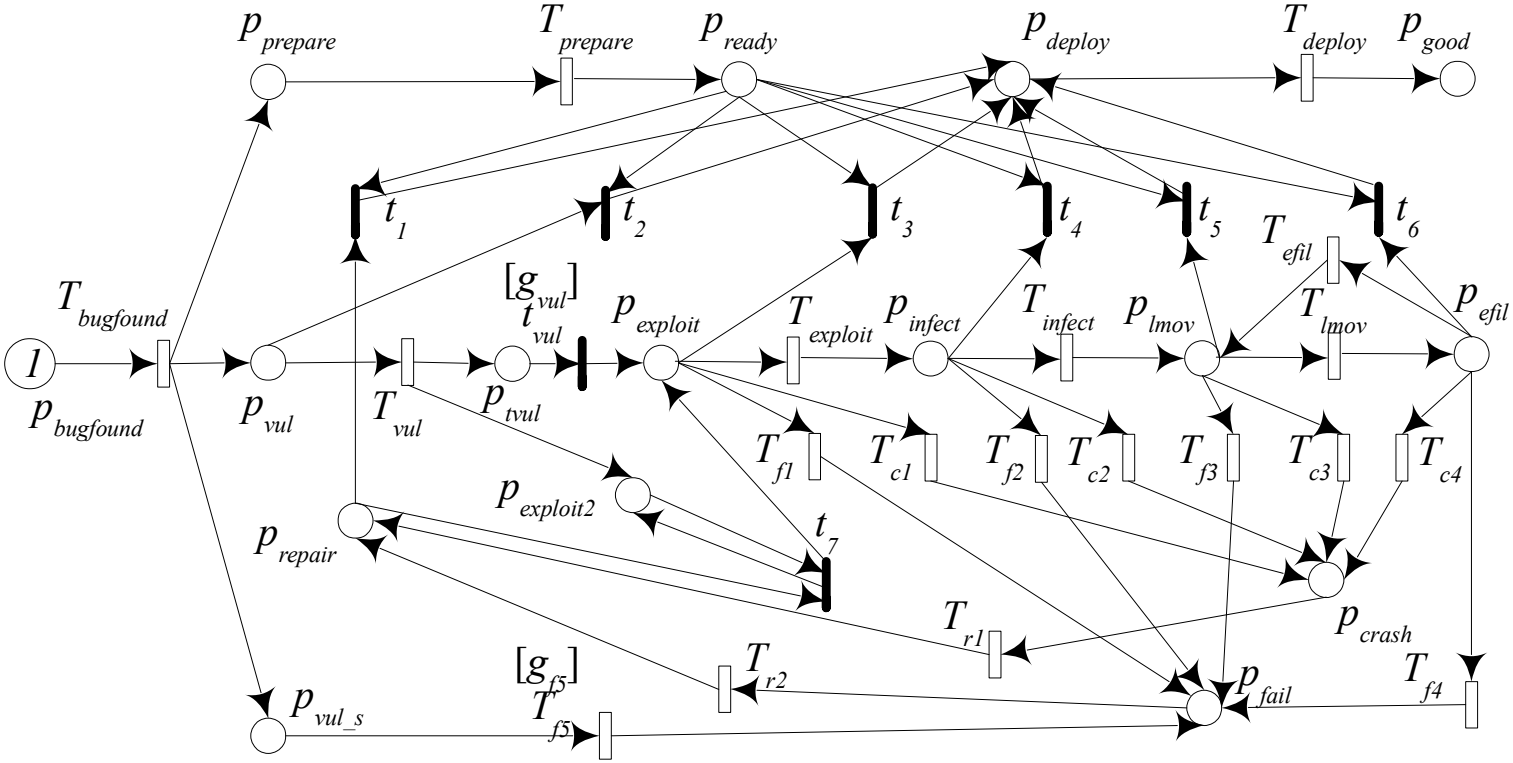
System Description and Model (II)



Survivability metrics defined

- m_1 Probability that the vulnerable system has been patched at time t
- m_2 Probability that the system is unavailable at time t
- m_3 Mean accumulated time that the system is unavailable in $(0, t]$
- m_4 Mean accumulated loss of system confidentiality and integrity in $(0, t]$

System Description and Model (III)



g_{vuln}	**if** $(\#(p_{vuln_s}) == 1)$ **then** 1 **else** 0
g_{f_5}	**if** $(\#(p_{vuln}) == 1)$ **then** 1 **else** 0

- m_1 Expected number of tokens of p_{good} at time t
- m_2 Expected number of tokens of $(p_{crash} + p_{fail} + p_{deploy})$ at time t
- m_3 Expected accumulated reward of $(p_{crash} + p_{fail} + p_{deploy})$ by time t
- m_4 Expected accumulated reward of p_{exfil} by time t

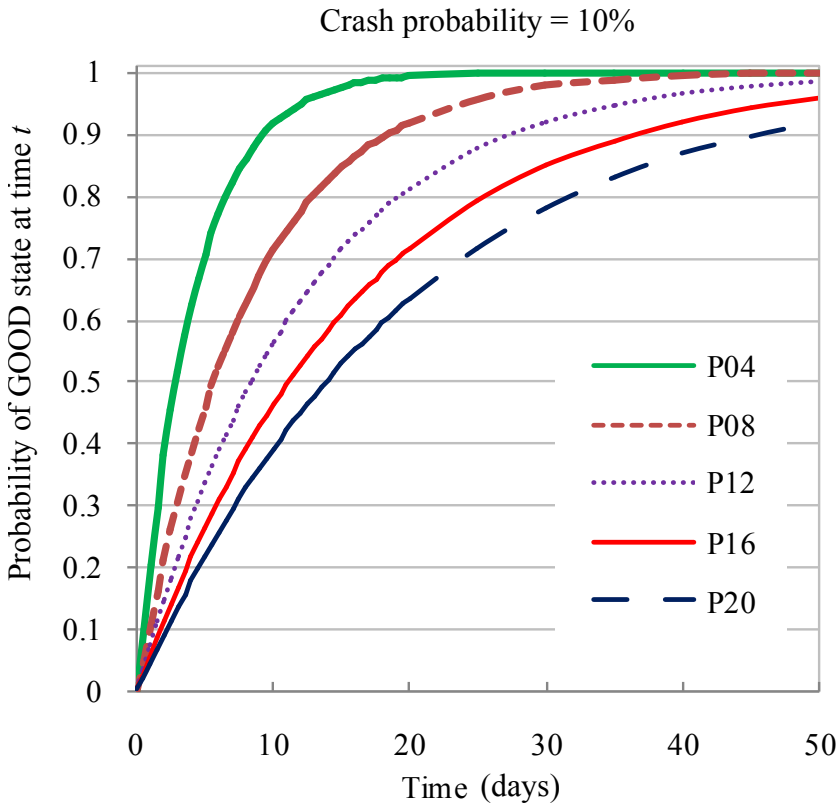
Experiments and Discussion (I)

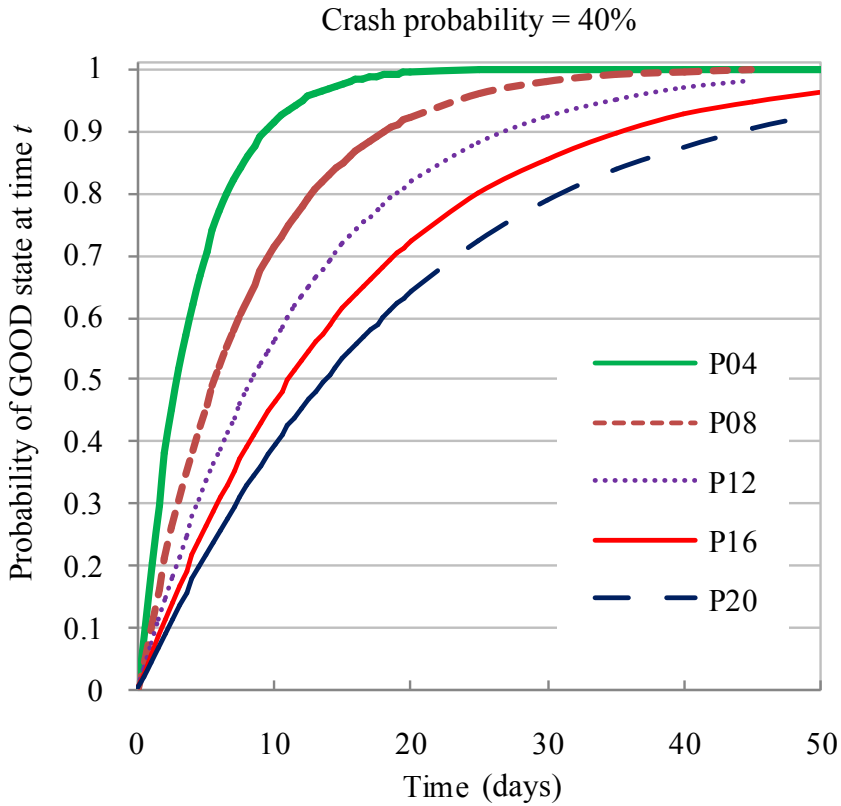
Symbol	Definition	Mean value
$1/\delta$	Mean time that the discovered vulnerability is known to all	30 min
$1/\lambda_{prepare}$	Mean time for implementing a mitigation strategy	20 days
$1/\lambda_{deploy}$	Mean time for installing the mitigation strategy	12 days
$1/\lambda_{vuln}$	Mean time for generating the exploit code	4 days
$1/\lambda_{fail}$	Mean time that the computer system fails	365 days
$1/\lambda_{fix}$	Mean time that the computer system completes the failure or crash fixing	2 days
$1/\lambda_{efil}$	Mean time that the attacker obtains the desired information	2 days
$1/\lambda_{exploit}$	Mean time for injecting the exploit code into the system	7 days
$1/\lambda_{inf}$	Mean time that the exploit code is persistent	1 days
$1/\lambda_{lmov}$	Mean time that the attacker finds sensitive data of interest	7 days
ρ_1	Probability that the exploit code works in the system	0.6
ρ_2	Probability that the exploit code is persistent	0.6
ρ_3	Probability that the attacker finds its target	0.6
ρ_4	Probability that the attacker obtains the desired information	0.6

- SPNP software
- P04, P08, P12 , P16, and P20 represent the results of $1/\lambda_{prepare} = \{4, 8, 12, 16, 20\}$ days, respectively
- Crash probability of 10% and 40%

Experiments and Discussion (II)

Probability of GOOD state at time t under different crash probabilities (metric m_1)

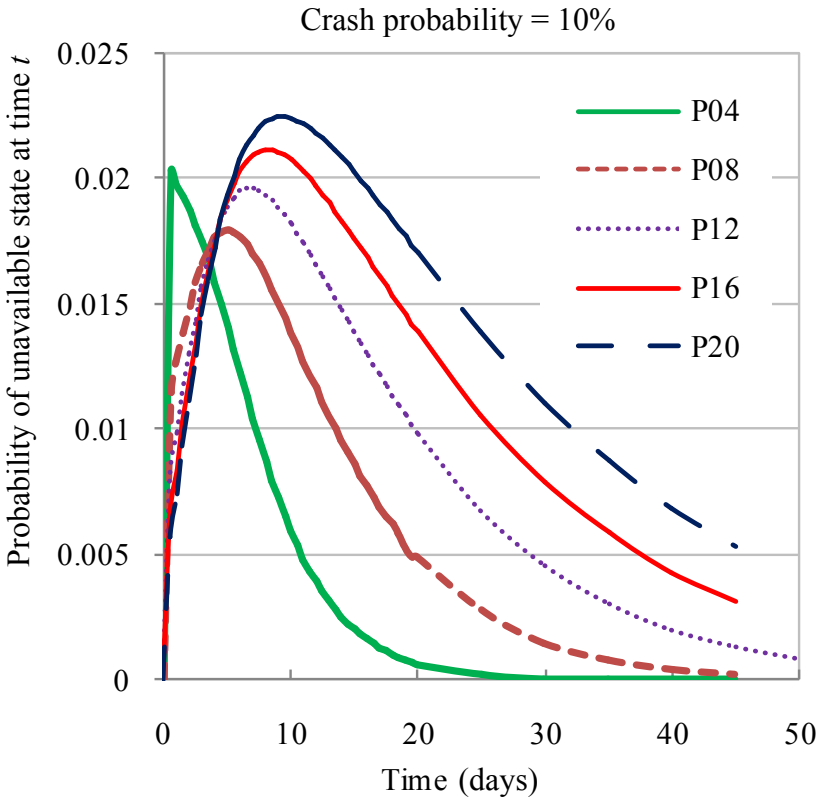


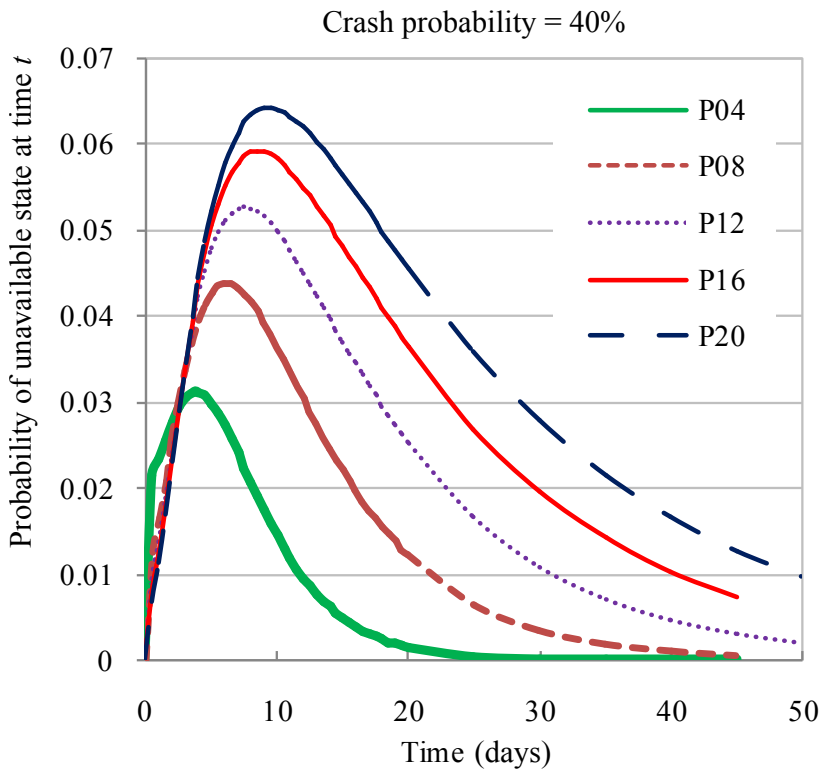


- Crash probability has little effect
  - Deployment starts when mitigation strategy is ready (regardless the system state is)
- The smaller $1/\lambda_{prepare}$, the larger increase in m_1

Experiments and Discussion (III)

Probability of unavailable system at time t under different crash probabilities (metric m_2)

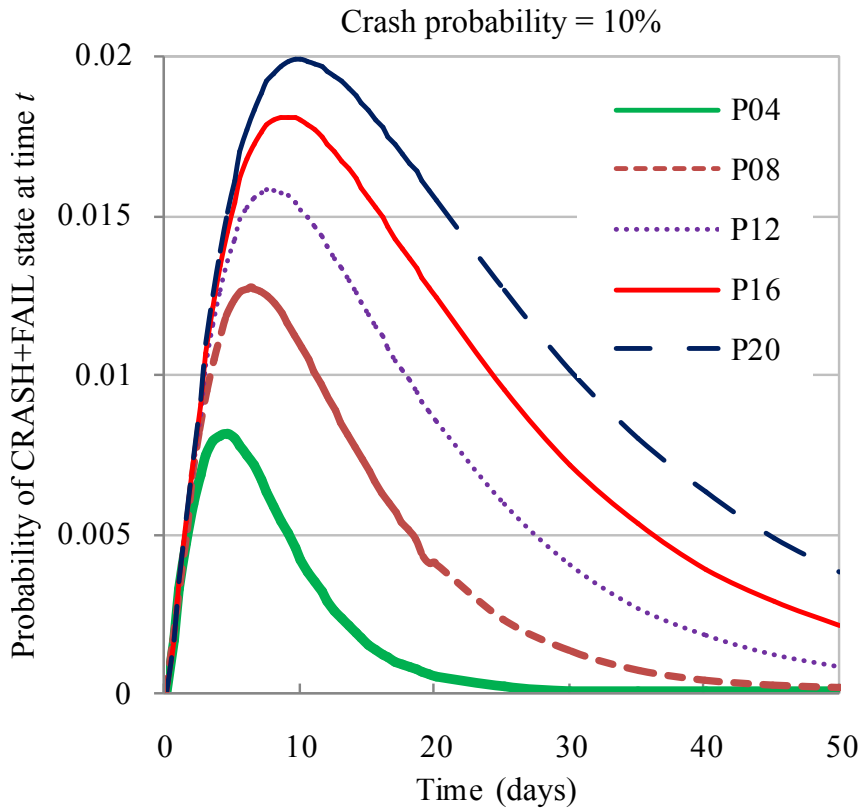




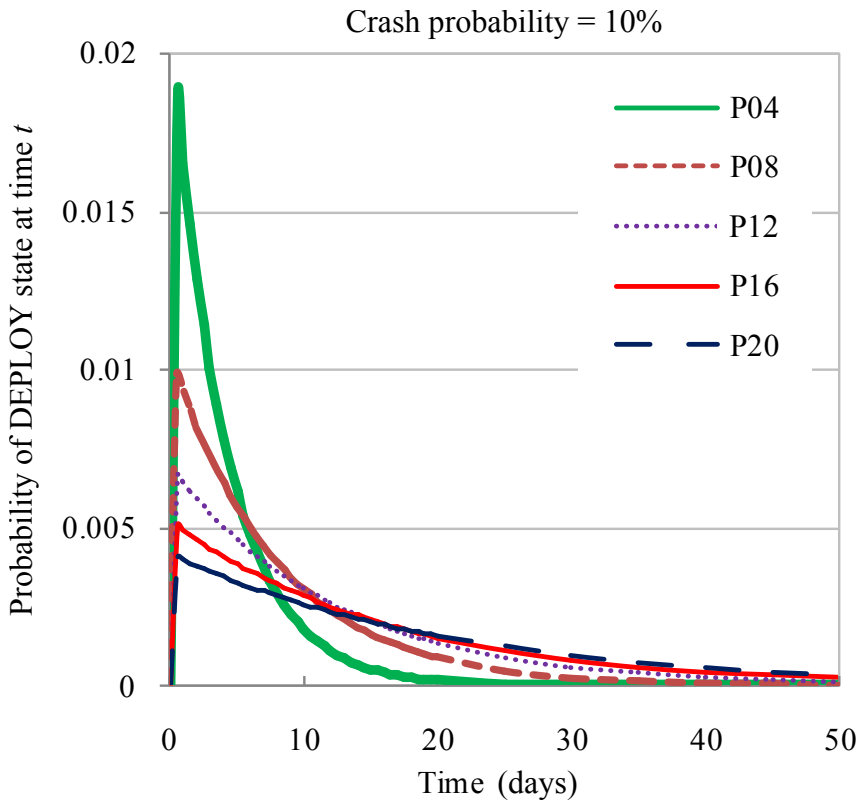
- Both crash probability and $\lambda_{prepare}$ affect unavailability
  - When exploit code is ready, system crashes frequently
  - Once mitigation strategy is ready, it starts deployment
- The larger $1/\lambda_{prepare}$, the larger increase in m_2 (not hold at beginning!)

Experiments and Discussion (IV)

Probability of (a) CRASH+FAIL and (b) DEPLOY state at time t under crash probability of 10%



(a)

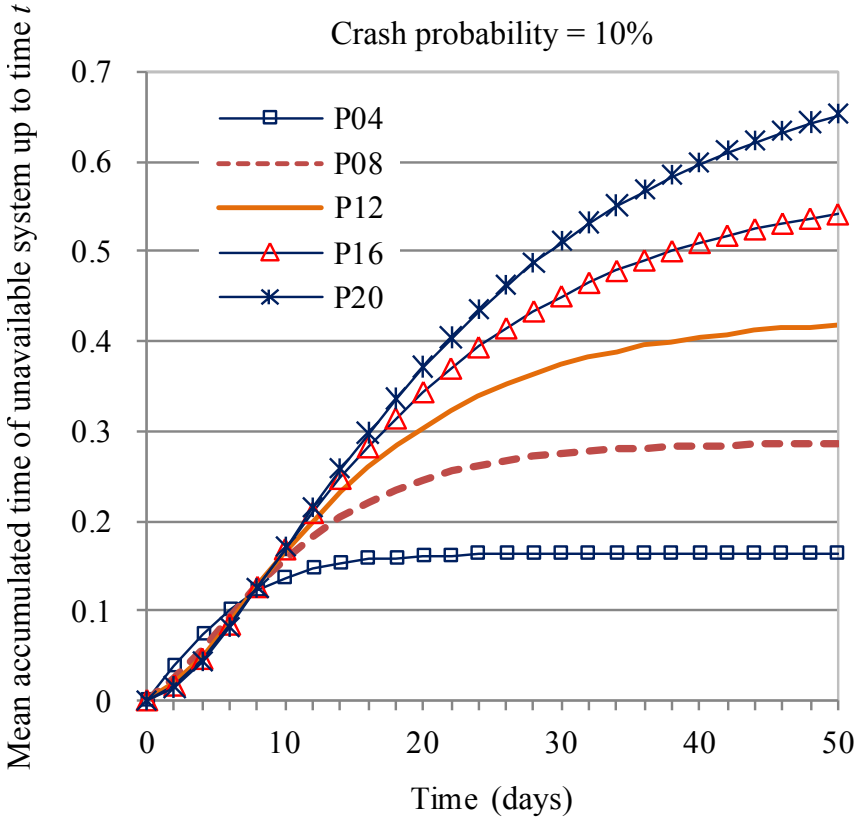


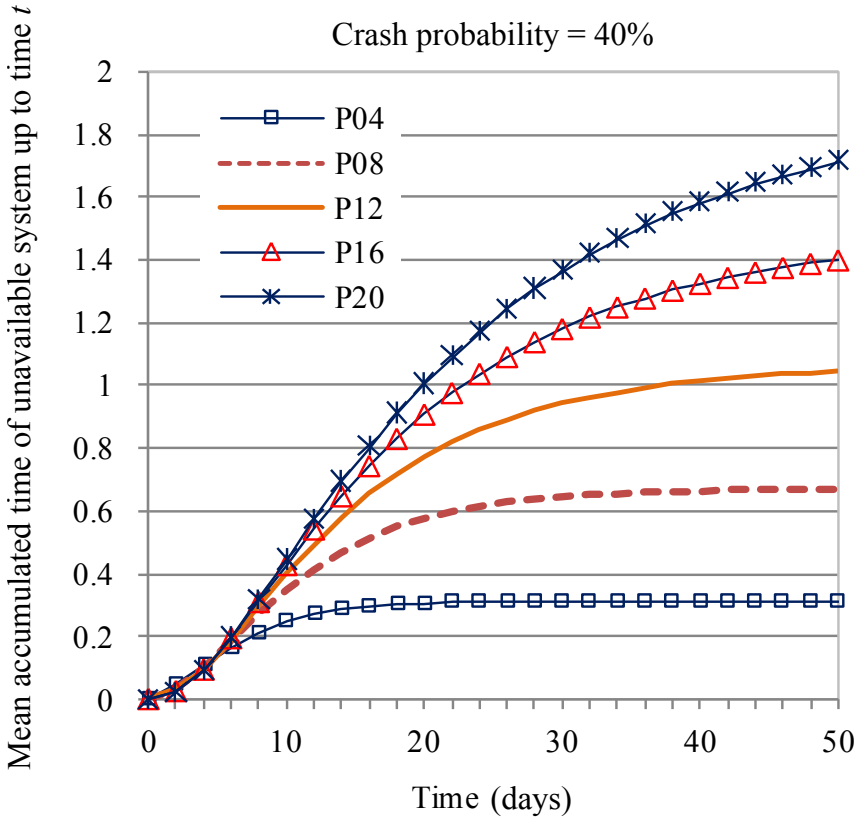
(b)

- At the beginning, the smaller $1/\lambda_{prepare}$, the larger increase in m_2
  - Mainly caused by the probability of DEPLOY state

Experiments and Discussion (V)

Mean accumulated time that the system is unavailable under different crash probabilities (metric m_3)



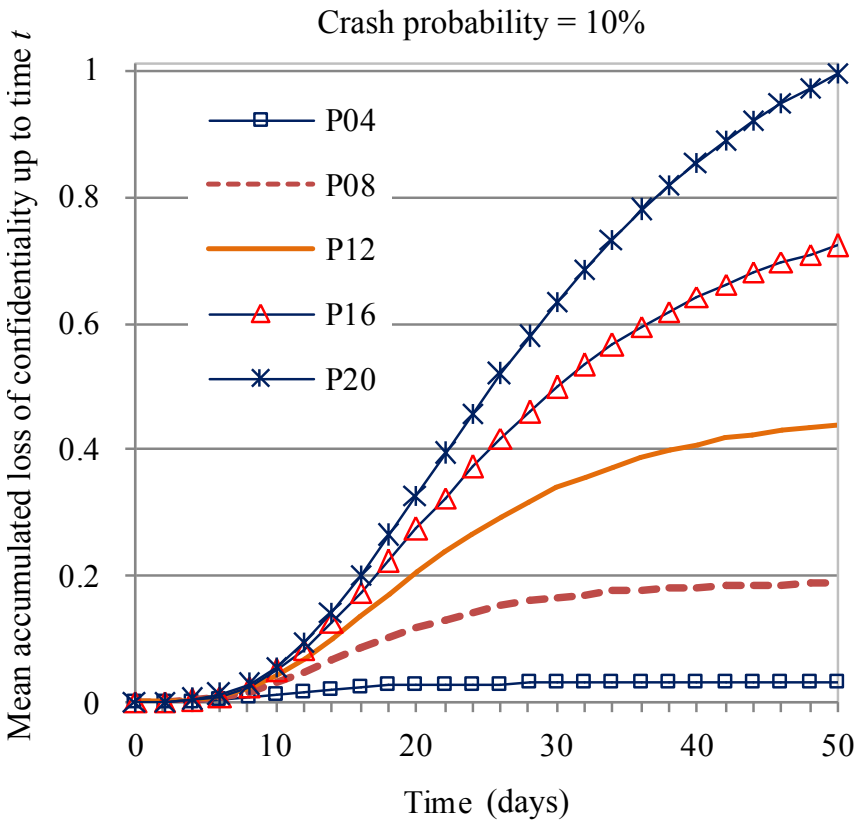


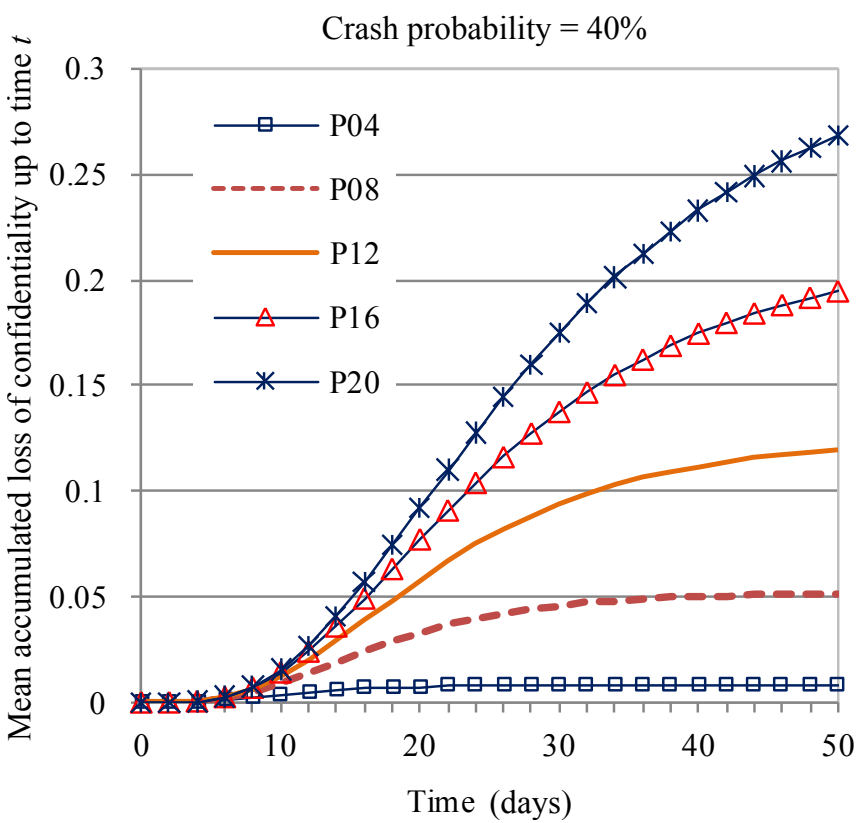
System Unavailability	1: **if** $(\#(p_{fail}) == 1$ **or** $\#(p_{crash}) == 1$ **or** $\#(p_{deploy}) == 1)$ 0: otherwise	*Confidentiality loss*	1: **if** $(\#(p_{efil}) == 1)$ 0: otherwise

- Same reasoning as for m_2
  - The larger $1/\lambda_{prepare}$, the larger increase in m_3 (not at the beginning)

Experiments and Discussion (VI)

Mean accumulated of system confidentiality and integrity loss by time t under different crash probabilities (metric m_4)





- The larger $1/\lambda_{prepare}$ and/or the smaller crash probability, the larger mean accumulated loss

Conclusions and Future Work

Conclusions

- Critical infrastructures mainly targeted by Advanced Persistent Threats: make persistent and send sensitive data out
  - Interest to survive these attacks, minimizing the impact
- CTMC model-based survivability analysis of a computer system under an APT
- Four metrics proposed to analyze system recovery, system availability, data confidentiality loss, and data integrity loss
  - Numerical results help to choose the best strategies
  - Insights on the cost/benefit trade-offs of investment efforts in system recovery strategies, as well as vulnerability mitigation schemes

Universidad Zaragoza 1542

Conclusions and Future Work

Conclusions

- Critical infrastructures mainly targeted by Advanced Persistent Threats: make persistent and send sensitive data out
  - Interest to survive these attacks, minimizing the impact
- CTMC model-based survivability analysis of a computer system under an APT
- Four metrics proposed to analyze system recovery, system availability, data confidentiality loss, and data integrity loss
  - Numerical results help to choose the best strategies
  - Insights on the cost/benefit trade-offs of investment efforts in system recovery strategies, as well as vulnerability mitigation schemes

Future work

- Extend the model to consider security improvements
- Multiple vulnerabilities; some event times no exponentially distributed
- Better modelling of restoration process

Survivability Analysis of a Computer System under an Advanced Persistent Threat Attack

Ricardo J. Rodríguez[†], Xiaolin Chang[‡], Xiaodan Li[§], Kishor S. Trivedi[§]

rjrodriguez@unizar.es, xlchang@bjtu.edu.cn, {xiaodan.li,ktrivedi}@duke.edu

Universidad Zaragoza

Duke UNIVERSITY

[†]University of Zaragoza
[†]Second University of Naples

[‡]Beijing Jiaotong University

[§]Duke University

June 27, 2016

3rd International Workshop on Graphical Models for Security
Lisbon, Portugal