Characteristic-Based Security Analysis of Personal Networks

Andrew Paverd Department of Computer Science
University of Oxford

Fadi El-Moussa BT Research
BT Technology, Service & Operations

Ian Brown Oxford Internet Institute
University of Oxford

https://www.cs.ox.ac.uk/people/andrew.paverd/home

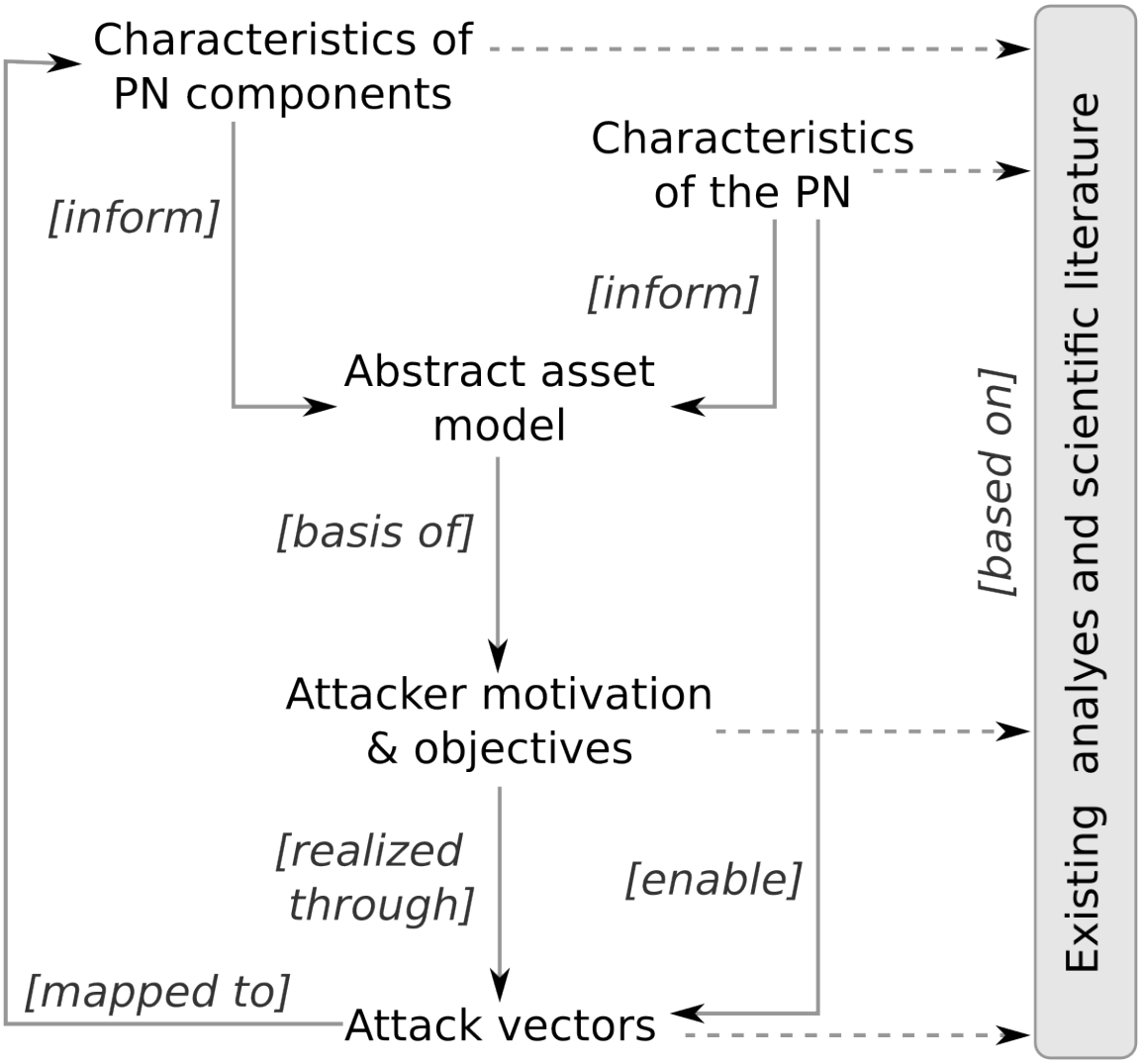
Home Network Security

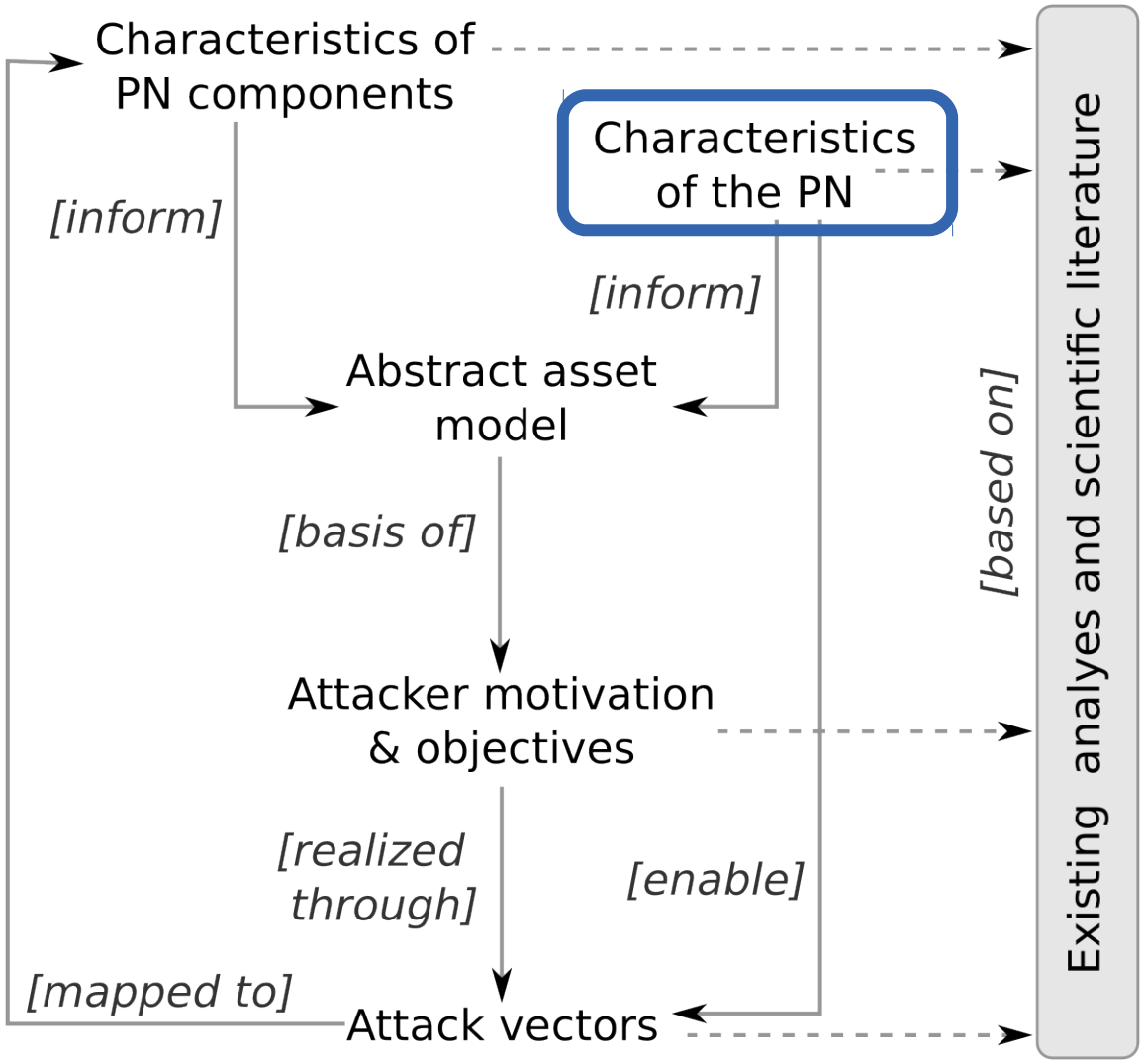
- Limitations of previous analyses
  - geographically-defined networks
  - category-based approaches
- Focus on Personal Network (PN)
  - home network + PAN + VAN + cloud
  - more representative of current systems
  - captures emergent characteristics
- Characteristic-based approach
  - maps device characteristics to attack vectors
  - more descriptive than category-based approaches
  - can adapt as technology changes

The Personal Network

- Limitations of previous analyses
  - geographically-defined networks
  - category-based approaches
- Focus on Personal Network (PN)
  - home network + PAN + VAN + cloud
  - more representative of current systems
  - captures emergent characteristics
- Characteristic-based approach
  - maps device characteristics to attack vectors
  - more descriptive than category-based approaches
  - can adapt as technology changes

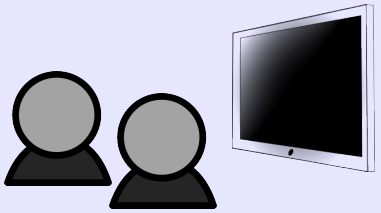
Characteristic-Based Security Analysis



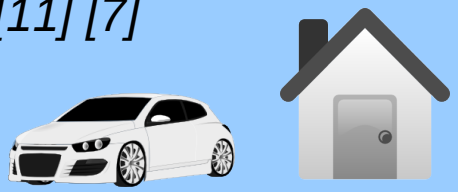

Characteristics of PN components
Characteristics of the PN
[inform]
[inform]
Abstract asset model
[basis of]
Attacker motivation & objectives
[realized through]
[enable]
[mapped to]
Attack vectors
[based on]
Existing analyes and scientific literature

PN Characteristics

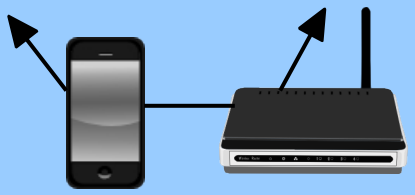
Shared components
[10] [7]



Absence of geographical locality *[10] [11] [7]*



Multihomed network topology
[3]

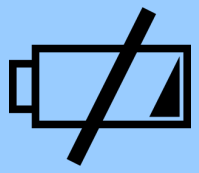


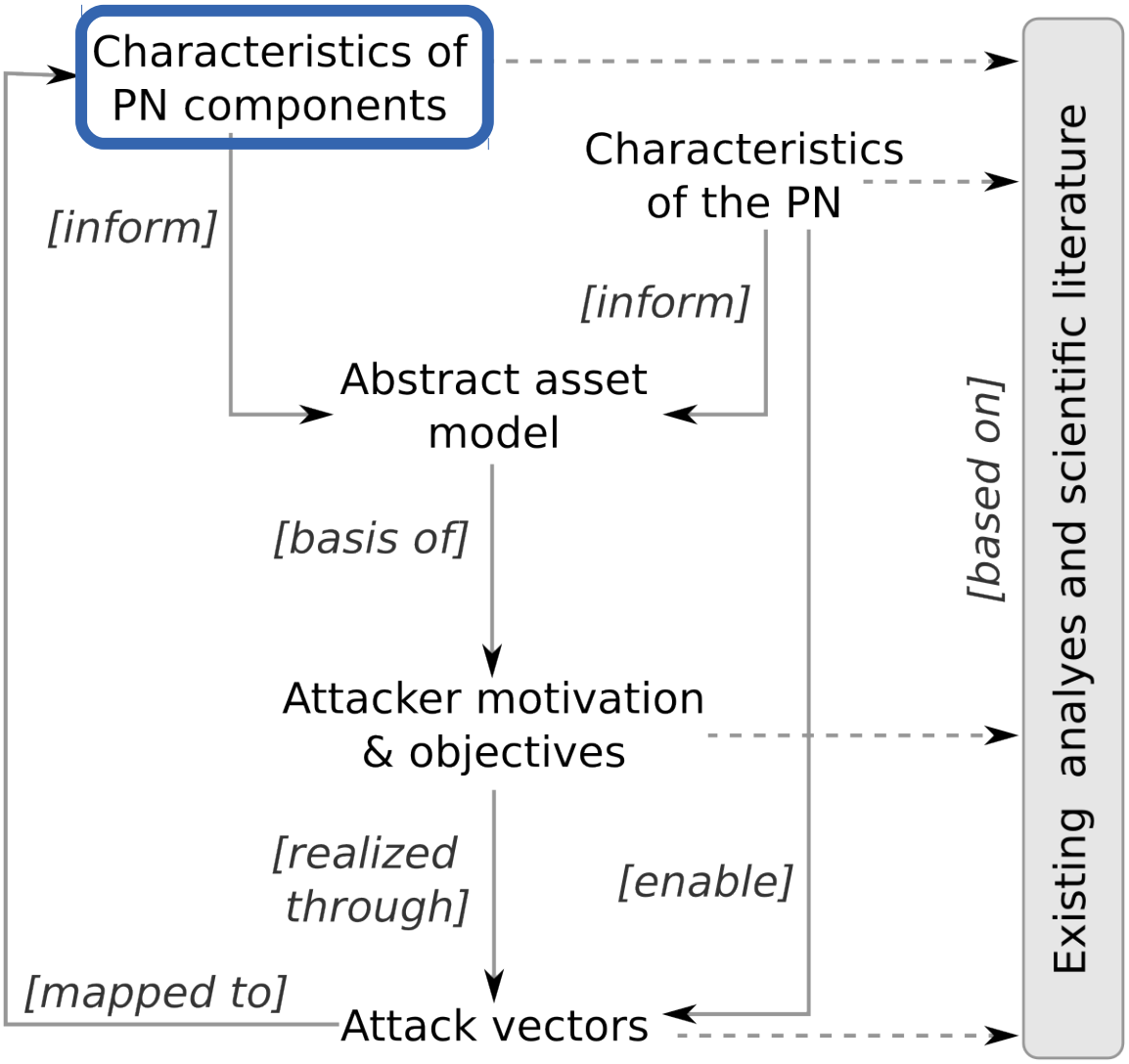
Device heterogeneity
[3] [12] [9]

Dynamic membership
[15]

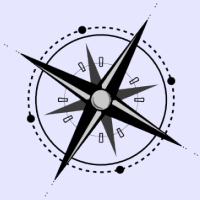
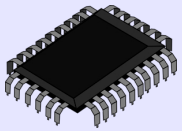
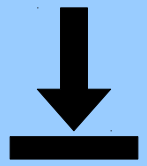
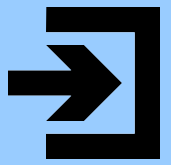
Communication diversity
[3] [10] [15]

Energy-aware systems
[14]



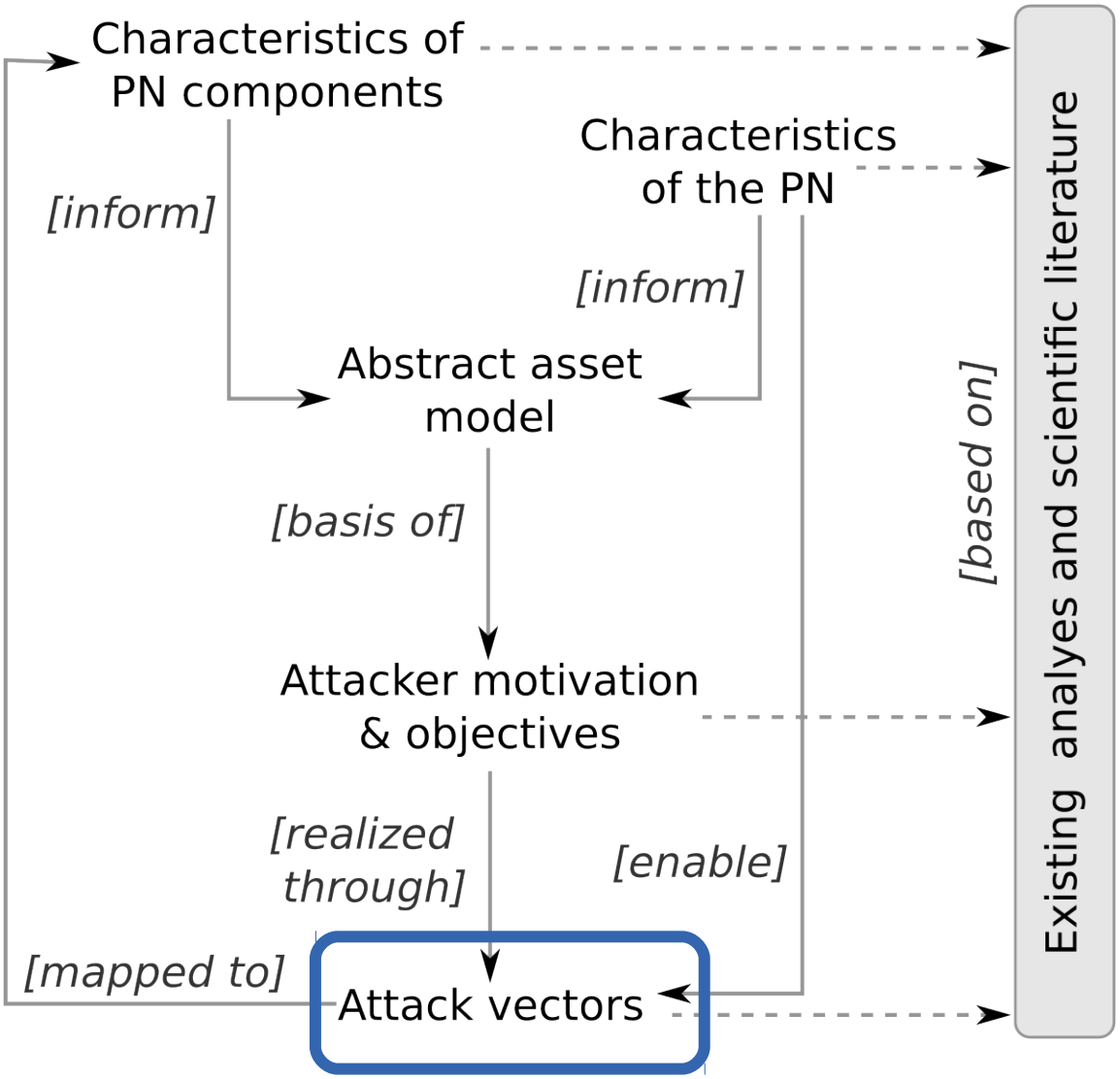

Characteristics of PN components
Characteristics of the PN
[inform]
[inform]
Abstract asset model
[basis of]
Attacker motivation & objectives
[realized through]
[enable]
[mapped to]
Attack vectors
[based on]
Existing analyes and scientific literature

Component Characteristics

Persistent storage 	Physical mobility 
Processing functionality 	Support for third party software 
Communication capabilities 	Control of other components
User interface capabilities 	Remote accessibility 
Control of physical infrastructure 	Provision of services
	Consumption of services

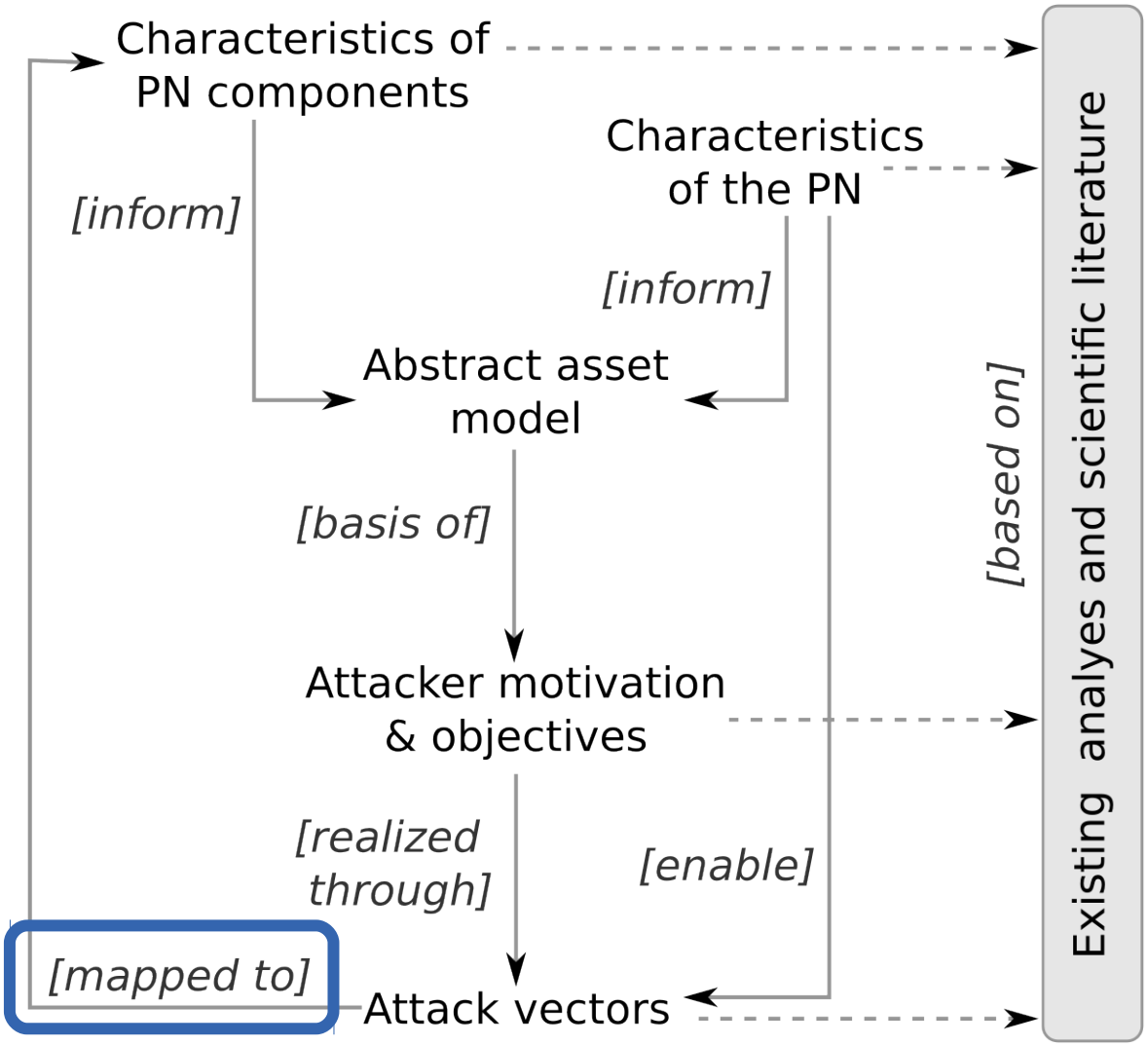
Component Characteristics

	Tablet	HEMS			
Persistent storage	✓	✓	Support for third party software	✓	✗
Processing functionality	✓	✓	Control of other components	✓	✗
Communication capabilities	✓	✓	Remote accessibility	✗	✓
User interface capabilities	✓	✗	Provision of services	✗	✓
Control of physical infrastructure	✗	✓	Consumption of services	✓	✗


Characteristics of
PN components
Characteristics
of the PN
[inform]
[inform]
Abstract asset
model
[basis of]
Attacker motivation
& objectives
[realized
through]
[enable]
[mapped to]
Attack vectors
[based on]
Existing analyes and scientific literature

Attack Vectors

Malicious software *[1][4][7][8][9]*	Impersonating a communicating entity *[3]*
Malicious hardware *[16]*	Unauthorized remote access *[3][7][9]*
Software exploits *[8]*	Unauthorized physical access *[3][7]*
Hardware exploits *[16]*	Misuse of device interoperability *[7]*
Interception of communication (eavesdropping) *[1][2][3][4]*	Protocols exploits *[1]*
Interruption of communication *[3][16]*	Eavesdropping on the UI (shoulder-surfing) *[3]*
Modification of communication *[3]*	Modification of communication routing *[1][3]*


Characteristics of
PN components
Characteristics
of the PN
[inform]
[inform]
Abstract asset
model
[basis of]
[based on]
Existing analyes and scientific literature
Attacker motivation
& objectives
[realized
through]
[enable]
[mapped to]
Attack vectors

Mapping Attacks to Characteristics

	Persistent storage	Processing functionality	Communication	User Interface	Control infrastructure	Physical mobility	Third party software	Control other components	Remote accessibility	Provision of services	Consumption of services
Malicious software	Y	Y					Y				
Malicious hardware	Y	Y	Y	Y	Y			Y			
Software exploits		Y					Y				
Hardware exploits	Y	Y	Y	Y	Y		Y				
Interception of communication			Y						Y	Y	Y
Interruption of communication			Y						Y	Y	Y
Modifcation of communication			Y						Y	Y	Y
Impersonation of communication			Y					Y	Y	Y	Y
Unauthorized remote access									Y		
Unauthorized physical access				Y		Y					
Misuse of device interoperability					Y			Y			
Protocol exploits		Y	Y					Y			
Eavesdropping on the UI				Y							
Modifcation of comm. routing			Y								

Conclusion

- Limitations of previous analyses
  - geographically-defined networks
  - category-based approaches
- Focus on Personal Network (PN)
  - home network + PAN + VAN + cloud
  - more representative of current systems
  - captures emergent characteristics
- Characteristic-based approach
  - maps device characteristics to attack vectors
  - more descriptive than category-based approaches
  - can adapt as technology changes

Characteristic-Based Security Analysis of Personal Networks

Andrew Paverd Department of Computer Science
University of Oxford

Fadi El-Moussa BT Research
BT Technology, Service & Operations

Ian Brown Oxford Internet Institute
University of Oxford

https://www.cs.ox.ac.uk/people/andrew.paverd/home