From A to Z:
Developing a Visual Vocabulary for Information Security Threat Visualisation

Eric Li[1,2], Jeroen Barendse[1], Frederic Brodbeck[1], Axel Tanner[3]

[1] LUST, The Hague; [2] Princeton University; [3] IBM Research, Zurich

outline

- motivation and introduction
- a parameterised approach
- case study: TREsPASS
- case study: Verizon DBIR
- conclusions and future work

outline

- motivation and introduction
- a parameterised approach
- case study: TREsPASS
- case study: Verizon DBIR
- conclusions and future work

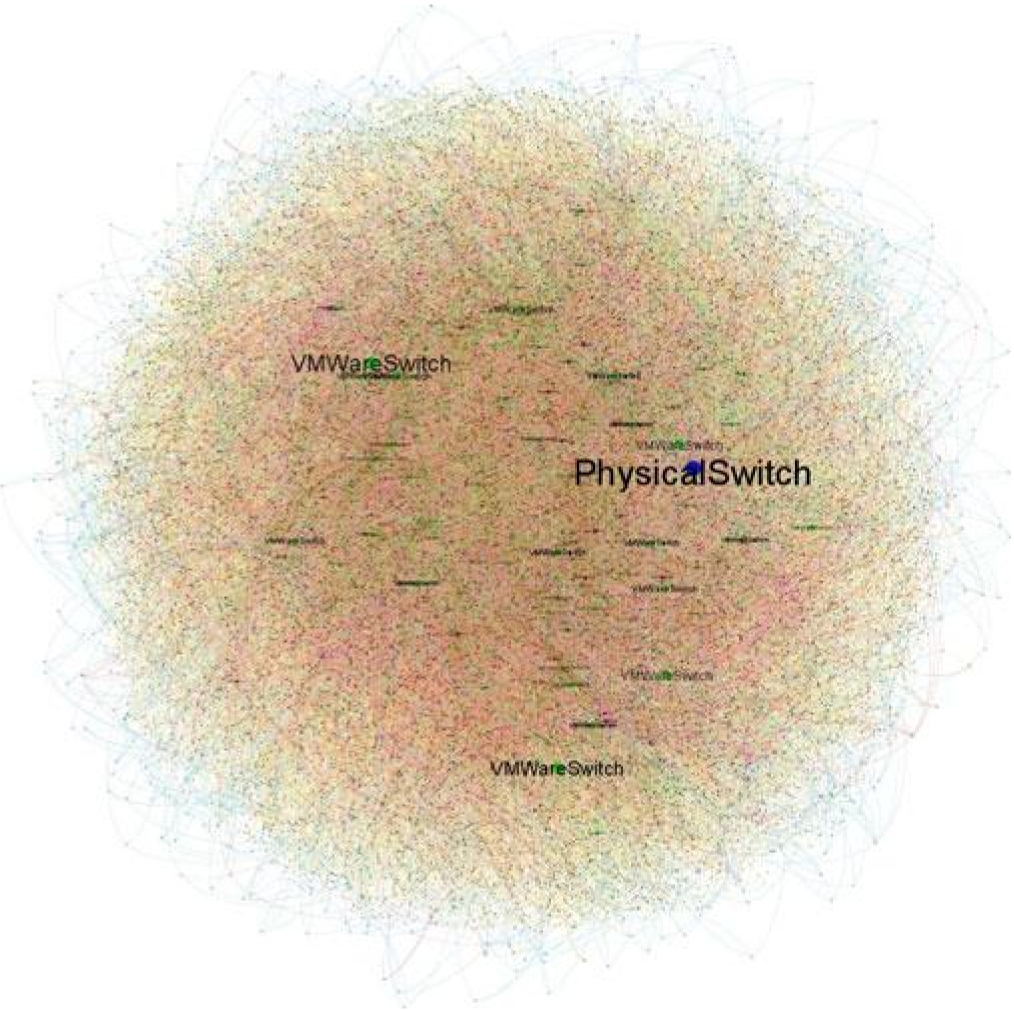
security visualization is hard

- data is complex
- vast amounts of information need to be made consumable
- have to be flexible (multiple audiences)
- there are no off-the-shelf solutions

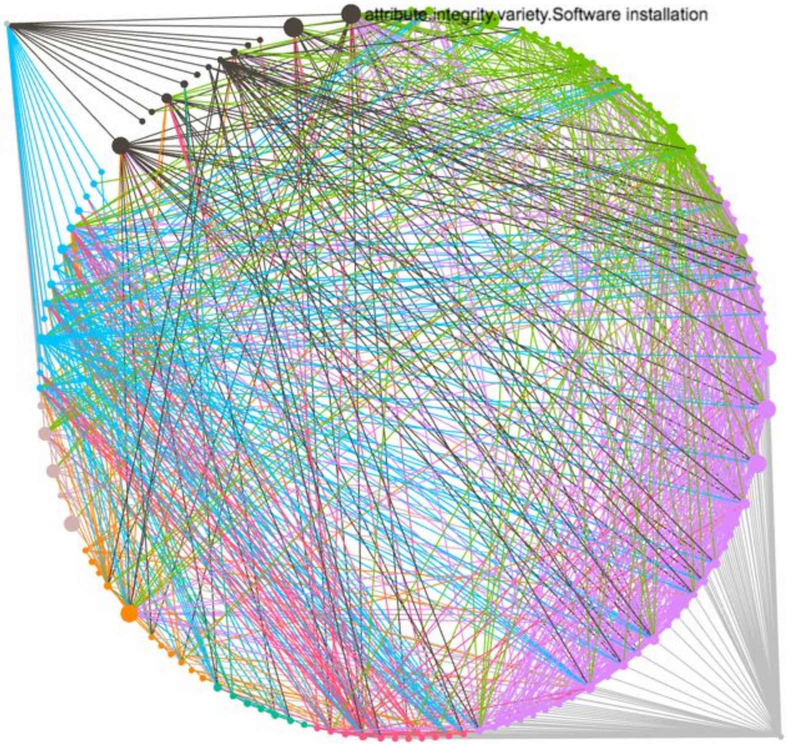
state of the art

- tends to be too complex
- … or over-simplified
- often purely functional
- missing a narrative / a context
- users needs to perform their own analysis, in order to draw meaningful conclusions

examples


VMWareSwitch
VMWareSwitch
PhysicalSwitch
VMWareSwitch
VMWareSwitch

examples



visualization goals

- not merely aesthetically pleasing
- aid users in forming a mental model
- provide the right level of abstraction
- while maintaining enough semantic detail
- bonus points: provide a narrative
  - aid decision-making
  - help getting actionable insights

visualization goals

- extend existing visualizations to support higher dimensionality
- flexible solutions that support individual aspects, as well as the model in its entirety

outline

- motivation and introduction
- a parameterised approach
- case study: TREsPASS
- case study: Verizon DBIR
- conclusions and future work

language as a metaphor

- alphabet → words → sentences

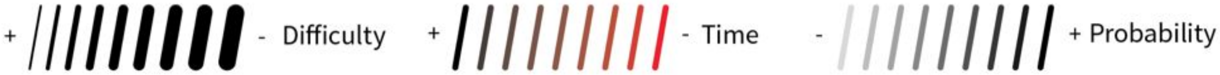
- the alphabet is a set of building blocks
  - to form words
- the richer the words, the more eloquent the sentences

the language of attack trees

alphabet	words	sentences
cost	nodes	paths
time	edges	tree
p		
...		

visual vocabulary and legend

- a set of symbols or graphics that function as building elements for larger visual entities
- map from security language to visual vocabulary



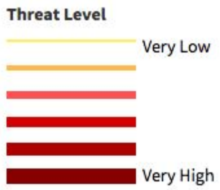
- important to consider which graphic elements to use and mapping (legend)

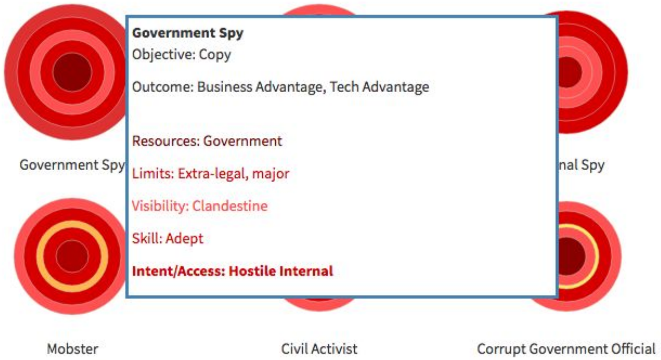
approaches

- stacking
- semantic zooming
- multiple views
- contextual awareness and highlighting

stacking

- # parameters > # visual variants
- find a visual element that can function as a generic
- use the same element for parameters and stack





Government Spy
Objective: Copy

Outcome: Business Advantage, Tech Advantage

Resources: Government

Limits: Extra-legal, major

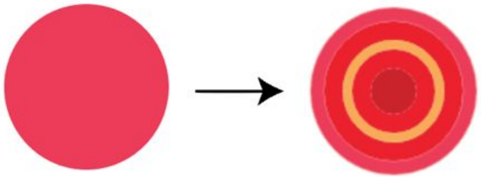
Visibility: Clandestine

Skill: Adept

Intent/Access: Hostile Internal

semantic zooming

- security visualisations can be complex
- some details may not be always necessary
- present semantically relevant details based on zoom



multiple views

- sometimes better to use multiple visualisations
- need to present multiple points of view
- tie things together to form bigger picture

contextual awareness and highlighting

- present details only when necessary
- prevents overwhelming viewers
- consider ways to highlight key points of vulnerability
- how to show results from analytical tools?
- consider how uncertainty should be highlighted
    - blurring
    - animation between multiple potential states

outline

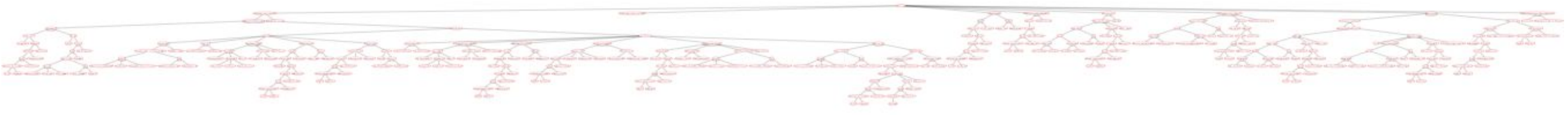
- motivation and introduction
- a parameterised approach
- case study: TREsPASS
- case study: Verizon DBIR
- conclusions and future work

predict
prioritise
prevent

TREsPASS

http://trespass-project.eu/

attack trees



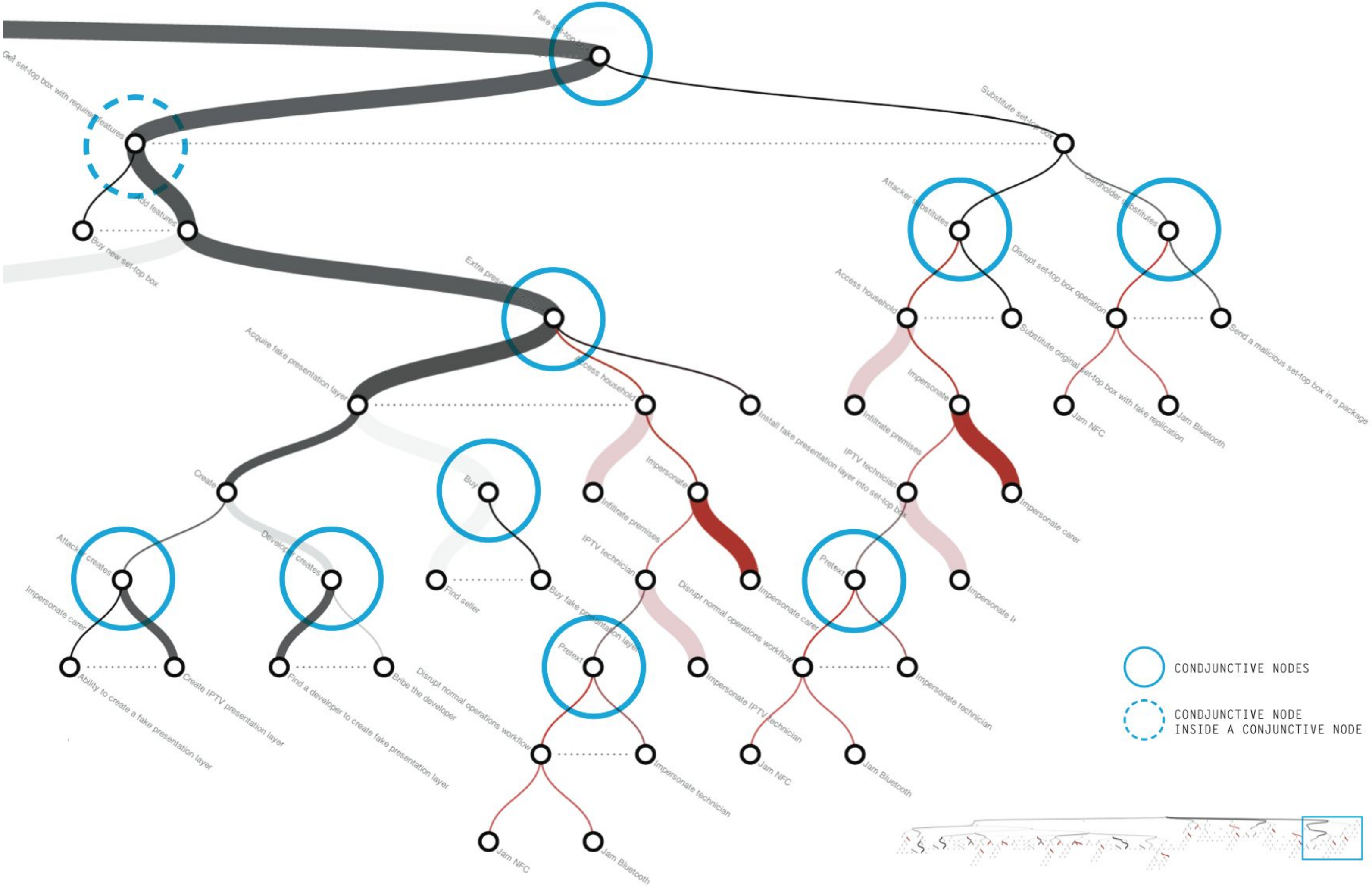
- problems:
  - tend to be very wide
  - can quickly become very complex
  - often repeat elements
  - conjunctive vs. disjunctive are heard to read

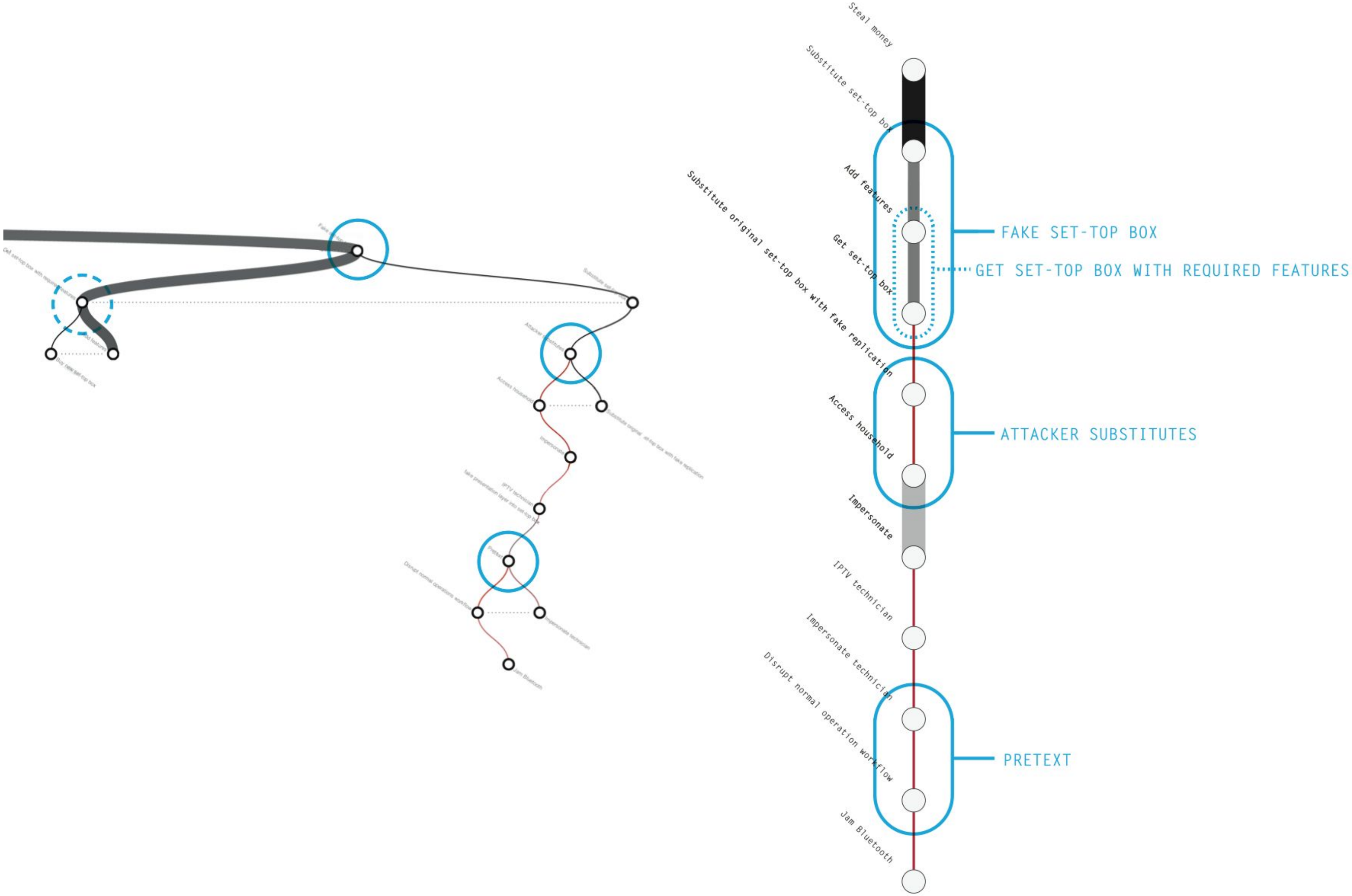
what we tried

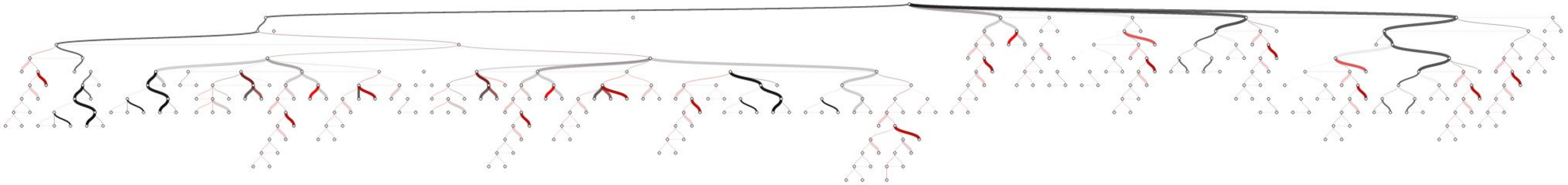
- alternative layout
- better labelling
- adding interactivity
- encoding parameters in edges
    - demo
- combining multiple views
    - demo

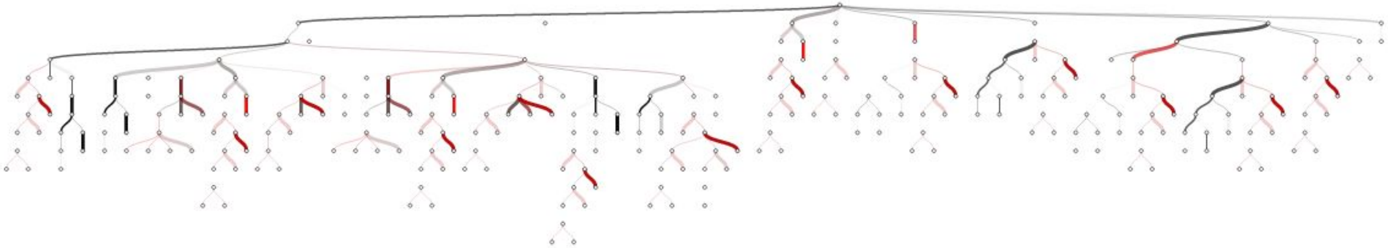
attack tree linearisation

- questioning the role of intermediate nodes
  - they are not actual steps, but make up a large part of the tree
  - mainly needed for calculations


Fake set-top box
Get set-top box with required features
Substitute set-top box
Add features
Buy new set-top box
Attacker substitutes
Cardholder substitutes
Extra presentation layer
Disrupt set-top box operation
Access household
Substitute original set-top box with fake replication
Send a malicious set-top box in a package
Acquire fake presentation layer
Access household
Install fake presentation layer into set-top box
Infiltrate premises
Impersonate
Jam NFC
Jam Bluetooth
IPTV technician
Impersonate carer
Create
Buy
Impersonate
Infiltrate premises
Attacker creates
Developer creates
IPTV technician
Disrupt normal operations workflow
Impersonate carer
Pretext
Impersonate I
Find seller
Buy fake presentation layer
Impersonate carer
Ability to create a fake presentation layer
Create IPTV presentation layer
Find a developer to create fake presentation layer
Bribe the developer
Disrupt normal operations workflow
Pretext
Impersonate IPTV technician
Impersonate technician
Impersonate technician
Jam NFC
Jam Bluetooth
Jam NFC
Jam Bluetooth
CONDJUNCTIVE NODES
CONDJUNCTIVE NODE
INSIDE A CONJUNCTIVE NODE

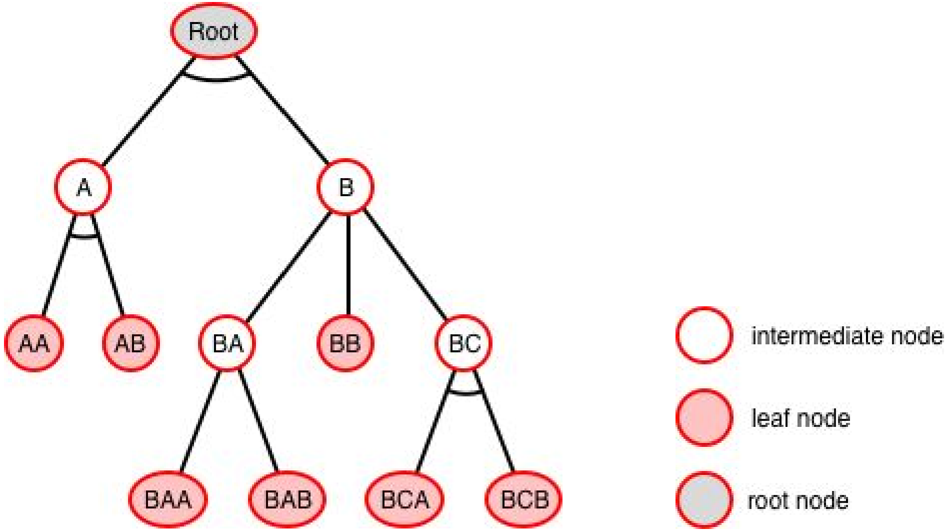

Fake set-top box
Get set-top box with required features
Add features
Buy new set-top box
Substitute set-top box
Attacker substitutes
Access household
Substitute original set-top box with fake replication
Impersonate
IPTV technician
fake presentation layer into set-top box
Pretext
Disrupt normal operations workflow
Impersonate technician
Jam Bluetooth
Steal money
Substitute set-top box
Add features
Get set-top box
Substitute original set-top box with fake replication
Access household
Impersonate
IPTV technician
Impersonate technician
Disrupt normal operation workflow
Jam Bluetooth
FAKE SET-TOP BOX
GET SET-TOP BOX WITH REQUIRED FEATURES
ATTACKER SUBSTITUTES
PRETEXT

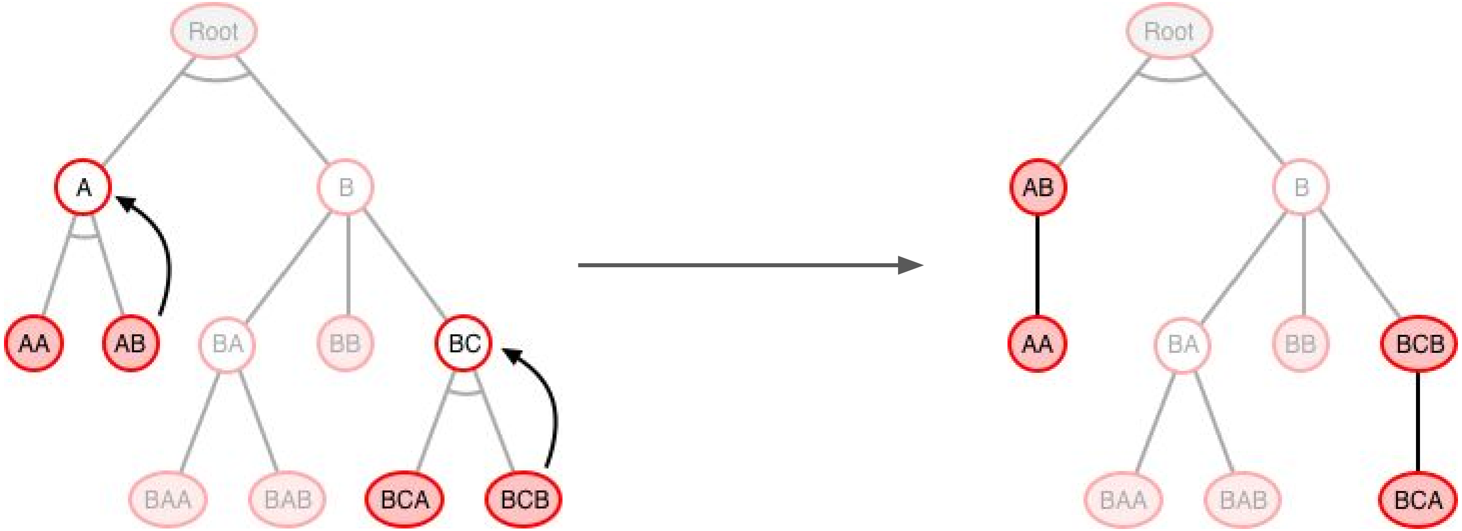


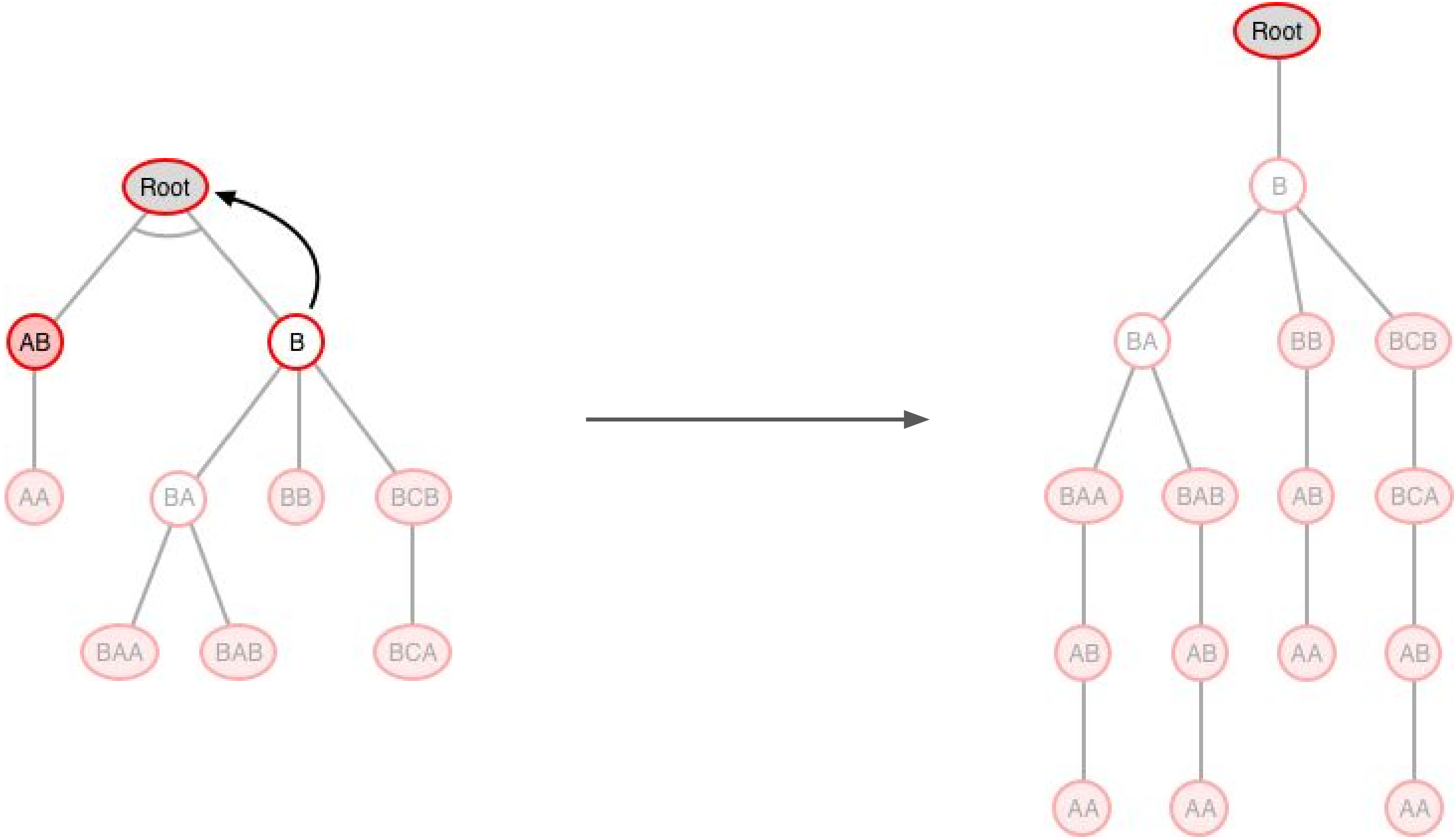


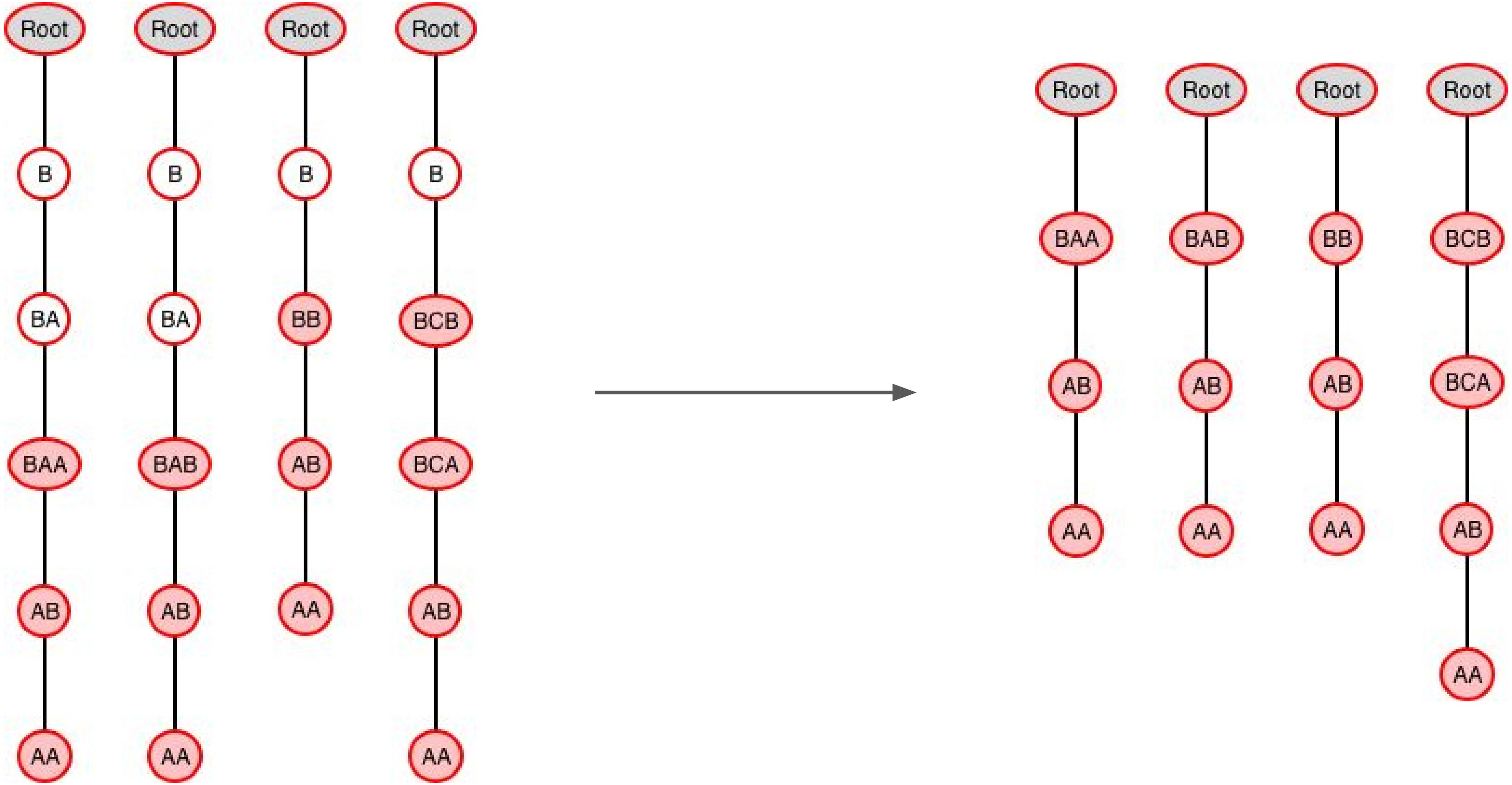
attack tree linearization

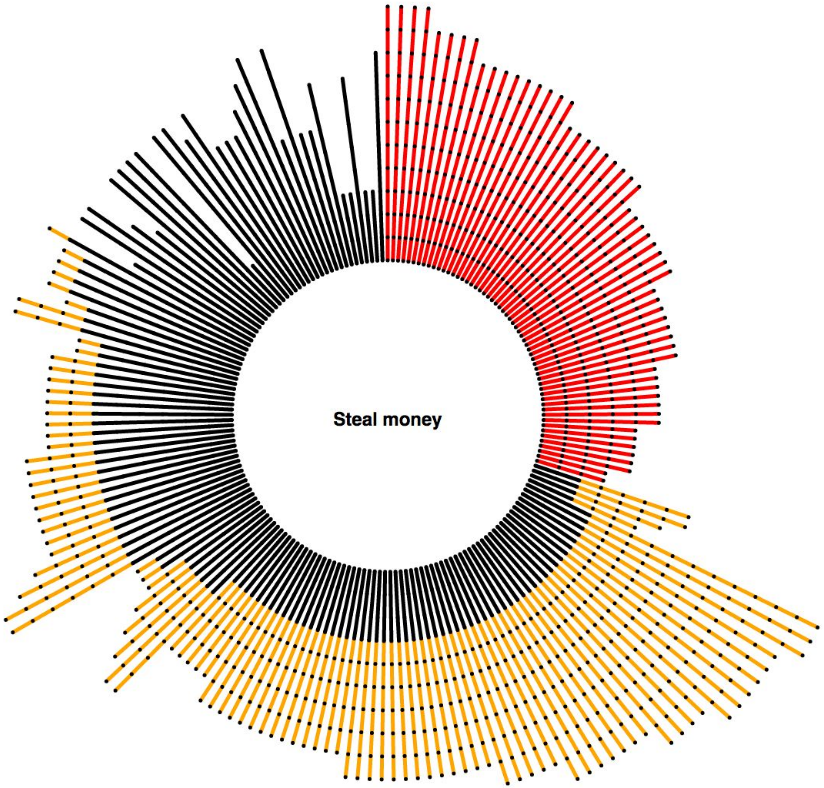
- simplifying the tree by removing conjunctive intermediate nodes
  - more, but smaller pieces
  - easier to follow and interpret

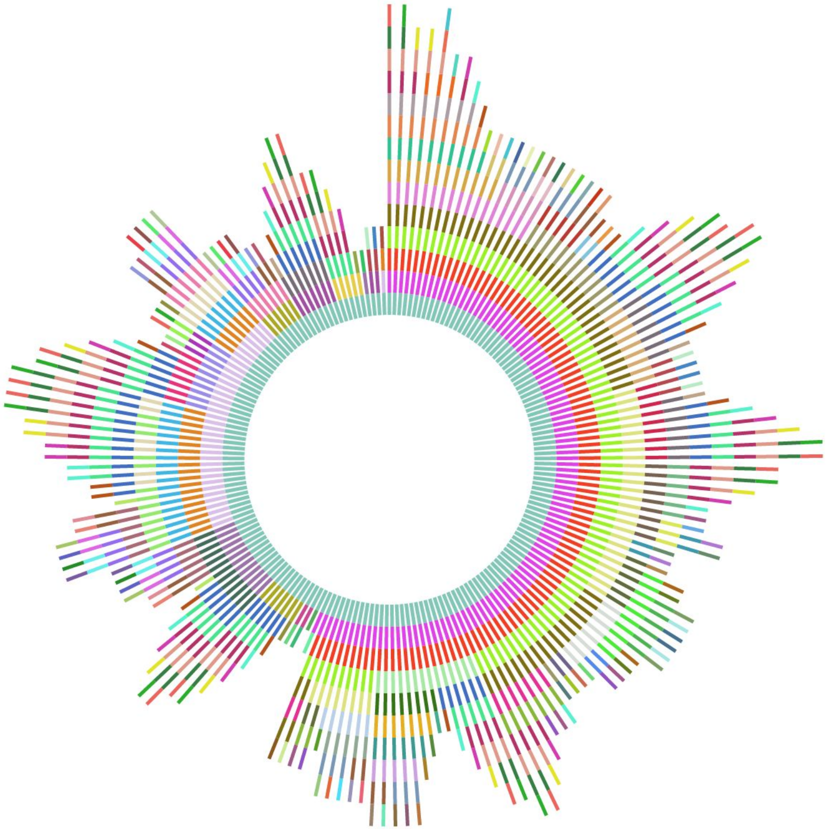

Root
A
B
AA
AB
BA
BB
BC
BAA
BAB
BCA
BCB
intermediate node
leaf node
root node


Root
A
B
AA
AB
BA
BB
BC
BAA
BAB
BCA
BCB
Root
AB
B
AA
BA
BB
BCB
BAA
BAB
BCA


Root
AB
B
AA
BA
BB
BCB
BAA
BAB
BCA
Root
B
BA
BB
BCB
BAA
BAB
AB
BCA
AB
AB
AA
AB
AA
AA
AA


Root
B
BA
BAA
AB
AA
Root
B
BA
BAB
AB
AA
Root
B
BB
AB
AA
Root
B
BCB
BCA
AB
AA
Root
BAA
AB
AA
Root
BAB
AB
AA
Root
BB
AB
AA
Root
BCB
BCA
AB
AA


Steal money



outline

- motivation and introduction
- a parameterised approach
- case study: TREsPASS
- **case study: Verizon DBIR**
- conclusions and future work

verizon✓

Verizon Data Breach Investigations Report 2016

attack graphs

- problems:
    - tend to be difficult to follow
    - gets complex and unreadable very quickly
    - unclear useage

what we tried

- goals
    - displaying/differentiating actions and attributes
    - indication of relative threat levels
    - showing potential attack paths
    - comparing mitigations and datasets

what we tried

- approaches
  - arc diagram (Wattenberg, 2002)
  - encoding meaning into nodes and edges
  - multiple views
  - contextual awareness
  - semantic zooming

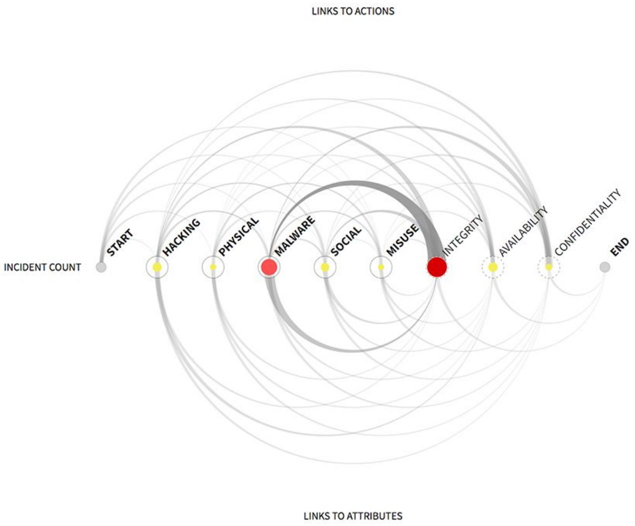
○ **ACTIONS**

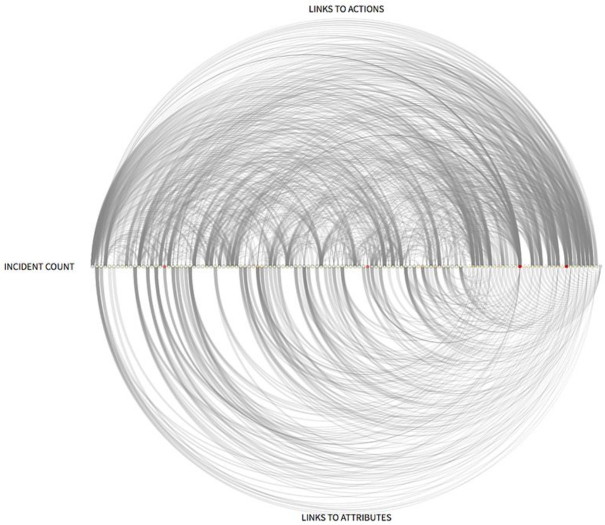
◌ ATTRIBUTES

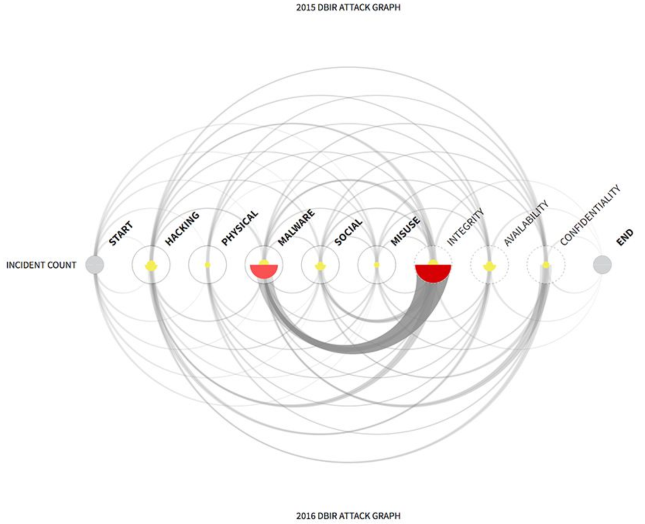
FREQUENCY IN INCIDENTS

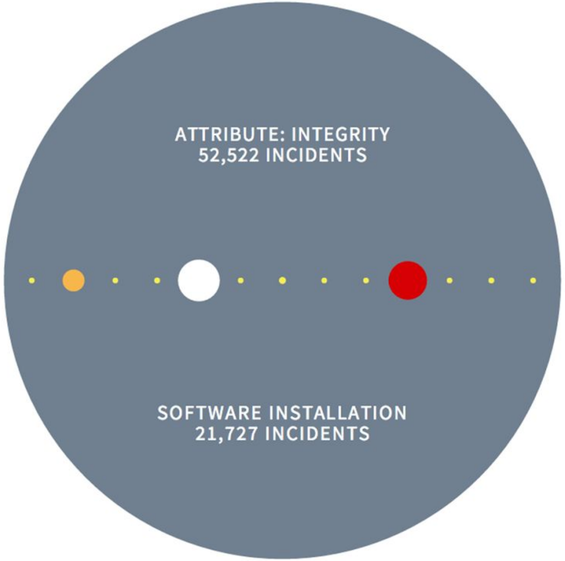
LOW **HIGH**

• ● ⬤ ⬤


LINKS TO ACTIONS
INCIDENT COUNT
START
HACKING
PHYSICAL
MALWARE
SOCIAL
MISUSE
INTEGRITY
AVAILABILITY
CONFIDENTIALITY
END
LINKS TO ATTRIBUTES

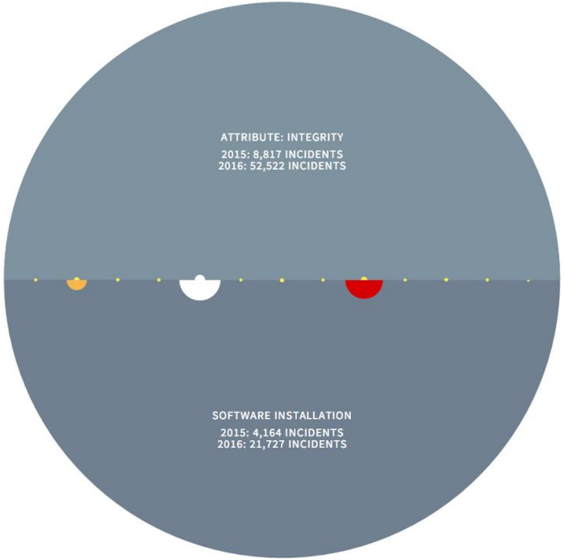

LINKS TO ACTIONS
INCIDENT COUNT
LINKS TO ATTRIBUTES


2015 DBIR ATTACK GRAPH
INCIDENT COUNT
START
HACKING
PHYSICAL
MALWARE
SOCIAL
MISUSE
INTEGRITY
AVAILABILITY
CONFIDENTIALITY
END
2016 DBIR ATTACK GRAPH



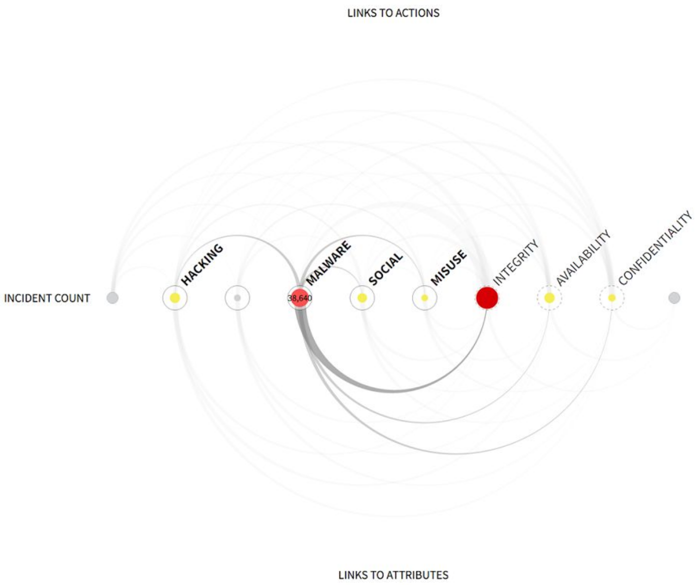
ATTRIBUTE: INTEGRITY
52,522 INCIDENTS

SOFTWARE INSTALLATION
21,727 INCIDENTS



ATTRIBUTE: INTEGRITY
2015: 8,817 INCIDENTS
2016: 52,522 INCIDENTS

SOFTWARE INSTALLATION
2015: 4,164 INCIDENTS
2016: 21,727 INCIDENTS



verizon 2016 dbir

demo

outline

- motivation and introduction
- a parameterised approach
- case study: TREsPASS
- case study: Verizon DBIR
- conclusions and future work

final thoughts and future work

- security visualisation is hard
  - Complex, multi-dimensional, wide ranging
- new tools in visualisation require us to rethink what is effective and useful to viewers
- by beginning from the most atomic elements, we can build rich and dynamic visualisations
- continued explorations in visualising attack trees

references

- The TREsPASS Project: Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security, www. trespass-project.eu
- Alberts, C.J., Dorofee, A.: Managing Information Security Risks: The Octave Approach. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA (2002)
- Barber, B., Davey, J.: The use of the ccta risk analysis and management methodology cramm in health information systems. Medinfo 92, 1589–1593 (1992)
- Barendse, J., Bleikertz, S., Brodbeck, F., Coles-Kemp, L., Heath, C., Hall, P., Kordy, B., Tanner, A.: TREsPASS Deliverable 4.1.1: Initial requirements for visualisation processes and tools
- Bassett, G., Solutions, V.E.: Dbir attack graph analysis (June 2015), http://dbirattack-graph.infos.ec/
- Bertin, J.: S´emiologie Graphique. Gauthier-Villars, Paris (1967)
- Harris, R.L.: Information Graphics: A Comprehensive Illustrated Reference. Oxford University Press, Inc., New York, NY, USA (1999)
- Kirk, A.: References for visualising uncertainty (February 2015), http://www.visualisingdata.com/2015/02/references-visualising-uncertainty/
- Koffka, K.: Principles of gestalt psychology. International library of psychology, philosophy, and scientific method
- Koffka, K.: Perception: An introduction to the gestalt-theorie. Psychological Bulletin 19(10), 531–585 (1922)
- Schneier, B.: Attack Trees: Modeling Security Threats. Dr. Dobb's Journal of Software Tools 24(12), 21–29 (1999), https://www. schneier.com/cryptography/archives/1999/12/attack trees.html
- Solutions, V.E.: 2016 data breach investigations report. Tech. rep., Verizon
- Ware, C.: Information Visualization: Perception for Design. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA (2000)
- Wattenberg, M.: Arc diagrams: Visualizing structure in strings. In: Information Visualization, 2002. INFOVIS 2002. IEEE Symposium on. pp. 110–116. IEEE (2002)