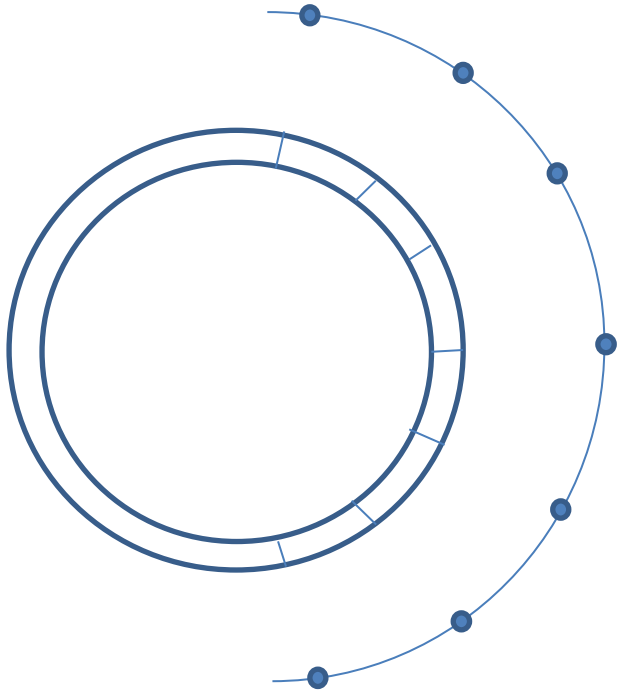
Attack Tree Analysis: Identifying and Ranking Cyberattack Paths

Martin Watford
Technical Consultant
isograph

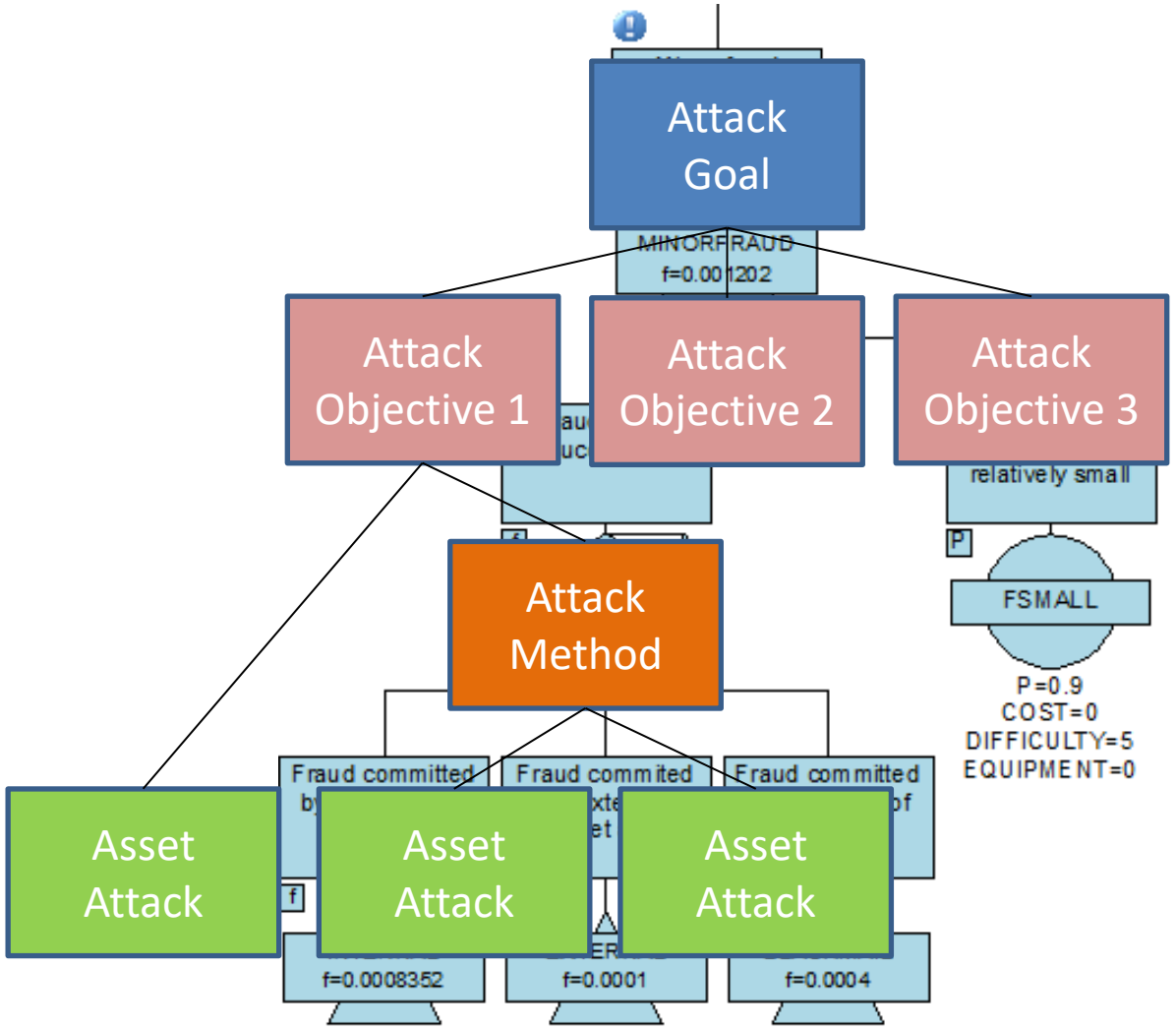
Agenda



1. Introduction
2. Construction
3. Events - Initiators and Enablers
4. Analysis Methods
5. Indicators and Likelihoods
6. Hypothetical Example
7. Conclusion

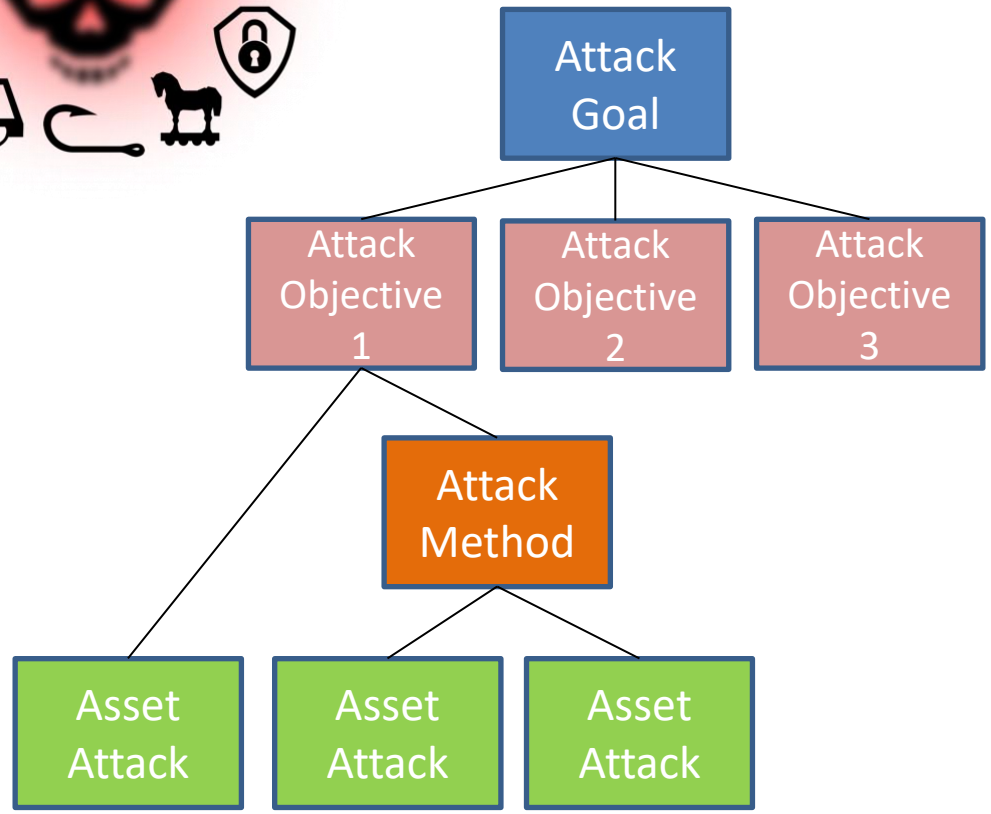
Introduction

- First described as ‘Threat Trees’
- Attack Tree Analysis (ATA)
  - Based on Fault Tree Analysis (FTA)
  - Determine paths and likelihood of attack
- Similarities to FTA
  - Logic gates and events
  - Qualitative and Quantitative analysis
- Differences to FTA
  - Consider obstacles to attack



Construction

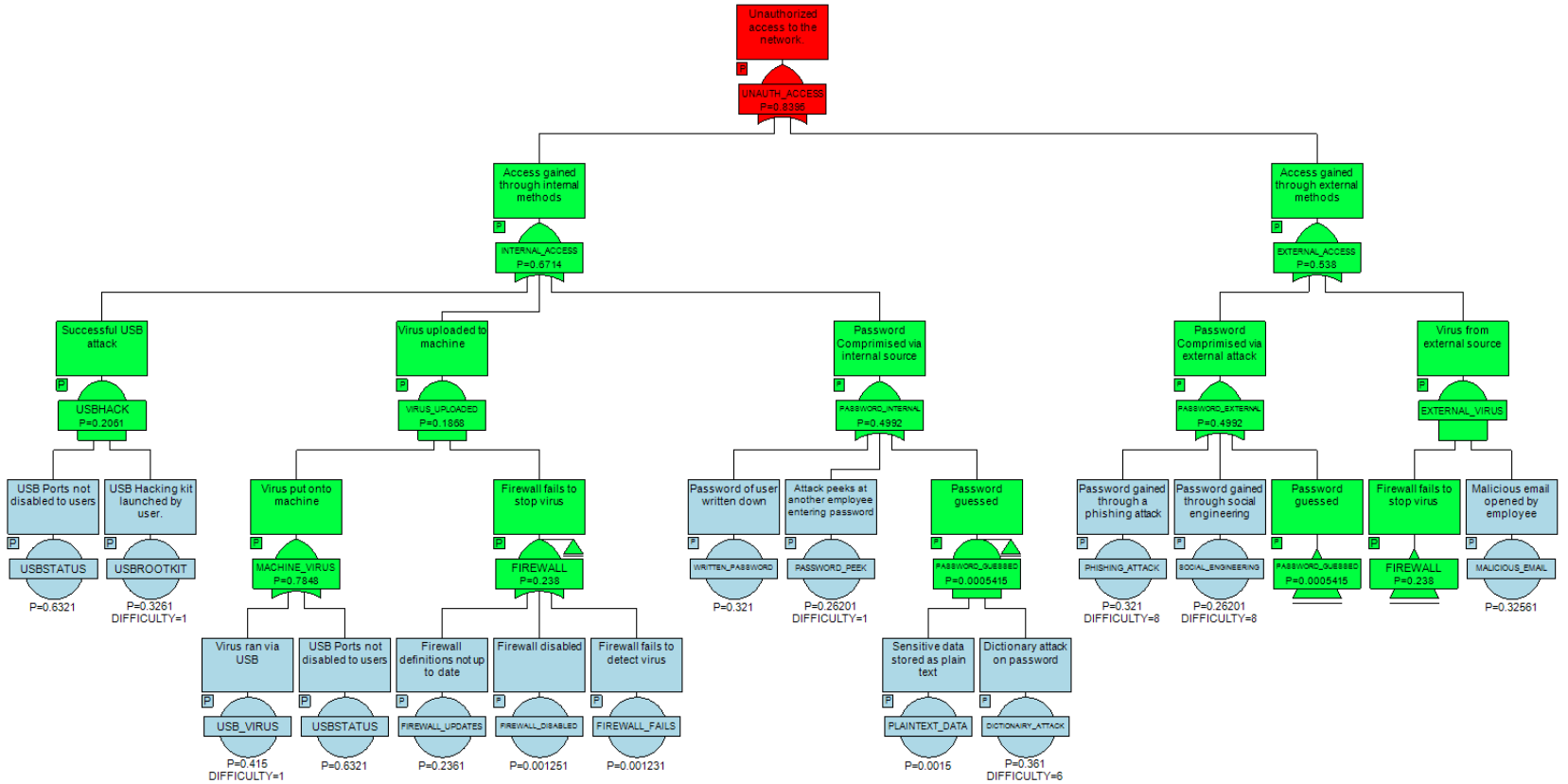
- Construct from POV of the attacker
- Identify goal (threat identification)
- Identify immediate objectives
- Continue through immediate levels of complexity
- Terminate with asset attacks and vulnerabilities
- Identify initiators and enablers



Construction…

Logic Gates:

- Represent interaction between events
  - OR
  - AND
  - VOTE m

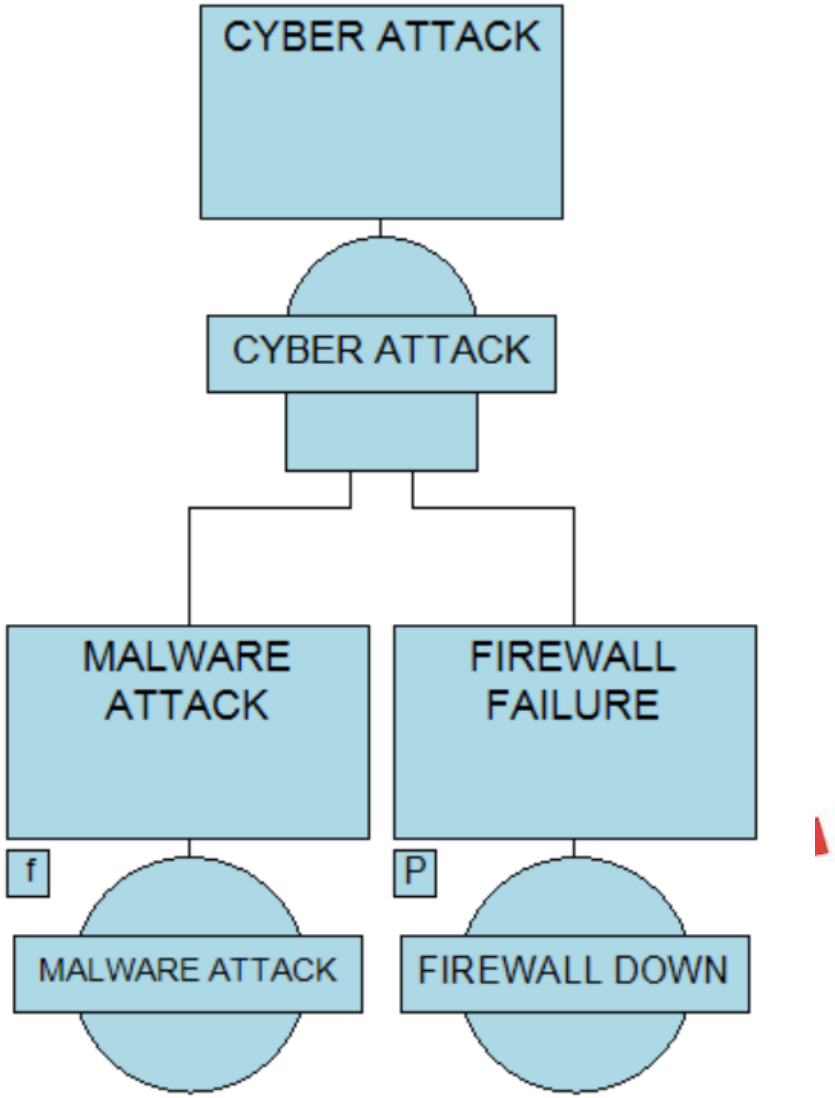


- TOP gate represents attacker(s) goal
- Logic gates key to qualitative analysis

Events

Initiator – event that triggers the hazardous situation (Frequency)

Enabler – event whose failure allows initiator to trigger hazard (Probability)

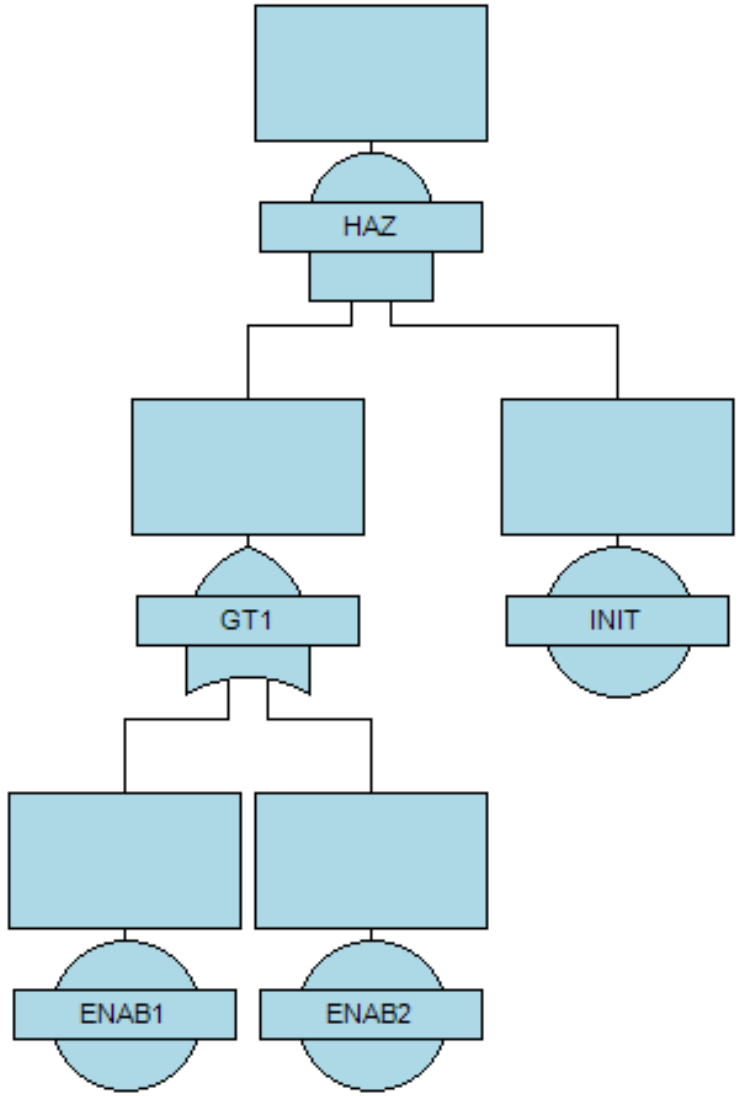


Qualitative Analysis

- Determine minimal cut sets
  - Potential paths of attack
  - Determined using Boolean algebra
  - One initiator per set

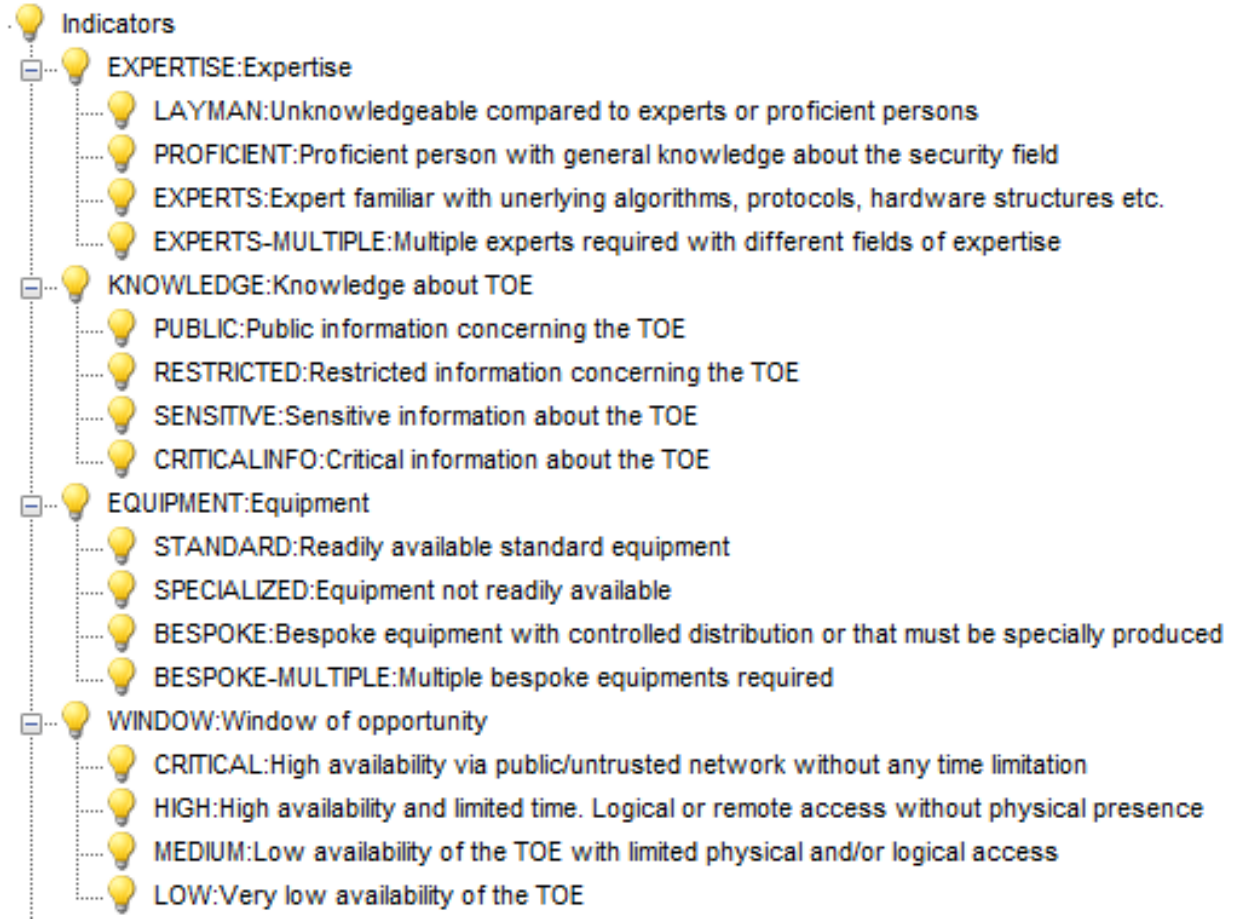
- Example:
  - HAZ = INIT (*AND*) GT1
  - GT1 = ENAB1 (*OR*) ENAB2
  - HAZ = INIT (*AND*) (ENAB1 (*OR*) ENAB2)
  - = INIT (*AND*) ENAB1 (*OR*) INIT (*AND*) ENAB2

- Quantitative Analysis possible



Indicators

- Allocated to events
- Represent obstacles to a successful attack
  - Each indicator has numerical value
- Must specify how indicator values are combined
  - Costs might be summed for AND logic, whereas lowest cost select for OR logic
- Indicator values of cut sets suggest which path of attack an attacker is most likely to select.



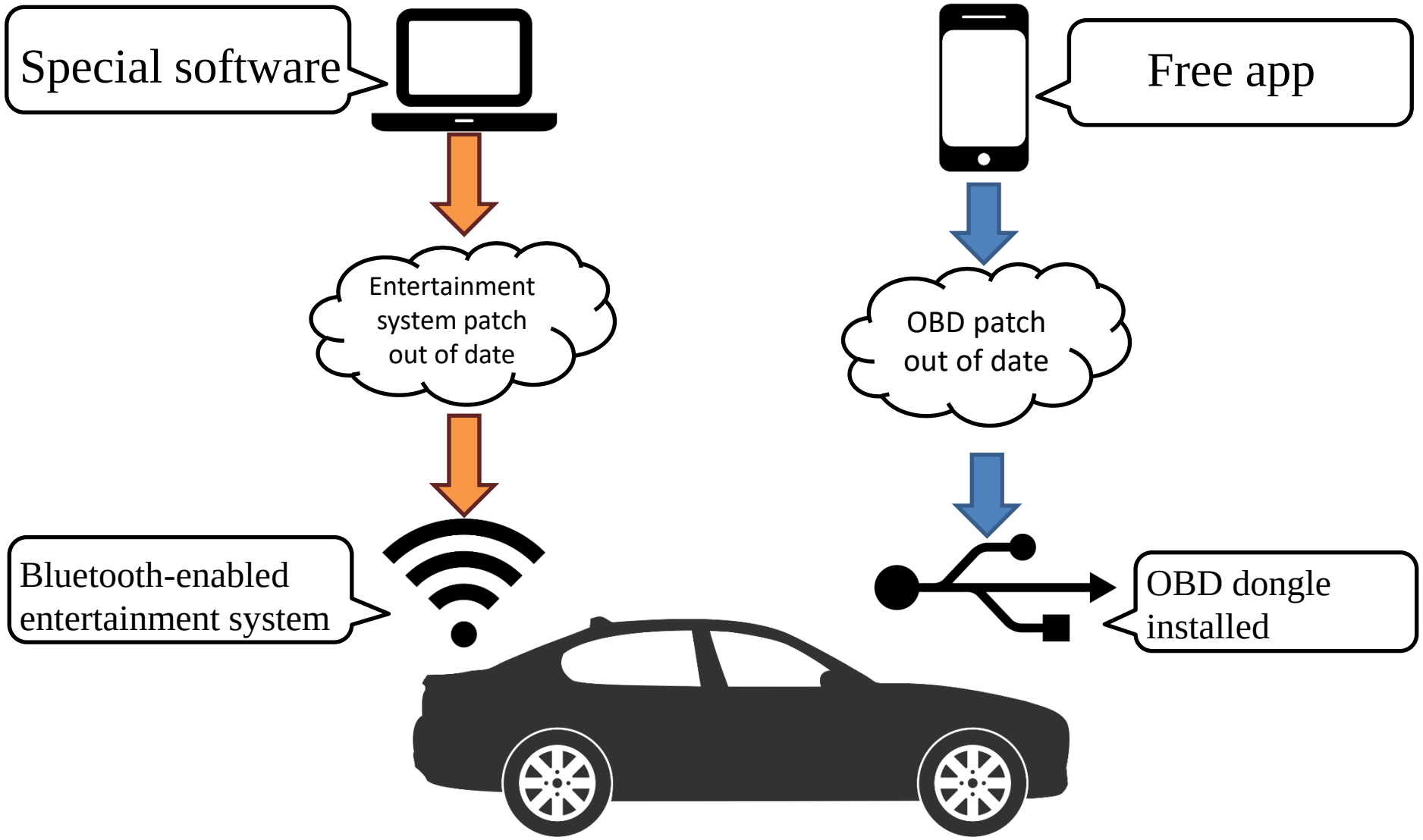
Likelihoods

- Allocated to primary events
  - Alternative to specifying Frequency and Probability values
- Represent user defined categories
  - E.g.: Low, High, Critical
- Indicator options may be used to determine likelihood
- Values determined by taking nearest likelihood to underlying frequency and probability
  - Uses median calculation

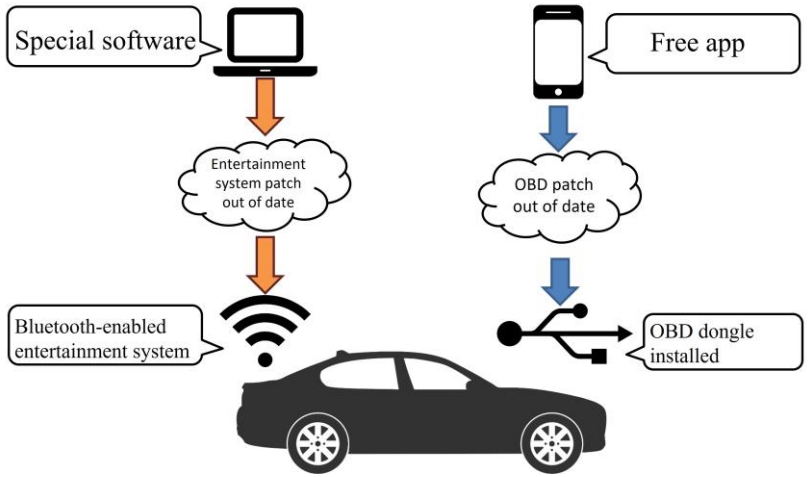
Consequences & Risks

- Consequences allocated to TOP event
  - Quantifies impact of successful attack
- Calculate numerical risk due to attack
  - Product of consequence weight and TOP gate probability/frequency
- Risk sensitivity calculated for each event
  - Indicates how risk might be most easily mitigated
  - Event with high sensitivity will give greater risk reduction if improved

Example


Special software
Free app
Entertainment system patch out of date
OBD patch out of date
Bluetooth-enabled entertainment system
OBD dongle installed

Example


Special software
Free app
Entertainment system patch out of date
OBD patch out of date
Bluetooth-enabled entertainment system
OBD dongle installed

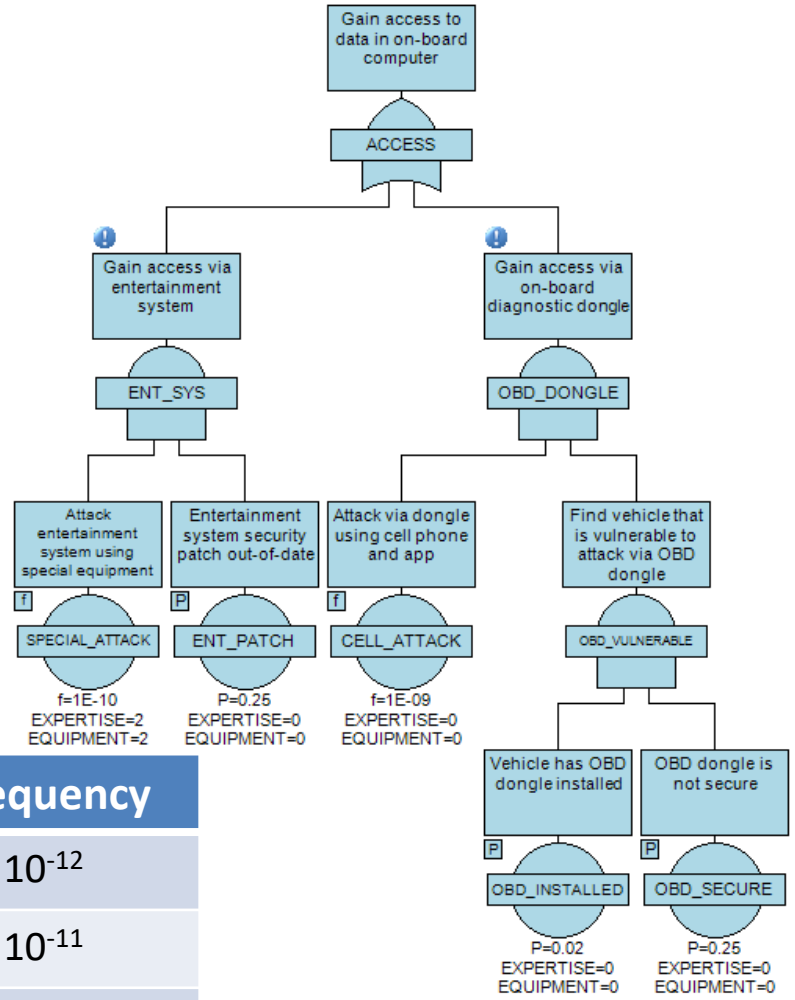
Example

- Basic event data.

Event	Initiator frequency	Enabler probability
SPECIAL_ATTACK	1×10^{-10}	
ENT_PATCH		0.25
CELL_ATTACK	1×10^{-7}	
OBD_INSTALLED		0.02
OBD_SECURE		0.25

- Event indicators.

Event	Expertise indicator	Equipment indicator
SPECIAL_ATTACK	EXPERTS (2)	BESPOKE (2)
CELL_ATTACK	LAYMAN (0)	STANDARD (0)



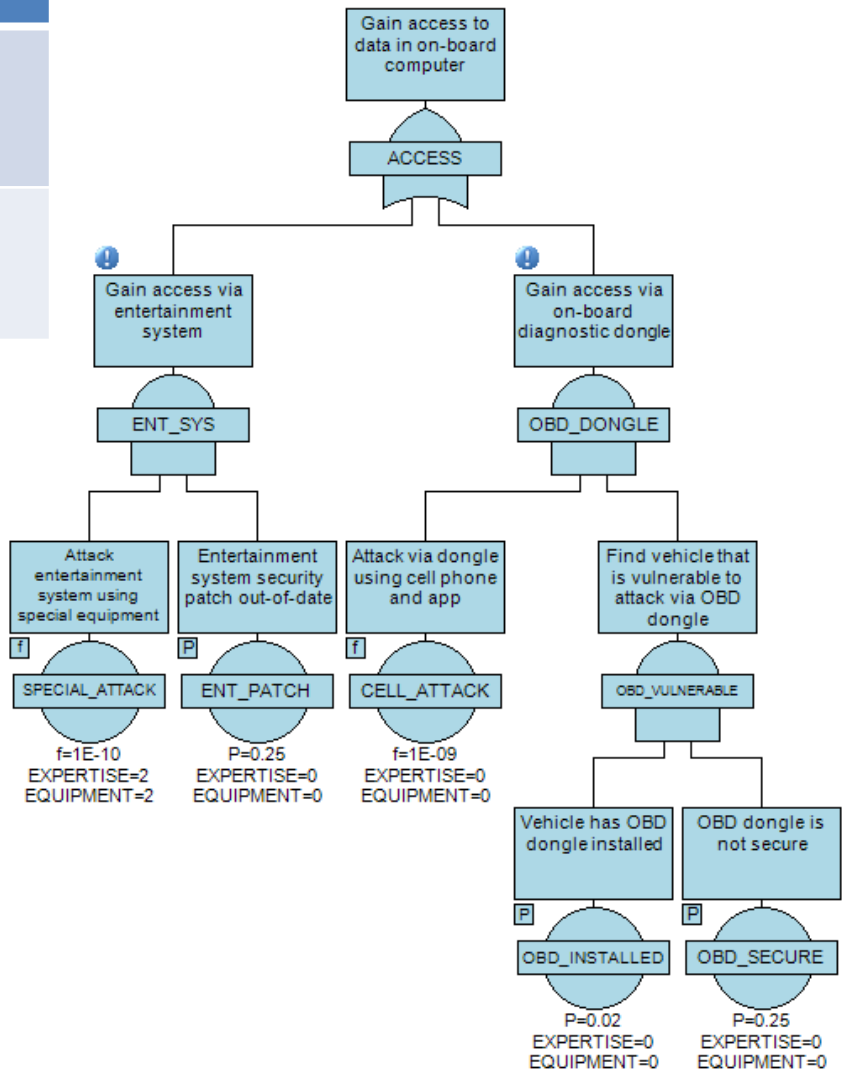
Likelihood	Level	Frequency
V. LOW	10	5×10^{-12}
LOW	5	1×10^{-11}
MED	3	1×10^{-10}
HIGH	1	1.1×10^{-9}
V. HIGH	0	1×10^{-9}

Example

Cut Set	Risk (hour^{-1})	Likelihood	Expertise	Equipment
CELL_ATTACK.OBD_INSTALLED.OBD_SECURE	5 x 10^{-10}	HIGH	0	0
SPECIAL_ATTACK.ENT_PATCH	2.5 x 10^{-11}	LOW	2	2

Likelihood	Level	Frequency
V. LOW	10	5 x 10^{-12}
LOW	5	1 x 10^{-11}
MED	3	1 x 10^{-10}
HIGH	1	1.1 x 10^{-9}
V. HIGH	0	1 x 10^{-7}

Event	Risk Sensitivity
ENT_PATCH	1 x 10^{-9}
OBD_INSTALLED	2.5 x 10^{-8}
OBD_SECURE	2 x 10^{-9}



Conclusion

- Attack Tree Analysis
  - Useful means to understand and model threats
  - Predict frequency and probability of successful attacks
  - Predict risk from attack and pinpoint weaknesses
  - Account for obstacles to attacker

References

- Amorso, E., 1994. Fundamentals of Computer Technology, *Prentice Hall;* US Ed.
- J3061™, 2016. Surface Vehicle Recommended Practice.
- Miller, C., and Vaselek, C., 2005. Remote Exploitation of an unaltered passenger vehicle. *In*: Black Hat USA 2015; Proc. Intern. Symp., Las Vegas, 1-6 Aug. 2015
- Foster, I., and Koscher, K. 2015. Exploring controller area networks, *In:* 24th Usenix Security Symposium; Proc. Intern. Symp., Washington D.C., 12-14 Aug. 2015

Thank You

Martin Watford
mwatford@isograph.com

isograph