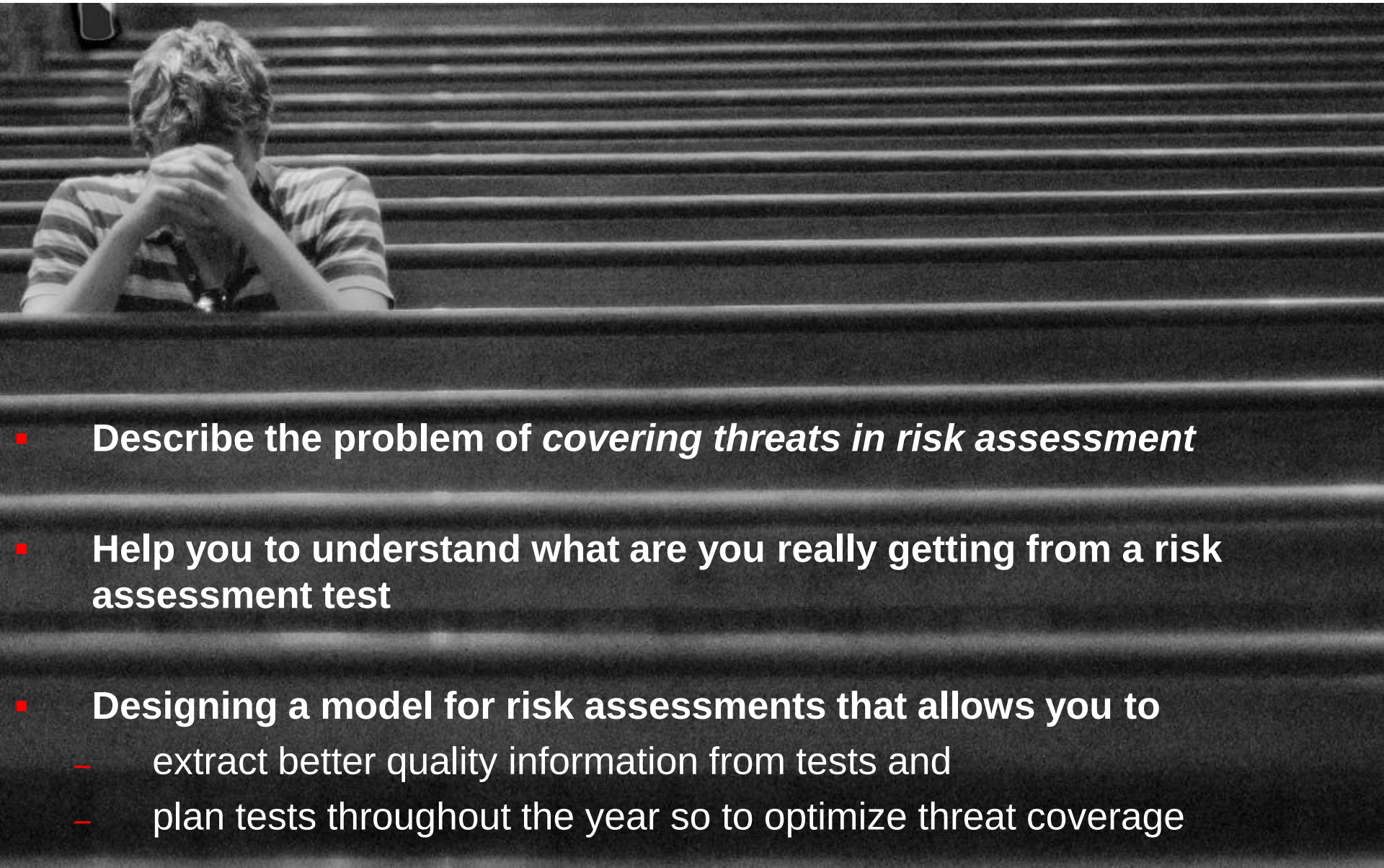
Risk assessment tactics optimizing efficiency and threat-space coverage

Fred.Pinkett@coresecurity.com

Agenda

- **Setup and context**
- **Intro to risk assessment**
- **Model for defining risk assessment**
- **Wrap-up**

What's this talk about



- **Describe the problem of *covering threats in risk assessment***
- **Help you to understand what are you really getting from a risk assessment test**
- **Designing a model for risk assessments that allows you to**
  - extract better quality information from tests and
  - plan tests throughout the year so to optimize threat coverage

Who is this talk for

A. **Chief Security Officers and executives that are responsible for the security in an organization**

B. **CFOs and anybody interested in metrics that measure risk**

C. **Penetration testers and security researchers**

D. **Risk assessment experts**

First things first - Terminology

- **A vulnerability is a property of a software which can be used by an attacker to exercise a feature that was not included by design**
  - E.g., an incorrect handling of memory may provide attackers with the means to compromise the computer where this software runs
  - E.g., an unsafe handling of input in a webapp might provide the attacker with the ability to steal, delete or modify the data in its DB.

- **An exploit is the piece of code that exercises this vulnerability with a non-zero probability of success**
  - All exploits are not 100% reliable, this depends on the quality of their code

Threat

- **A threat is a set of actions that an attacker could potentially exercise (e.g., using exploits) that affects negatively the target organization's assets**

- **It underlies loss for the organization and gain for the attacker**

- **Examples include:**
  - **Using a botnet to launch a DDoS attack that makes the company's webservers unavailable**
  - **Inserting a work into the corporate network**
  - **Hacking into a C-level exec's laptop and stealing critical information**

Agenda

- **Setup and context**
- **Intro to risk assessment**
- **Model for defining risk assessment**
- **Wrap-up**

What is Risk Assessment? (in terms of computer security)

- **A set of test methodologies for discovering and analyzing threats**
- **In computer security we are interested in threats that an attacker might exercise today**
- **Providing a prioritization or valorization for each threat**
- **An assessment is often a step of a "risk management" process, where each threat is:**
  - Avoided, mitigated, transferred or retained

Hire ninjas, they'll always come handy!

- **Risk assessment starts by scoping:**
  - Which kind of attackers I want to anticipate
  - What would they go against
  - How much resources can be allocated to this task

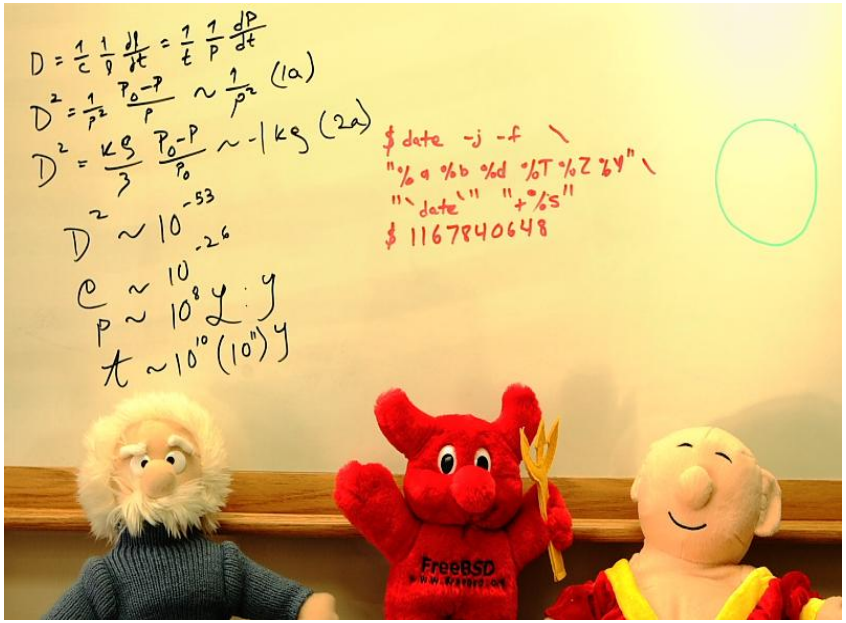
- **The risk assessment team/solution will then**
  - look for threats constrained by the above limitations
  - for each threat analyze its relevance and how likely is it to be exercised

- **Different risk assessment methodologies have different levels of accuracy and cost**

When the going gets weird the weird turn pro (HST)

- **All methodologies in use**
  - Start with the extraction of raw data through tests
  - Followed by analysis

- **Two methodologies that come to mind are**
  - Penetration testing
  - Vulnerability scanning and attack tree simulation



Penetration test and Vuln Scan

Penetration Test

- **Have a group of experts attempt to break into an organization**
- **They start with a "scope" that defines limitations and objectives**
- **They exercise threat in the organization**
- **Report threats, their criticality and suggest countermeasures**

Vulnerability Scan / Attack Tree

- **Forming a perspective of the network's topology and configuration**
  - This is typically done importing configs. from network devices
- **Deducing the version of the software**
  - This is done through passive information gathering, e.g., banner grabbing
- **Matching this with a vulnerabilities database**
  - E.g., that says that IE v6 is has a remotely exploitable vulnerability
- **Producing a report describing (potentially) vulnerable software and added information**

Blind spots in risk assessment methodologies

- **We cannot aggregate the results from different tests**
- **We cannot understand what threats have been covered with the tests and which haven't**
- **We cannot understand what results are valid after some time**
  - e.g., make predictions
- **We cannot anticipate attackers for unknown threats,**
  - e.g., what is the impact of a 0day in our firewall?

Agenda

- **Setup and context**
- **Forms of risk assessment**
- **Model for defining risk assessment**
- **Wrap-up**

Expected applications of the model

- **Aggregate past tests and suggest new ones**
  - E.g., we do a network penetration test monthly, yet we never tried the WIFI attack vector.
  - E.g., you tested for internal attackers from network segments A, B and G against critical server S, but never from server N to server S
- **Allow what-if simulations with unavailable exploits**
  - E.g., to investigate potential threats and anticipate attackers
- **Given a threat, find out how long has it been possible**
  - E.g., all the steps in the threat could be done for the last two months but not before –since server S wasn't vulnerable back then.

Some model requirements

- **This is a work in progress: We are not ready to define a model explicitly**
- **We have a set of requirements that we follow to present**
- **We've been playing with some models for defining attacks which we want to extend to cope with these requirements**
  - I'll provide pointers to this material in the Bib section

Requirement: Agnostic

- **It should allow input from vulnerability scanner A, scanner B or next pen-testing suite C**

- **If a new attack vector is discovered tomorrow (e.g., wifi, voip, webapps), the model should allow the analysis of the threats derived from it**

Requirement: Objective and Consistent

- **Two analysts with the same given raw information should not derive inconsistent conclusions**

Requirement: Levels of Granularity

- **It must allow users to look at all the threats faced by an organization in one of these levels**

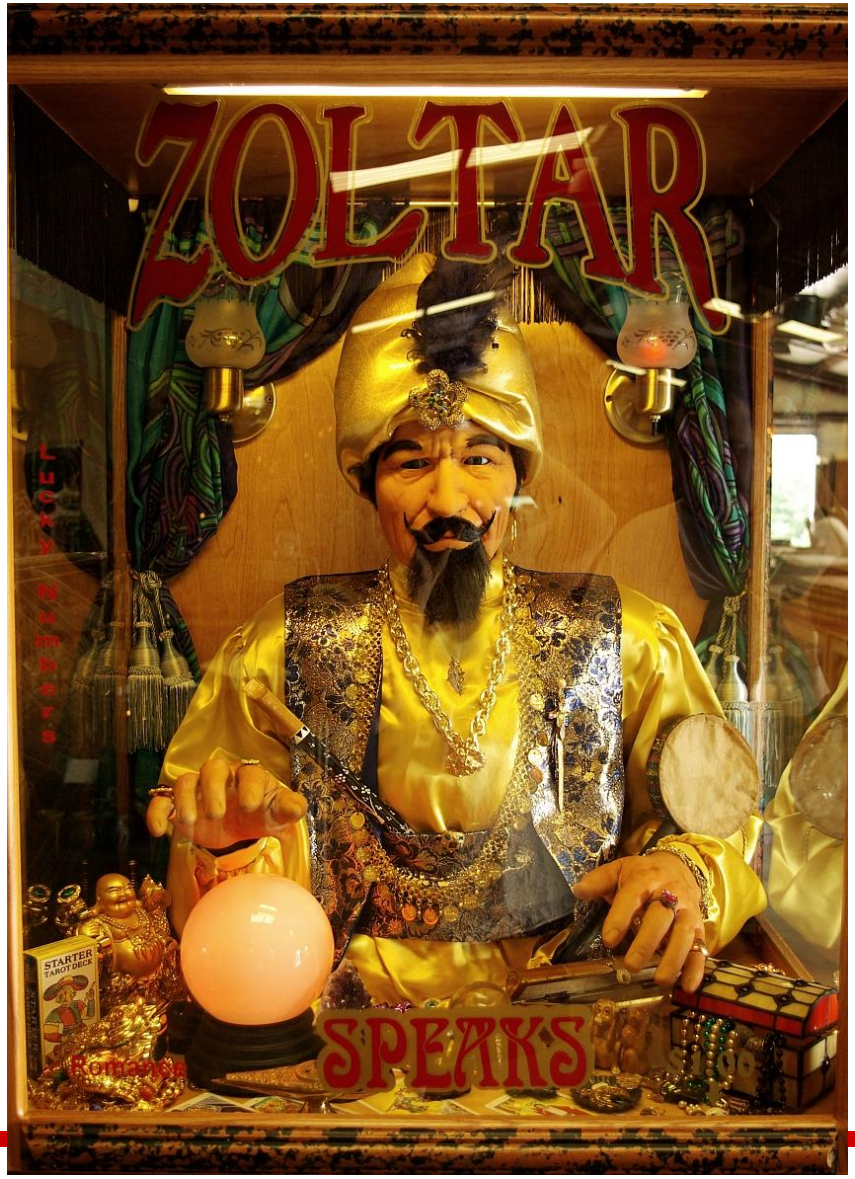
- **Another level should provide the granularity to define a threat with complete detail**
  - So that objectivity and consistency are ensured

Requirement: Inclusion of the Time Variable

Zoltar foresees threats…

… and the next vulnerability you will have to consider is…

A model must allow users to make predictions and assist them in the decision making process



Requirement: Inclusion of the Time Variable

- **Raw information from different tests cannot be combined ignoring time**
- **It must allow to combine past information to deduce how old is a threat discovered today**
- **It must allow *what if* simulations to deduce the impact of vulnerabilities that might appear tomorrow**

Agenda

- **Setup and context**
- **Forms of risk assessment**
- **Model for defining risk assessment**
- **Wrap-up**

Usefulness of the proposed model

- **We defined some requirements for performing risk assessment experiments, aggregating the results and analyzing it**
- **We've shown that building a model to do this analysis can be used to be better prepared at anticipating attacks**
- **We've seen that some models available today do not allow this analysis and showed where they can be improved**

Ulterior Objectives

- **The final goal of our research is producing a model and framework for:**
  - Describing single tests
  - Measuring the efficiency of these tests
  - Aggregating several security tests
  - Measuring the impact of the threats discovered
  - Allowing the analysis of this information
  - Planning future tests optimizing resources
    - » E.g., what is the most-likely threat that a hacker would try and I haven't tested yet

Thanks!

Fred Pinkett
VP of Product Management

Questions to:
Fred.Pinkett@coresecurity.com
Ariel.Waissbein@coresecurity.com

Bibliography

1. “Building Computer Network Attacks” by Futoransky, Notarfrancesco, Richarte, Sarraute. *Corelabs Technical Report, 2003*. Available at http:\\corelabs.coresecurity.com

2. “Fast Attack Planning,” by Sarraute. Submitted, June, 2009. Preprint available at http:\\corelabs.coresecurity.com

3. “Simulation of Computer Network Attacks,” by Miranda, Orlicki, Sarraute. In *Argentine Symposium on Computing Technology (AST) in 36avas Jornadas Argentinas de Informatica e Investigacion Operativa (JAIIO 36)*. Eds. Castineira Moreira and Finochietto. Mar del Plata, Buenos Aires, Argentina, 2007

4. “Simulating Cyber-Attacks for Fun and Profit,” Futoransky, Miranda, Orlicki, and Sarraute. In *2nd International Conference on Simulation Tools and Techniques (SIMUTools'09),* 2009.

5. “Your risk is not what it used to be,” Waissbein. In *ToorCon X*. September 26-28, 2008. San Diego, CA, USA.

Photo Credits

All photos are from Flickr and have creative commons license

- Soldiers by *gnasherku*
- Praying man by *lesser kudu*
- Earnie the Emu by bluegum
- Einstein, devil and Buda by totalaldo
- Martial arts kids by eam
- Puzzle face by *onkel*
- Open lock by woodsy (from sxc.hu)
- Zoltar by *House of Sims*