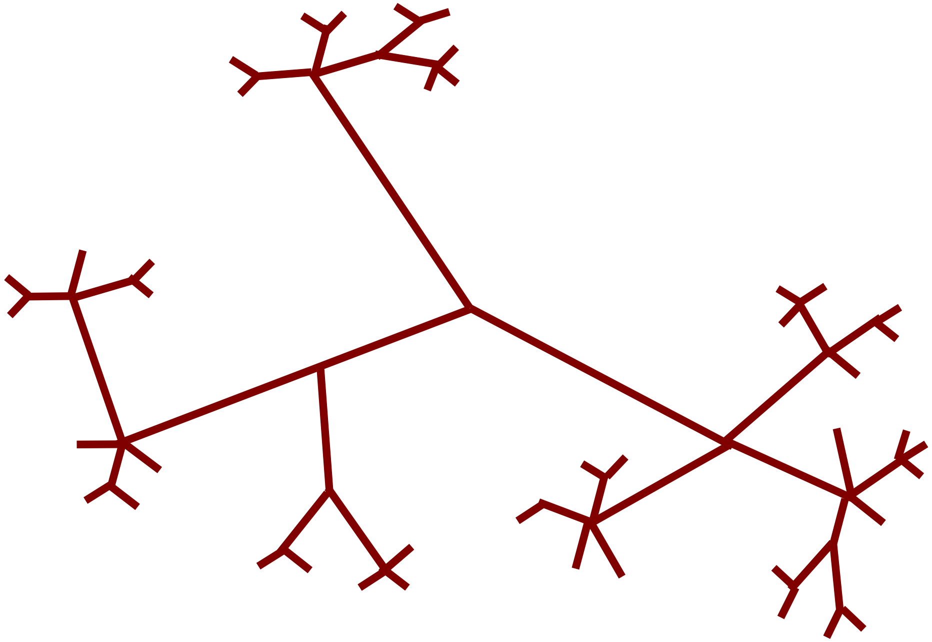
IBM Zürich Research Laboratory

Billy Goat Overview

James Riordan
Diego Zamboni
Yann Duponchel
IBM Research Zurich Switzerland

© 2006 IBM Corporation

Short Worm Summary

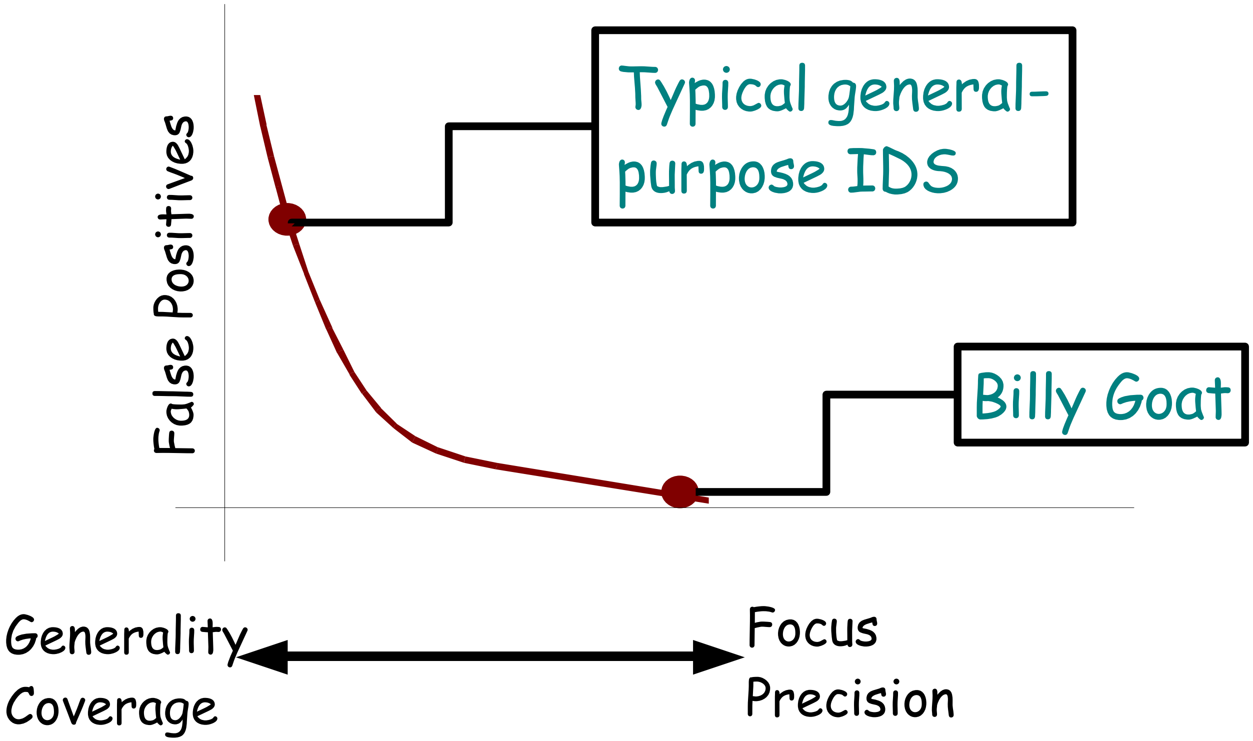


- Attackers, attacks, worms,...
  - Faster propagation with faster networks
  - Ever greater numbers
  - Increasingly sophisticated
    - Optimized propagation
    - Modular with respect to exploits
    - Multi-vectored
    - Stealth and explosive (hot lists)
    - Parasitic worms
    - Worm authors learning from virus techniques

- Resulting in
  - Direct damange
  - Poor user experience
  - Wasted bandwidth
  - Dis-infection costs
  - DDOS Zombies
  - Firewall tunnels
  - Potential liability

© 2006 IBM Corporation

Precision versus focus



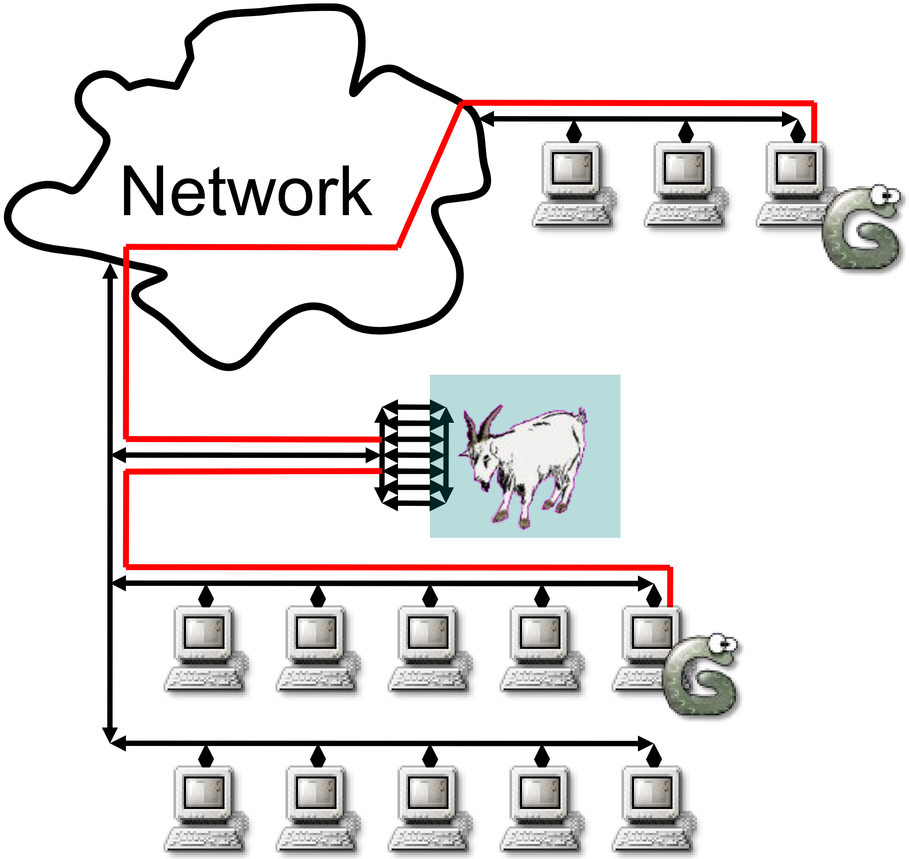
Typical general-purpose IDS

Billy Goat

Generality
Coverage

Focus
Precision

Billy Goat overview: the basic idea



- Billy Goat is an intrusion detection sensor
  - Virtualization of unbound address subnets
    - Catches only traffic that should not exist
    - First person participant in protocols
    - Try to download actual worm code
  - Very low false positive rate
  - Modular alarm and reporting infrastructure
    - Policy based
    - syslog, TEC, e-mail, database,...
  - Well suited toward automated attack
  - Example: Zurich Research Lab BG spoofs existence of ~49,000 different hosts

© 2006 IBM Corporation

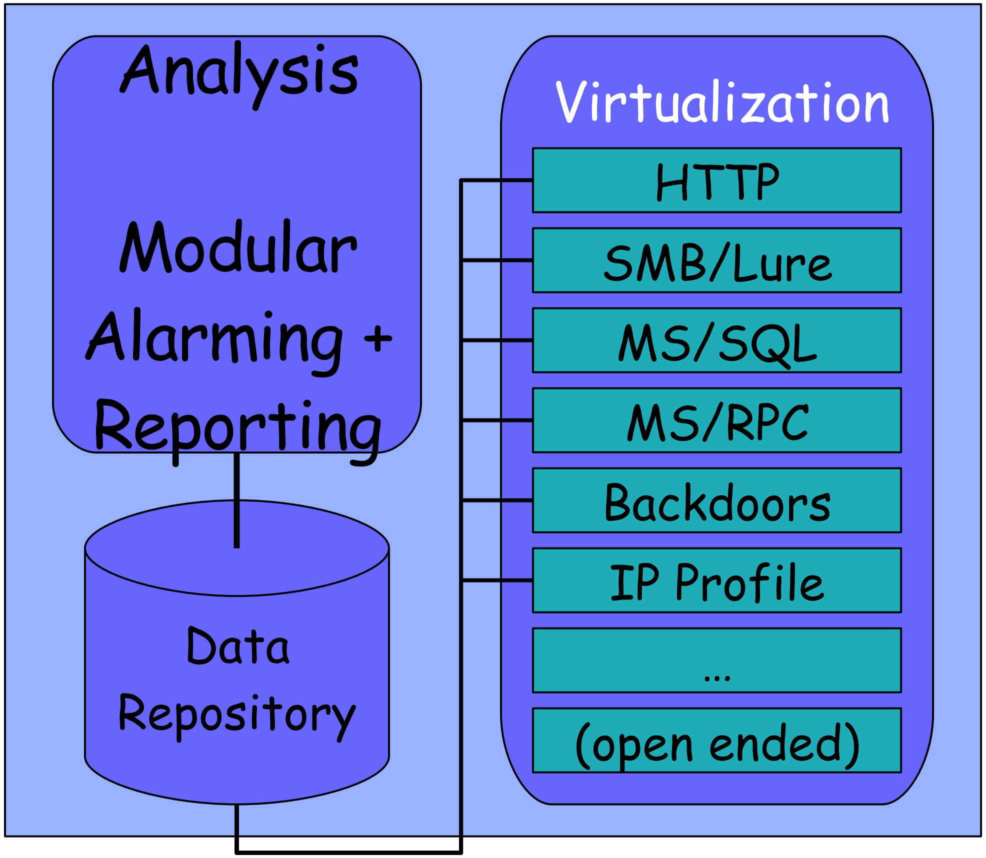
Engineering

- Recovering rather than resistant
- Cryptographic checksums for database keys
- SMB/Lure idea
- One way database synchronization
- Very low deployment effort (encourage grass roots)
  - Boot a live Linux distribution...
  - `wget -O- -q https://billygoat/myconfig.xml|/bin/sh`
- Inter-operating components vs. übersystem
  - e.g. created an isolation system based on VLAN tags, plug the two together and we have automated intrusion response
- Using IBM's BEEPLite implementation of BEEP
  - http://www.beepcore.org

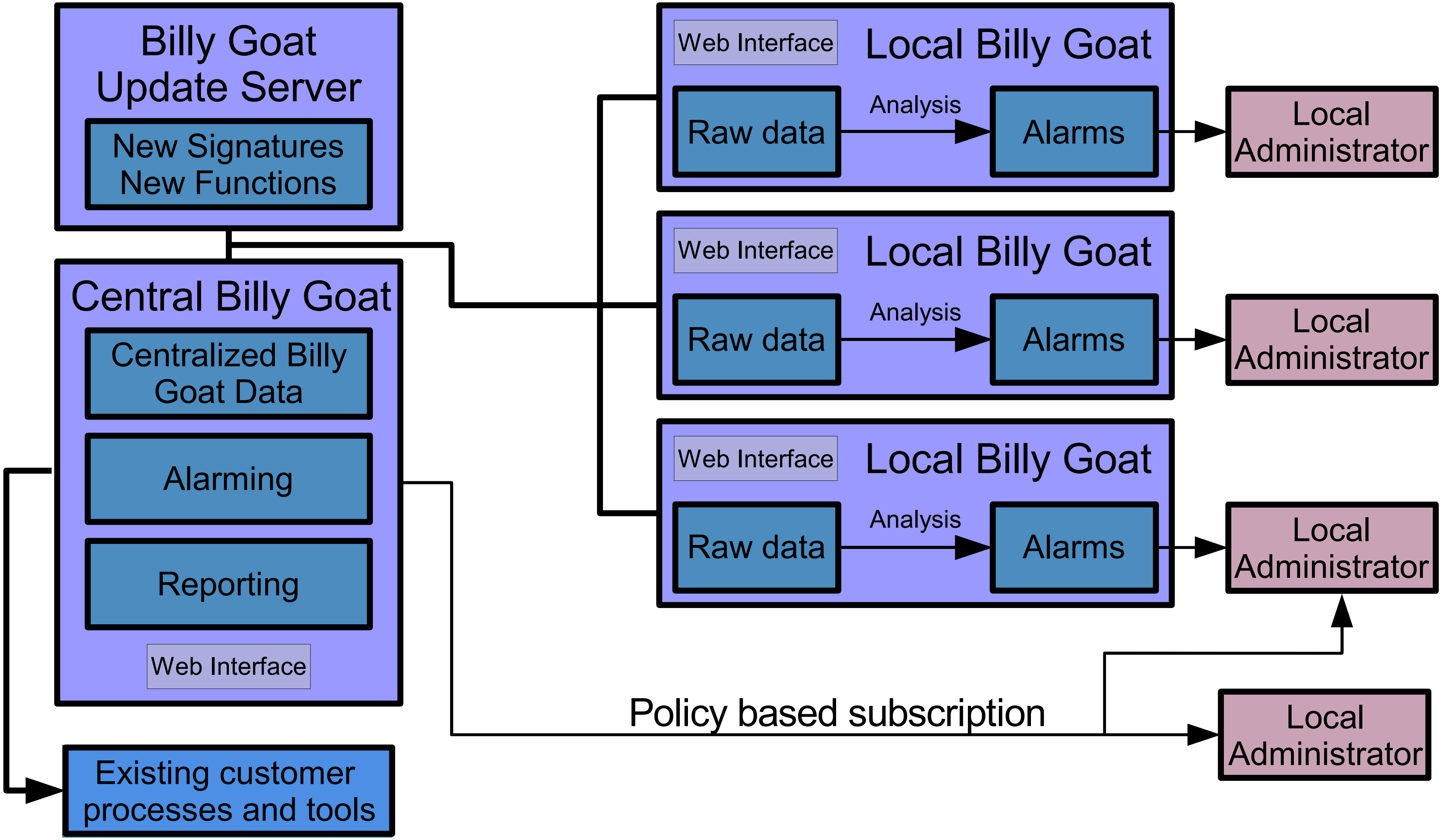
© 2006 IBM Corporation

Billy Goat overview: individual sensors

- Many application-layer sensors
  - HTTP, HTTPS, DCOM, MS/SQL, Kerberos,...
  - SMB/Lure (based on Samba)
  - e-mail worm backdoors (MyDoom, beagle.b, beagle.e,...)
  - General purpose TCP/UDP
  - Open ended and easily expandable
- Traffic anomaly (IP profiling)
- On-box correlation
- Relationship to honey pots
  - Not advertised (hence all traffic suspicious)
  - Hardened machine (difficult to crack)
  - No real services offered



Distributed Billy Goat Architecture



Integration into security system as a whole

- Originally alarms
- Simple web page for dig down

- Information integration platform
  - Data presented as "semantic" XML at various URLs
    - `http://billygoat/topattacks.xml?n=10`
    - `http://billygoat/topattackers?n=10&network=9.4.0.0/16`
  - Presentation via XSLT stylesheets
  - Service descriptions via RDF and web ontologies
  - Enables automatic integration of other data source (local and otherwise)
    - Vulnerability information, NIDS output,....

© 2006 IBM Corporation

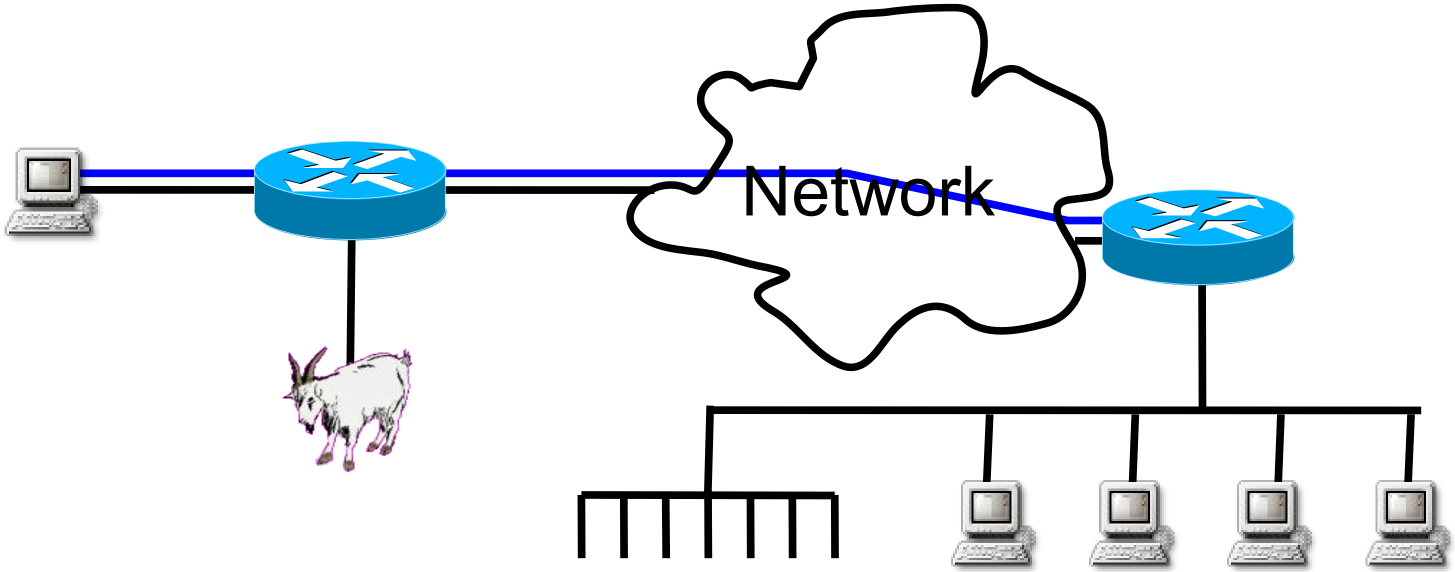
Modes of deployment

- Static route
  - Safe but need to talk with networking people
- ARP spoofing
  - Don't need to talk with networking people
  - Very dangerous
- BGP
  - Automatically adapts to network
  - Potentially dangerous
  - Lessons for intrusion response
- ICMP based
  - Huge address space, locally relevant information
  - Potentially dangerous

© 2006 IBM Corporation

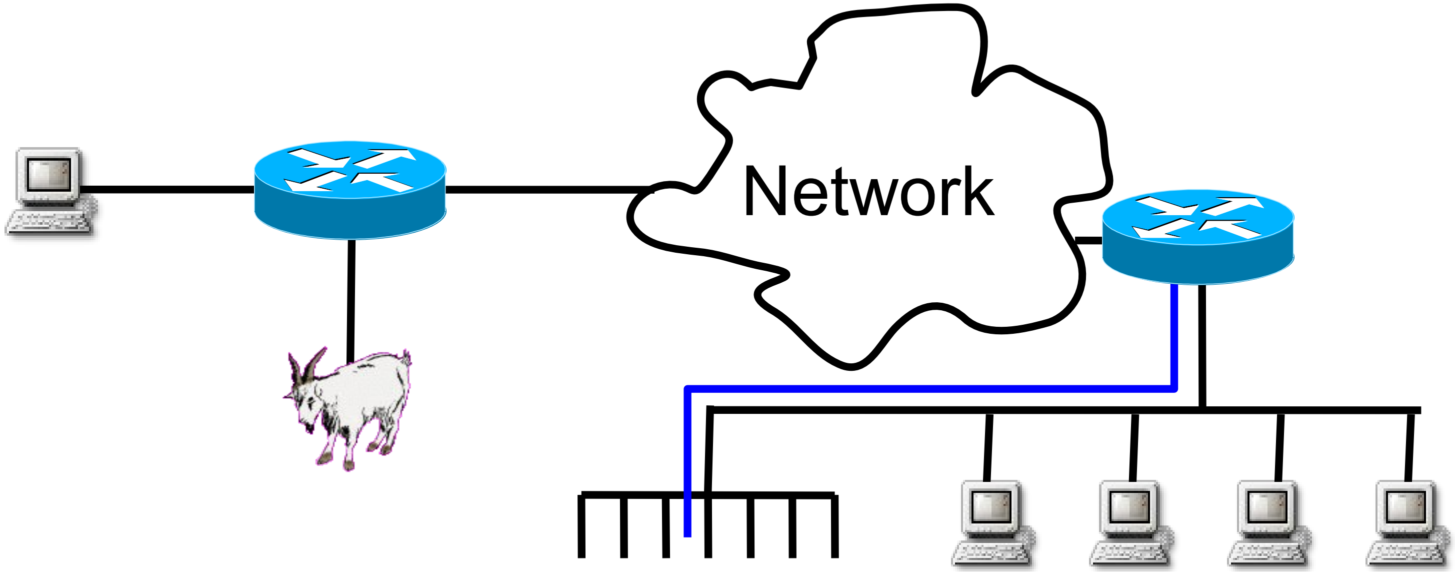
Router Based Billy Goat

1. Worm tries to contact remote host
2. Remote router ARPs for host
3. Remote router returns ICMP (net or host) message
4. Local router intercepts ICMP and sets local route
5. Worm retransmits to Billy Goat



Router Based Billy Goat

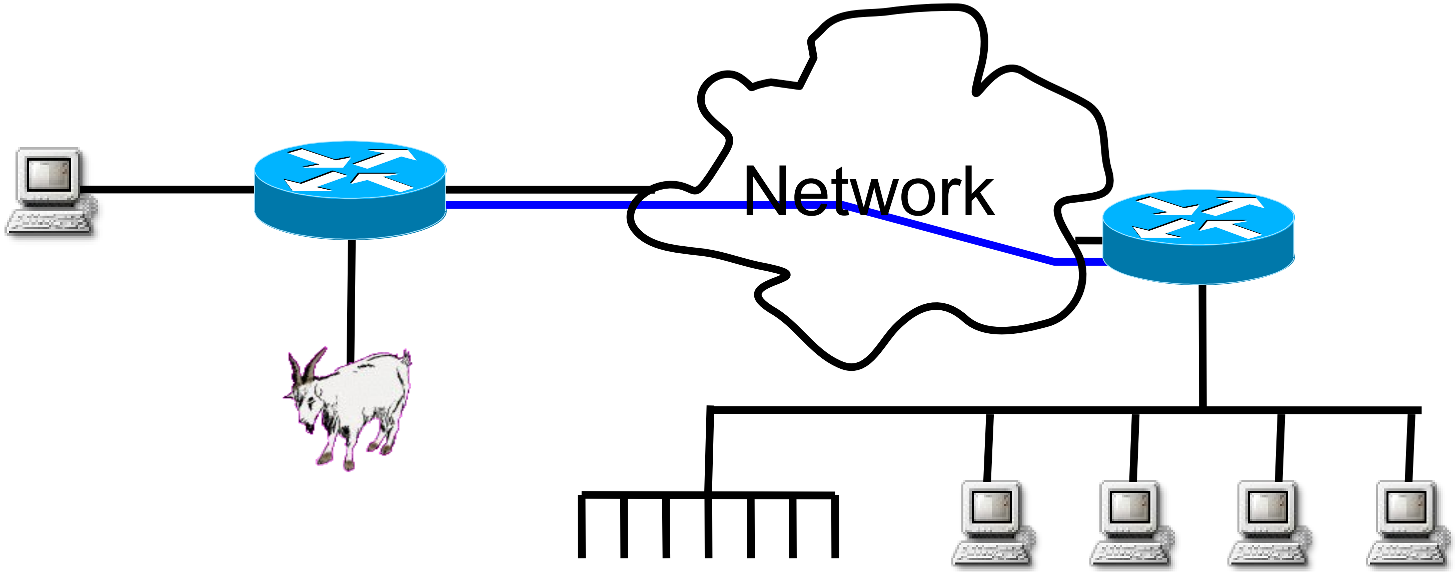
1. Worm tries to contact remote host
2. Remote router ARPs for host
3. Remote router returns ICMP (net or host) message
4. Local router intercepts ICMP and sets local route
5. Worm retransmits to Billy Goat



© 2006 IBM Corporation

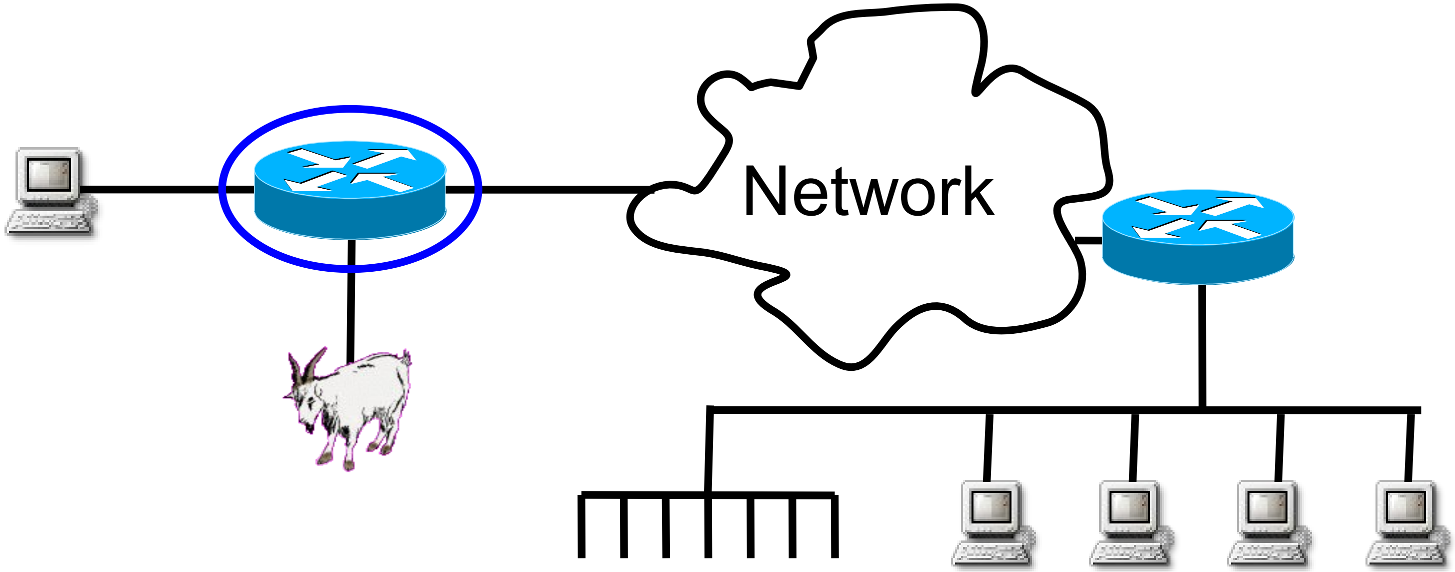
Router Based Billy Goat

1. Worm tries to contact remote host
2. Remote router ARPs for host
3. Remote router returns ICMP (net or host) message
4. Local router intercepts ICMP and sets local route
5. Worm retransmits to Billy Goat



Router Based Billy Goat

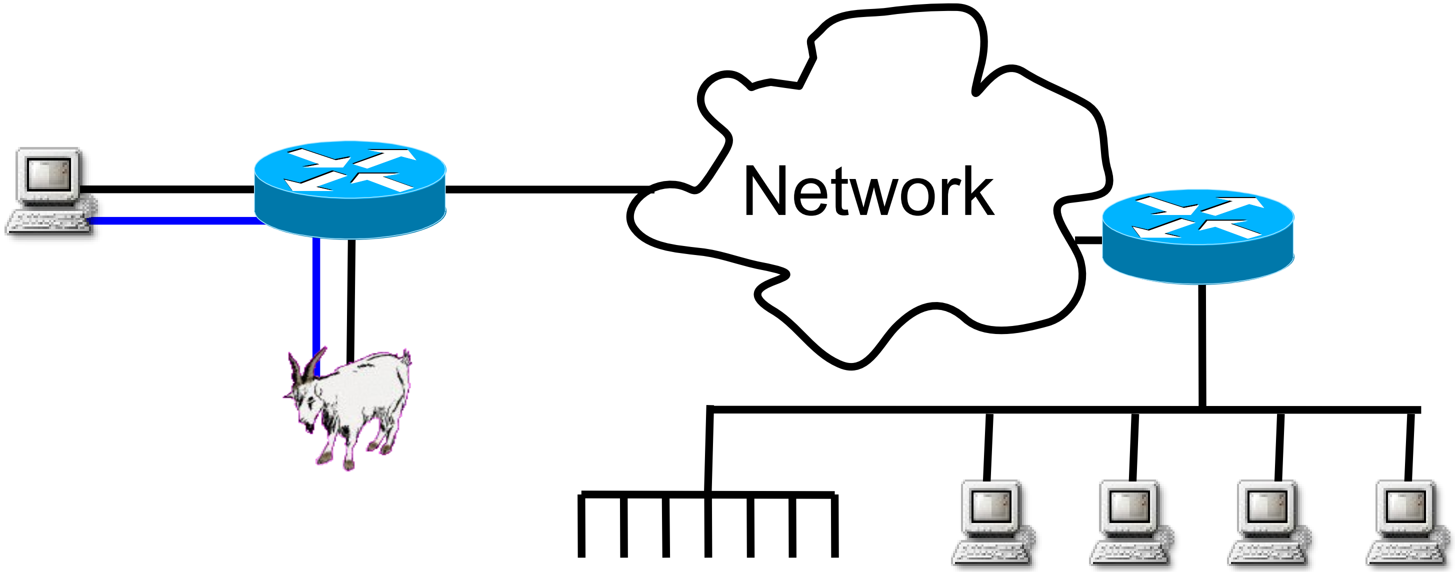
1. Worm tries to contact remote host
2. Remote router ARPs for host
3. Remote router returns ICMP (net or host) message
4. Local router intercepts ICMP and sets local route
5. Worm retransmits to Billy Goat



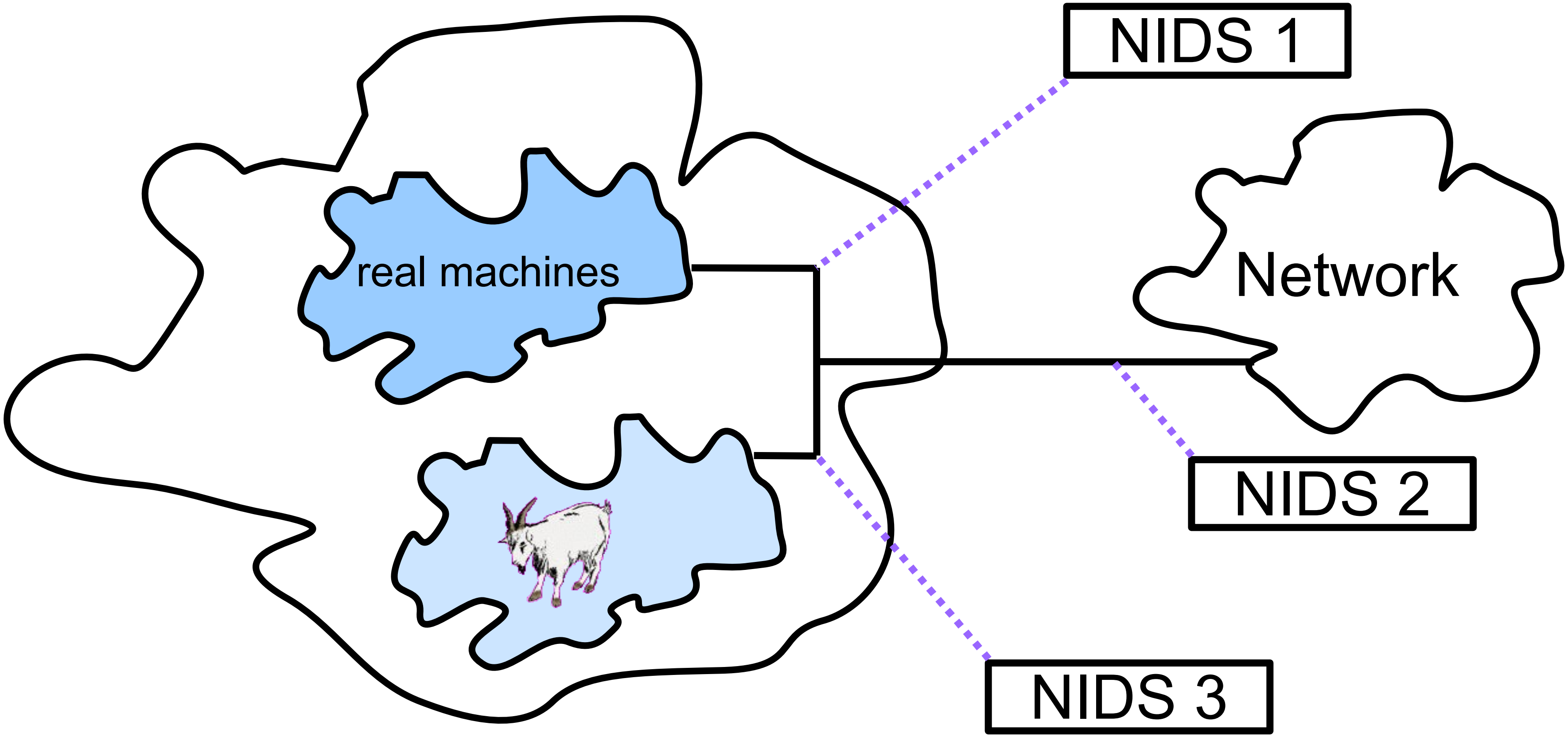
© 2006 IBM Corporation

Router Based Billy Goat

1. Worm tries to contact remote host
2. Remote router ARPs for host
3. Remote router returns ICMP (net or host) message
4. Local router intercepts ICMP and sets local route
5. Worm retransmits to Billy Goat

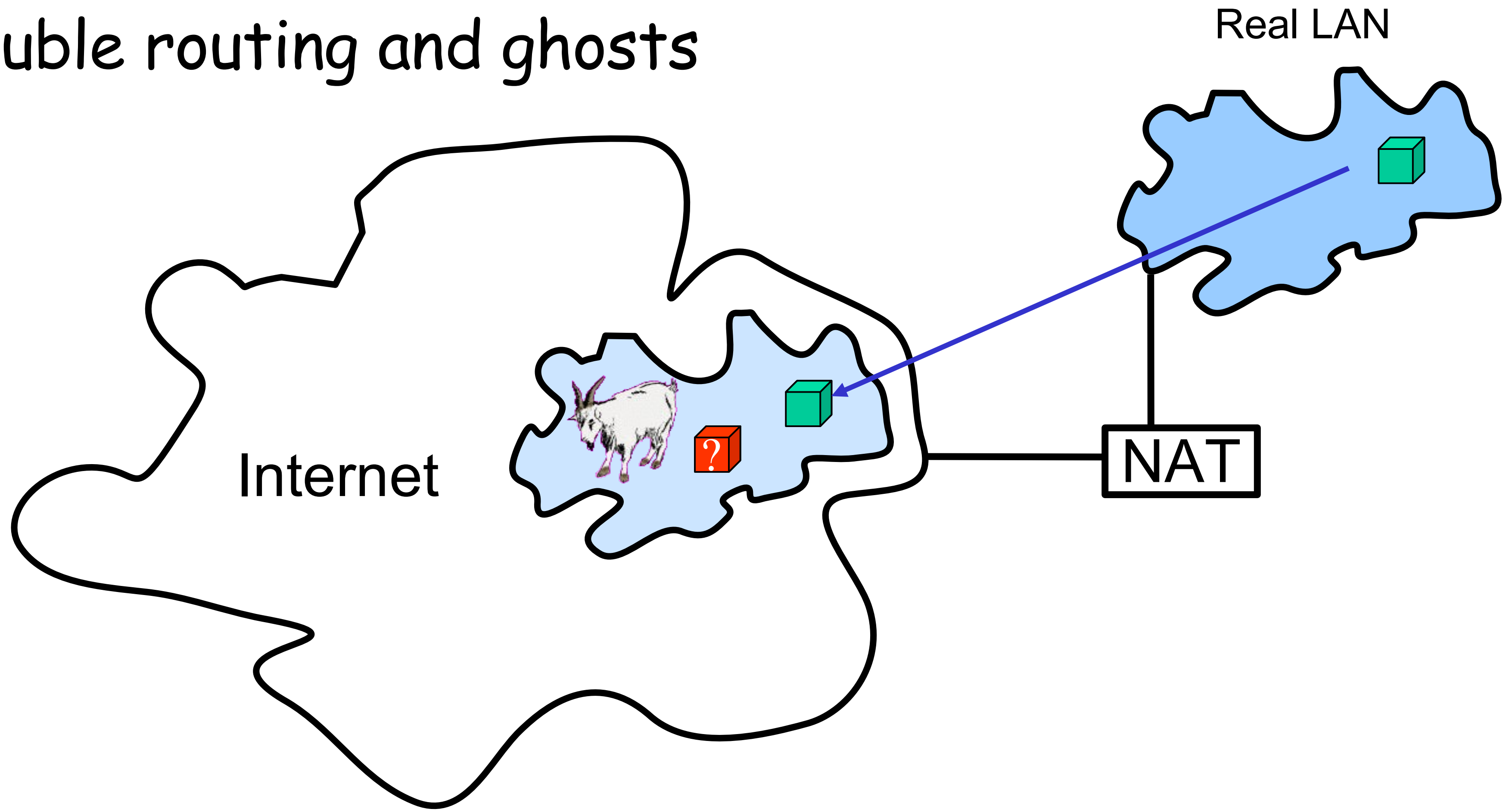


Effect on network sensors



© 2004 IBM Corporation

Double routing and ghosts



© 2004 IBM Corporation

Summary

- Billy Goat is an very accurate intrusion detection sensor
  - focused rather than general
    - Value is in integration
  - detects and identifies network worms
- Several existing and planned deployments
  - IBM intranet
  - Several customers
  - Internet (early warning system)

© 2006 IBM Corporation