Threat Assessments and Attack Trees

April 19, 2018 | You Can Do This (!)

Bevan Watkiss

Security Engineer, GENIVI Alliance

About Me

- Security Engineer at Irdeto
- Member of the ethical hacking team
- Member of and contributor to GENIVI security subcommittee

cloakware™ for connected transport by irdeto

linkedin.com/in/bevan-watkiss

bevan.watkiss@irdeto.com

GENIVI®

Agenda, etc.

- Motivations: Why would I want to do this?
- What are Attack Trees? What are Threat Assessments?
- How can I do this?
- Should I do this?
- Feel free to stop me for questions at any time

GENIVI®

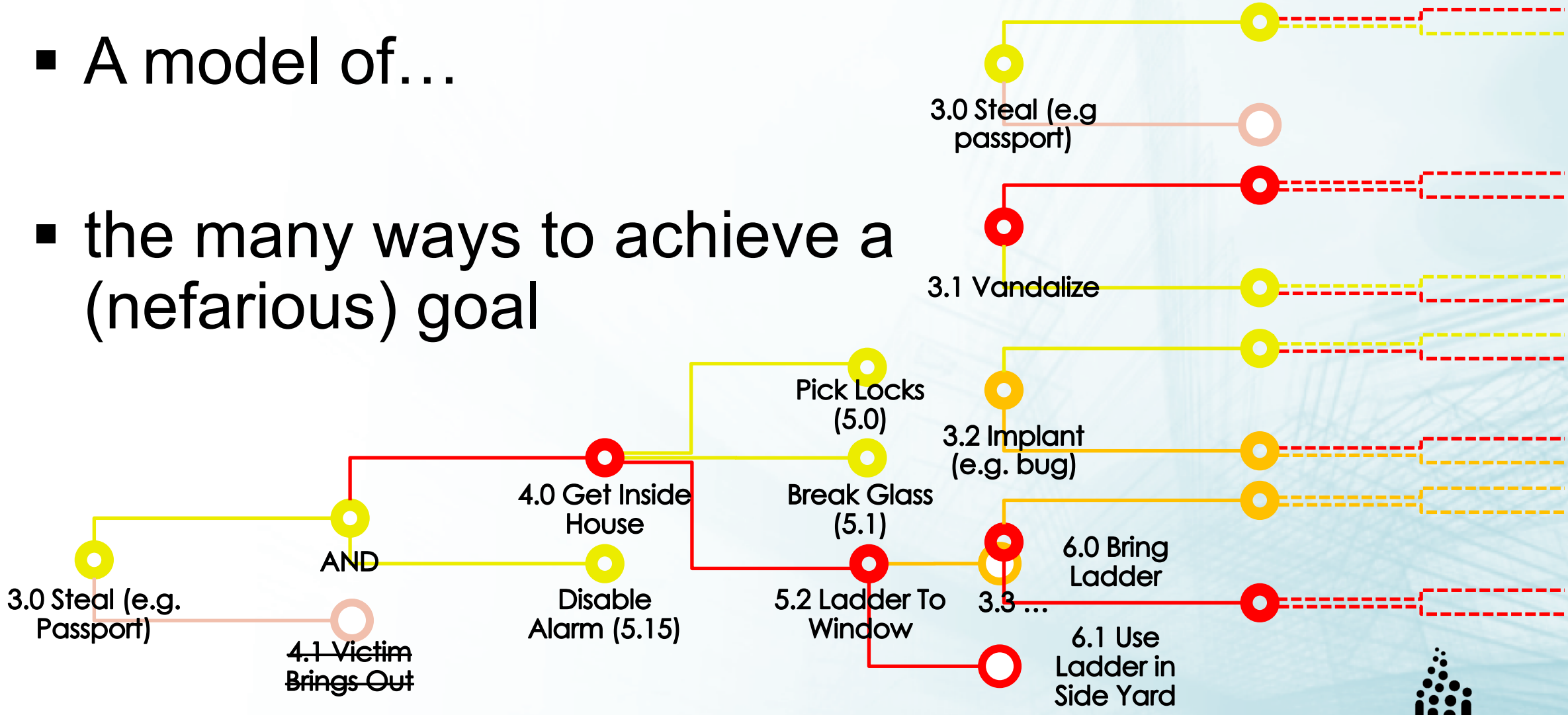
Motivation: More Effective to Fix Early

- Fixing Later → Overhauls
- Does take time now, but could save time in the long run
- And focuses efforts to areas that need it

GENIVI®

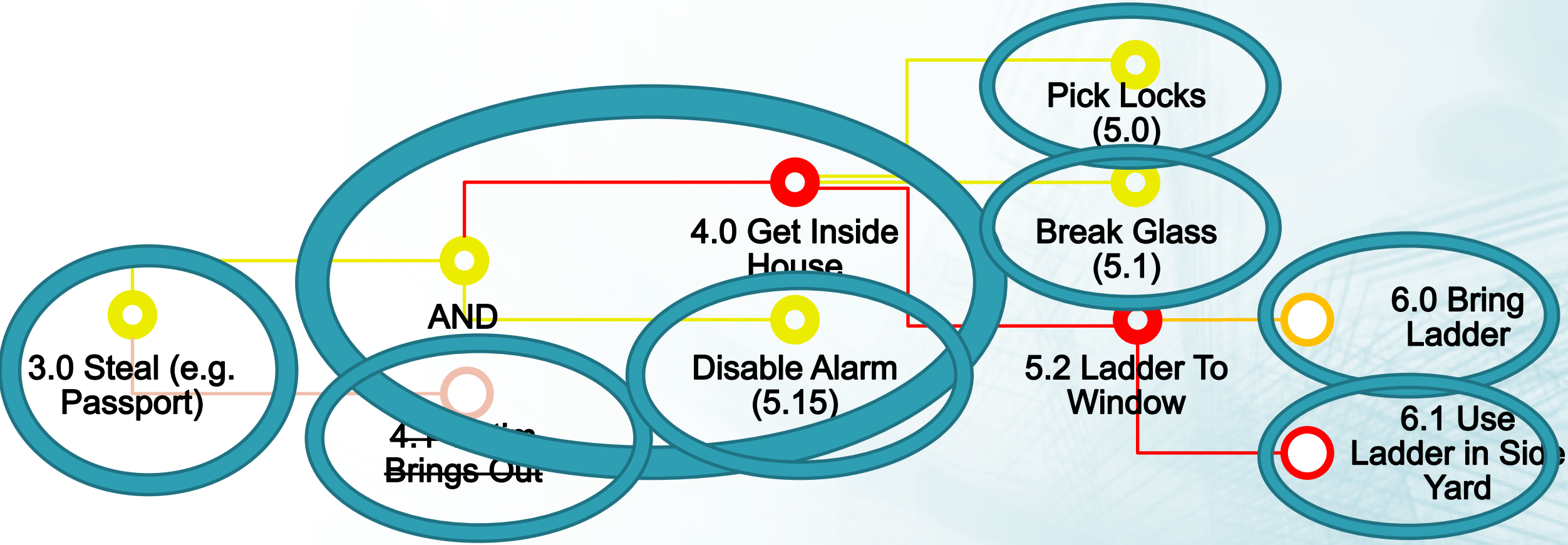
Attack Trees?

- A model of…
- the many ways to achieve a (nefarious) goal



GENIVI®

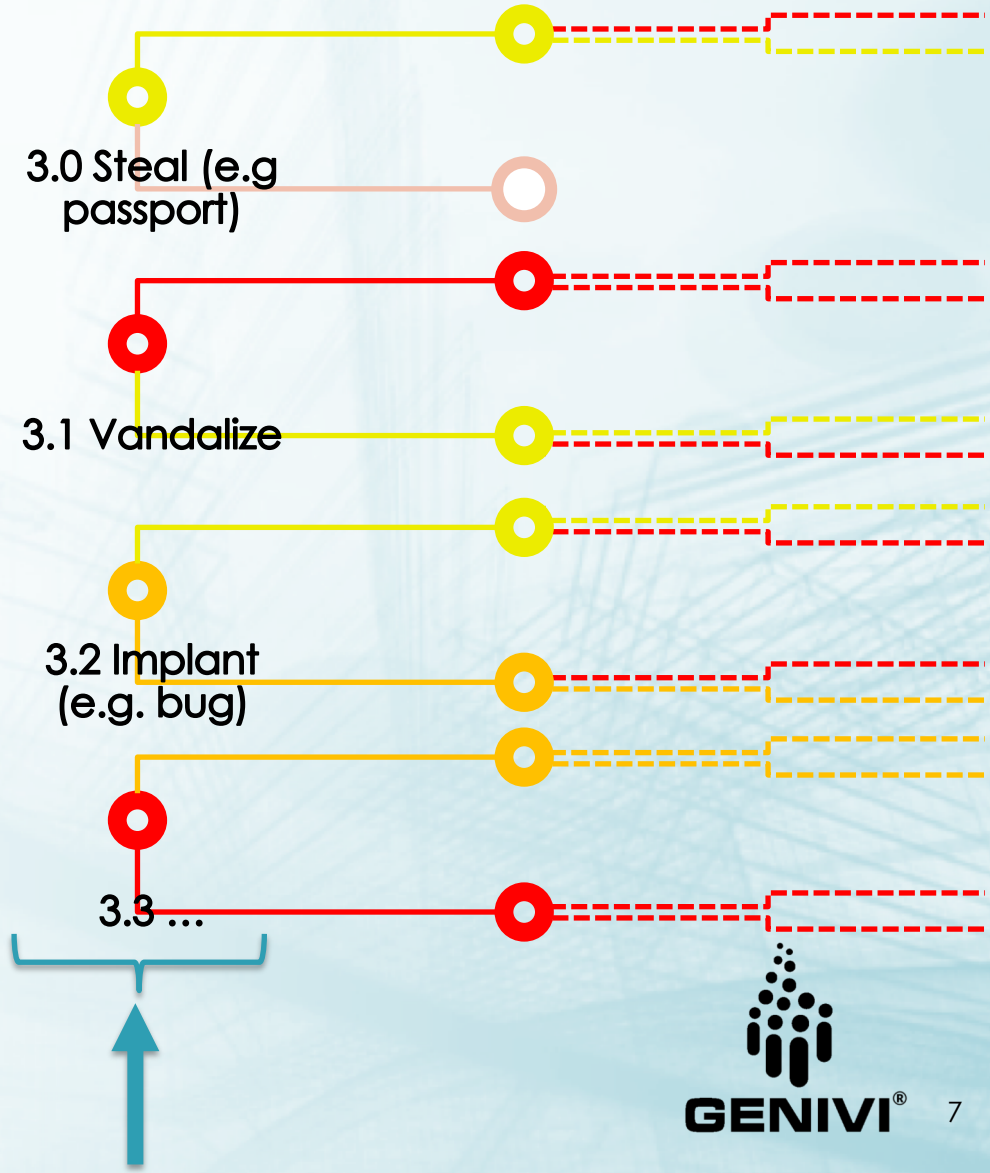
Anatomy of an Attack Tree



GENIVI®

Attacker Objectives are…

- Attacker Objectives have both:
  1. Clear Attacker Motivations
  2. Clear Impacts (Severities) on the Company / Org. / Stakeholders



To List Attacker Objectives…

Making a List: things an Attacker might like to do.

E.g. “Game Over”s or Attacker Money Makers

It helps to ask: ”What affects the bottom line?”

- E.g. Revenue Loss, IP Theft, Brand Damage …

Attack Trees: What Are They Good For?

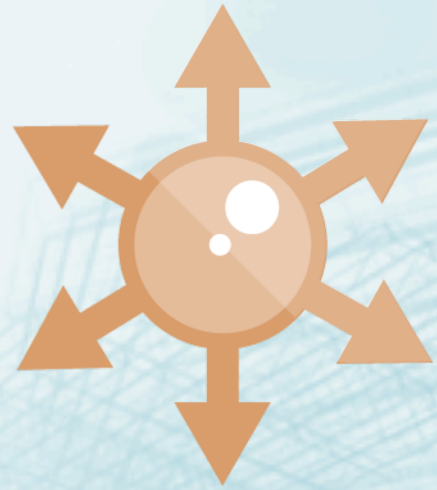
They are a Tool With Multiple Applications:

When Narrowly-Focused:

- Preparing Offensive Plans (pentesting)
- Considering Causes of Bugs
- Brainstorming Defenses

When Broadly-Focused:

- **Threat Assessments**



Threat Assessments

1. …(revealed later)
2. …(revealed later)
3. …(revealed later)
4. A list of mitigations

GENIVI®

Modeling Goal

- It's important to put it all in context…
- We model the attacker's available paths so that we can:
  - **Brainstorm / Be Exhaustive** – so we can try to think of all the things the ***the attackers*** will think of.
  - **Plan the Implementation (**of Mitigations) – so we can spend our development effort wisely. There will always be more *TODO* than *time to do it*.

GENIVI®

Modeling Principles

- So that we can **“Brainstorm / Be Exhaustive”**, we:
  - Include all attack ideas, but mark some things out of scope
  - Develop attack trees assuming no mitigations are present
  - Develop attack trees with **generalizations**

- So that we can **“Plan the Implementation (of Mitigations)”**, we:
  - Make **specific** mitigations (so the impact of each is modeled distinctly)

- So that we can **do both** (strike a balance), we:
  - Don’t generalize so much that we lose a distinct mitigation.

GENIVI®

Before you Start: Establish a Common Language

Create an ***Architecture Summary***

Do it from your (perhaps naïve) perspective

The result will

- highlight knowledge gaps and
- establish a vocabulary for the Attack Trees and Threat Assessment

Capture the data flows in the system

GENIVI®

Generating The Trees

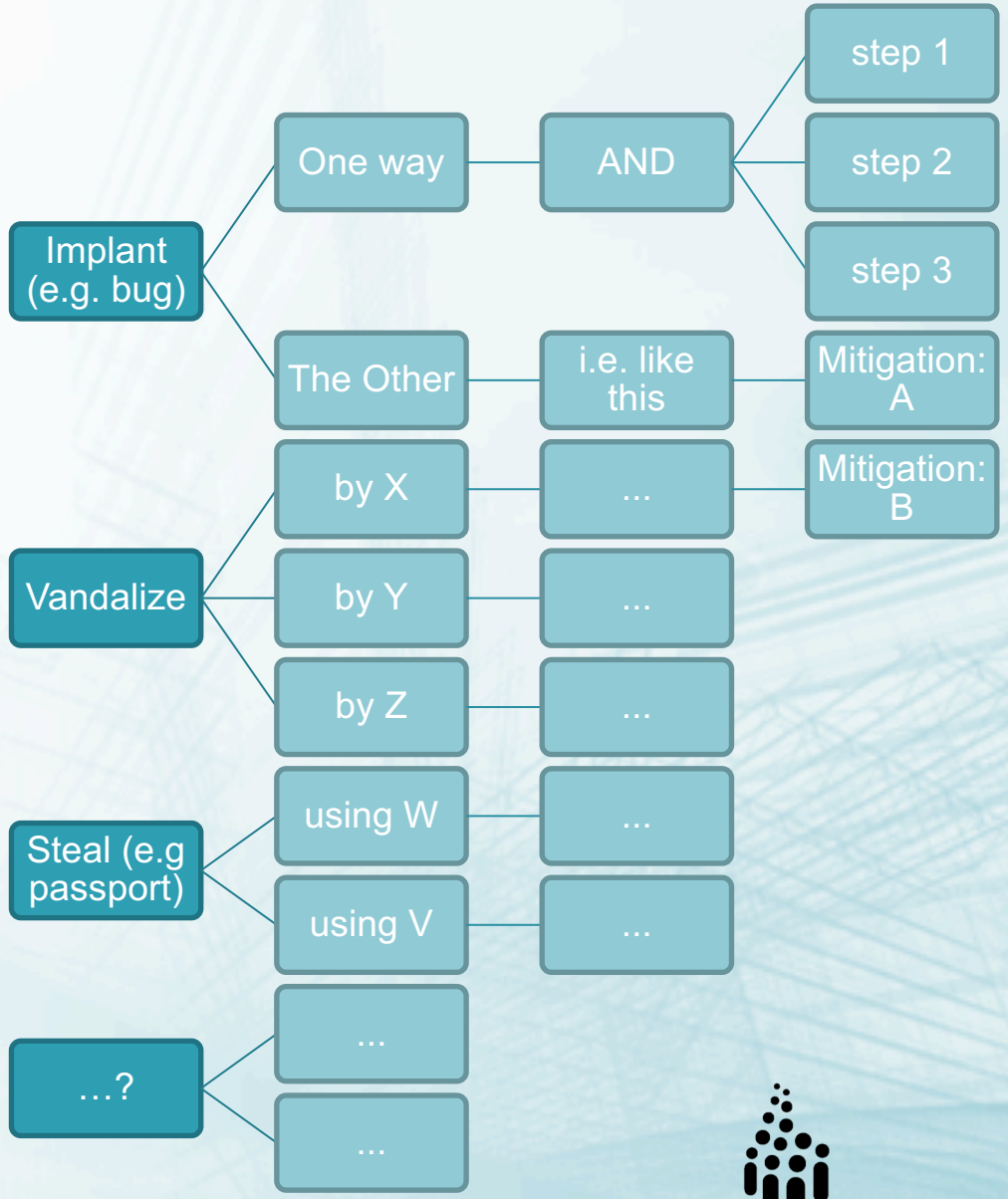
Do a Tree for Each Attacker Objective

Descend, descend, …

Worry about *what*, not *how*

- *Consult your data flows*

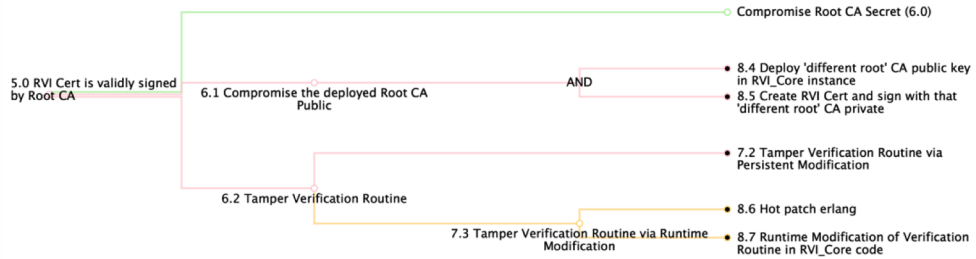
At the bottom: ascribe ‘likelihood’ and capture all mitigations



Using the Trees: Threat Assessments

1. **A summary of all attacker objectives**
2. **A detailed look at the attack vector nodes of the trees**
3. **An analysis of risk (of the attacker objectives)**
4. A ***prioritized*** list of mitigations

Subtree 5.0 RVI Cert is validly signed by Root CA



5.0 RVI Cert is validly signed by Root CA Attack Subtree

Attack Vector Node 8.4 Deploy 'different root' CA public key in RVI_Core instance

An attacker tampers with a deployed RVI_Core instance's resources where the public key of the root CA is stored. They replace this public key with their own so that they can spoof the authentication server. If they spoof the authentication server then they can generate their own credentials.

Mitigation Required

For Implementors of RVI

Credentials for RVI_Core need to be protected a rest and in memory against tampering (and replacement).

GENIVI®

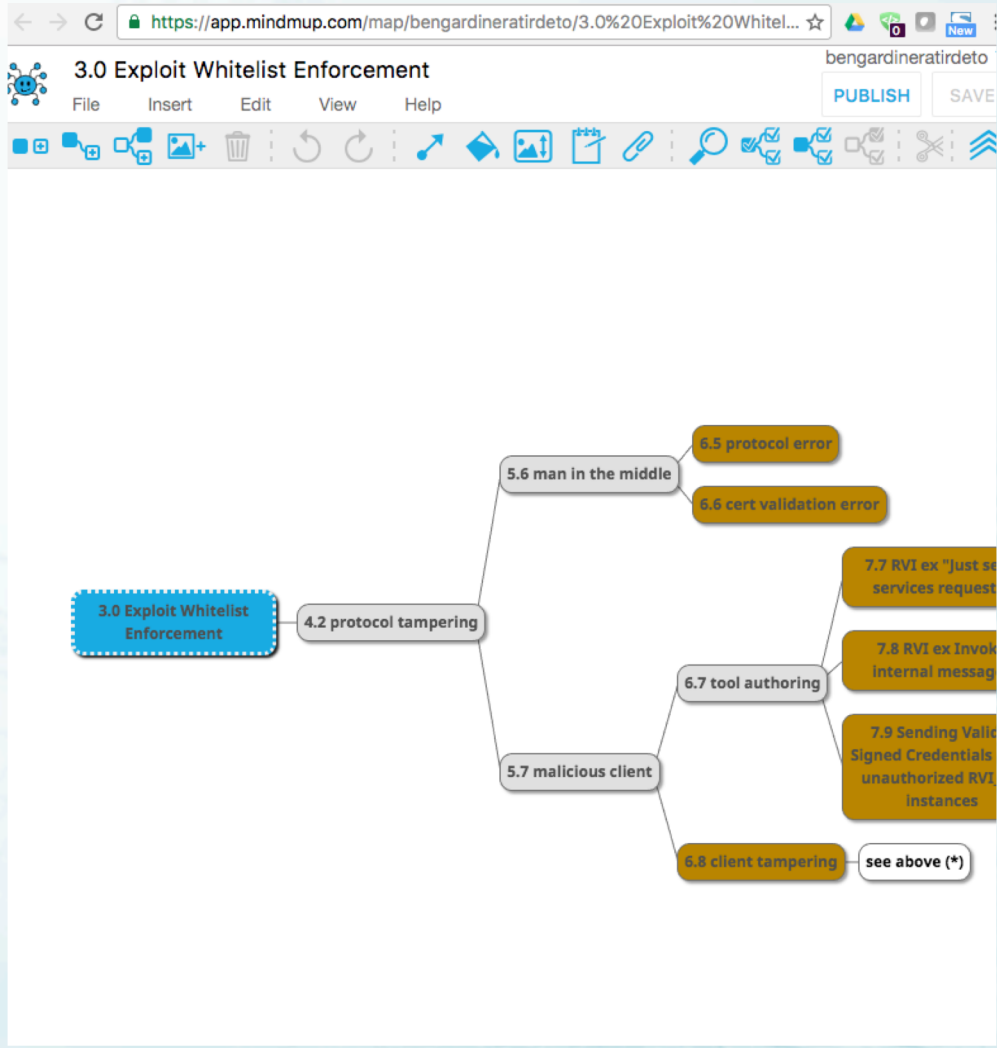
Tools For Attack Trees

$$

- Word Smart-Art
- Visio
- Omnigraffle
- Also purpose-built commercial products

Free

- Graphviz DOT
- Any indented text
- Mindmup (e.g. at right)



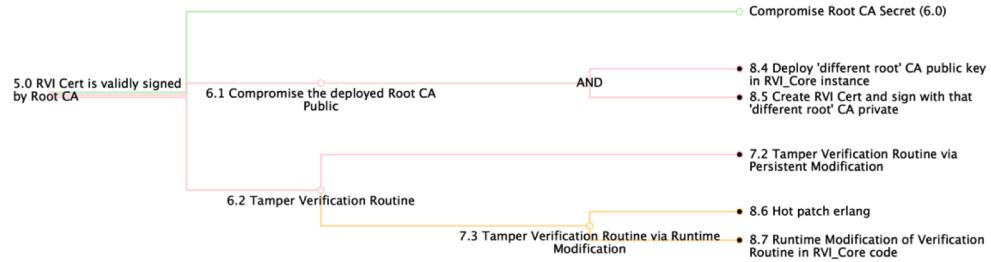
Tools For Threat Assessments

Any Attack Tree Tool and

A means to calculate risk and generate a report

- Purpose-built commercial tools
- Manual: Spreadsheets and Word Processing
- See also https://www.owasp.org/index.php/Application_Threat_Modeling
- https://github.com/BenGardiner/mindmup-as-attack-trees

Subtree 5.0 RVI Cert is validly signed by Root CA



5.0 RVI Cert is validly signed by Root CA Attack Subtree

Attack Vector Node 8.4 Deploy 'different root' CA public key in RVI_Core instance

An attacker tampers with a deployed RVI_Core instance's resources where the public key of the root CA is stored. They replace this public key with their own so that they can spoof the authentication server. If they spoof the authentication server then they can generate their own credentials.

Mitigation Required

For Implementors of RVI

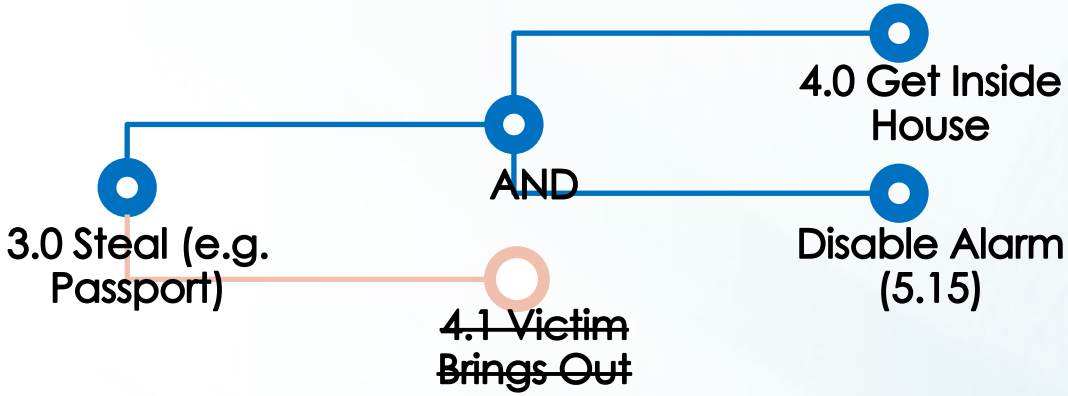
Credentials for RVI_Core need to be protected a rest and in memory against tampering (and replacement).

What To Expect

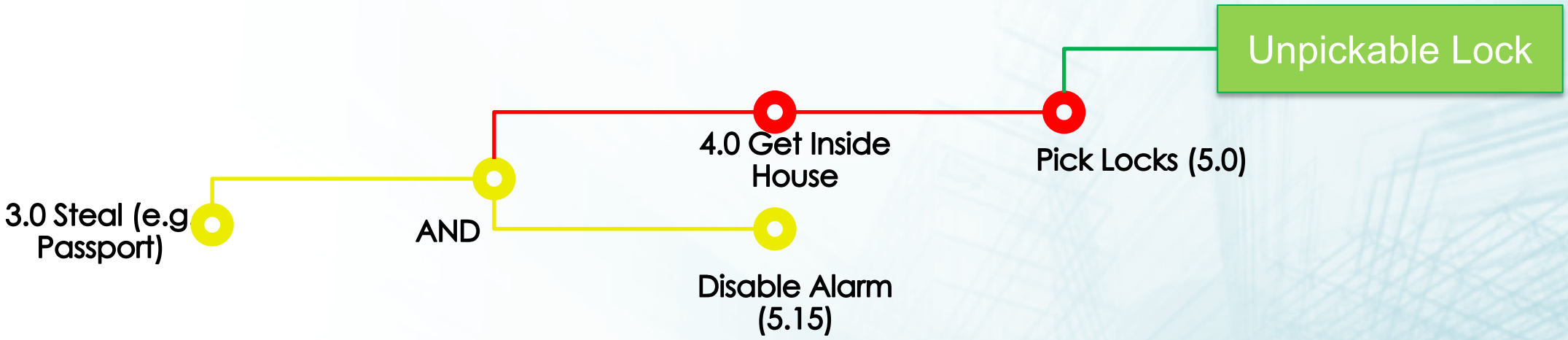
This is a different way of looking at the design for some people

GENIVI®

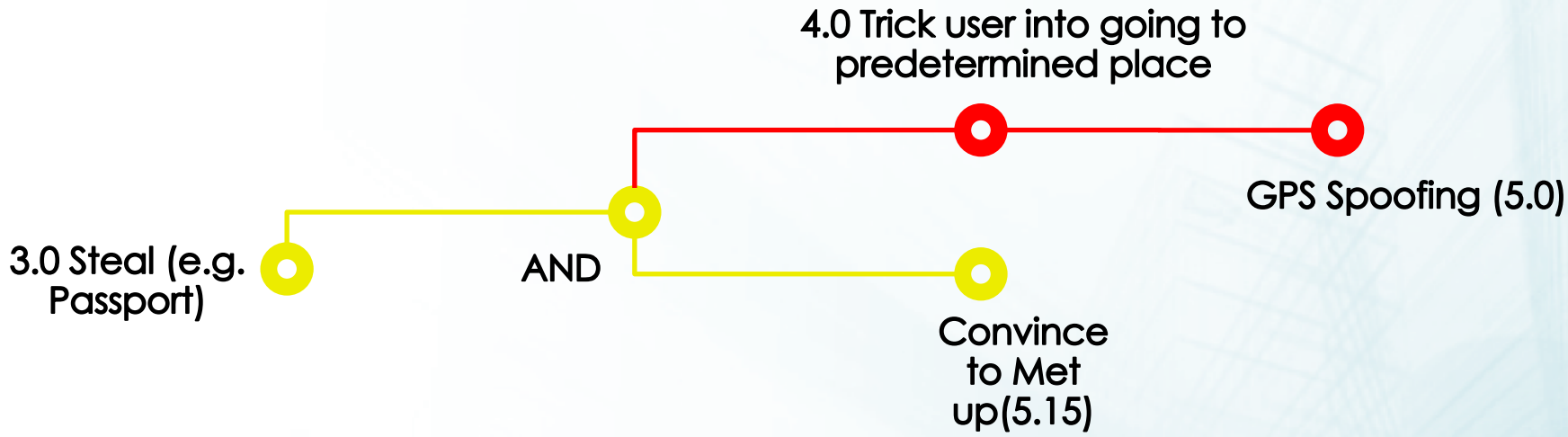
Overconfidence



Proving a Mitigation



Attack Vector Looking for an Objective



Terrifying Attack Tree

You Are the Subject Matter Experts

Your Domain-Specific knowledge is key

You know the data flow

GENIVI®

See? You CAN do this!

Threat Assessments up-front will save time

Threat Assessments up-front will target efforts

You are the SMEs. You can do this

Your Future:

- Releases with no re-designs
- Threat Assessments in the design phases

GENIVI®

Thank you!

Visit GENIVI at http://www.genivi.org or http://projects.genivi.org

Contact us: help@genivi.org

GENIVI®