securiCAD solutions description

This document is an introduction to the securiCAD concept, the securiCAD software and the research behind the securiCAD attack simulation engine.

Introduction

securiCAD is a unique tool for decision-making and risk management in IT security. A securiCAD report typically provides insights into current risk exposure and material for objective and data-driven decisions to reduce the risk exposure. Other powerful applications of the tool are proactive security evaluation of systems under development or in the design and change phase.

The securiCAD concept

securiCAD conducts automated attack simulations to models of current and future IT architectures, identifies and quantifies risks holistically including structural vulnerabilities, and provides decision support based on the findings. The attack simulations quantify the potential attackers' actions with probability of success, most likely attack path and TTC (Time to compromise) to high value assets. Since all simulations are conducted on a model of the IT architecture, there is no impact on availability or any connection to the online systems. Below is a brief summary of the methodology and the steps involved when doing risk assessments with securiCAD.

1. Create a model

securiCAD conducts all attack simulations on a model of the systems under assessment. Therefore, the tool will have no impact on availability or have any active connection to the actual systems. The model is created by adding objects and connecting them to each other to represent Systems, Networks, Services, Routers, Users etc. Anything you typically find in an IT architecture.

2. Simulate attacks

The attack simulations are probabilistic and features statistical data on success rates and time frames for most types of attacks (e.g. how long it typically takes an attacker to find and exploit a software vulnerability). The simulation is fully automated and is started by adding an Attacker to an entry point in the model (e.g. the internet) which will then try every possible weakness and exploit to reach and compromise the systems.

3. Mange risk exposure

Based on the simulations data, securiCAD will generate reports on risks, weaknesses and most probable attack paths. securiCAD will also suggest security controls that will lower the risk exposure which can be applied and evaluated in additional simulations to find the most effective actions for the systems under assessment. Furthermore, new system designs or planned changes can be objectively compared against each other and the cost of security controls and design decisions can be evaluated against the risk exposure.

securiCAD Professional

securiCAD Professional enables risk and IT security architects to design virtual models of current and future IT infrastructures. Through virtual attack simulation, and mitigation testing, securiCAD Professional will provide detailed information about successful attack paths and most likely kill chains. Customers are able to virtually assess security mitigations deployed in securiCAD in order to find the most effective way to eliminate cyber threats. securiCAD Professional requires no installation or external connections to run.

Key features

Security by Design

Be proactive; simulate attacks to your planned architecture designs or changes and manage risks before deployment

Structural Vulnerabilities

Find the structural weaknesses (e.g., the combination of a technical vulnerability and a bad user) in your architecture

Proactive Modeling Tool

Create models of your architecture in our modeling tool or refine models that are automatically generated in securiCAD Enterprise

Attack Simulations

Run non-biased, non-disruptive and automated attack simulations on a model of your architecture

Critical Paths

Find the most critical paths from a potential attacker to a high value asset

Explore Weaknesses

Find exploited weaknesses and possible improvements in your architecture based on the attack simulations

Components

Create and share reusable components (collection of objects) for more efficient modeling

Export Data

Export the result of attack simulations for reporting or integration with external tools

Non-disruptive

All attack simulations are run on models of your architecture and will not affect, or in any way connect to actual systems during simulation

Get started within minutes

securiCAD Professional requires no installation and can be used on all modern workstations and laptops

Features

Proactive modeling

The user builds a model manually by selecting components or objects, dropping them onto the canvas, connecting them and setting defense attribute values. The advanced user can also personalize attack steps by changing individual attack step time-to-compromise distributions.

Components

Components are collections of securiCAD objects that can be reused and shared for more efficient modeling. securiCAD comes with a collection of predefined components that represents standard assets typically found in an IT architecture. Components can be created directly in securiCAD and will be automatically added to a local component library.

Attack simulations

Attack simulations are conducted locally in the built-in simulation engine. The simulations leverage the data and expertise that is built into securiCAD in combination with potential user-defined time-to-compromise distributions and defense attributes.

Analysis and decisions support:

- Time-to-compromise analysis
  For each object and attack step in the model, securiCAD produces a time-to-compromise distribution, i.e. a distribution of the time it is expected to take for the defined attacker to succeed with this specific object and attack step, given the input in the model and the architecture.

- Risk matrix
  The risk matrix shows (1) probability of compromise and (2) consequence of compromise, for all objects/attack steps where the user has defined a cost/consequence of compromise. The probability of compromise is taken from the time to compromise analysis as described above.

- Attack path analysis
  For each object and attack step in the model, the user can visualize the critical path(s) and the imperfect defenses in this critical path(s). The critical path(s) is the most probable way(s) that a rational attacker would succeed in their attack (in the modeled architecture and scenario). This shows the weakest link(s) in the modeled architecture. securiCAD also provides insight into what defenses are “imperfect” to help the user identify opportunities to improve the model.

Export

The result of the simulations can be exported to a .csv file. The exported file will contain all relevant data from the simulations, such as: time-to-compromise values, probabilities, attack paths, consequences and cost.

Installation and licensing

securiCAD Professional is distributed as an installer or as a .zip that does not require any installation. Upon purchase of securiCAD Professional, the user is provided with a license file that can be used to activate the software. The license dictates for how long the software can be used as well as how many objects that can be used in each model. Furthermore, the license can also bind securiCAD Professional to specific hardware so that licenses can't be shared, if required.

Requirements

securiCAD Professional requires a 64-bit version of any of the supported operating systems. The supported operating systems are:

- MS Windows 7, 8.1 and 10
- Mac OS 10.8.3 or higher

A Linux build of securiCAD Professional is regularly made but Linux is currently not an officially supported platform.

securiCAD Enterprise

securiCAD Enterprise features cyber risk simulation, collaboration, and reporting features. securiCAD Enterprise can be deployed on-premise, air-gapped, or in cloud environment with access- and permission controls for sensitive information. Use securiCAD Enterprise for continuous risk assessment of your IT-architecture while planning, sharing and assessing models of future architectural designs. Assess security mitigations automatically suggested by securiCAD and generate reports of results. securiCAD Enterprise also features the possibility of parsing data from e.g. common inventory and scanning tools for automatic modeling.

Key features

Risk Assessments

Get your current risk exposure based on quantitative and automated attack simulations

Structural Vulnerabilities

Find the structural weaknesses (e.g., the combination of a technical vulnerability and a bad user) in your architecture

Model Generation

Leverage your existing data to automatically generate parts, or a complete model of your existing architecture

Attack Simulations

Run non-biased, non-disruptive and automated attack simulations on a model of your architecture

Critical Paths

Find the most critical paths from a potential attacker to a high value asset

Chokepoints

Find chokepoints (or key assets) in your architecture that the attacker exploits to reach all your high value assets

Suggested Mitigations

Get automatically generated mitigation suggestions based on the attack simulations to lower your risk exposure

Report Generation

Generate and export reports based on results from one or several attack simulations

Cloud Deployment

Deploy your securiCAD Enterprise solution in any cloud environment or use our Managed AWS solution

On-premise or Air-gapped

Use existing hardware on-premise to run our securiCAD Enterprise VM. Operation does not require external access

Non-disruptive

All attack simulations are run on models of your architecture and will not affect, or in any way connect to your actual systems during simulation

API & SDK

Use the API for custom integrations or continuous and automated risk assessment. Develop your own data parsers with our SDK to support automatic modeling of proprietary or custom data sources

Features

Project and user management

Create projects where models can be uploaded and analyzed. With projects, the user can control which other users will have access to the models and simulation results. The administrator can add and remove users to securiCAD Enterprise as well as providing different level of control and visibility.

Web-based modeling

The new web-based modeling in securiCAD Enterprise makes the securiCAD product suite fully web-based. With a brand-new modeling framework, modeling comes more intuitive, flexible, automated and will also allow for collaborative modeling as well as more dynamic objects and components.

Model management

Upload, share and download models and components between projects and users of securiCAD Enterprise. Inspect the model by looking at the Views of the model (either created manually in securiCAD Professional or generated automatically by Transform in securiCAD Enterprise). securiCAD Enterprise will also provide a model status that denotes if the model is ready (Valid) to be simulated or not.

Model generation

securiCAD can automatically generate models of deployed IT architectures by harnessing existing data sources, on-premise and in the cloud.

Model merge and transform

Models in a Project can be merged and transformed. Transform lets the user apply configurations (such as tags, defense attributes and custom time-to-compromise distributions) to the model. Merge helps the user to automatically connect models to each other based on tags in the model.

Simulate attacks

The user places an attacker in the model (either with Transform or manually in securiCAD Professional). The attacker can be put at different places in the model to simulate different attack scenarios such as e.g. Internet-based attacks or insider attacks. Once the attacker is placed and the model is Valid, the user can Start Trail to simulate attacks to the generated model. The simulation is done with probabilistic attack graphs.

Advanced analysis and decision support:

- Scenarios
  Create multiple Trails in a Project to analyze different attack scenarios on the same model or to analyze different models in the same Project. Results from different Trails can be compared and reported on.

- Risk metrics and matrix:
  The risk metrics are based on (1) probability of a successful attack (calculated by securiCAD) and (2) consequence of a successful attack (assigned by the user). As such, the extent of the risk assessment is based on how many consequences the user has defined. Total Risk is the aggregation of all risk metrics in the simulation. Confidentiality, Integrity and Availability Risk

will also consider which type of attack the consequence is assigned on (e.g. Read on a Datastore will affect the Confidentiality Risk).

- Critical paths:
  For all attacks with a consequence assigned to it, securiCAD Enterprise will be able to visualize Critical Paths. The Critical path(s) is the most probable way(s) that a rational attacker would take to success with the specified attack in the simulation. The path(s) will contain all steps the attacker would have to take, as well as which weaknesses (imperfect defenses) the attacker has exploited.

- Risk Time-to-compromise (TTC) details:
  For all attacks with a consequence assigned to it in the model, securiCAD produces a time-to-compromise distribution, i.e. a distribution of the time it is expected to take for the defined attacker to succeed with this specific object and attack step, given the input in the model and the architecture.

- Tag-based Time-to-compromise (TTC) aggregation:
  Provided that the user has assigned tags (“team” or “system”) with Transform or manually in securiCAD Professional, securiCAD Enterprise will provide the user with an aggregation of metrics (Average TTC and Average Probability of success) based on those tags and a set of predefined attack steps.

- Chokepoints:
  Chokepoints is an aggregation of all Critical Paths to attack steps with consequence on them. A chokepoint is an asset where attacks (towards attack steps with consequence on them) converge in the model. The width of the lines (between the chokepoint and the attack step with consequence on it) and the chokepoint bars indicates how much of the total risk the chokepoints contribute to.

- Suggested mitigations:
  securiCAD Enterprise will automatically suggest mitigations based on weaknesses (imperfect defenses) in the Critical Paths. Suggested mitigations are also enumerated with a Frequency which denotes how many times it is exploited in all Critical Paths to all attack steps with consequence on them.

- Labs:
  In Labs, all applied Suggested mitigations will be collected. The user can also add their own mitigations, tags and custom Time-to-compromise distributions to evaluate (by running new simulations) mitigations and configurations not suggested by securiCAD Enterprise.

- Trends and comparisons:
  The risk metrics of the simulations in a Trail will be automatically plotted in the Trail Overview. Results from multiple simulations (either in a single Trail or across several) can be compared to each other (provided that they share one or more attack step with consequence assigned to it). The comparison will contain the risk metric of each attack step with consequence on it as well as probability of a successful attack and a risk enumeration (Low, Medium, High, Critical).

Installation

foreseeti provides securiCAD Enterprise customers with a distribution package which contains all necessary binaries as well as an installation script that will automatically install securiCAD Enterprise on the selected host. A full technical installation guide is provided with the distribution package.

Licensing

Once the installation is finished, securiCAD Enterprise is ready to be used and can be activated by providing the system with a license via the user interface. The license dictates the number of users, size of models as well as which features that are available. No additional setup or customization is needed to get started. During the installation, an administrator account is automatically generated, and the credentials are reported during the installation. That account can then be used to create additional users in the system.

Requirements

securiCAD Enterprise is a web-based platform that can be deployed on most modern servers or workstations. foreseeti strongly recommends a system with GPU support for increased simulation performance for models with 100 or more endpoints.

Hardware Requirements:

Minimum: 8 GB RAM, Dual Core CPU, 10 GB HDD
Recommended: 16 GB RAM, Quad Core CPU, 50 GB HDD, GPU (2GB RAM and OpenCL 1.2)

Software Requirements:

Supported Operating Systems: Ubuntu Server 16.04 LTS, RHEL 7 and CentOS 7. The installation will also require a dedicated account with sudo privileges.

(Note: There are instances of securiCAD Enterprise running in Windows environments but foreseeti does not currently supply any automatic installers for Windows deployments)

Network Requirements:

The installation script requires internet access (or a local repository) during installation to fetch the latest Linux libraries. Operation requires no internet access.

Hardware Acceleration with GPU:

The simulation performance of securiCAD Enterprise can be greatly increased by using hardware acceleration via a GPU and is the recommended method of simulation by foreseeti. To utilize GPU accelerated simulations one must have an integrated GPU from Intel (3rd gen or newer) or a dedicated GPU from Nvidia or AMD with support for (OpenCL 1.2 or newer)

securiCAD Community Edition

The securiCAD Community Edition is a free threat modeling, simulation and reporting solution intended for models up to 100 objects. This allows for a hands-on experience how to model, simulate and work with the threat insight reports created by the foreseeti suite of tools.

The securiCAD Community Edition consists of the securiCAD Desktop software and an account in the securiCAD Simulation Service. The securiCAD Desktop software is used for creating and editing models and the securiCAD Simulation Service is an online service hosted by foreseeti that runs the model simulations and generates reports on the results.

Key features

Modeling

The user builds a model manually by selecting components or objects, dropping them onto the canvas, connecting them and setting defense attribute values. The advanced user can also personalize attack steps by changing individual attack step time-to-compromise distributions. The models are limited to 100 objects in the Community Edition.

Attack simulations

Attack simulations are conducted locally in the built-in simulation engine as well as in the online simulation service for securiCAD Enterprise report previews.

Analysis and decisions support:

- Time-to-compromise analysis
  For each object and attack step in the model, securiCAD produces a time-to-compromise distribution, i.e. a distribution of the time it is expected to take for the defined attacker to succeed with this specific object and attack step, given the input in the model and the architecture

- Online Reports
  With securiCAD Community Edition you get a preview of the reporting features of securiCAD Enterprise. When you simulate in the tool, the model will be automatically and securely sent to our online simulation service that will generate a report based on your model and its high value assets. The report content is restricted to an overall risk report and attack path analysis.

Sign up and Installation

Users can get access to the Community Edition by signing up to the securiCAD User Community at https://securicad.community. After signing up, you will receive a confirmation email with credentials to the online simulation service and an installer to securiCAD Community Edition can be downloaded. When the installation is finished, securiCAD Community Edition will connect to the online simulation service to verify the credentials. If you are new to securiCAD, there are plenty of guides and tutorials available at https://securicad.community.

Requirements

securiCAD Community Edition requires a 64-bit version of any of the supported operating systems. The supported operating systems are:

- MS Windows 7, 8.1 and 10
- Mac OS 10.8.3 or higher

securiCAD simulation engine

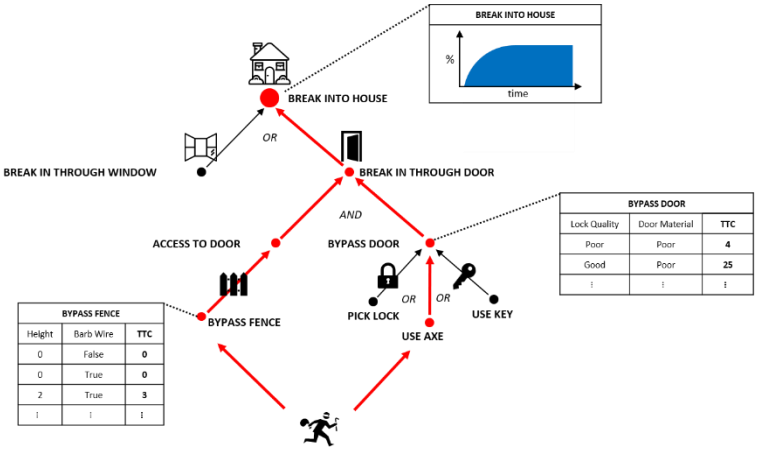
securiCAD assesses the time it takes for a highly capable adversary to compromise different assets in your architecture by generating attack graphs from a model of an IT architecture. The attack graphs are populated with probability distributions that specifies the amount of time it would take the attacker to traverse the steps in the attack graph. Monte Carlo simulations are then used to sample the distributions of all attack steps in the model.

securiCAD provides insight to the attack times as a probability distribution – a Time to Compromise (TTC) -distribution and most likely attack paths.

Attack graphs and Bayesian networks

To be able to obtain a correct aggregation of data and statistics one must recognize the relation between components in an IT architecture i.e. how attackers can use separate vulnerabilities and weaknesses to advance an intrusion. Attack graphs are used to model the composition of vulnerabilities found in a network or system and aggregate them as possible intrusion paths, calculate their likelihood of success or the loss value.

In the figure on the right there is an example of an attack graph where each node represents an attack step an attacker can take to break into a house. The edges represent how the attack steps relate to each other i.e. that you need to access and bypass a door before you can break in through it.



However, in such graphs the dependencies are not deterministic; the attacker might not always succeed with picking the lock and it will take some time, time that may vary somewhat between different attempts. In order capture these uncertainties securiCAD uses Bayesian probability theory. (Bayesian statistics is commonly used in many scientific disciplines and engineering applications such as artificial intelligence.) Bayesian attack graphs are the combination of general attack graphs and Bayesian networks. Bayesian networks use directed edges to represent the casual dependencies between probabilistic variables of a nodes in a graph. There are several implementations of Bayesian attack graphs with the goal of calculating general security metrics combined with the probabilistic dependencies of Bayesian networks. They have later been modified and extended to include mitigation strategies and defenses. In the figure above, we have illustrated that the time and probability of our house being broken into depends on the parameters (defenses) of the assets (e.g. whether or not we have barb wire on our fence).

Time-To-Compromise (TTC)

Time-to-compromise is a measure of the effort expended by an attacker for a successful attack assuming effort is expended uniformly. In the attack graph, this can be seen as the time it takes for the attacker to “travel” between the nodes i.e. the attack steps. The attacker will then take the shortest path i.e. the least time-consuming way to the end node in the graph (see the figure above).

As the TTC increases, the likelihood of a successful attack, and thereby risk, decreases (McQueen, 2006). In securiCAD, we calculate TTC by repeated random sampling using the Monte Carlo method.

Each sample is based on the outcomes of the probabilities in a cumulative distribution functions (CDF) and the results of the sampling is then aggregated to an empirical mean (sample mean).

Monte Carlo simulations and the implementation

The calculation engine builds on an implementation of the shortest path problem which is a classical network optimization problem which arises in many practical situations. The algorithm exists in many variations and the most common variant, *Dijkstra's Single-Source Shortest Path Algorithm,* marks a node as source and finds the shortest path from the source node to all other nodes.

The implementation of *Dijkstra's Single-Source Shortest Path Algorithm* used in securiCAD is called *Dial's Approximate Buckets*. A description of the algorithm is available in Cherkassky et al., "Shortest Paths Algorithms: theory and Experimental Evaluation", 1993. Another description is available in Ahuja, et al., "Network Flows: Theory, Algorithms, and Applications", 1993.

Hardware acceleration

Graph representations are common in many scientific and engineering domains and parallel algorithms on the CPU can get you very far. However, as graphs grow past millions of vertices, even parallel CPU implementations of the algorithms mention above become less cost- and time efficient. Dedicated or integrated graphics hardware (GPU) has become a cost-effective and commonplace parallel processing platform for many consumer products, even in laptops and tablets. Even though the GPU is most commonly used for image processing and rendering graphics, the flexible architecture of modern GPUs allows for alternate programming models with CUDA and OpenCL. The simulation performance of securiCAD can be greatly increased by using hardware acceleration via a GPU. The GPU implementation of the shortest path algorithms mentioned above is based on "Accelerating large graph algorithms on the GPU using CUDA", 2007 by by Parwan Harish and P.J. Narayanan.

Probabilities, logic and how they are updated

Statistics (probability distributions) and logic (generation and connection of attack steps) in the tool is based on research and development continuously ongoing within foreseeti and KTH Royal Institute of Technology, but also other researchers' study results.

All statistics, logic and data employed in securiCAD are derived from scientific studies, experiments, surveys, expert judgement and vulnerability data as a part of continuously ongoing research within foreseeti and KTH Royal Institute of Technology, but also other researchers' study results (previous work includes studies on vulnerability discovery (including zero days), arbitrary code execution exploits, denial of service attacks, intrusion detection effectiveness, network scanner effectiveness, phishing, configuration faults and unknown entry points, password cracking and guessing). The collected data is aggregated and represented as logical necessities or distributions on attack steps to denote the probability over time for a successful attack. All sources are publicly available or available through journals or scientific publications.

Probabilities are customizable and can be edited by the user to represent special cases, incorporate more detailed knowledge about defense mechanisms or non-standard attack.

Updates and validation

securiCAD is continuously revised and updated with the methods mentioned above. Furthermore, securiCAD is continuously validated and benchmarked against security experts from a wide variety of industries in Turing tests. In the Turing tests, domain experts within IT security have investigated and estimated the security aspects of a given system and network architecture. The same architecture

has also been modelled and analyzed using securiCAD. The results of the experts and securiCAD have then been anonymized and blended together and finally the results have been compared and judged to find out how well securiCAD is conforming with the domain experts' assessments. With the tests, it has been scientifically established that securiCAD performs on par with the sharpest minds in threat modelling.

Vulnerability data

For software-specific probabilities, securiCAD leverages a deep neural network based on vulnerability data from the National Vulnerability Database (NVD). Given a specific product and product version, securiCAD can tailor the statistics to better represent the probability and time to new vulnerabilities in software products.