Science of CyberSecurity: some reflections

Paulo Veríssimo
Univ. of Luxembourg, SnT
Luxembourg
paulo.verissimo@uni.lu
http://wwwen.uni.lu/snt/people/paulo_verissimo

IFIP WG10.4 Meeting
Tortworth-Bristol, UK
22-26Jan 2015

Some philosophy

- □ Objective of science:
  - advancement of knowledge -> improvement of society/nation (wealth, welfare, “security/safety”)
- □ Science of cybersecurity (SoCS): ibid

Frameworks for SoCS
example alternatives

- □ A nation wishes to interpret as efficiently and effectively as possible, massive forests of data it somehow has access to:
  - About the legitimate use of systems for ilegitimate purposes
  - About the ilegitimate use of systems for ilegitimate purposes
- □ A nation wishes to improve prevention/ tolerance of ilegitimate use of systems
  - Direct attacks (inc. APT) onto systems and infrastructures
  - Intentional weakening or subversion of security and trust mechanisms in ICT

Frameworks for SoCS

immediate scope

1. A nation wishes to interpret as efficiently and effectively as possible, massive forests of data it has access to
2. A nation wishes to improve prevention/ tolerance of ilegitimate use of systems/infrastruct.

A. Intelligence

B. Information gathering

C. Espionage

D. Infras. Security

E. Infras. Protection

F. Infras. Resilience

G. Counter-espionage

Frameworks for SoCS

strategic objectives

1. A nation wishes to interpret as efficiently and effectively as possible, massive forests of data it has access to
2. A [illegible]ion wishes to improve pre[illegible]ion/ tolerance of [illegible] use of systems

A. Intelligence
B. Information gathering
C. Espionage

D. Infras. Security
E. Infras. Protection
F. Infras. Resilience
G. Counter-espionage

Local - Protecting its own backyard
Global – Constructing healthy ICT ecosystems

Local – Snooping at its own backyard
Global – Looking at others' backyards

Frameworks for SoCS

Some points of logic for reflection about the breadth of SoCS

- Suppose we can only have one of them, which one to pick?

1?

  - Then it is bound to be a zero-sum game, unless a nation thinks it is already superiorly secure, but is that wise?
  - Might make sense, should global construction of healthy ICT ecosystems be considered inconvenient, but is that wise?

2?

  - Should work for all nations individually (defence)
  - Might be a good idea for global mutual protection (UN-like concert of nations)

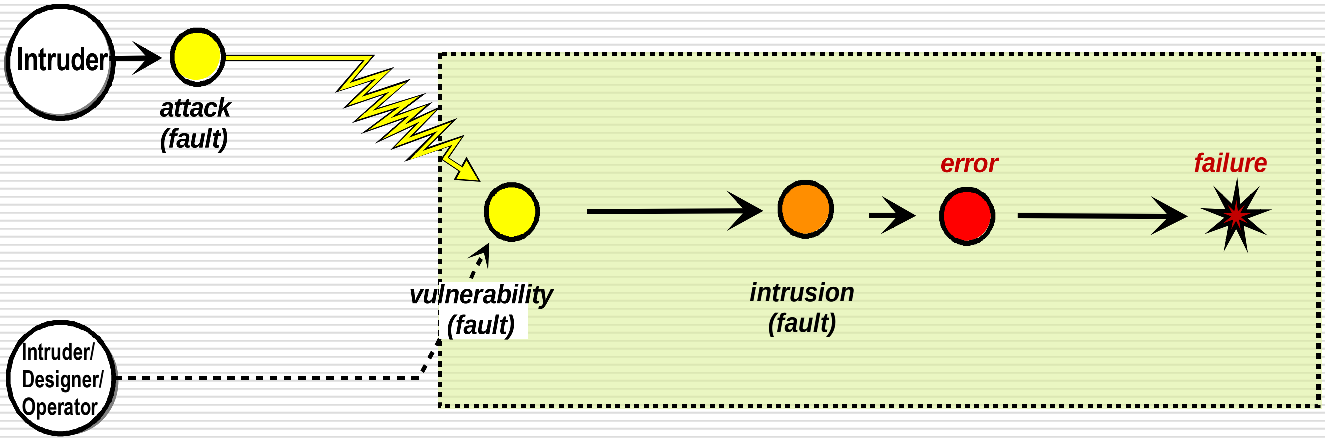
- So, (1) or (2)?
  - Some say "The best defense is a good offense‟
  - But History is full of bold generals who lost wars at their backyards
  - It is hard to conceive that an international definition of SoCS can live without encompassing **both (1) and (2).**
  - That implies considering all facets: theory, architecture, algorithmics, modeling and simulation, experimentation

Some notes about modeling and algorithmics in SoCS

- … wishing to improve prevention/ tolerance of ilegitimate use of systems / infrastructures …

Understanding faults & intrusions

Attack-Vulnerability-Intrusion composite fault model



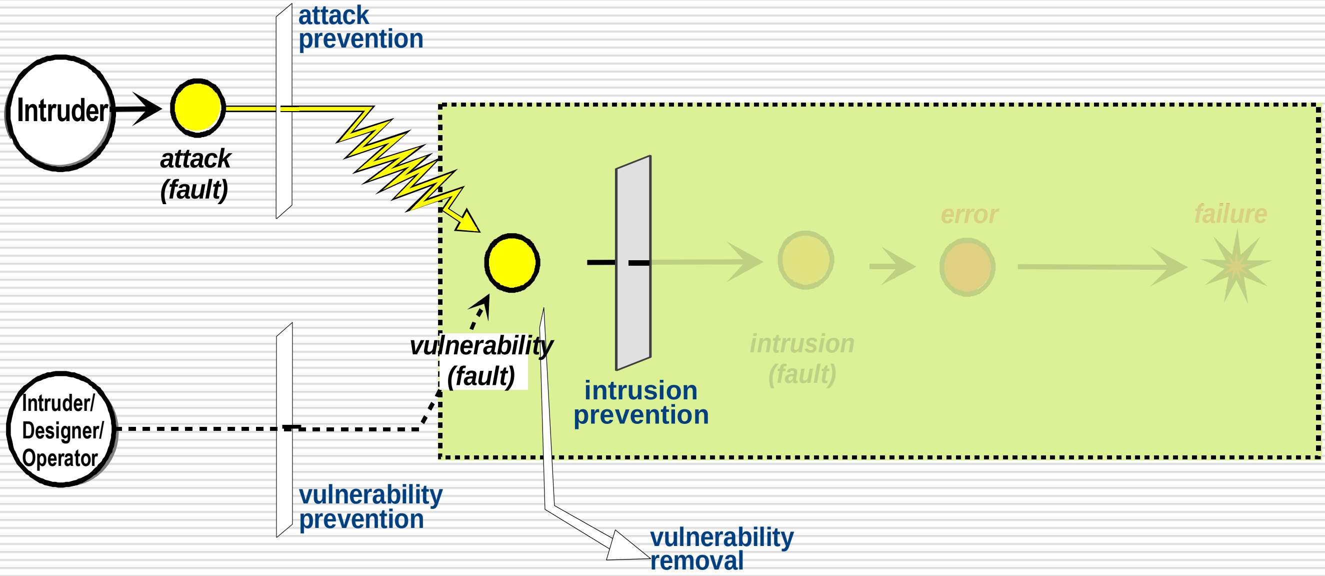
AVI sequence : *attack + vulnerability → intrusion → error → failure*

□ *Intrusion-Tolerant Architectures: Concepts and Design* . **P. Veríssimo, N. Ferreira Neves, M. Correia.** Architecting Dependable Systems, pp. 3-36, Springer-Verlag LNCS 2677, 2003. Extended version in http://www.di.fc.ul.pt/tech-reports/03-5.pdf

Security as Intrusion Prevention

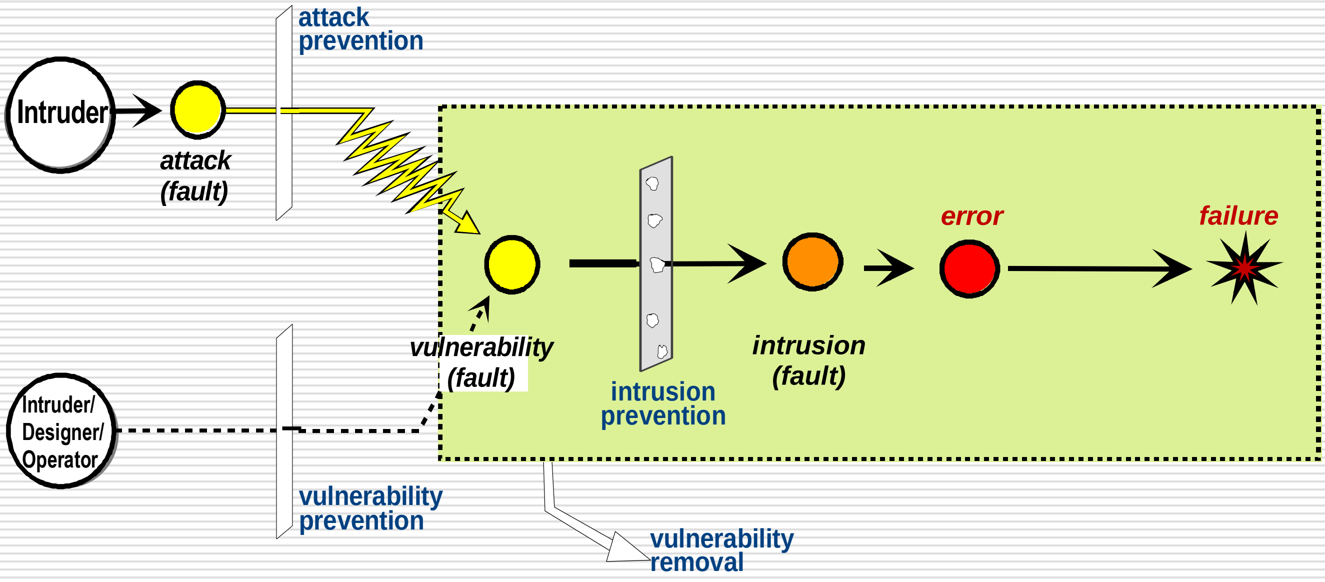
- Fundamental axioms:
  - A system without vulnerabilities is perfectly secure
  - A system without threats is perfectly secure
- Traditionally, security has involved one or several of:
  - Trusting that certain attacks will not occur
  - Removing vulnerabilities from initially fragile software
  - Preventing attacks from leading to intrusions

Intrusion prevention in action

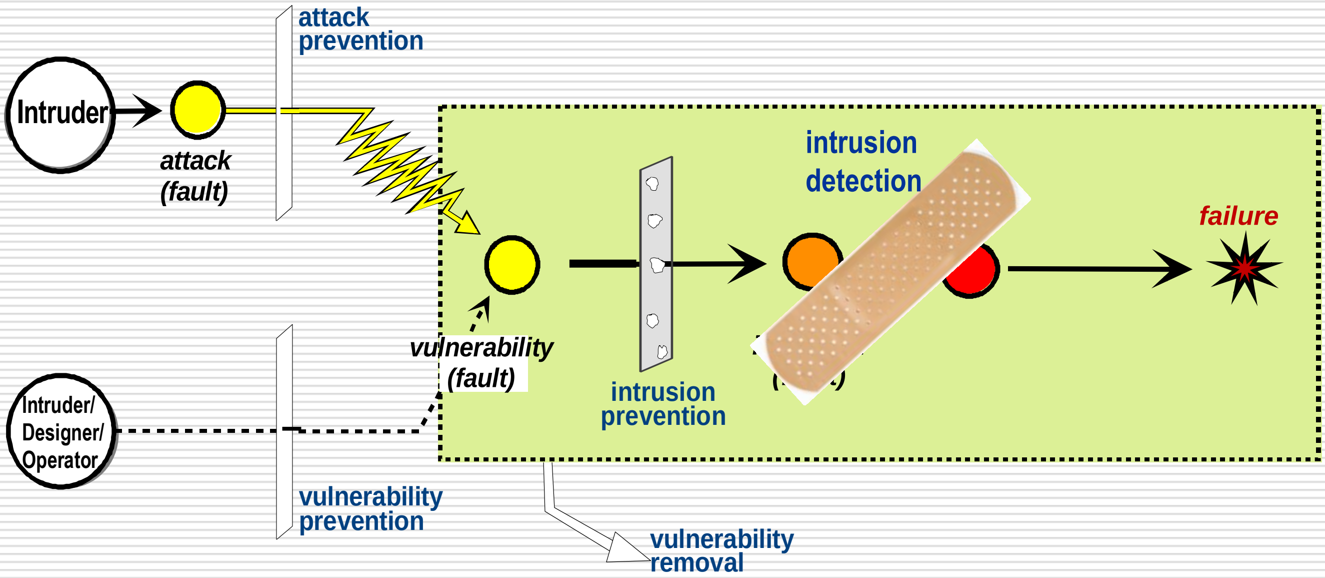


AVI sequence : *attack + vulnerability→ intrusion → error → failure*

Intrusion prevention not perfect



Intrusion detection in aid



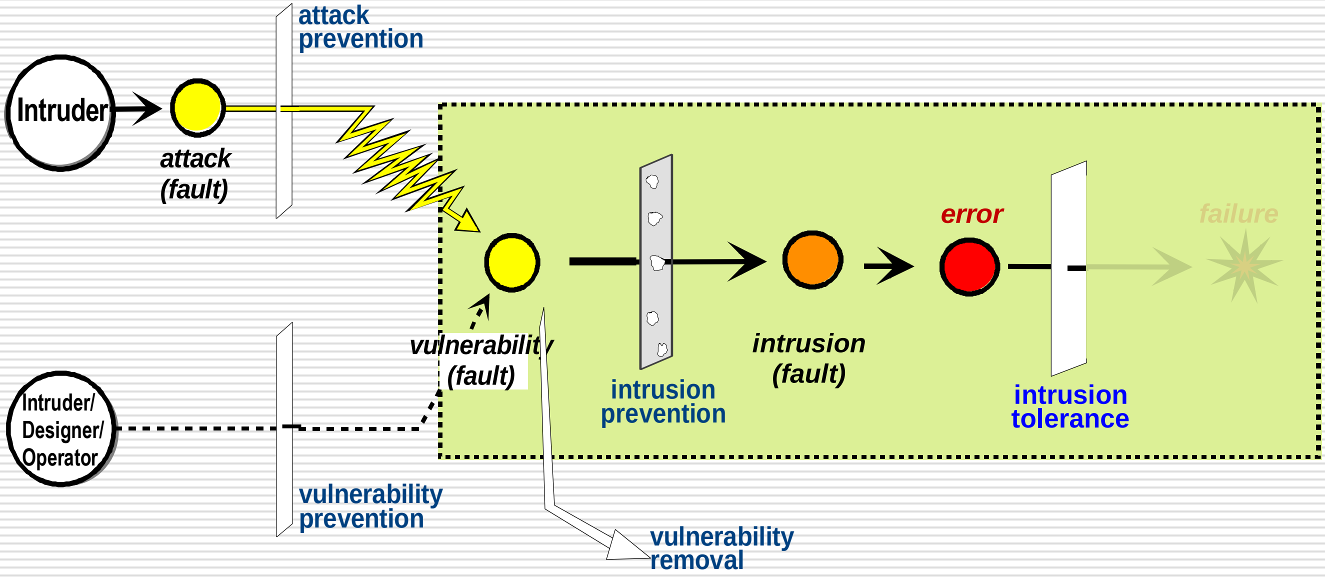
- □ Absolutely necessary, but not a principled approach: it acts if and when the principle ('prevention') was not fully fullfilled

Security as Intrusion Tolerance

- Whereas the tolerance paradigm in security:
  - Assumes that systems remain to a certain extent vulnerable
  - Assumes that components or sub-systems will be attacked and some attacks will be successful
  - Ensures that the overall system nevertheless remains secure and operational
- Basic objective:
  1. we want systems to operate through faults and attacks in a perfectly consistent manner, in an automatic way

I.e., without human intervention.

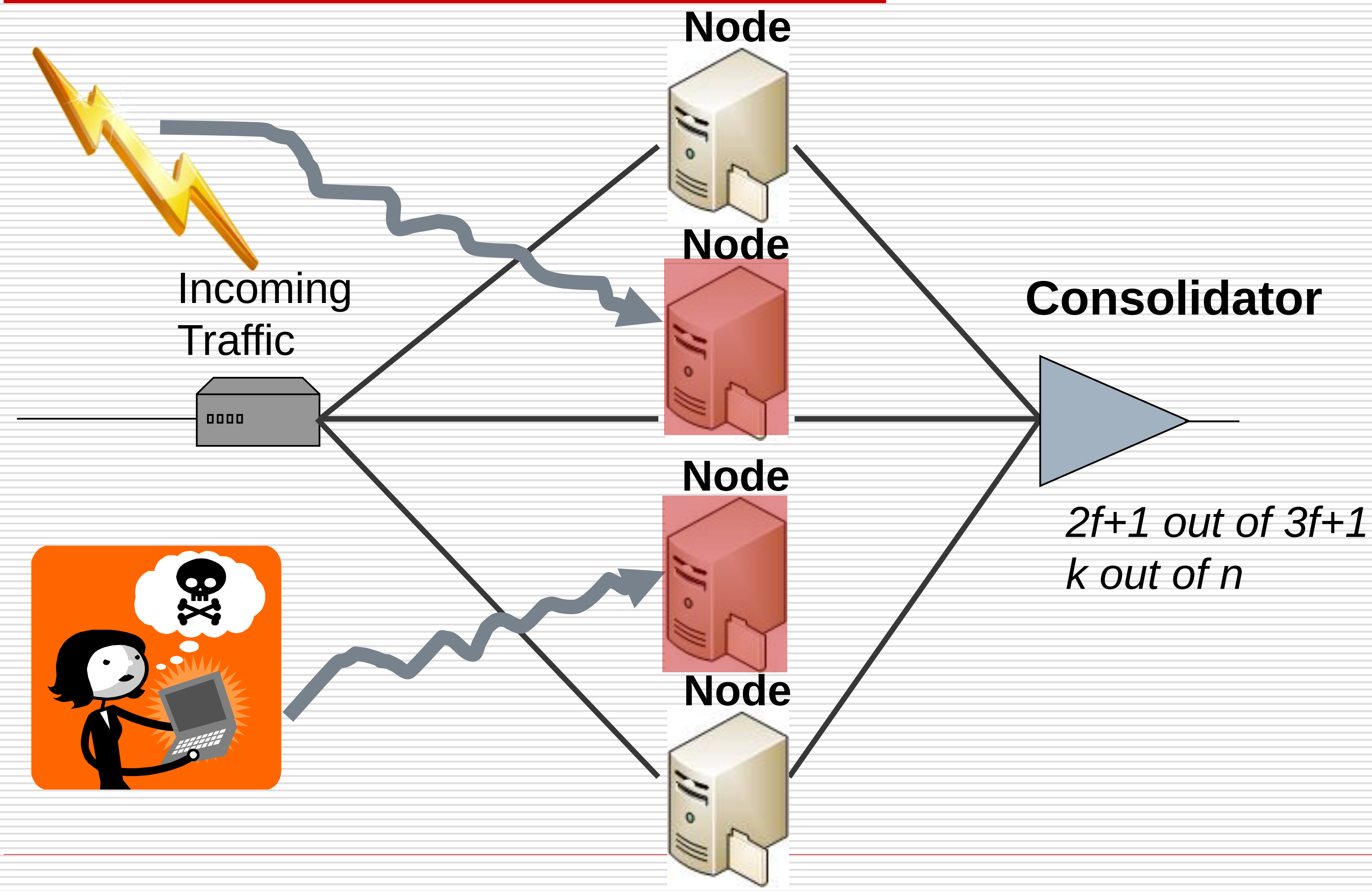
Intrusion tolerance in action



Fault/Intrusion Tolerance (FIT)

An abstract solution

Tolerating Faults and Intrusions automatically



2f+1 out of 3f+1
k out of n

f = max. number of faulty replicas (f=1 in this example)

Tolerance

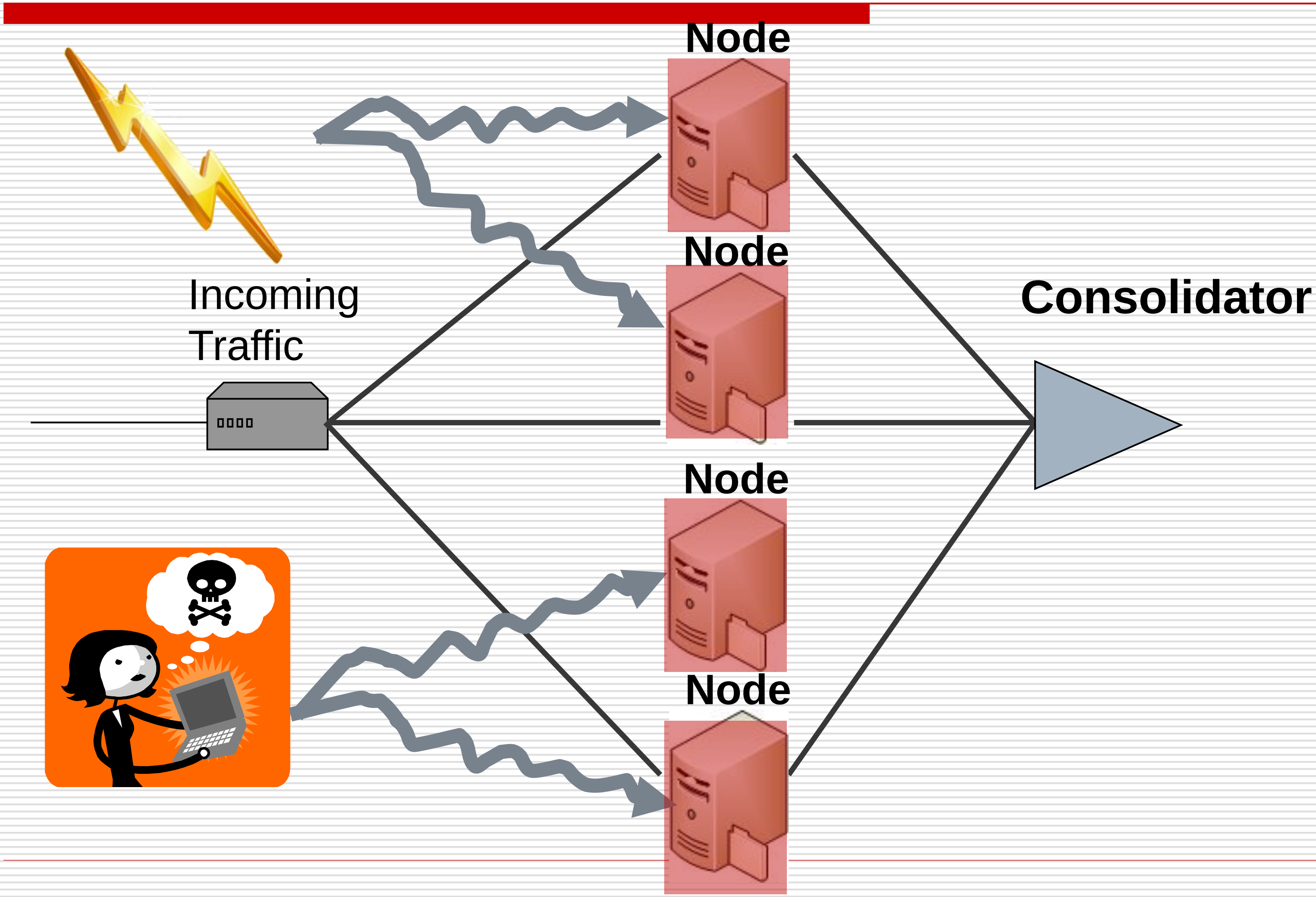
- □ **Tolerance Goal**: operate correctly as long as at most f *faults* of any quality occur

Given *n* processes and *f* function of *n*, and a set *H* of assumptions on the environment, then for at least *n-f* correct processes, algorithm A satisfies a pre-defined set of safety and liveness properties, i.e. executes correctly

- □ This well-known formal proposition however, says very little about an important objective:
- □ will f+1 faults **not happen** *“during my watch”*?

Tolerance

The resource exhaustion problem
a matter of time and power



f = max. number of faulty replicas (f=1 in this example)

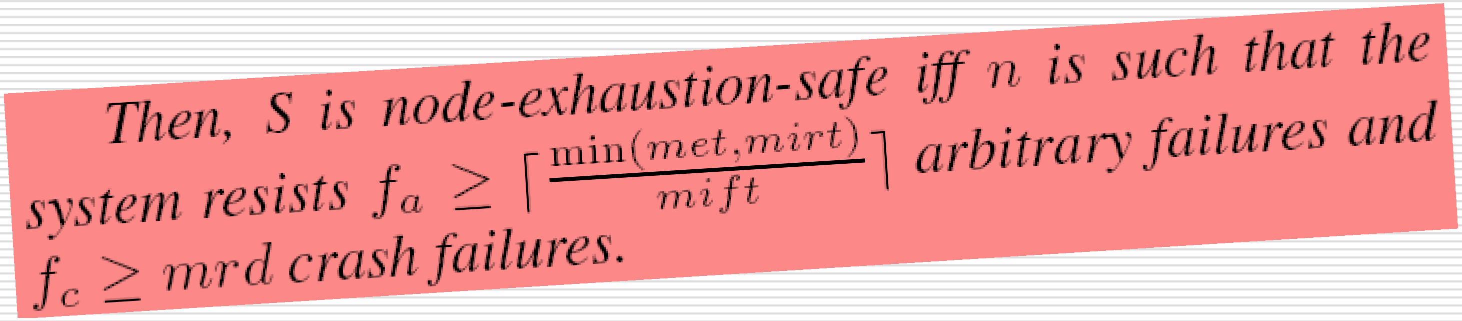
Motivation *(wrap-up)*

We need models and algorithms supporting systems that operate long enough to fulfill their mission, through threats of increasing magnitude

A nation wishes to improve prevention/ tolerance of ilegitimate use of **systems**

Resilience

- □ **Resilience Goal**: tolerate any quality and quantity of faults *over time*
  - *as long as the power of the threat is bounded*
  - *(i.e.* at most f occur *within a given interval)*



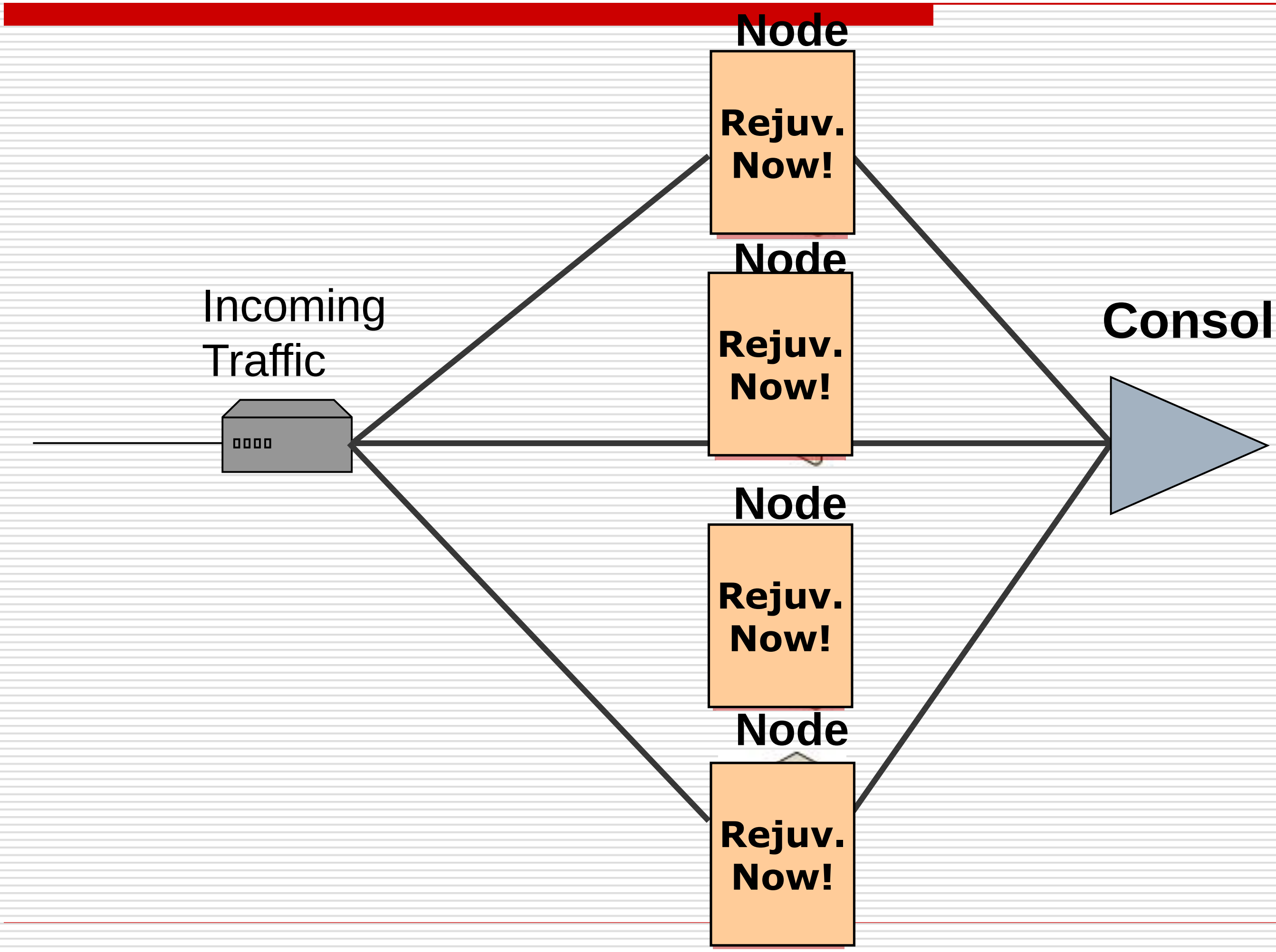
Then, S is node-exhaustion-safe iff n is such that the system resists $f_a \geq \lceil \frac{\min(met,mirt)}{mift} \rceil$ arbitrary failures and $f_c \geq mrd$ crash failures.

- □ How to fulfil this formal proposition?
  - self-healing, ex. proactive/reactive recovery (PRR)
  - structure (hardening, trusted components)
  - diversity and obfuscation

Proactive/Reactive Recovery

An abstract solution

Resisting Continued Threats



f = max. number of faulty replicas (f=1 in this example)

Resilience *(the whole picture)*

- □ Additional objectives, in increasing levels of demand:
  2. we want systems to endure the fact that operating conditions and environments are everyday more uncertain and/or hostile
  3. we want systems to be deployed in unattended manner
  4. we want systems to attain very high levels of assurance

The reasoning and formal principles stated in the last slides, allow us to enunciate some constructive guidelines for architecting and designing resilient systems

Designing for resilience

in architecting intrusion-tolerant systems

1. we want systems to operate through faults and attacks in a seamless manner, in an automatic way

Tolerating Intrusions

2. we want systems to endure the fact that operating conditions and environments are everyday more uncertain and/or hostile

Handling Threat Severity and Vulnerability Pervasiveness

3. we want systems to be deployed in unattended manner

Resisting Persistent Threats

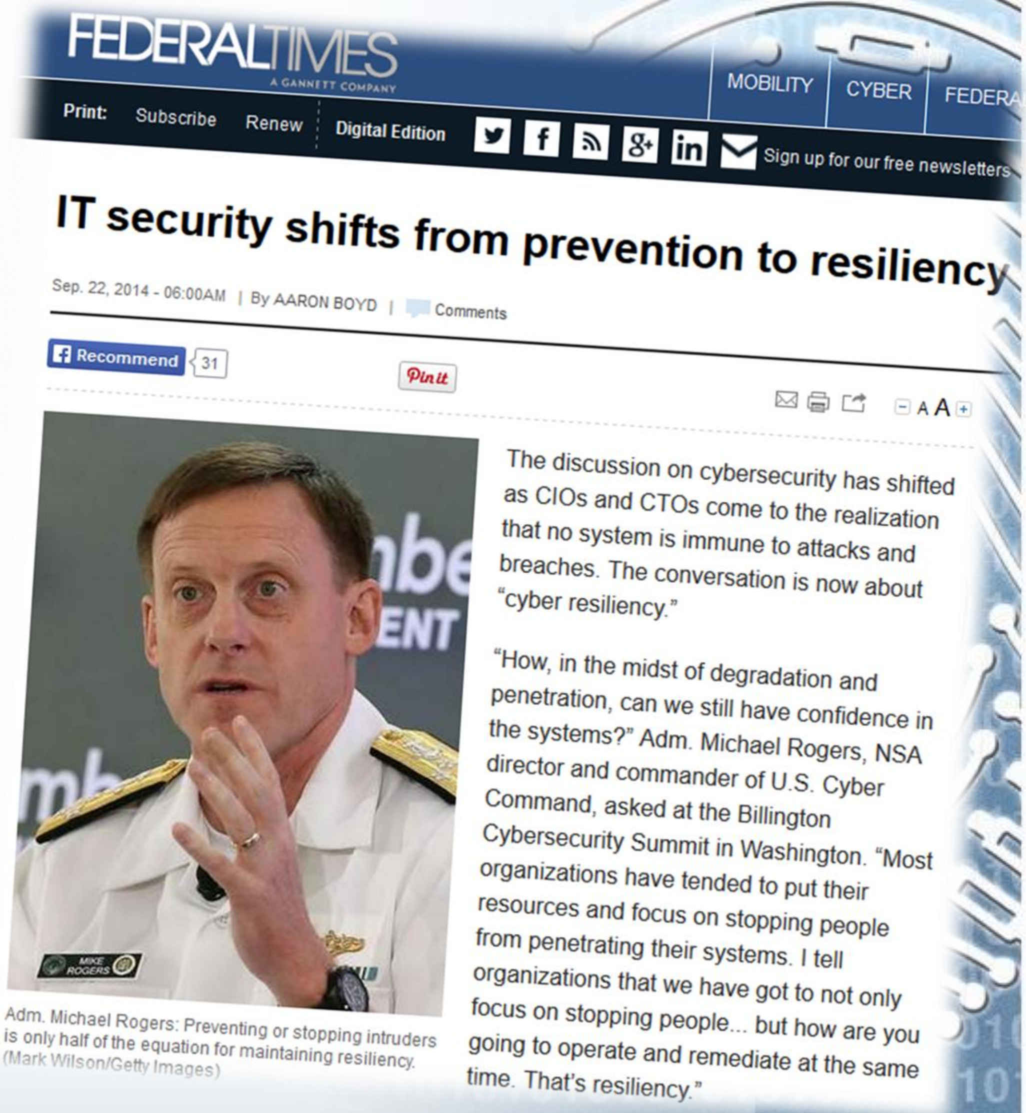
4. we want systems to attain very high levels of assurance

Validating Threats and Vulnerabilities

Intrusion-Resilient Middleware Design and Validation **. Paulo Veríssimo, Miguel Correia, Nuno Ferreira Neves, Paulo Sousa. Information Assurance, Security and Privacy Services (Handbooks in Information Systems, vol. 4), Emerald, 2009.**

Is resilience really necessary?

- Adm. Michael Rogers, NSA Director and commander of US Cyber Command, said that the question "How, in the midst of degradation and penetration, can we still have confidence in the systems?" is better served by focusing on resilience rather than on prevention.
- [Editor's Note]: This is the new theme for cybersecurity - the ability to continue fighting when you're hurt is the differentiator between a successful security organization and the one picking up the pieces after an incident and wondering what happened.



IT security shifts from prevention to resiliency

Sep. 22, 2014 - 06:00AM | By AARON BOYD | Comments

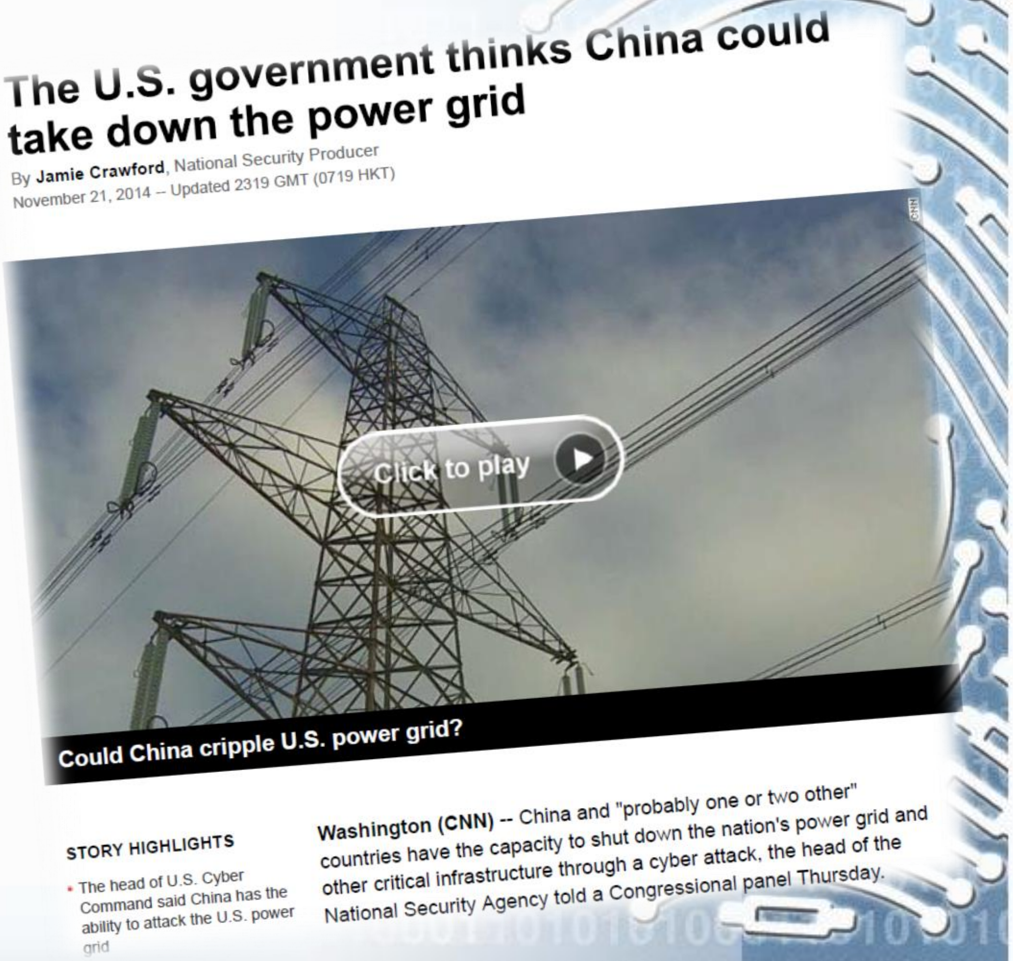
The discussion on cybersecurity has shifted as CIOs and CTOs come to the realization that no system is immune to attacks and breaches. The conversation is now about "cyber resiliency."

"How, in the midst of degradation and penetration, can we still have confidence in the systems?" Adm. Michael Rogers, NSA director and commander of U.S. Cyber Command, asked at the Billington Cybersecurity Summit in Washington. "Most organizations have tended to put their resources and focus on stopping people from penetrating their systems. I tell organizations that we have got to not only focus on stopping people... but how are you going to operate and remediate at the same time. That's resiliency."

Adm. Michael Rogers: Preventing or stopping intruders is only half of the equation for maintaining resiliency. (Mark Wilson/Getty Images)

But will really bad things happen to CII?

- «China and "probably one or two other" countries have the capacity to shut down the nation's power grid and other critical infrastructure through a cyber attack». [Adm. Michael Rogers, NSA Director and commander of US Cyber Command]
- … a recent prediction by technology experts says that a catastrophic cyber-attack that causes significant losses in life and financial damage would occur by 2025.
- "It is only a matter of the when, not the if, that we are going to see something traumatic." [Ibid.]



The U.S. government thinks China could take down the power grid

By **Jamie Crawford**, National Security Producer
November 21, 2014 -- Updated 2319 GMT (0719 HKT)

Could China cripple U.S. power grid?

STORY HIGHLIGHTS

- The head of U.S. Cyber Command said China has the ability to attack the U.S. power grid

Washington (CNN) -- China and "probably one or two other" countries have the capacity to shut down the nation's power grid and other critical infrastructure through a cyber attack, the head of the National Security Agency told a Congressional panel Thursday.

Paulo Esteves Veríssimo

University of Luxembourg Faculté des Sciences, de la Technologie et de la Communication
and SnT, the Interdisciplinary Centre for Security, Reliability and Trust

paulo.verissimo@uni.lu _

http://wwwen.uni.lu/snt/people/paulo_verissimo _

CritiX @SnT, *Critical and Extreme Security and Dependability*

We’re hiring bright post-docs and research associates willing to address these challenges!

Thank you! _