Architecture and Components for Data Management Security: NRL Perspective

Carl E. Landwehr
Judith N. Froscher
Naval Research Laboratory
{landwehr | froscher @itd.nrl.navy.mil
(202)767-3381

What is needed?

System architecture that

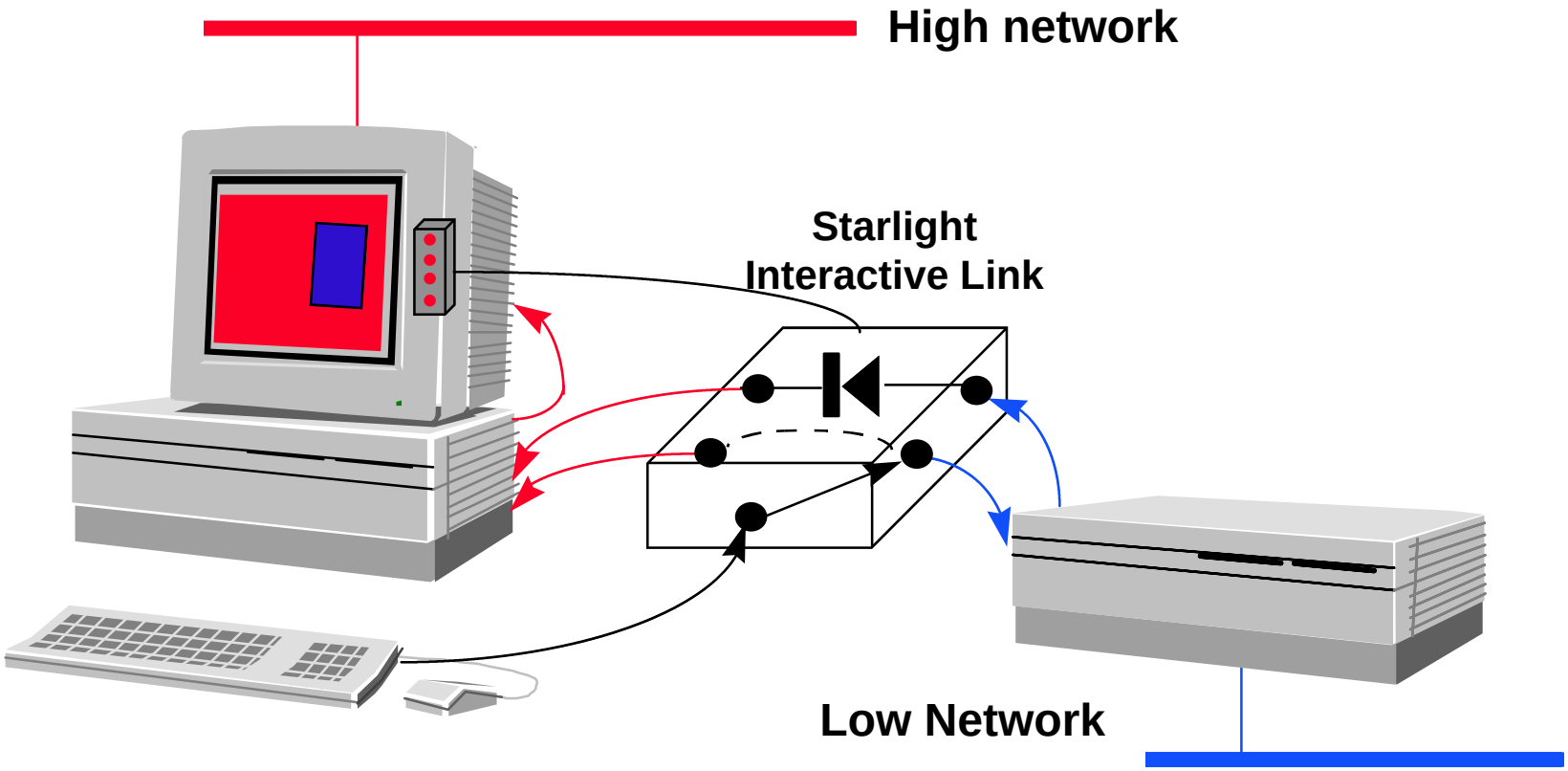
- permits flexible use of COTS, including COTS DBMS
- enforces DoD security policies
- can incorporate legacy systems
- is affordable, understandable, preserves local autonomy, permits heterogeneity

Approach

- Assign high assurance security policy enforcement to separate, simple components
- Create environments where commercial threat model is appropriate and rely on COTS enforcement

Components to enforce information flow policy

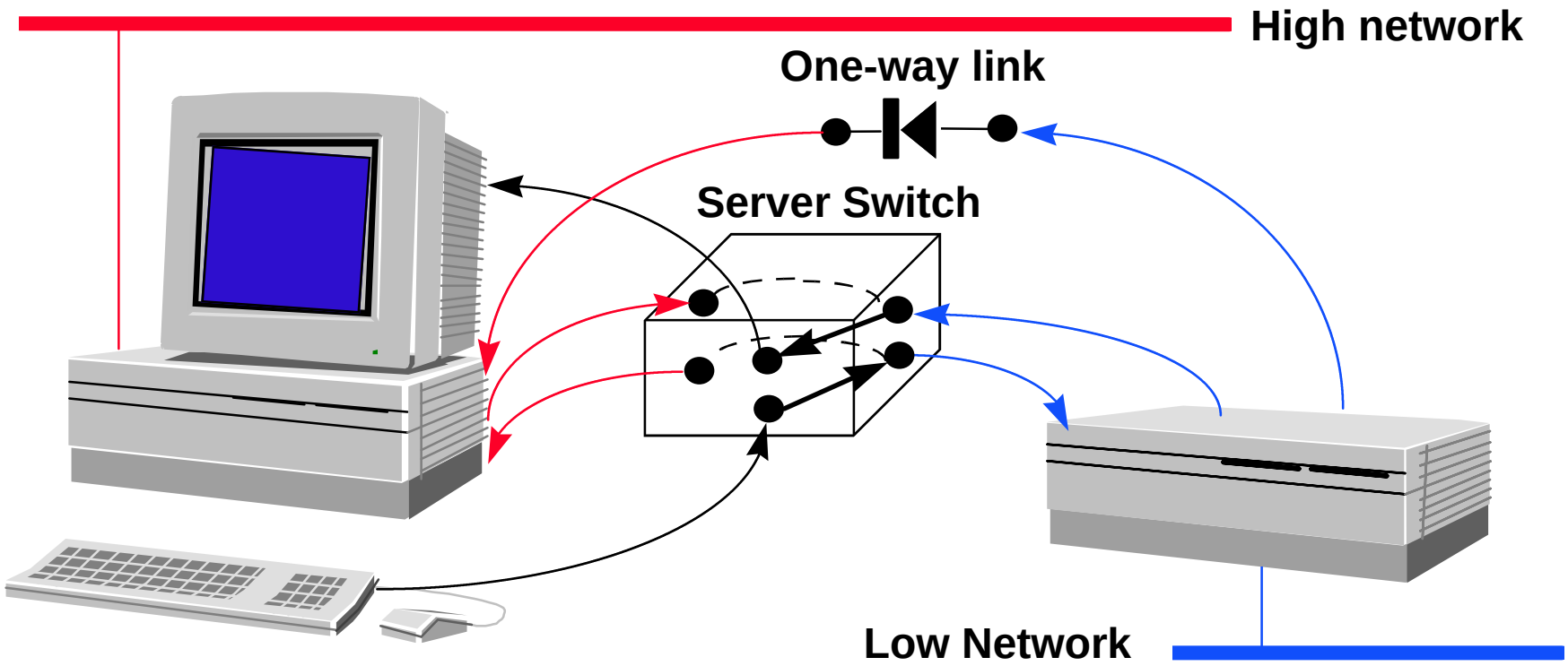
Starlight Interactive Link



- Starlight ILconnects keyboard/mouse either to Low or High server
- Low X-events echoed to High over data diode
- Cut and paste upwards is supported
- Trust: switch, data diode, keyboard/mouse storage
- Target evaluation level: E6

Components to enforce information flow policy

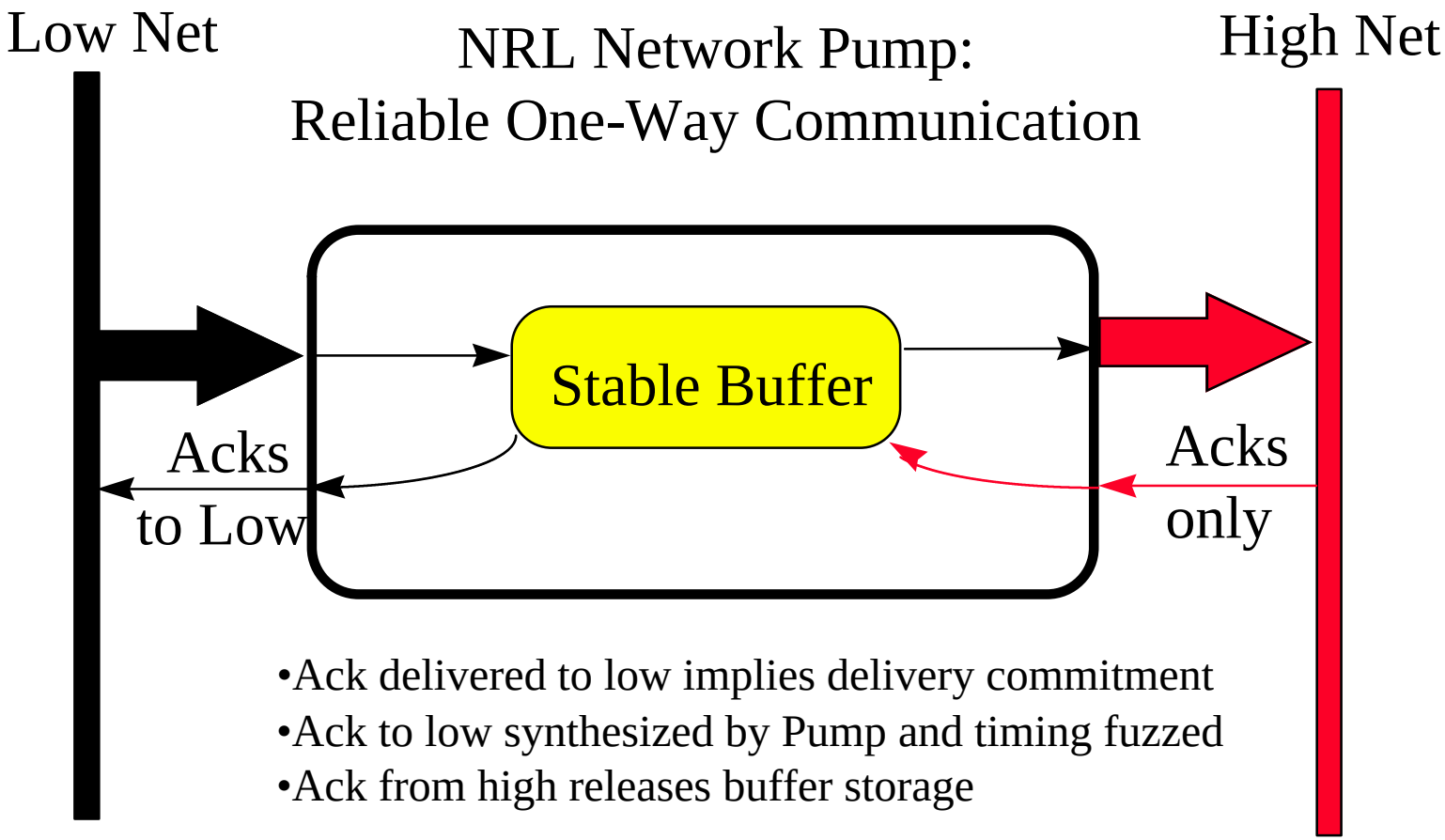
COSPO Switched Workstation



- Server switch connects keyboard/mouse and monitor either to Low or High server
- Upward file transfer via separate one-way link
- Upwards cut and paste, via OWL (soon); no X-windows requirement
- Trust: switch, one-way link, keyboard/mouse storage
- Certified for secret/unclas

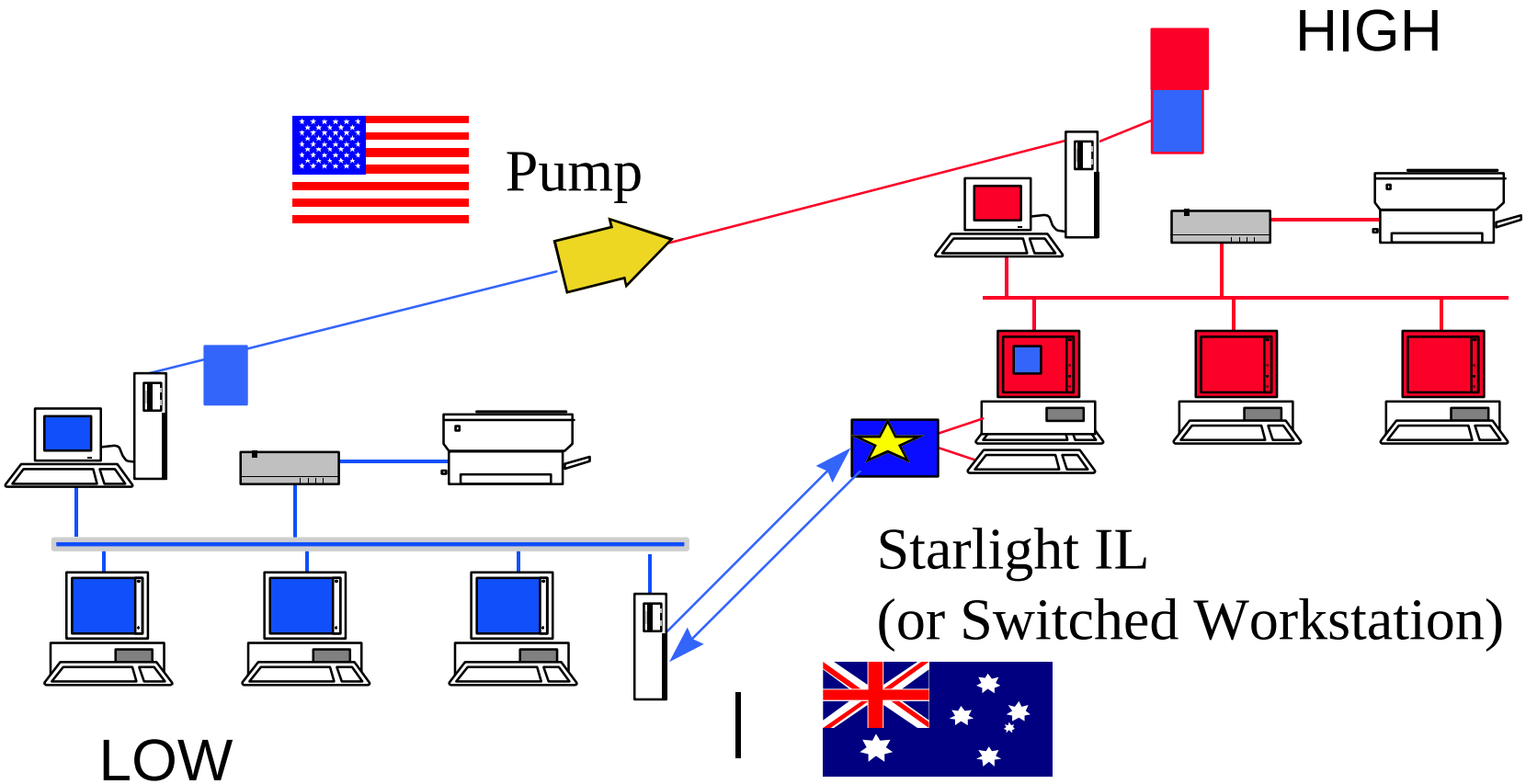
Components to enforce information flow policy

The NRL Pump



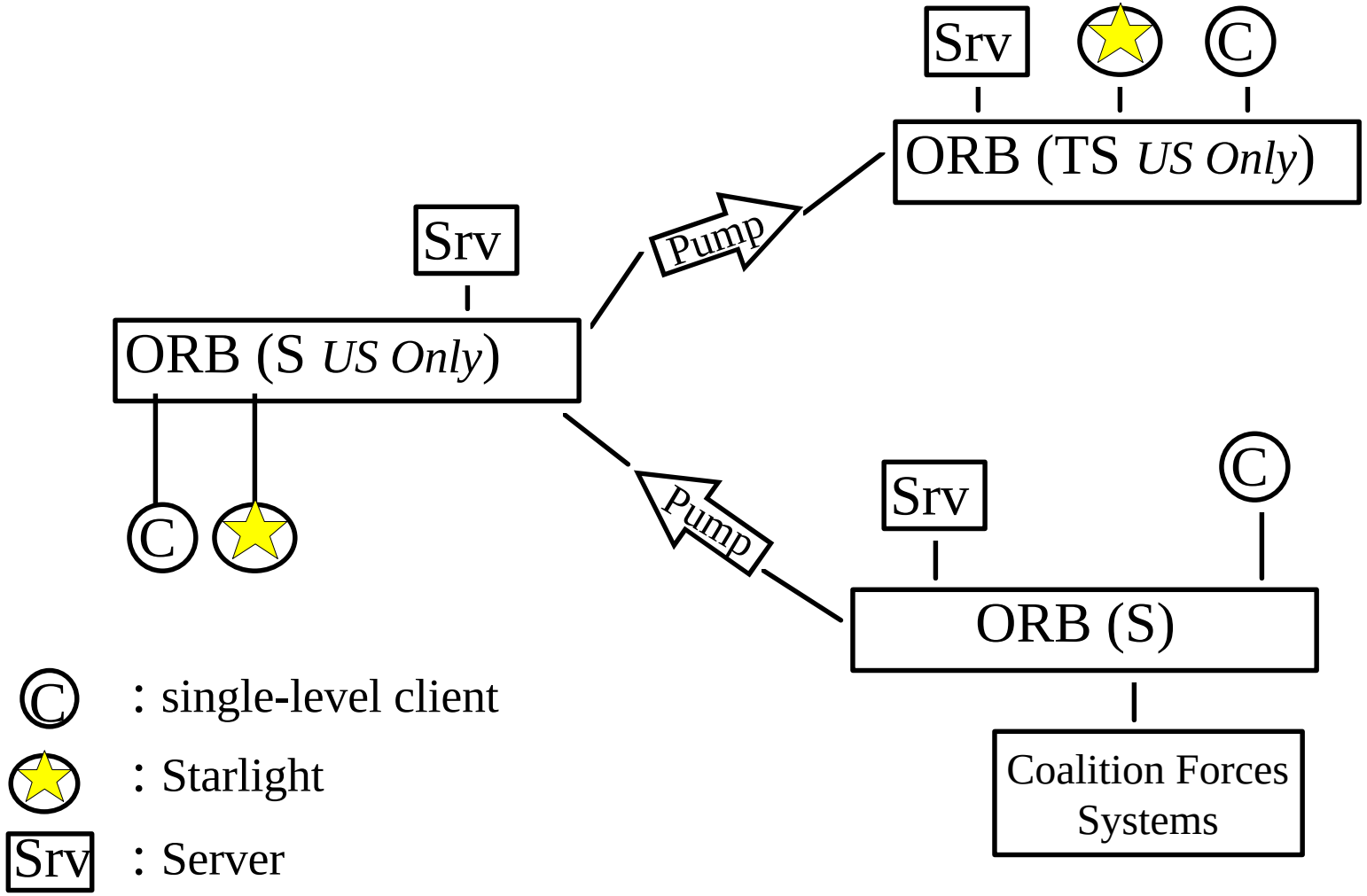
Architecture to enforce information flow policy

MLS Client and Server Functions



Achitecture to enforce information flow policy

MLS System with Single Level COTS CORBA Clients and Servers



Detection Objects and Filters

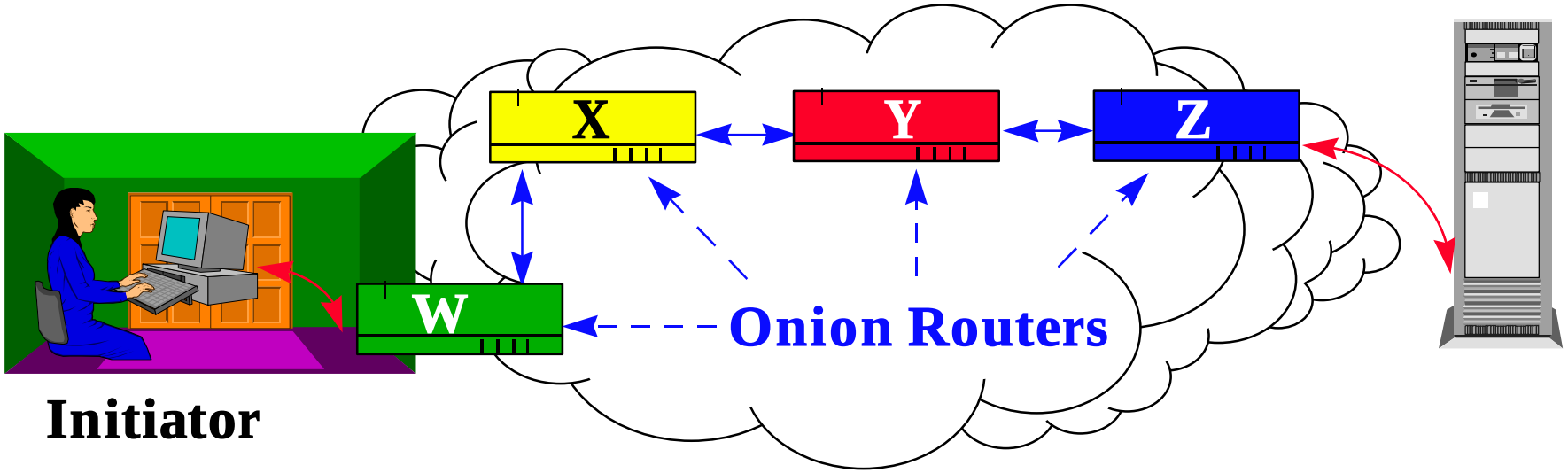
- COTS DBMS integrity controls defend primarily against errors and accidents, sometimes against fraud
- DoD needs protection against more subtle and malicious attacks
- Detection objects (McDermott) can be used with COTS DBMS to reveal such attacks

- Data propagated from Low to High may carry viruses or malicious code of various sorts
- If there is a single upward path, virus checkers and filters of various sorts can be used to check data before it is transmitted upwards (COSPO one-way link)

Components to protect DBMS access against traffic analysis

Onion Routing

Proxies hide infrastructure for anonymous communication from users and applications

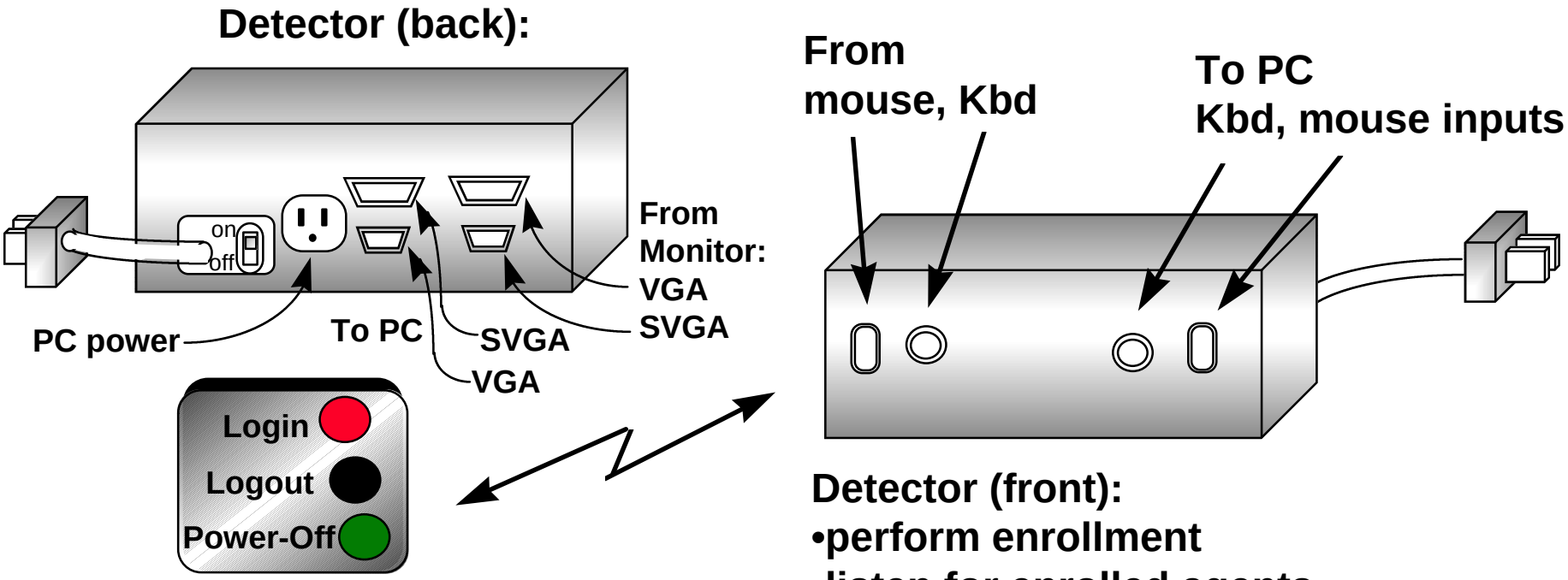


Internet routers cannot determine who is talking to whom.

Components to provide continuous authentication

Wireless Identification System

- State of the practice for DBMS authentication: passwords
- Needed: system that provides user-friendly authentication and can detect when user leaves the workstation



Agent (transceiver):
•compute / transmit ID code
•signal power down/departure

Detector (front):
•perform enrollment
•listen for enrolled agents
•enable / disable kbd, monitor, mouse

Conclusion

Needed: Architectures and Components

Expect:

- Increasing integration of data management systems
- Increasing pressure to provide security at low cost
- Increasing pressure for architectures that can incorporate COTS and legacy systems

DoD should move toward data management architectures that rely on

- Simple, high assurance components to enforce DoD-specific policies
- COTS to enforce security policies where COTS threat models are valid

NRL is developing components and demonstrating architectures to meet these needs