

Incident Report Database

by Pascal Meunier

- Web-based, open source, uses free engines
- Incident cost estimation
- New incident classification
- Sanitization
- Real-Time use (“As-It-Happens” approach)

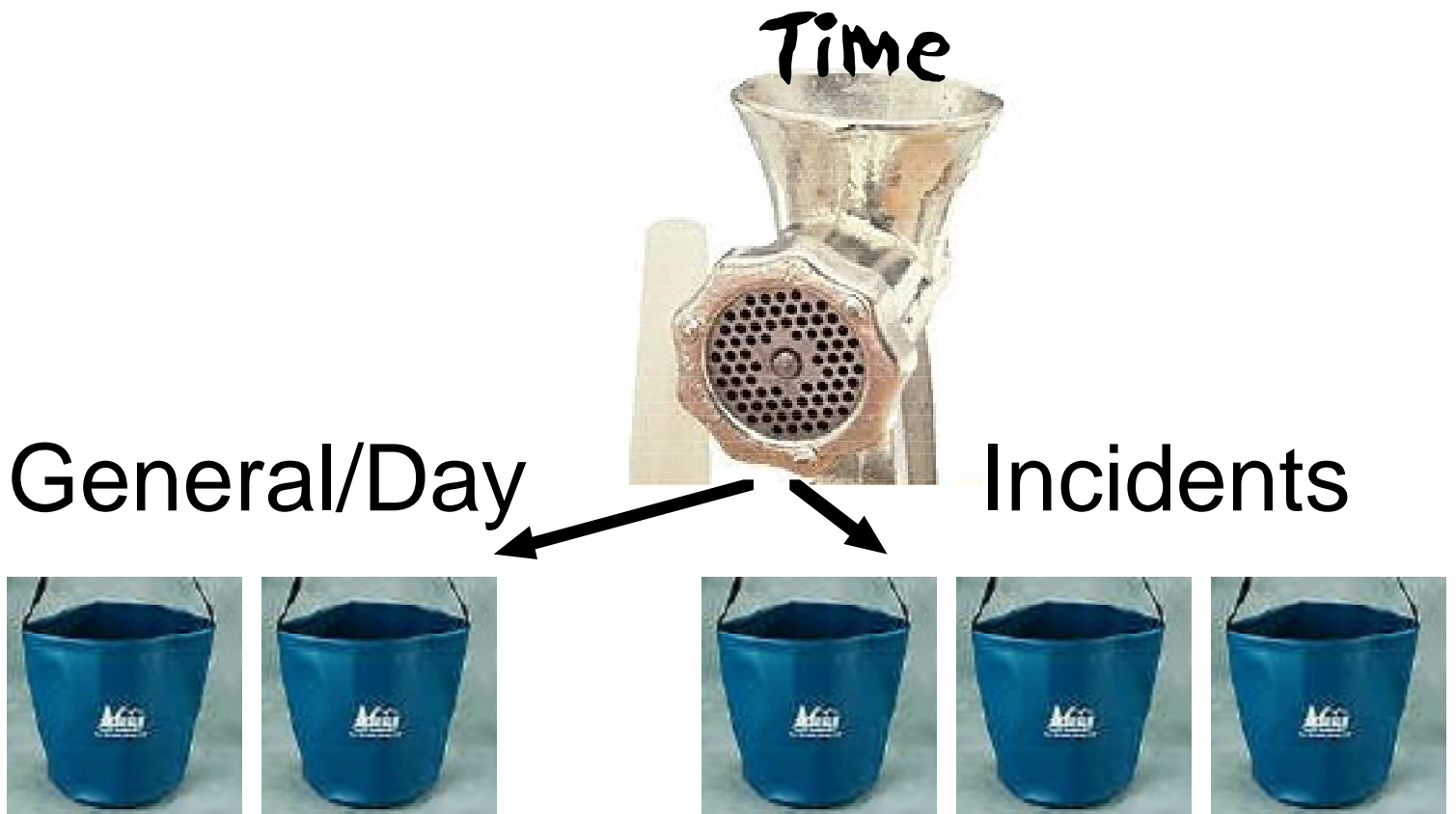
FEATURES

- Independent domains of privileges fully in **your** control.
- ***FAST*** entry of routine incidents with types (presets)
- Compatibility with Intrusion Detection Data Model IETF idwg Draft v.2.
- Support for an integrated risk database (CVE-compatible)
- Email support
- Evidence, contacts and resource modeling support

Why Web Access

- Allow some remote security researchers access to sanitized data (ICAMP project and FERPA compliance)
- Allow CERT or other remote trusted expert entity read access to your data to provide assistance.
- Allows access to your data and support from the IRDB even if you get hacked
- Cross-platform
- Can be secured through SSL

Total Time Accounting



Time spent per incident, per role

- Differential (opportunity) cost
- raw cost (incl. hardware expenses)
- Willingness to pay

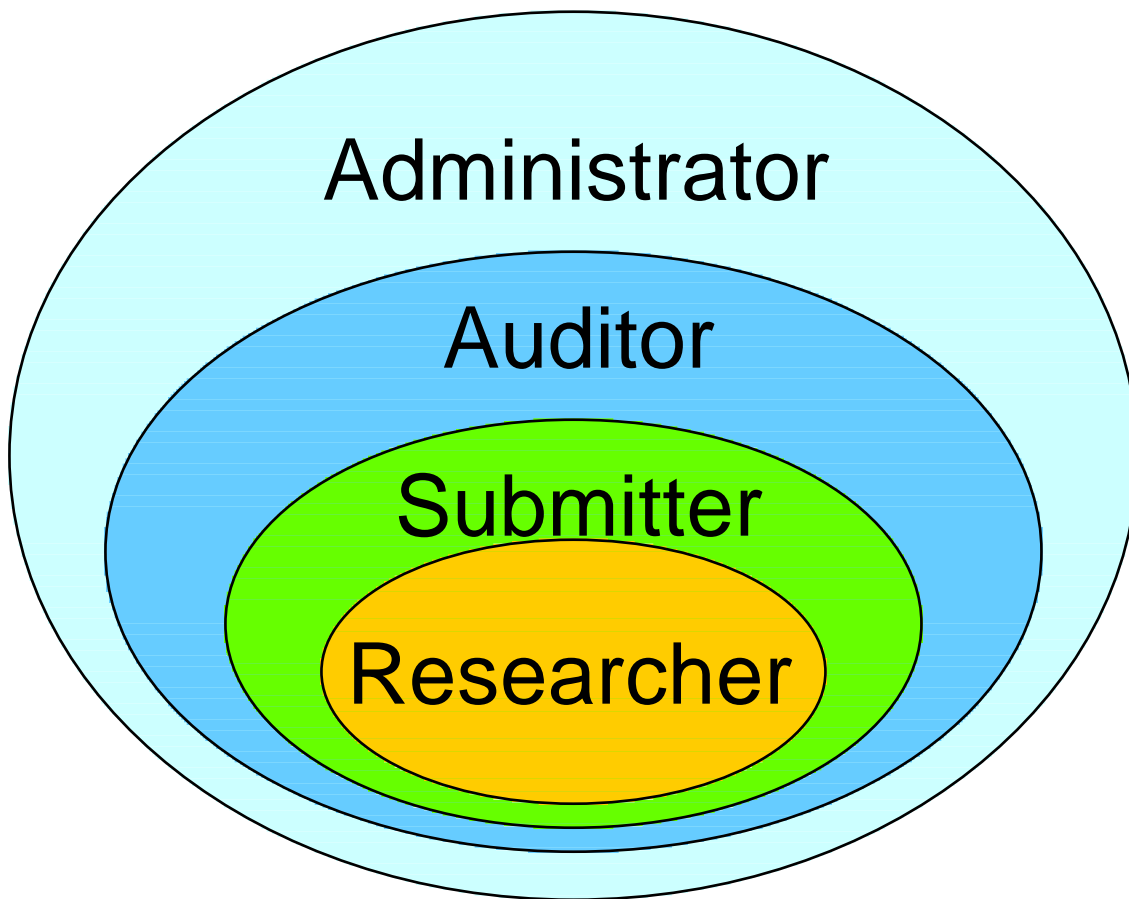
+ Time spent per day doing general management activities

= Total time logged in

The Wonderful, Amazing, Miraculous, Incredible Folding Bucket from <http://www.hitthetrail.com/bucket.htm>

Deluxe Meat Grinder from <http://www.appliances.com/porkert26510.html>

Privileges



Example: Margaret Bouquet has privileges:

<u>Domain</u>	<u>Privilege</u>
Biology	Submitter (submit)
Math	Auditor (read everything)
PUCC	Researcher (sanitized data)

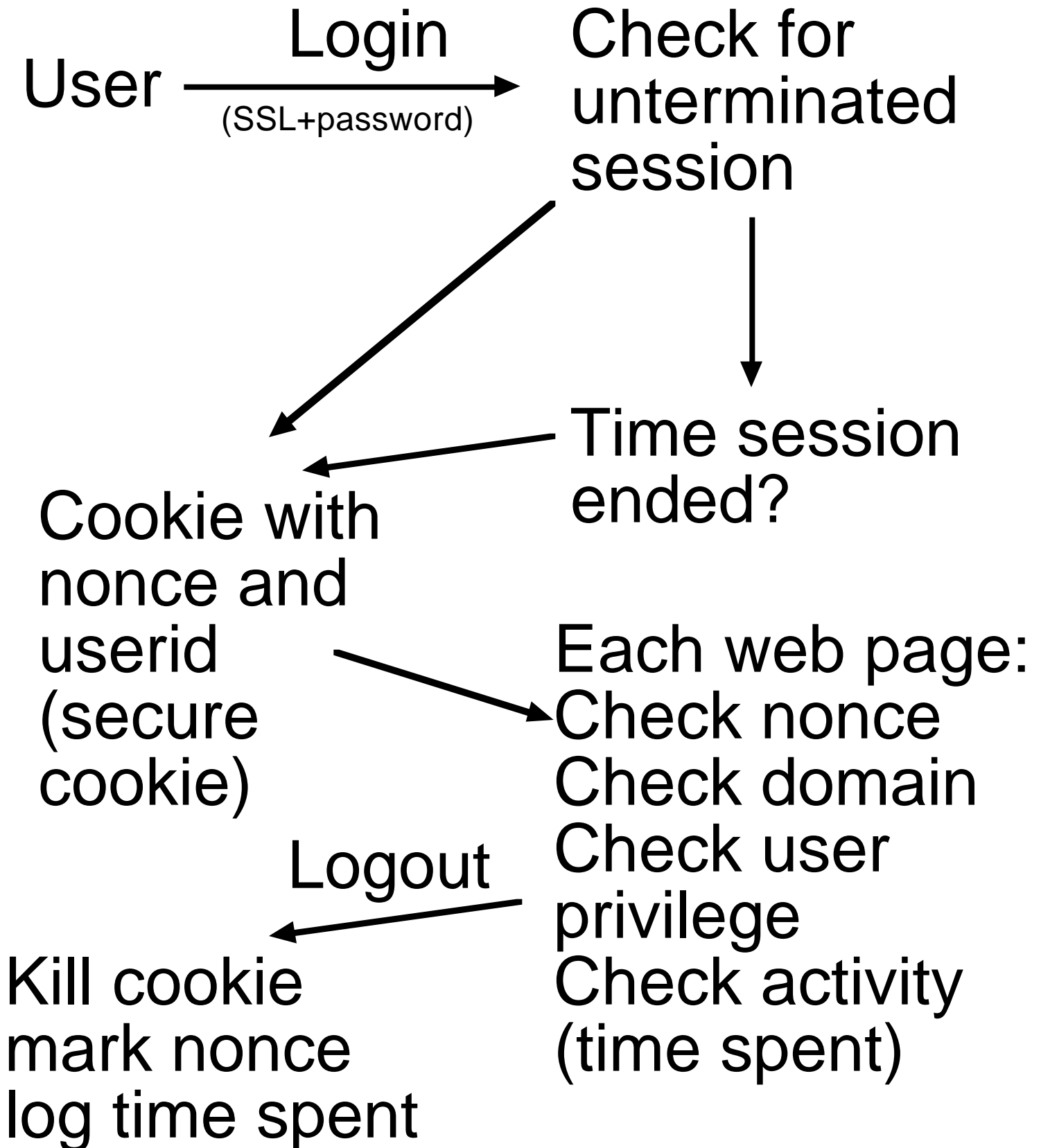
As-It-Happens Approach

Reporting incidents after they have been processed and closed is a chore likely not to get done, and is likely to be inaccurate or incomplete.

For this reason, the database attempts to be as supportive of incident response as possible.

- Specify classifiers as you discover them.
- Search for matching risk types.
 “Unknown” settings function as wildcards in searches.
- Send email
- Generate a CERT assistance request
- Look for similar past incidents

Authentication



Classification Modes

- By types (presets, quick), requires exact knowledge of what happened
- By each classifier (longer), may be done over several sessions
- Assisted: which types match the properties entered so far?

All Incidents

- verification status
- authentication classifier
- intent classifier
- nature classifier
- incident status (closed/open states)
- timestamps
- role relations with people

Technical Incidents

-level

"unknown", "risk report", "recon", "attempt",
"confirmed exploitation"

-source

"Provisionned", "Intrusion Detection Tool"

-consequence

"unknown", "exposure", "account access",
"execute commands", "install software", "bypass
filtering", "service loss", "service theft", "power
loss", "A/C loss"

-access_type SET

"list files", "read files", "write files", "execute
files"

-privilege_type

"N/A", "root", "privileged", "normal"

-origin SET

"local", "external"

-mode

"unknown", "overflow", "other"
(subclass overflow for overflow data)

Human Incidents

-mode

"unknown", "service", "possession",
"reception"

-motive

"unknown", "hate", "fraud", "theft",
"commerce", "sex", "human error"

-property SET

"bulk", "copyright", "threat", "harassment",
"minors", "credentials"

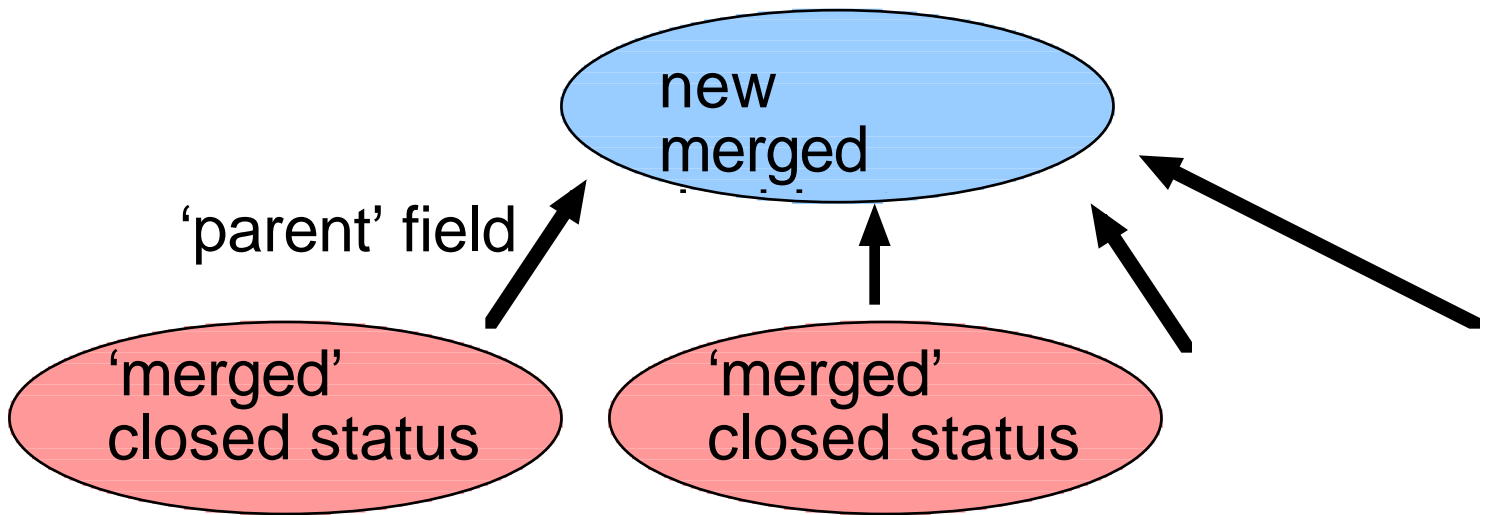
-medium

"unknown", "multimedia", "binary", "text"

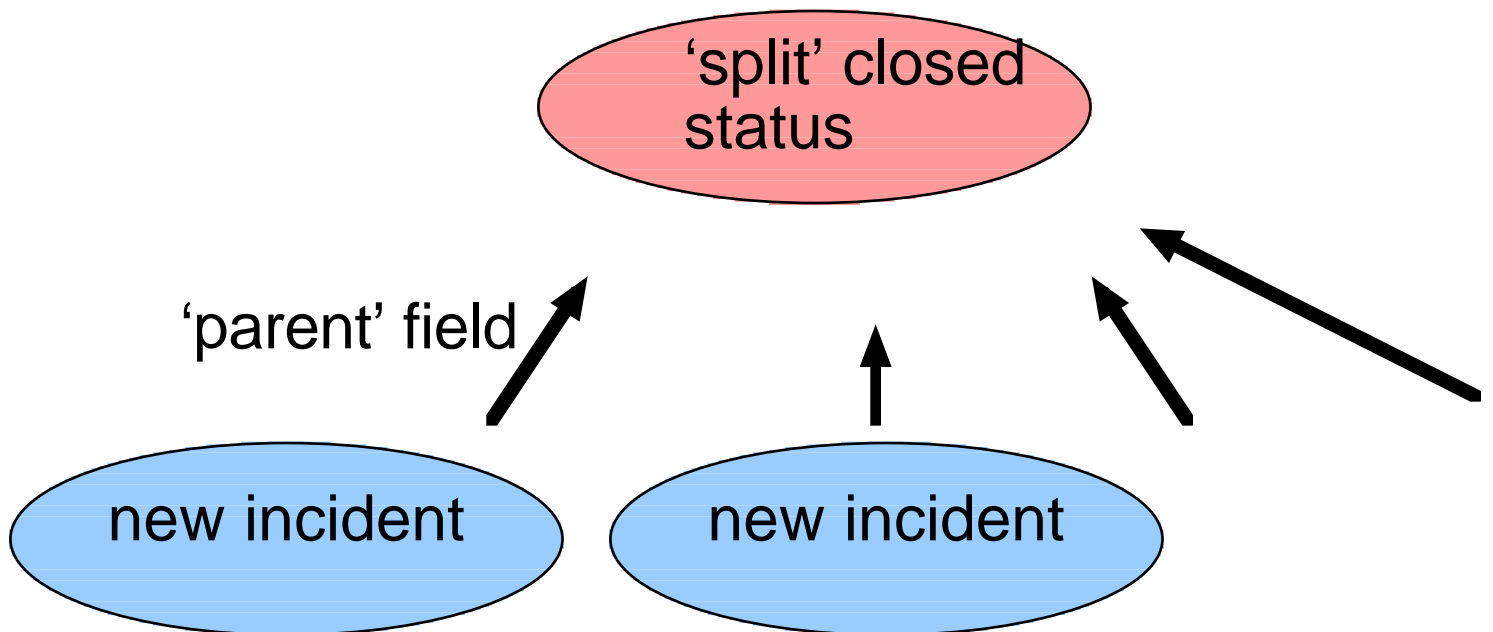
-consequence SET

"annoyance", "confidentiality", "physical
safety", "intimidation", "mental cruelty",
"monetary loss", "other"

Merging Incidents



Splitting Incidents



Sanitization

- a) Canned queries
- b) Student owned resources (equipment, accounts) are flagged
- c) Each object has permissions (an access control list) attached, with respect to the role of people with regards to an incident (law enforcement, expert, original submitter, CERT, other victims, ...)
- d) Costs are logged by role for an incident, not by user ID.

Classification Examples

```
insert into techthreat
(name, consequence, access_type,
privilege_type, origin, description)
values ("Mail Bomb", "service loss", 0,
"N/A", "local,external", "The mailbox gets
filled completely by junk and can't
receive valid messages");
```

```
insert into techthreat
(name, CERT, CVEentry,
consequence, access_type,
privilege_type, origin, description)
values ("SYN flood", "CA-
96.21.tcp_syn.flooding", "CVE-1999-
0116", "service loss", 0, "N/A",
"external", "The computer allocates all
TCP/IP resources to record half-
completed handshakes");
```

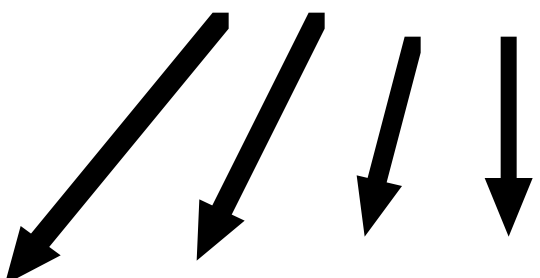
Classification Examples

insert into humanthreat
(name, mode, motive, property,
medium, consequence) values
("Death Threat", "reception", "hate",
"threat", "unknown", "physical
safety,intimidation");

insert into humanthreat
(name, mode, motive, property,
medium, consequence) values
("Child Pornography", "possession",
"sex", "minors", "multimedia",
"physical safety,intimidation,mental
cruelty");

Future Work

Incident → Risks
(CVE)



Fundamental
Vulnerabilities

Additional features

- Store hash of password with salt instead of plain password.
- Integration with CERIAS vdb
- Expert system.

Thanks to:

BRIAN POOLE

Dan Ingevaldson

Gene Spafford

Steve Hare

and the CERIAS staff

IRDB Details

- PHP and MySQL
- IP addresses inserted into stop-list after several login failures on the same day