



VRDA

Prioritizing Vulnerability Response Efforts

2009 GFIRST Conference

CERT Vulnerability Analysis

Vulnerability discovery

- Tools and techniques to find vulnerabilities
 - Ideally, before the software ships

Vulnerability remediation

- Awareness
- Technical analysis, reproduction
- Mitigation
- Vendor coordination
- Public disclosure
 - US-CERT Vulnerability Notes
 - US-CERT Technical Alerts

Prioritizing Vulnerability Response

Vulnerability Response Decision Assistance (VRDA)

How do I best respond to thousands of new vulnerability reports per year?

Vulnerability management

- Prioritization
 - Focus on vulnerabilities that matter most to you
 - Allocate scarce resources
- Consistent response
- Structured, sharable vulnerability data

VRDA Concepts

Expert system

- Collect and apply organizational knowledge

Decision support

- Accurately model and predict responses
- Triage

Status

- Design
- Implementation
- Testing
- Operation

CONTAMINATED

Personal Property Receipt* Evidence Tag *413730*

Destination _____ Via _____ *413730*

TRIAGE TAG *413730*

S L U D G E
Salivation Lacrimation Urination Defecation G.I. Distress Emesis

AUTO INJECTOR 1 2 3 4 5

Yes	No	Gross Decon
Yes	No	Secondary Decon

Solution

<input type="checkbox"/>	Blunt Trauma
<input type="checkbox"/>	Burn
<input type="checkbox"/>	C-Spine
<input type="checkbox"/>	Cardiac
<input type="checkbox"/>	Crushing
<input type="checkbox"/>	Fracture
<input type="checkbox"/>	Laceration
<input type="checkbox"/>	Penetrating Injury

Age _____

Male Female

Other: _____

VITAL SIGNS

Time	B/P	Pulse	Respiration

Time	Drug Solution	Dose

EVIDENCE

MORGUE Pulseless/Non-Breathing *413730*

IMMEDIATE Life Threatening Injury *413730*

DELAYED Serious, Non Life Threatening *413730*

MINOR Walking Wounded *413730*

Components

Response decisions: **Tasks**

- Prioritization: **Must, Should, Might, Won't**

Vulnerability information: **Facts**

- Classes: **Vulnerability, World, User**

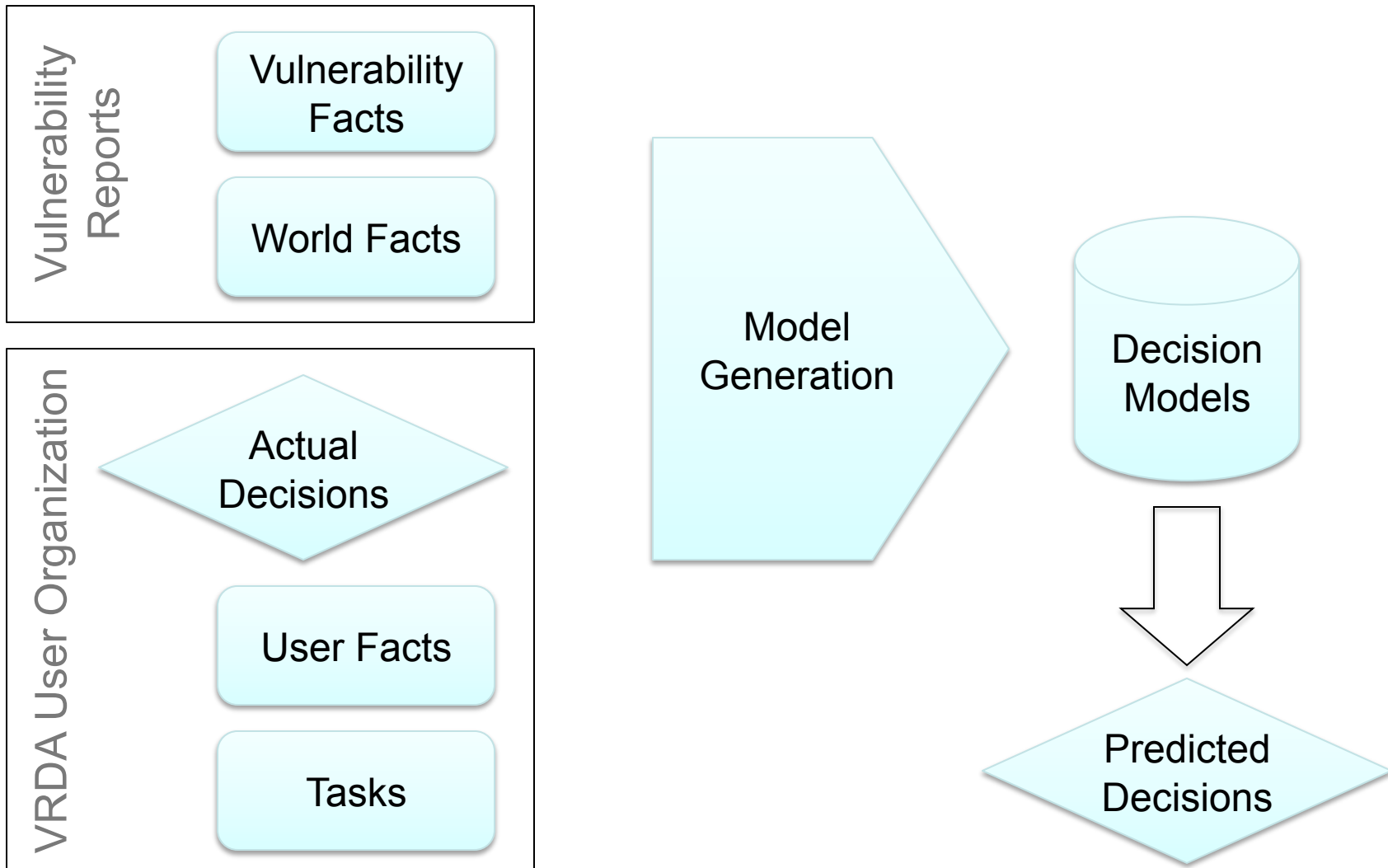
Inventory: **LAPTs**

Decision making: **Decision trees**

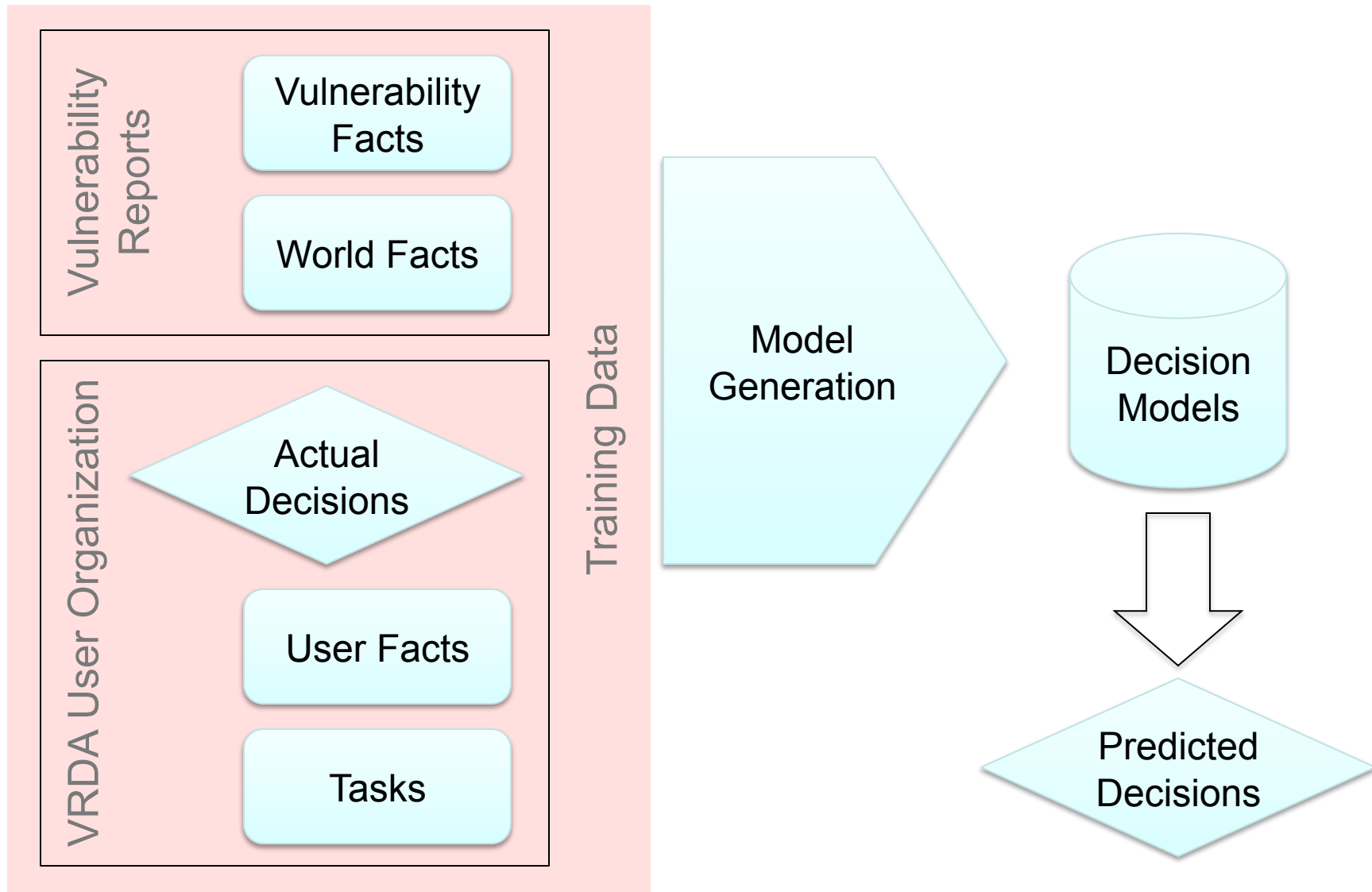
Training data

- Facts and actual decisions

Framework



Framework



KENGINE Demonstration

KENGINE Software

- Developed by JPCERT/CC
- Ruby on Rails, PostgreSQL

Demonstration

- Components
- Vulnerability report entry
- Compare predicted and actual responses



Effectiveness

Experiment with three responders

Accuracy

- Compare VRDA predictions to actual
- Response process complexity
- Human versus computer
- Training data size

Efficiency

- Effort per vulnerability
- Not measured

Accuracy

Task	Sample Size	Hit Rate	NMR	MSE	ME
<i>Overall Performance (all tasks)</i>	2,147	70%	94%	0.56	0.05
Assign Analyst (D1)	215	90%	100%	0.10	0.05
Perform Surface Analysis	215	88%	90%	0.83	0.20
Perform Technical Analysis	215	68%	93%	0.56	-0.02
Coordinate	215	58%	93%	0.68	0.01
Publish Vulnerability Card	215	68%	95%	0.50	0.08
Publish Vulnerability Note	215	66%	94%	0.57	0.12
Publish Technical Alert	215	60%	89%	0.81	0.08
Publish Security Alert	215	63%	92%	0.67	0.01
Publish Special Communication	215	80%	99%	0.27	0.21
Publish Current Activity	212	57%	94%	0.60	-0.21

Error Distribution

Task	Error						
	-3	-2	-1	0	1	2	3
<i>Overall Performance (all tasks)</i>	4	40	256	1,500	264	52	31
Assign Analyst (D1)			6	193	16		
Perform Surface Analysis	2	1	3	190	1	2	16
Perform Technical Analysis		3	39	146	16	9	2
Coordinate		4	44	125	32	7	3
Publish Vulnerability Card		2	27	147	31	6	2
Publish Vulnerability Note		2	28	141	33	9	2
Publish Technical Alert	1	9	27	129	36	10	3
Publish Security Alert	1	10	26	135	36	6	1
Publish Special Communication				173	40		2
Publish Current Activity		9	56	121	23	3	
			Design goal (NMR)				

Other Findings

VRDA only includes relevant facts in decision trees

- Unused facts for CERT decision trees
 - Access Required
 - User Interaction Required
 - Information Source Reliability
 - Security Product

Effort requirements

- For 215 vulnerability reports CERT needs:
 - 51 effort days to complete all Must tasks
 - 455 effort days to complete all Should tasks

References

Slides from FIRST 2007

<http://www.cert.org/archive/pdf/VRDA_JPCERT-CERTCC.pdf>

Vulnerability Response Decision Assistance

<<http://www.cert.org/archive/pdf/VRDA-2008.pdf>>

Effectiveness of the Vulnerability Response Decision Assistance (VRDA) Framework

<http://www.cert.org/archive/pdf/VRDA_Effectiveness.pdf>

JPCERT/CC VRDA Feed

<<http://vrda.jpCERT.or.jp/feed/en/atom.xml>>

Art Manion

<amanion@cert.org>