Incident Taxonomy: Best Current Practice

Andrew Cormack

JANET-CERT

Andrew.Cormack@ukerna.ac.uk

Aims

A brief survey

- what exists already?
- what do teams do now?

Don’t want to re-invent things

Want something usable

Methods

Survey of existing literature

- IETF Intrusion Detection Working Group
- Common Vulnerabilities and Exposures list
- Common Language for Security Incidents

Questionnaire to European and FIRST teams

- preliminary results only, so far

IDWG

Communication between IDS components

Multiple vendors, so need a common language

Sensors talk to management stations

Reporting individual events

Many reports make up a single incident

Currently just a framework

CVE list

Unique references for vulnerabilities

References to others (CERT, vendor, ...), e.g.

Limited scope, but good for what it does

Common Language

John Howard/Tom Longstaff

Designed to describe incidents for analysing trends

Used to study all CERT-CC reports from 1989 to 1996

Common Language Event

An event is:

- action: probe, scan, flood, authenticate, bypass, spoof, read, copy, steal, modify, delete
- target: account, process, data, component, computer, network, internetwork

Common Language Attack

An attack is:

- tool: physical attack, information exchange, user command, script or program, autonomous agent, toolkit, distributed tool
- vulnerability: design, implementation, configuration
- 1 or more Events (previous)
- unauthorised result: increased access, disclosure of information, corruption of information, denial of service, theft of resources

Common Language Incident

An incident is:

- attacker: hacker, spy, terrorist, corporate raider, criminal, vandal, voyeur
- 1 or more Attacks (previous)
- objective: challenge, political gain, financial gain, damage

Common Language Examples

Web defacement:

hacker->user command->configuration->modify->
data->corruption of information->political gain

Denial of service:

vandal->distributed tool->implementation->
flood->process->DoS->damage

These are my choices, you may think otherwise...

Common Language Concerns

Attacker and objective are usually conjecture

Too abstract?

- doesn't say web, mail, dns, …
- or solaris, linux, NT, ...

Hard to use?

- different teams had different results
- 1989-1996 survey uses a variant

Survey Conclusions

None is a complete solution

Useful ideas

- IDWG may have higher level applications
- CVE list is a good dictionary for reporting
- Common Language multiple-factors

Essential

- Usability & consitency !

Questionnaire

Sent to European and FIRST teams

Mix of education, government and commercial

To establish what teams do now

Analysis of first 11 responses

Questions

Use of Information

- how and why teams record incident information?

Details recorded

- what information is recorded?

Information sharing

- is this shared with others?

Use of Information

All respondents record information

- for incident handling
- for statistics (most)

About 60% in a database; rest in action logs

Other uses mentioned

- identifying repeat offenders (attackers or victims)
- planning for future trends
- sending pro-active information

Details Recorded

Four factors

- victim of attack: identity, class(some)
- source of attack: identity(some), class(few)
- system targeted: OS, service, vulnerability (all some)
- result: immediate effect, cost (few)

Most also record information for incident handling

Information Sharing

Most teams share information during incidents

- but not all
- trust is important

Funding often requires statistics in return!

Few publish even statistics openly

- damaging to constituency?

Conclusions

No obvious “off the shelf” solution

Many teams are recording relevant information

- but considerable variation in detail

Information sharing may be new to some

Benefits of any solution must be clear