The Information Security Case

M. Anthony Aiello

Overview

- The major players
- The hunt
- The epiphany
- The end of the story

Overview

- The major players or: Motivation
- The hunt
- The epiphany
- The end of the story

An HSARPA BAA

- Information Security Cases: Security assessment must not merely result in a single number — a one-dimensional metric cannot possibly capture the range of properties or aspects that need to be assessed. This has long been recognized in safety critical systems where assessment is multidimensional and captures both process and product elements in a safety case - a reasoned coherent argument that supplies evidence to support the system designer claims. Research is needed to define appropriate argument structures in the case of information security, and to create supporting tools to aid the construction and maintenance of information security cases.

The Safety Case

- "A safety case should communicate a clear, comprehensive and defensible argument that a system is acceptably safe to operate in a particular context."

Kelly, Timothy P. "Arguing Safety – A Systematic Approach to Managing Safety Cases" PhD Thesis, York, 1998

The ~~Safety~~ Information Security Case

- "~~A safety~~ An information security case should communicate a clear, comprehensive and defensible argument that a system is acceptably ~~safe~~ secure to operate in a particular context."

Kelly, Timothy P. and Tony Aiello "Arguing Safety – A Systematic Approach to Managing Safety Cases" PhD Thesis, York, 1998

The HSARPA BAA

- Information Security Cases: Security assessment must not merely result in a single number — a one-dimensional metric cannot possibly capture the range of properties or aspects that need to be assessed. This has long been recognized in safety critical systems where assessment is multidimensional and captures both process and product elements in a safety case - a reasoned coherent argument that supplies evidence to support the system designer claims. Research is needed to define appropriate argument structures in the case of information security, and to create supporting tools to aid the construction and maintenance of information security cases.

What kind of evidence?

Overview

- The major players
- The hunt finding Evidence
- The epiphany
- The end of the story

Evidence in Safety Cases

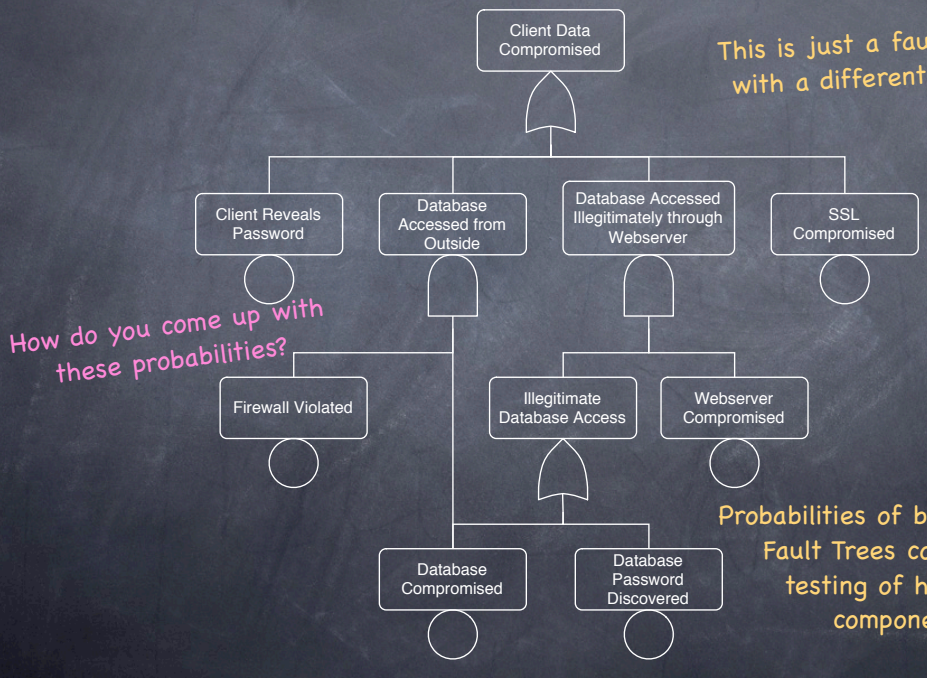
- Mathematical Analysis
- Event Trees
- Fault Trees
- FMECA
- Hazop

Evidence in Information Security Cases

- Attack Trees

...but these are hardly rigorous

An Attack Tree



This is just a fault tree with a different name

How do you come up with these probabilities?

Probabilities of basic events in Fault Trees comes from testing of hardware components.

Evidence in Information Security Cases

- Attack Trees
- Evidence that a process has been followed
  - For example, that certain precautions have been taken with certificate storage
  - That certain technologies have been employed to mitigate risks (SSL, etc.)

These aren't too exciting...

http://www.megatokyo.com

Overview

- The major players
- The hunt
- The epiphany I've seen this before...
- The end of the story

This Kind of Evidence is Familiar

- Attack Trees (formal, but non-rigorous)
- Evidence that a process has been followed
  - For example, that certain precautions have been taken with certificate storage
  - That certain technologies have been employed to mitigate risks (SSL, etc.)

(varying degrees of rigor, but informal)

Evidence in Safety Cases

- Mathematical Analysis
- Event Tree
- Fault Trees
- FMECA
- Hazop

These are for Hardware

Software Evidence

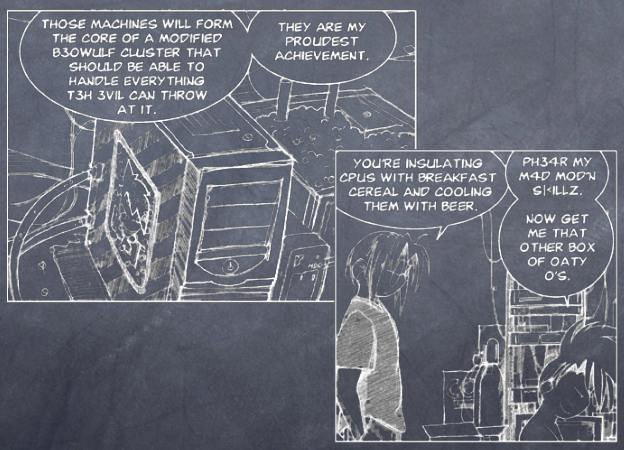
- What kinds of evidence might be generated for software systems?
  - Lots of evidence that processes have been followed
  - Meaningless fault trees (how meaningful are made-up probabilities?)
  - Some formal analysis

rarely system-wide

Information Security Evidence

- At best, we can hope to match the rigor of software evidence
- And this makes sense: software forms the basis of information security…

...and security is only as strong as the weakest link



http://www.megatokyo.com

Overview

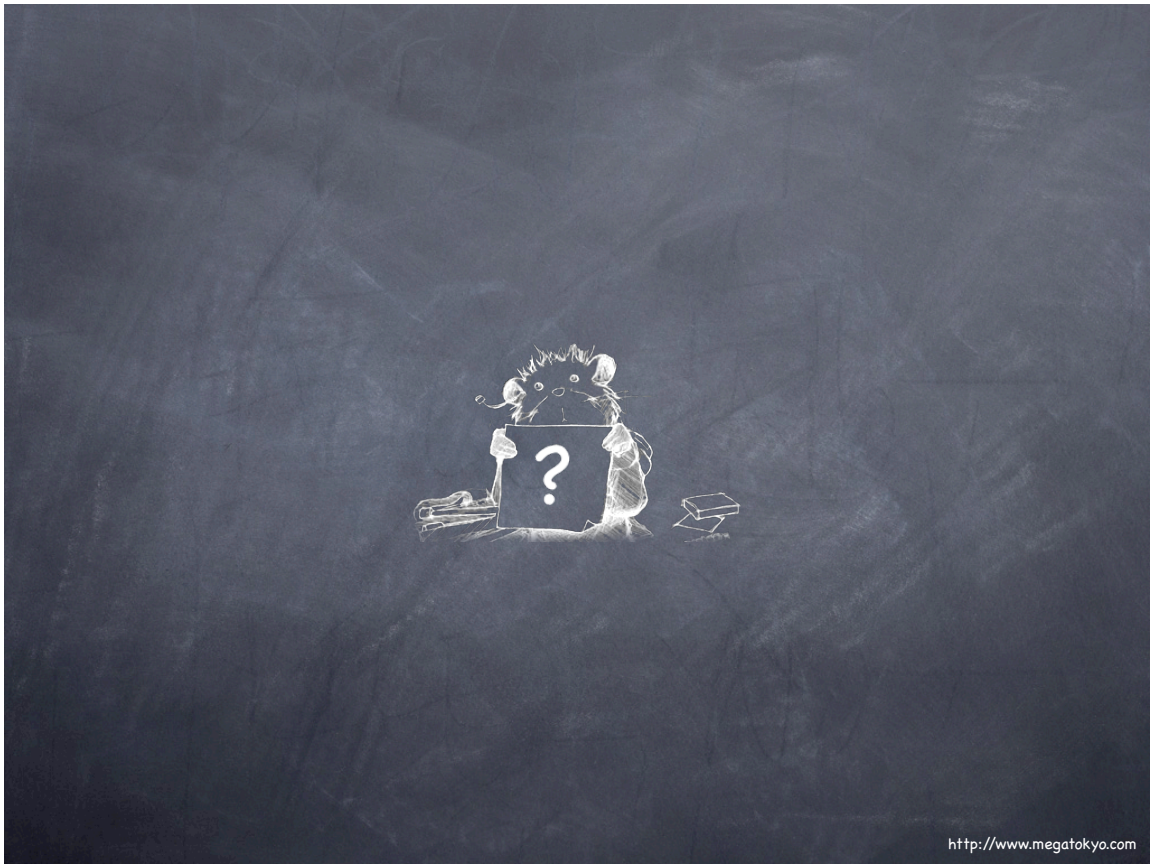
- The major players
- The hunt
- The epiphany
- The end of the story My conclusions

Place for the Information Security Case

- It will have its place as a semi-formal structure
- It will enable better forensic analysis:
  - Tracing from the failed goal to its evidence should reveal what went wrong

Looking Forward

- We need better kinds of evidence
  - More formal techniques
- Practically, this will be hard:
  - Our ability to reason about security is limited by our ability to reason about the underlying software


?
http://www.megatokyo.com