

implementing and testing a biologically-inspired security system

jamie twycross

uwe aickelin

university of nottingham

- my work is part of a 3-year multidisciplinary EPSRC-funded adventure project exploring algorithms inspired by new paradigms in immunology.
- **research areas:** computer security, biologically-inspired computing, immunology, artificial immune systems (AIS), robotics.
- **motivation:** not one solution for one problem:
  - *how to build better AIS and computer security systems in general?*
- **specific questions:**
  - *what are the important components AIS should extract from biology?*
  - *what are good problem-domains for AIS?*
- **experimental methodology:** theorise, implement and experimentally explore.
  - implement a general implementational framework - **libtissue**.
  - use this framework to build one solution for one problem!

- short answers to the questions.
- the libtissue implementation.
- applying libtissue to a computer security problem.
- an example algorithm - twocell.
- validation experiments with twocell.
- current work - pad1a and wu-ftpd.
- future directions. references.

- *how to build better AIS and computer security systems in general?*

engineer artificial systems within a paradigm of

**lots of multilevel input data sources**

and

**simple distributed processing**

- *what are the important components AIS should extract from biology?*

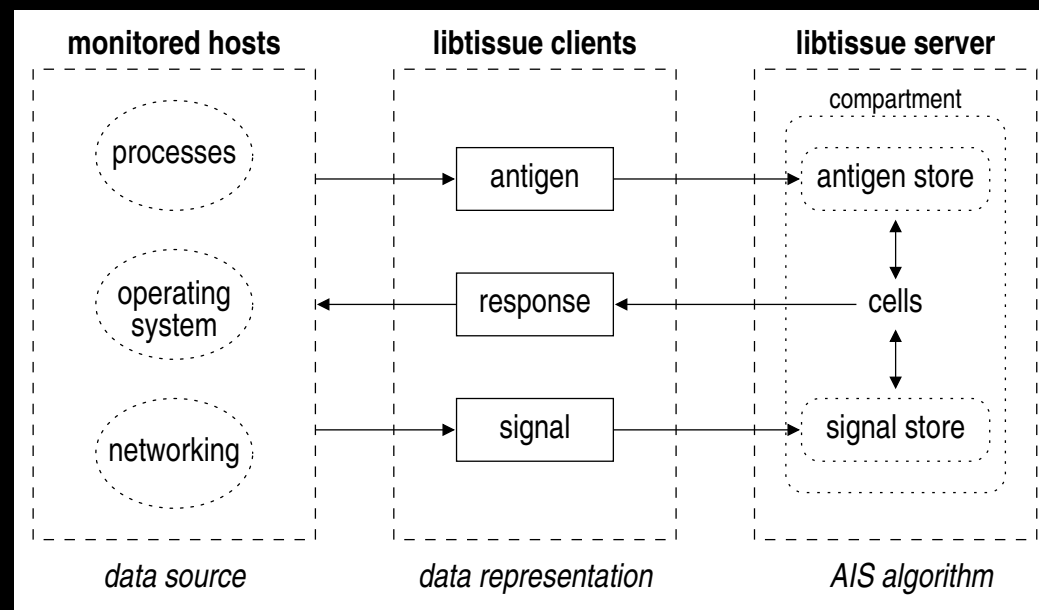
**cells, signals, antigen, compartments**

- *what are good problem-domains for AIS?*

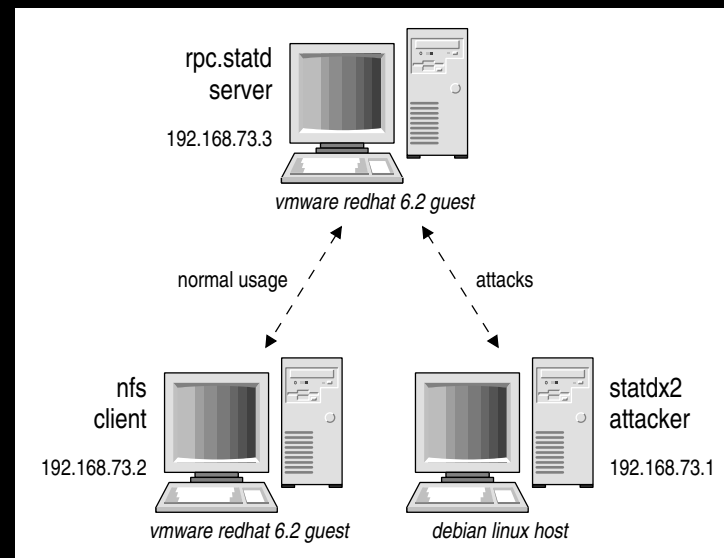
**ones with a wide range of dynamic input data sources -**

**computer security**

*libtissue is a software system for implementing and evaluating AIS algorithms on real-world monitoring and control problems.*

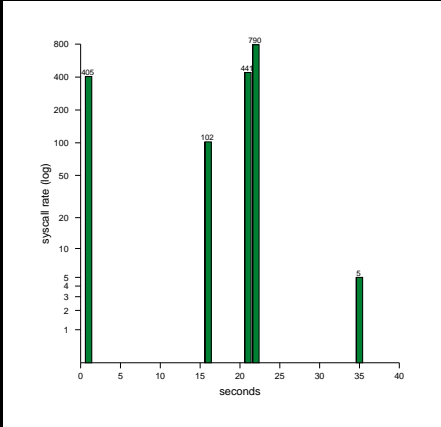
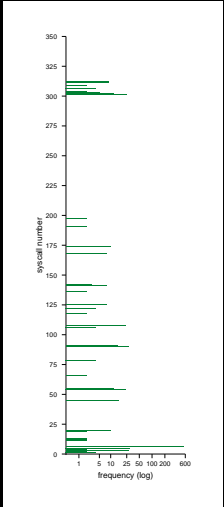


- the problem: **process anomaly detection**.
- current research areas are *problem representation* and *solution implementation*.
- redhat 6.2 rpc.statd statdx2 exploit (format string, 2000).

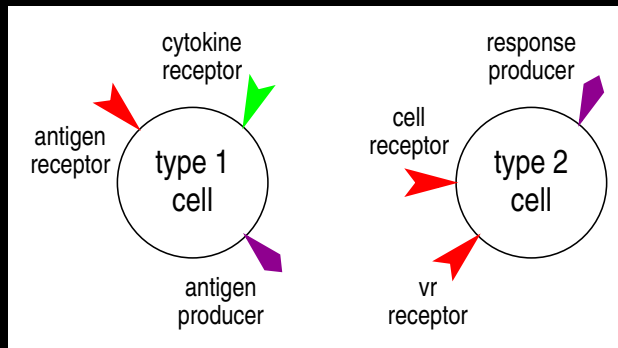


rpc.statd dataset

dataset	total time	total antigen	max antigen rate
success1	55	1739	1102
success2	36	1743	790
failure1	54	518	405
failure2	68	495	405
normal1	38	434	405
normal2	104	450	405

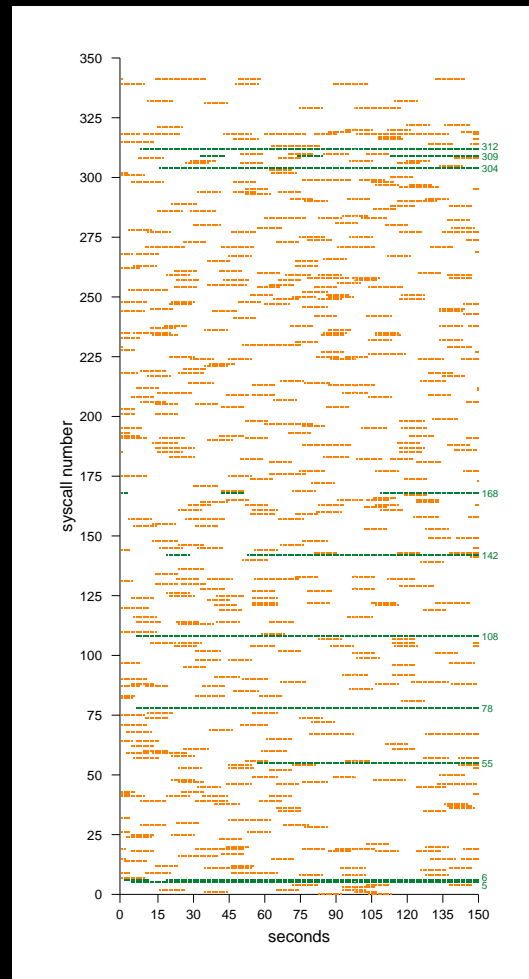
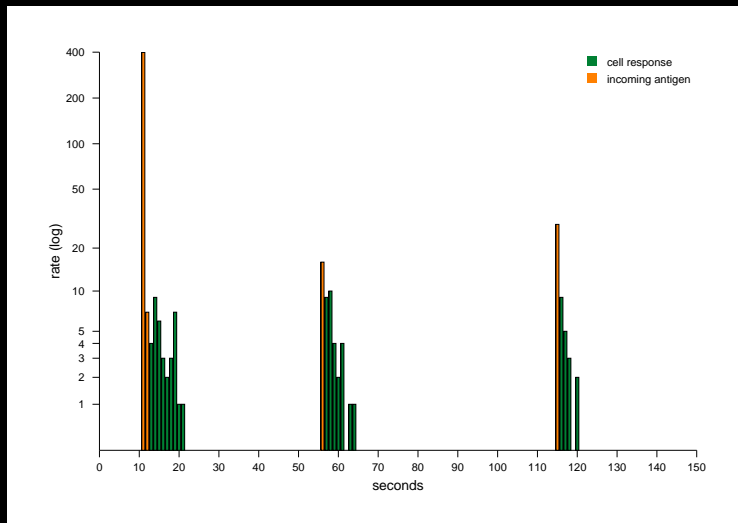


twocell algorithm



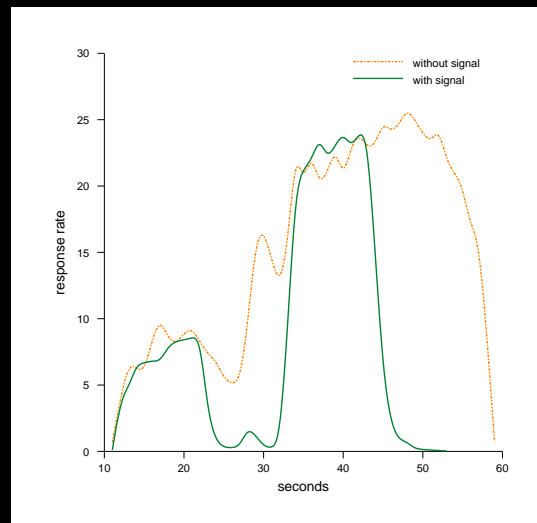
max_antigen	1000
max_cytokines	0
max_cells	100
cell_update_rate ( $\mu secs$ )	100000
antigen_multiplier	10
num_cells 1	50
num_antigen 1	100
num_antigen_receptors 1	10
num_antigen_producers 1	10
antigen_producer_action_time	10
num_cells 2	50
cell_lifespan 2	100
num_cell_receptors 2	2
num_vr_receptors 2	20
num_response_producers 2	1
probe_rate ( $\mu secs$ )	1000000

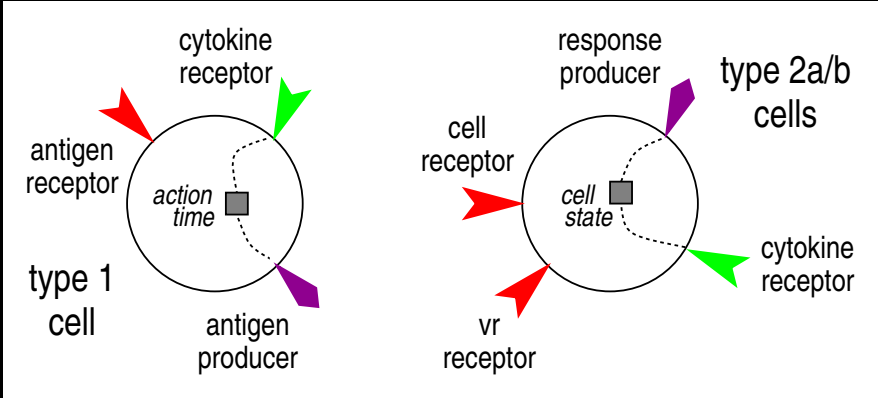
# two-cell experiments



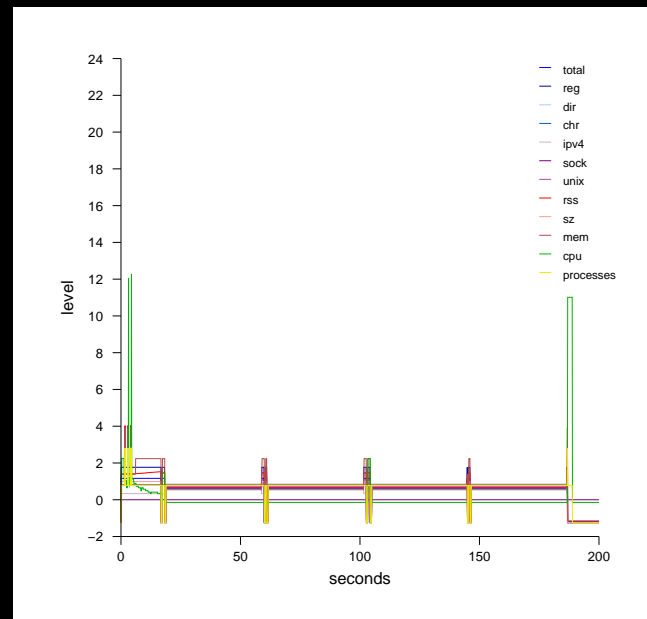
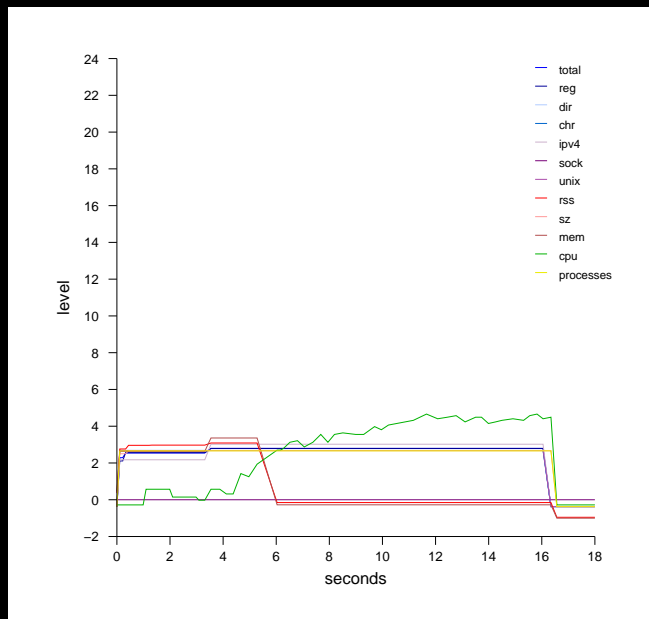
two-cell experiments

dataset	success1	success2	failure1	failure2
normal syscalls	23%	23%	81%	87%
attack syscalls	76%	76%	18%	12%
naive permit	90%	90%	99%	99%
naive deny	9%	9%	0%	0%
two-cell permit	47%	47%	69%	68%
two-cell deny	52%	52%	30%	31%





- syscall number and EIP as antigen.
- external signals control cells: action time parameter and cell state.
- compare to naive approach and simple negative selection.
- *how does adding signals change the behaviour of the system?*
- *can changes in behaviour be used to detect process anomalies?*



- redhat 6.2 wu-ftp daemon exploit (SITE EXEC format string, 2000).
- LBNL-FTP-PKT traces: *“the trace ran from Jan 10-19, 2003, containing 22 thousand connections and 3.2 million packets. The connections are between 320 distinct servers and 5832 distinct clients.”*

## future directions

- more normal usage and exploit data (redhat 7.1 apache openssl, distcc misuse).
- signal relevance and function. innate immunity.
- evolution of simple neural networks as cell controllers.
- libtissue as a general implementational framework for AIS.

## references

- a preprint of a paper (*libtissue - implementing innate immunity*) accepted for CEC 2006 which describes the libtissue implementation and the validation experiments with twocell and rpc.statd is available from my website.
- datasets and sourcecode (all GPL) from my website too.

jamie twycross

research associate, university of nottingham

jpt@cs.nott.ac.uk, <http://www.cs.nott.ac.uk/~jpt>