UNIVERSITÀ DI PISA

Sicurezza Informatica: nulla è più difficile che difendere un sistema

ICT Security: the real challenge is cyberdefence

F.Baiardi
Dipartimento di Informatica
Università di Pisa

Informally:

Theorem: Crashing is simpler than defending

Proof: At the end of the talk

ICT risk assessment and management – Dipartimento di informatica, Università di Pisa

- We are computer scientists from the oldest computer science department in Italy
- Several know-hows and background in our group to cover a wide set of areas ranging from security to audit, to OS, high performace computing, artificial intelligence ….
- We love challenges from the real world
- We love to work in Italy

Our background

- Joint projects with
  - Comando Generale Arma CC (infrastructure security policy)
  - Polizia Postale e delle Comunicazioni (ethical hacking)
  - Veolia (ICT security of waste management)
  - Terranova (ICT security of gas distribution)
  - Enel, Enel Ingegneria (ICT security of power production)
  - Stato Maggiore Difesa - Comando C4
    - Locked Shield 2014
    - Locked Shield 2015
  - Qatar University, Imperial College, Univ. of Arizona
  - NDA, NDA, …
- Members of working group: ENISA/Cloud Sec. Alliance

Haruspex Suite

- An integrated set of tools to automatically assess and manage the risk due to an ICT infrastructure through a scenario analysis
- In each scenario the infrastructure is targeted by intelligent agents (attackers) each aiming to reach some predefined goals
- Goal = a set of access rights an agent reaches by planning and implementing a sequence of attacks
- The tools
    - Automatically build a model of the target infrastructure
    - Simulate in details how each agent collects information, plans and executes a sequence of attacks
    - Apply a Monte Carlo method to build a statistical sample

Haruspex Suite: output statistics

- Fully automated computation of statistics
- High confidence level (even more than 50.000 simulations)
- Some possible statistics
  - Success probability of each agent
  - Average time to reach a goal
  - Shortest time to reach a goal
  - Lowest number of attacks to reach a goal
  - Probability to attack a component
  - ….

Haruspex suite: the agents

- We have modeled how an intelligent agent
    - Plans alternative attack sequences
    - Selects the best plan according a set of priorities
    - Minimizes the overall amount of work
- Distinct agents are characterized in terms of goals and of
    - Available resources to implement their attacks
    - Available information (insiders vs outsider)
    - The strategy they adopt to collect information and select the sequence of attacks to implement

Plans in real life

- (An hacker site) This hack shows how to exploit an Android weakness to subvert a corporate network. It involves *multiple stages*: Remote exploitation of the handset, Privilege Escalation to root, Post-Exploitation tricks, and then pivoting over the phone via it's 3g interface, and compromising a network via a wifi interface
- (Another site) Cisco Unified Communications Manager (Unified CM) contains multiple vulnerabilities that an unauthenticated, remote attacker can chain to gather user credentials, escalate privileges, and execute commands to gain full control of the vulnerable system. Then the attacker can access, create or modify information in Cisco Unified CM.

Haruspex: Agent Simulation

- Agent simulation is driven by an intelligence that adopts AI strategy to select and implement attacks of each agent according to the agent parameters
- Agents can be specialized to cover cases such as malware or worms
- High efficient code optimization resulting in several order of speed up of execution time on a multicore architecture

Haruspex Suite: how long does it takes?

- Risk Assessment and Management of an industrial control system
  - 2 days to collect info to build the infrastructure model (without stopping the infrastructure)
  - 1 day to validate the data and build the model
  - 2 days to simulate the agent and compute statistics of interest

The simulation engine uses a 96 core machine

that is a IBM Shared University Grant

Haruspex: Security by Design

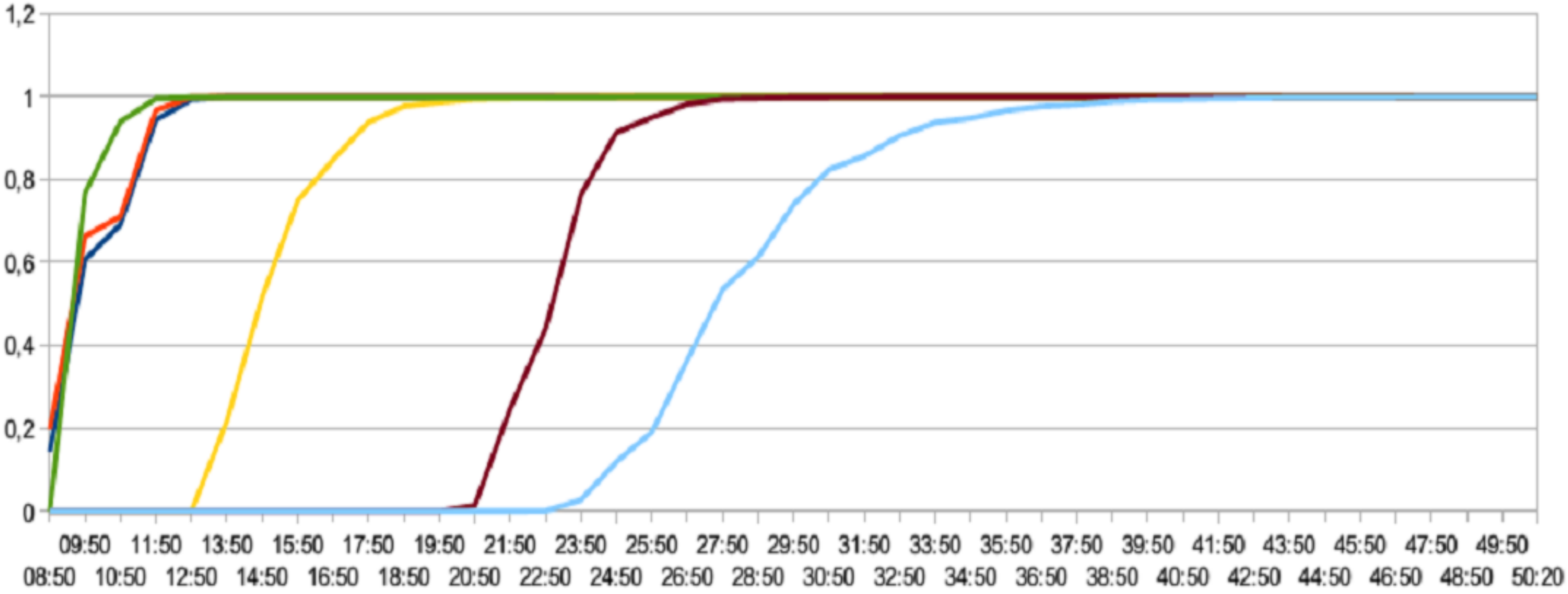
- The suite tools can build an infrastructure model in the design step of the infrastructure
- By simulating attacks, the designer can discover
  - How the infrastructure resists to attacks *before* it is actually attacked
  - How alternative versions of the infrastructure resist to the same agent(s)/attack(s)
  - The return of the investment to change some features of the infrastructure

Haruspex: what we have learnt

- Assessing an infrastructure full of holes is much more time consuming than assessing a robust one
- If an infrastructure can be easily attacked then
  - A huge number of alternative plans are enabled
  - Each attacker has a huge number of alternatives
  - Most alternatives are equivalent
  - Huge execution time to simulate the agents

Haruspex: synthetic robustness measure

- Security stress = success probability of an agent as a function of available time for attacks
- Strongly simplifies the comparison of versions/agents



An interesting discovery (first step of the proof)

- We have bumped into a paradox:

  an investment to increase the robustness of a component may decrease the overall robustness of the infrastructure

- This paradox has been originally discovered by Braess in 2005 in the case of transport networks

  an increase in the number of routes a traveler has available may result in an increase of the average time of some routes

Haruspex precautionary principle

- *Simulation of the agent attacks*
- *Improve the robustness of the infrastructure*
- *New simulation to avoid some unpleasant surprise*

Being paranoic is not required but it helps

Our last tool

- A risk manager that automatically selects a set of countermeasures (changes to the infrastucture) to achieve one or more of the followings
  - Increase the average time to reach a goal
  - Increase the shortest time to reach a goal
  - Reduce the success probability of some agents

- Obviously, the countermeasures it selects should be cost effective, have a return ….

The tool we are currently developing

- A SIEM tool where the output of attack simulation drives the infrastructure monitoring. This tool can
  - Attribute attacks to an active agent
  - Predict the next attack of each active agent
  - Discover and characterize 0-day exploits used against the infrastructure

- We are currently debugging the tool and tuning its mining and correlation algorithms

The SIEM tool: how we are doing?

Something better than John’s forecasting stone …

JOHN’S WEATHER FORECASTING STONE

CONDITION	FORECAST
Stone is Wet	Rain
Stone is Dry	Not Raining
Shadow on Ground	Sunny
White on Top	Snowing
Can’t See Stone	Foggy
Swinging Stone	Windy
tone Jumping Up & Down	Earthquake
Stone Gone	Tornado

Risk manager: the outputs

- This tool considers several countermeasures:
  - patching a vulnerability
  - closing a port
  - adoption of
    - Host intrusion detection system
    - Network intrusion detection system
    - Sandbox and confinement
    - Virtual machines
- It guarantees cost effectiveness but not the minimal cost of countermeasures

Risk manager: agent adaptivity

- Agents react to countermeasures by changing their plans against the infrastructure
- To avoid Braess paradox, the manage applies Haruspex precautionary principle:

```
repeat
      1. select a set of countermeasures
      2. deploy the selected countermeasures
      3. simulate attacks against the new system
until user constrains satisfied
```

- Each iteration can discover new attack plans

Risk manager: the challenges - 1

- Alternative approaches for the intelligence underlying countermeasure selection
  - *Incremental* : no backtracking
  - *Global* : each time a new plan is discovered, tune adopted countermeasures to minimize the overall cost
- A global approach returns an optimal solution with a minimal cost and a large return of the investment at the expense of an increase in execution time
- The incremental approach only approximates the optimal solution but it minimizes the execution time

Risk manager: the challenges - 2

- Assume that some system components are affected by a 0-day vulnerability that an attacker knows
- Can we adopt countermeasure to stop this attacker even without knowing the vulnerability and the attack?
- ***Yes, we can*** provided that the 0-day vulnerability does not enable an attack that is the only element of an attack plan

The original theorem

- A comparison of the intelligences that support, respectively, attack simulation and countermeasure selection confirms the huge differences between the two problems.
- Divide et impera
  - strongly simplifies attack planning
  - does not hold for countermeasure selection because problems are strongly correlated (butterfly effect)
- The know-hows and the abilities to attack widely differ from those to select countermeasures
- One does not cover the other one

Simple ☺ risk management problems

○ Does the adoption of defense in depth increase the overall robustness of the infrastructure even if some firewall vulnerabilities enable attacks against the firewall?

○ Is it convenient to patch a vulnerability enabling a long and complex sequence of attacks against the infrastructure ?

Security as an holistic property

- Security cannot be achieved through *divide-et-impera*
- A change in some security properties of a module also affects those of some related module

⇔ By improving traffic in one area we increase congestion in a close area

- We do not know related modules in advance
- Attack is fully modular, after crashing a subnet we crash the next one and never need to backtrack

Discovery and improve

- Cyber defence increases the time, the resources, the know-how required to attack a system
- Offensive security is mostly useless and risky in cyber war retargeting a weapon is rather simple
- Discovering how a system may be attacked returns critical information provided that
  - fully disclosure of information on attacks
  - it occurs as a design step before the system is deployed
- Be proactive replace *penetrate-and-patch* with *discovery-and-improve*

Being proactive

- Proactivity implies discovering problems in your infrastructure and removing them before they are exploited against you
- It is not related to a product or to red teams but to an overall strategy where security is the output of a system wide analysis
- Any technology that simplifies and automates the assessment and the management of ICT security is a key enabler of proactivity
- Think as a good guy not only as a bad one :-D

Thanks for this opportunity,

for lending me your ears

for your time

for your questions

f.baiardi@unipi.it

www.di.unipi.it/~baiardi