UNIVERSITÀ DI PISA

QSec: Supporting Security Decisions on an IT Infrastructure

F.Baiardi, F. Corò, F. Tonelli,
Dip. di Informatica, Univ. di Pisa
L Guidi
ENEL Ingegneria ed Innovazione

CRITIS 2013 Amsterdam

The research group

- Methodologies and tools to support risk assessment and management of complex ict infrastructures
- Complex ICT infrastructures
  - SCADA architectures
  - Pollution ICT control systems
  - Cloud Architectures
- Our work aims to define an approach that is
  - Formal
  - Quantitative
  - Repeatable

Past and Current Cooperations

- Cooperation with
  - Comando Generale Arma CC (definition of the security policy for their ICT infrastructure)
  - Polizia Postale e delle Comunicazioni (ethical hacking course)
  - Enel
- Assessment of ICT and SCADA infrastructure
- Connection with ENISA /Cloud SA
- Currently involved in
  - Haruspex (NATO CRME + Promostudi)
  - Security Horizon – National Research Project
  - Cooperation with Qatar University and University of Arizona

Our Threat Model

- We consider intelligent threat agents (APT) able to
  - select some goals before starting its attacks
  - design and follow a multistep attack plan involving several nodes even in distinct infrastructures
  - select a plan with an optimal benefit/cost ratio
- A multistep attack plan
  - is a sequence of elementary attacks
  - the rights acquired through an attack are used to implement the next one

Plans and Agents

- Agents are
  - Intelligent
  - Goal oriented

  and minimize their efforrs
- Hence they avoid plans with attacks that
  - do not increase their rights
  - result in rights useless for their goal

Global vulnerability - I

- We map each elementary attack *at* into
  - *pre(at)*, the precondition of *at*: the set of rights to implement at
  - *post(at)*, the postcondition of *at*: the set of rights that are acquired if *at* is successful
  - *vuln(at),* the local vulnerabilities in an infrastructure component that enable *at*

Global vulnerability - II

- Given *pre, post* and *vuln* for each attack *at*

  we can define for each vulnerability *v*
  - *att(v),* the attacks enabled by *v*
  - *pre(v)*, the union of the preconditions of the attacks enabled by *v*
  - *post(v)*, the union of the postconditions of the attacks enabled by *v*

Global vulnerability - III

- A set of local vulnerabilities such that
  - Enable a set of elementary attacks
  - These attacks can be, totally or partially, sequentialised so that the attacker gains the rights in an attack precondition because of the postconditions of the previous attacks
- Each sequence = an attack plan
- A sequence is enabled by a global vulnerability

Global vulnerability -IV

- at_1, at_2, at_3 three elementary attacks where
  - $vuln(at_1)=\{v_1, v_2\}$ $pre(at_1)=\{r_1, r_2\}$ $post(at_1)=\{r_3\}$
  - $vuln(at_2)=\{v_2, v_3\}$ $pre(at_1)=\{r_1, r_3\}$ $post(at_1)=\{r_4\}$
  - $vuln(at_3)=\{v_4, v_5\}$ $pre(at_1)=\{r_2, r4\}$ $post(at_1)=\{r_5\}$
- $\{v_1, v_2, v_3, v_4, v_5\}$ is a global vulnerability because the three elementary attacks it enables can be sequentialised

  $$at_1; at_2 ; at_3$$

  where $\{r_1, r_2\}$ and $\{r_3, r_4, r_5\}$ are the pre and post cond of the global attack or attack plan

Global vulnerability -V

- As shown in the example, to discover global vulnerabilities we need to know
  - Local vulnerabilities
  - Pre/post conditions of the attacks they enable
  - Pre/post conditions of vulnerabilities
- This also sufficies but only when the local vulnerabilities affect components in the same node of the ICT infrastructure

Discovering lobal vulnerabilities

- As shown in the example, to discover global vulnerabilities we need to know
  - Local vulnerabilities
  - Pre/post conditions of the attacks they enable
  - Pre/post conditions of vulnerabilities
- This also sufficies when the local vulnerabilities affect components in the same node of the ICT infrastructure

Global vulns and topology

- A global attack may spread among several nodes if the threat exploits a vulnerability in n_i through a remote attack from n_j
- This only happens if and when

$$n_i \textit{ is allowed to communicate with } n_j$$

- We need to know also the logical topology of the ICT infrastructure

QSec

- It builds a relational database with information to classify and correlate local vulnerabilities
- Offers pre-built queries and mechanisms that return information on global vulnerabilities and attack plans to support a security assessment
- Focus on global attacks that spread among several infrastructure nodes

QSec: pre and post conditions

- Qsec classifies vulnerabilities to determine their pre and post conditions
- The classification
  - is independent from the adopted scanner as it refers to the descriptions in Common Vulnerability Enumeration, CVE, a de facto standard
  - exploits a context dependent search for some patterns (predefined keywords) in the CVE description
  - can also consider CVE details

The classification - I

- Three main classes
  - Vulns that enable the full control of a node,
  - Vulns that enable the full control of a node when paired with privileges acquired through distinct attacks
  - Vulns that cannot enable the full control of a node
- A classes may be further partitioned into subclasses

The classification - II

- First class = Remote code exec as admin /Man In The Middle
- Second class = Local Privileges Escalation

  Remote code execution as user

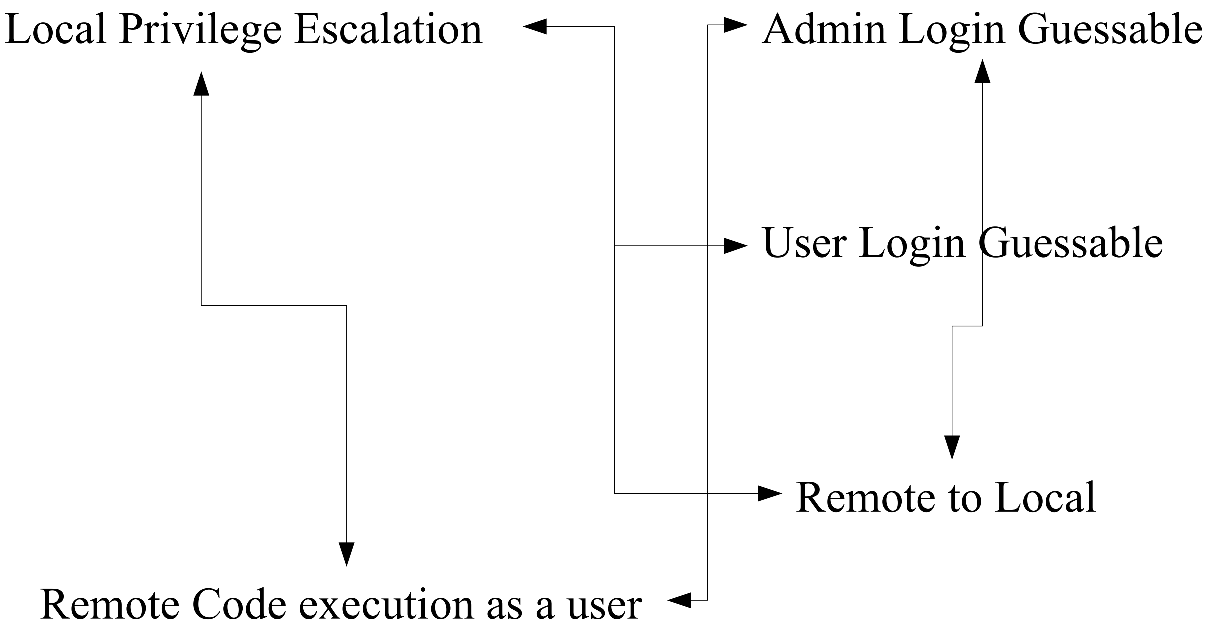
  Admin login guessable

  User login guessable

  Remote to local
- Third class = Minor Vulnerabilities

  Further output

The classification - III



Local Privilege Escalation

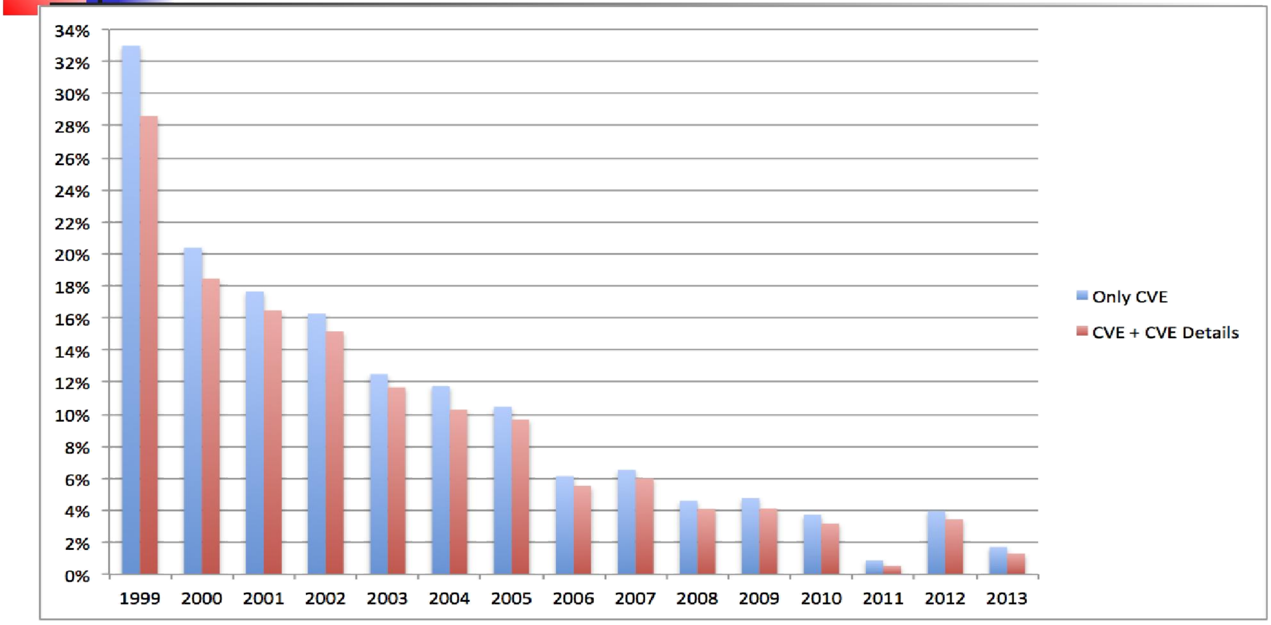
Admin Login Guessable

User Login Guessable

Remote to Local

Remote Code execution as a user

Accuracy of QSec



No misclassification only some missed classification if the CVE description does not match any pattern, reduced through CVE details

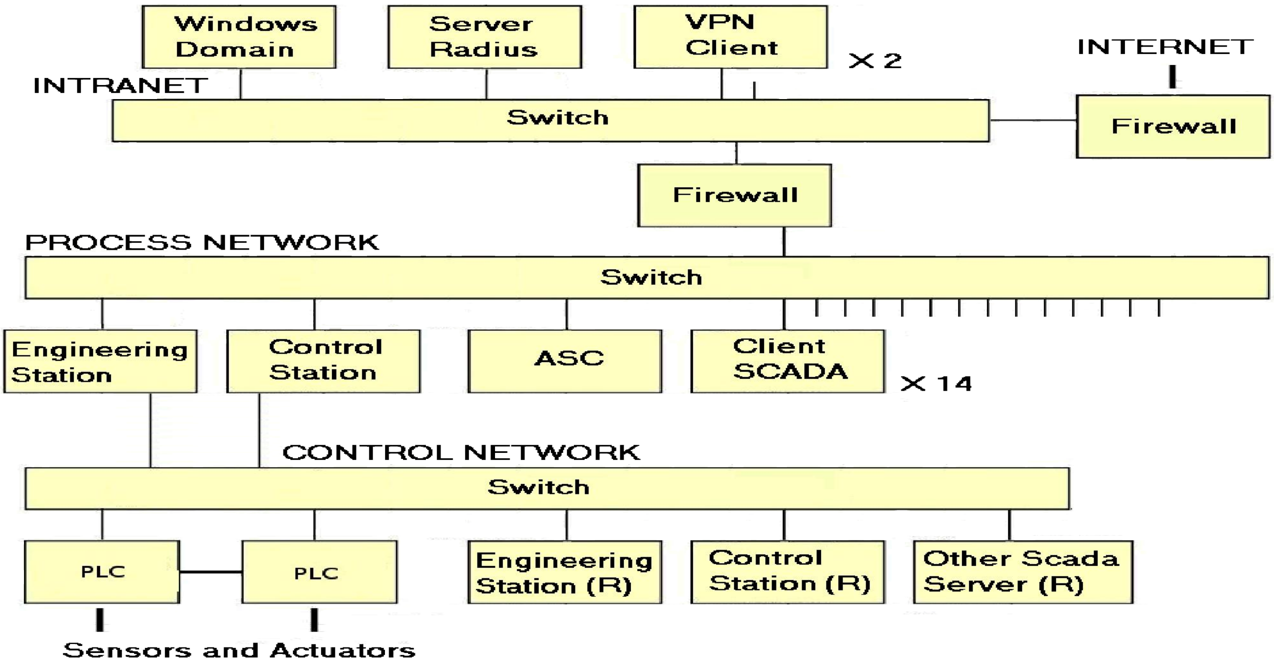
QSec database

- The input of QSec describes the vulns and the logical topology of the infrastructure
- By classifying and correlating vulns, QSec builds a database with information on
  - Global vulnerabilities in a node
  - Global attacks to control a node
  - How these global attacks can be sequentialized to spread among nodes

Qsec: querying the database

- Critical information for an assessment may be computed by properly querying the database
- A set of predefined queries to compute
  - Local vulns that appear not appear in a global one
  - Local vulns affecting a node
  - Which nodes can be attacked from a given node
  - The global vulns that affect a node
  - The global attacks that involves an intermediate node
  - Ranking of global vulns through the CVSS score of local ones

A case study



Some details - I

- The 6 intranet nodes interface an external production plant with access privileges to some control nodes
- A Windows Domain Server and two VPN Clients in the intranet can remotely access the process network.
- The 17 nodes in the process network run SCADA servers and clients that act as the supervision and control system. Some nodes are redundant for safety reasons.
- The 7 control network nodes simulate the electric power production plant through proper hydraulic circuits and PLC systems.

Some details - II

- The whole infrastructure is affected by 2700 local vulnerabilities, about 900 for each network.
- The Windows domain server is the node with the largest number of vulnerabilities, 61
- The ASC server is the process network, node with the largest number of local vulnerabilities, 634,
- The PLCs are the control network nodes with the largest number of vulnerabilities, 10

Correlation and global vulns

- There are about 700 global vulnerabilities
- About 50 of these vulns enables a complex attack starting in the intranet and resulting in the control of a node in the control network
- Further attacks start in the process network and reach a target in the control network

Further info from QSec

- Useful information not only to assess the risk but also to manage it
- All the global attacks that starts
  - from the intranet or
  - from the process network

  can be prevented by patching two local vulns

Further info from QSec

- Useful information not only to assess the risk but also to manage it
- All the global attacks that starts
  - from the intranet or
  - from the process network

  can be prevented by patching two local vulns