Network Security:

New Essentials for Safeguarding Network Systems

IEEE LCN2007

October 16, 2007

Alan Crouch
Director and General Manager
Communications Technology Lab

Security Concerns are Impacting Business and Consumers…

"Approximately 150 to 200 viruses, trojans and other threats emerge each day."[1]

"Underground hackers are hawking zero-day exploits for Microsoft's new Windows Vista operating system at $50,000 a pop"[2]

Time to exploit vulnerability ~6.8 days. Time from vulnerability exposure to patch availability ~49 days.[3]

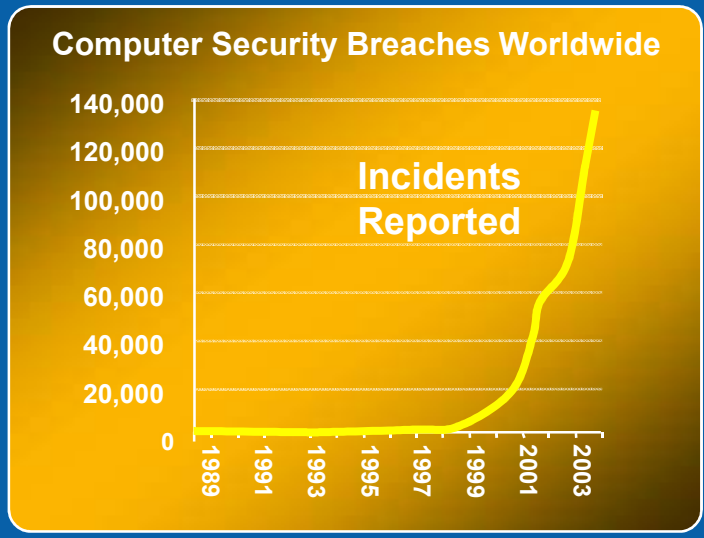
Country-wide botnet based cyber attacks cause significant disruption[4]

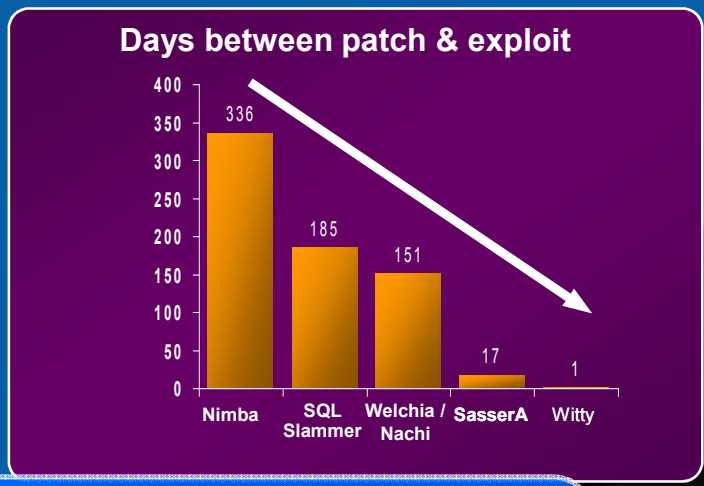
"50% of consumers are concerned about their financial information being safe online. 24% performed fewer transactions online as a result."[5]

1. McAfee, 2006
2. eWeek.com, Dec 15, '06
3. Symantec Internet Security Threat Report Trends for July 05 – December 05
4 http://www.technologynewsdaily.com/node/7032
5. Consumer affairs poll, May 2006

… and are a Top IT Concern

- New security challenges
  - Not just fast spreading worms
  - Rising stealthy attacks
  - Rootkits & system bots
- Software patch management alone is insufficient
- Attack virulence makes manual intervention ineffective
- Device Proliferation: pocket-able internet devices mean both ***new devices*** and ***new local nets*** (CSLL, ON-MOVE, etc) to attack





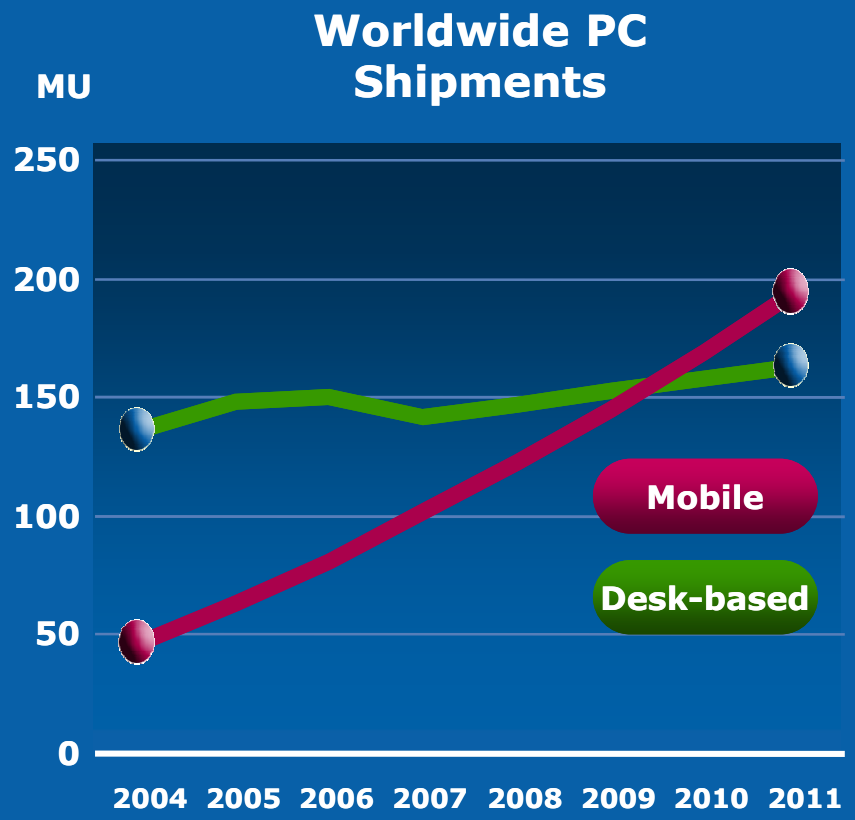
Security *is Costing Billion's of Dollars in* ***Operation*** *and* ***Lost Productivity***

Source: Forrester

Source: Computer Emergency Response Team

The Problem is Only Getting Worse

- Intelligent and devious intruders
  - Constantly finding and exploiting vulnerabilities
- Mobile shift adding complexity
  - Fixed perimeters and physical controls no longer adequate
- Insider attacks defeat enterprise perimeter solutions
- Financial gain becoming motivation for malware



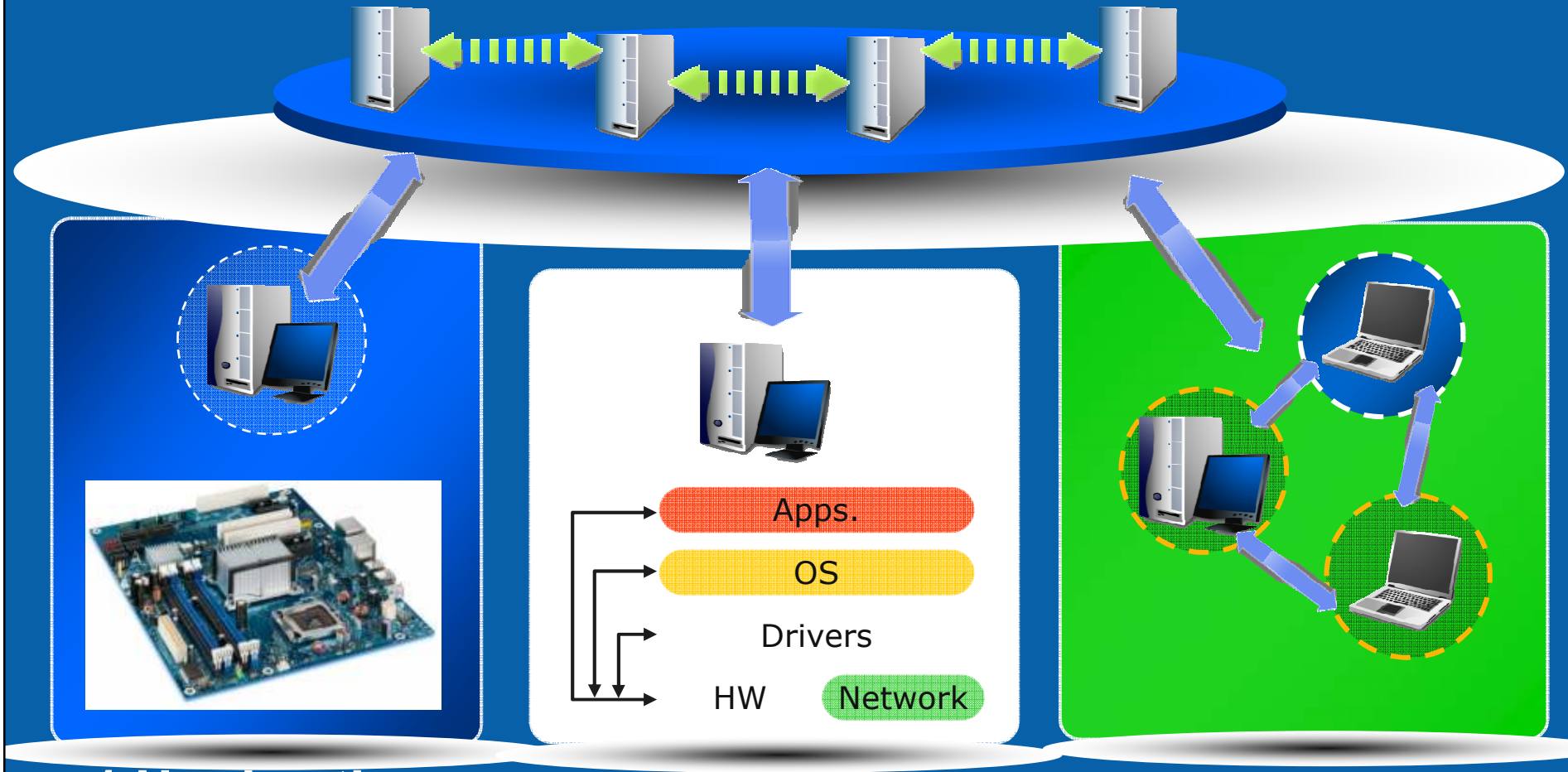
New Security Paradigms Needed

Security Doesn't Come for Free

- Performance Impact
  - Security Tax = Overhead
  - Overhead is not trivial
  - Overhead is not one time payment
  - Overhead is additive
- System Scalability
  - Scalability = consistent protection as system complexity grows
    - Number of nodes
    - Bandwidth/line rates
    - Usages/SW applications

Today's security solutions optimized for *Performance or Scalability*

Layers Provide Scaleable Performance



1 Harden the Platforms

2 Secure the Links

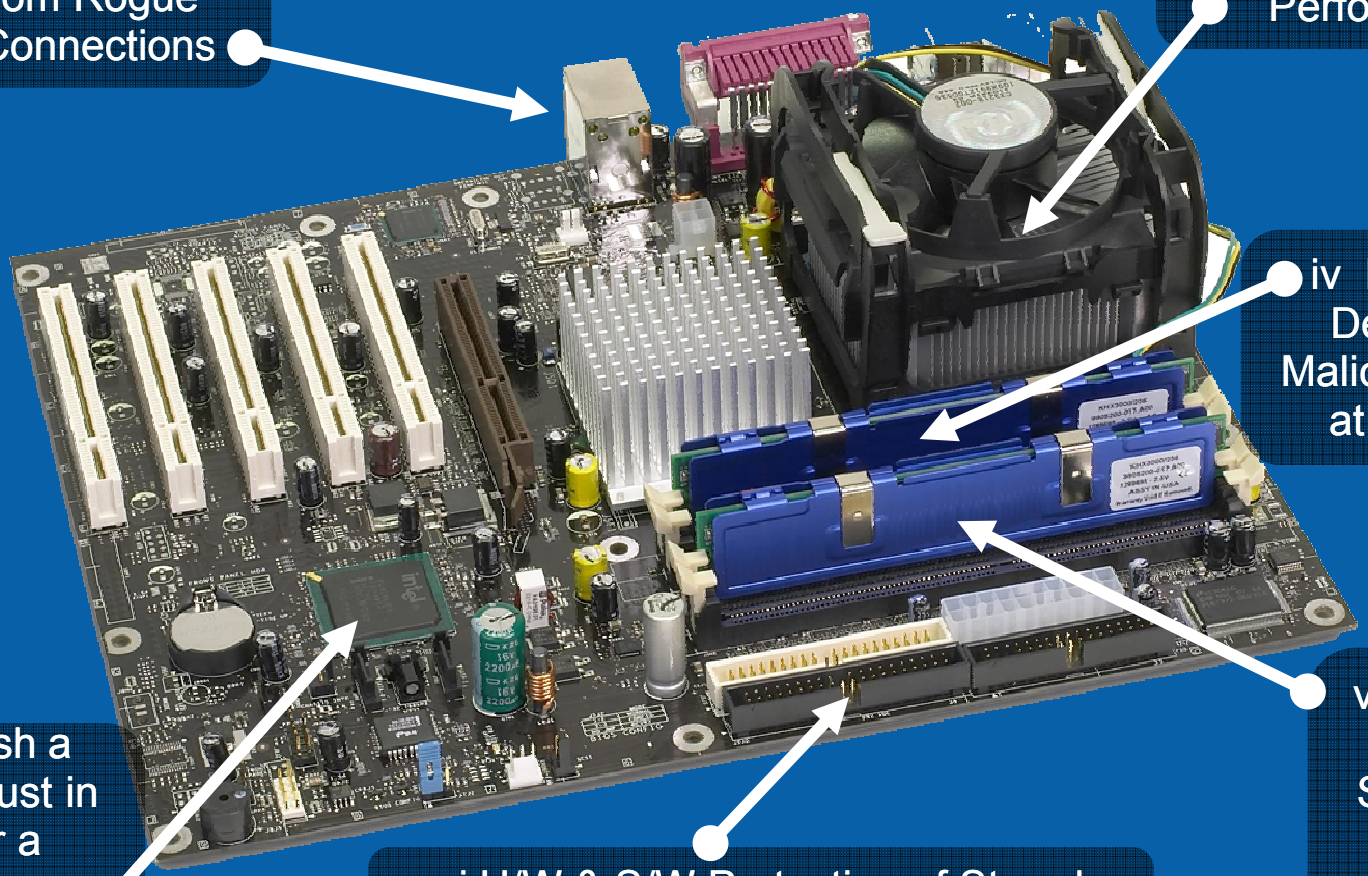
3 Leave Nowhere to Hide

4 Collaboration

1 Harden the Platform

ii Access Controls to Protect from Rogue Network Connections

iii New Instructions for Cryptography Performance



iv H/W-based Detection of Malicious Attacks at Run Time

i Establish a Root-of-Trust in H/W for a Secure Foundation

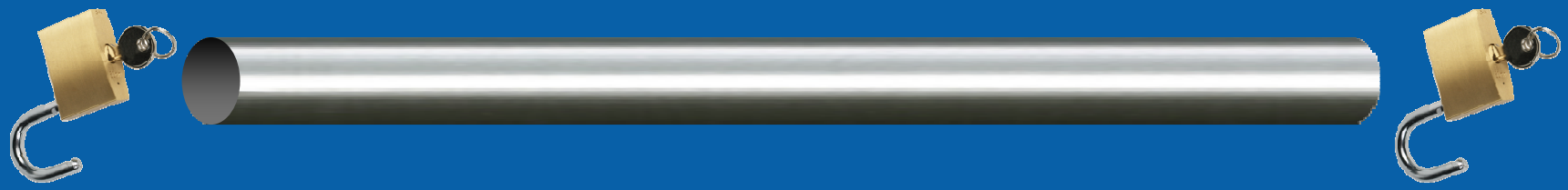
vi H/W & S/W Protection of Stored Data at Rest and In Transit

v Protection of Known-Good Software from Run Time Attacks

Applies to all distributed systems:
Server, Router/Switch, PC, Notebook, MID

2 Securing the Links: End-to-End Confidentiality

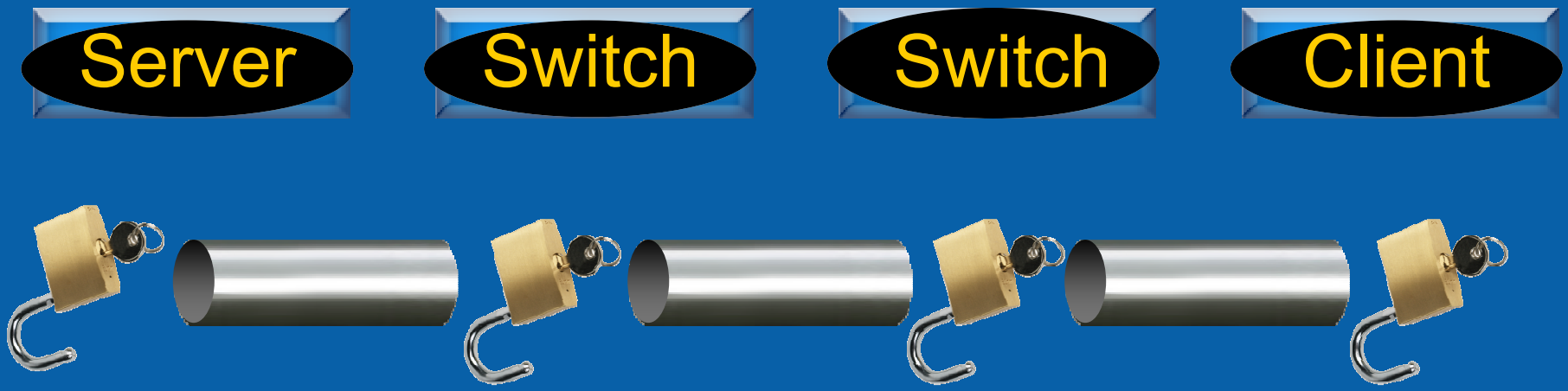
IPSec – End-to-End Encryption



- End to end solution: Valuable for encrypting IP Layers, not suitable for link layer threats
- Issues with scalability and manageability
- Complementary solutions:
  - LinkSec
    - Converts end-to-end protection into link-by-link protection
  - Secure Network Enclaves
    - Builds on LinkSec, current area of active research
    - Provides end-to-end solution with manageability

Securing the Links: LinkSec

- Traffic available for analysis at IT-controlled switching points
- Protects against eavesdropping hackers



LinkSec – Hop-to-Hop Encryption

LinkSec Demo

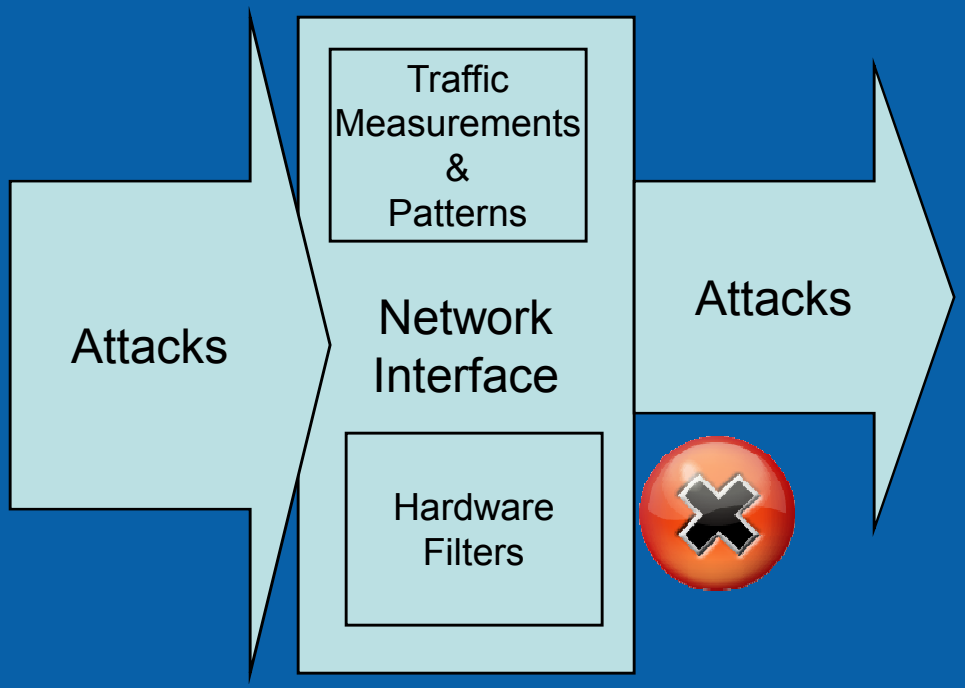
3 Secure Network Enclaves: Leave Nowhere to Hide Current Research Emphasis

- Integrates the best approaches
  - From End-to-End and hop-by-hop encryption
- Derivation mechanisms trade storage for computation
- Permits manageability and IT-visibility into traffic
- Scalability based on coordinated key management

Performance based on hardware support at nodes

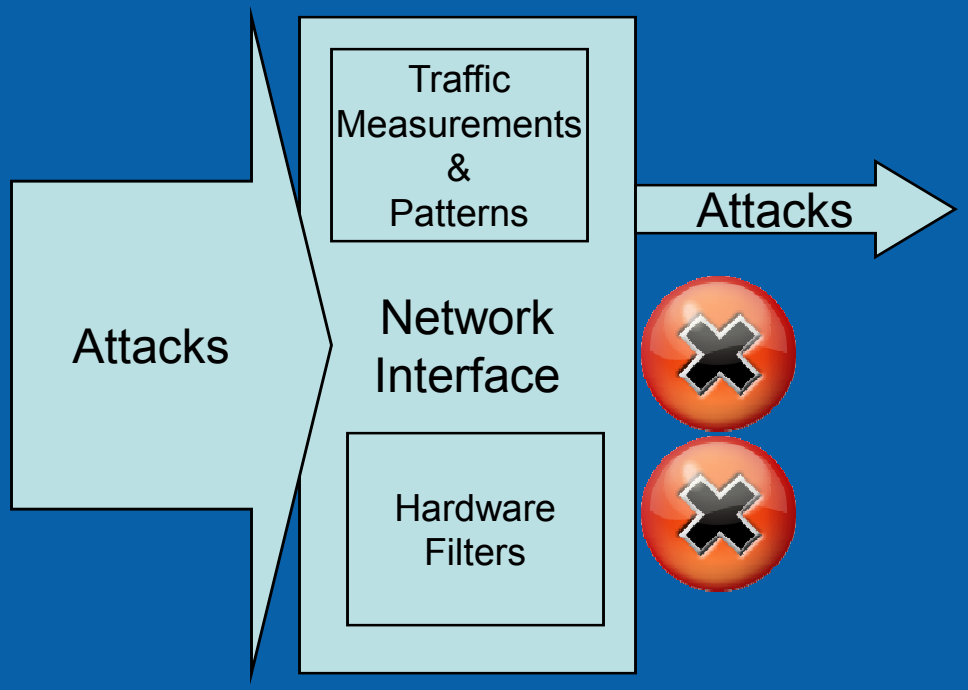
4 Collaborative Defense: Step 1: Hardware Filters

- Hardware filters that look for specific patterns in the data
- Cannot be subverted by modifying the software
- Deployed in Intel platforms today (AMT)

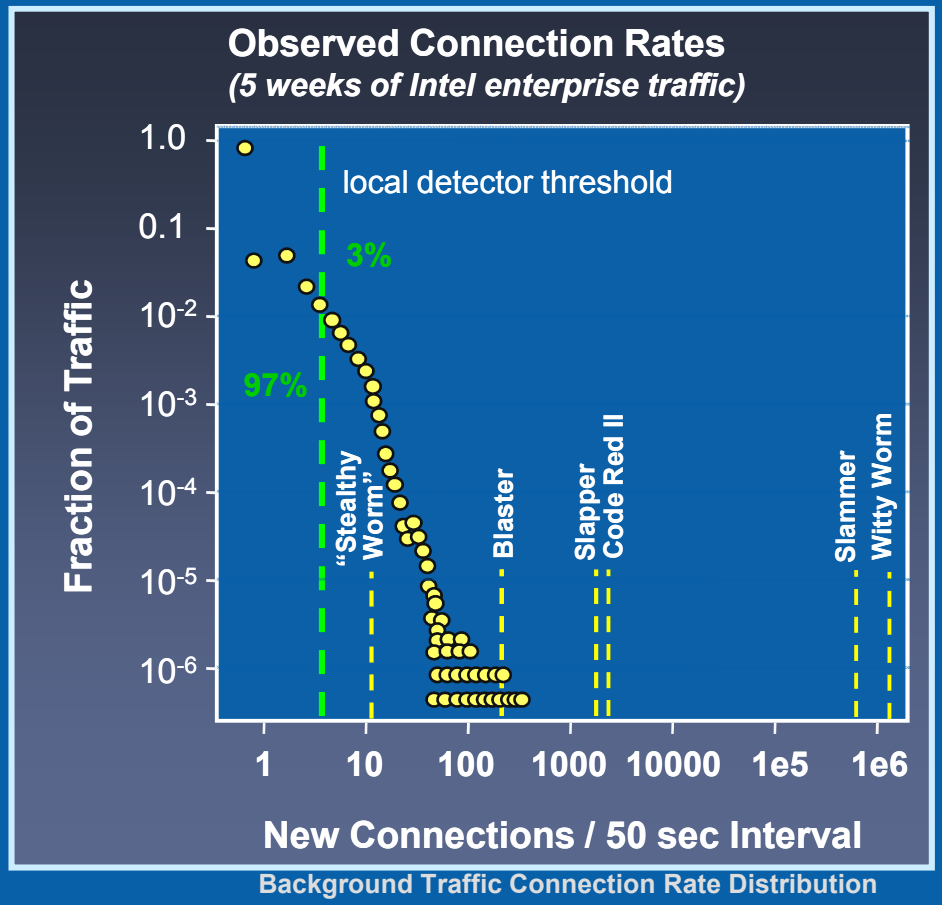


Collaborative Defense: Step 2: Heuristics

- Rules that encode typical behavior of malware
- Multi time-scale rules capture known worms
- Worms that remain "hide" in the background traffic



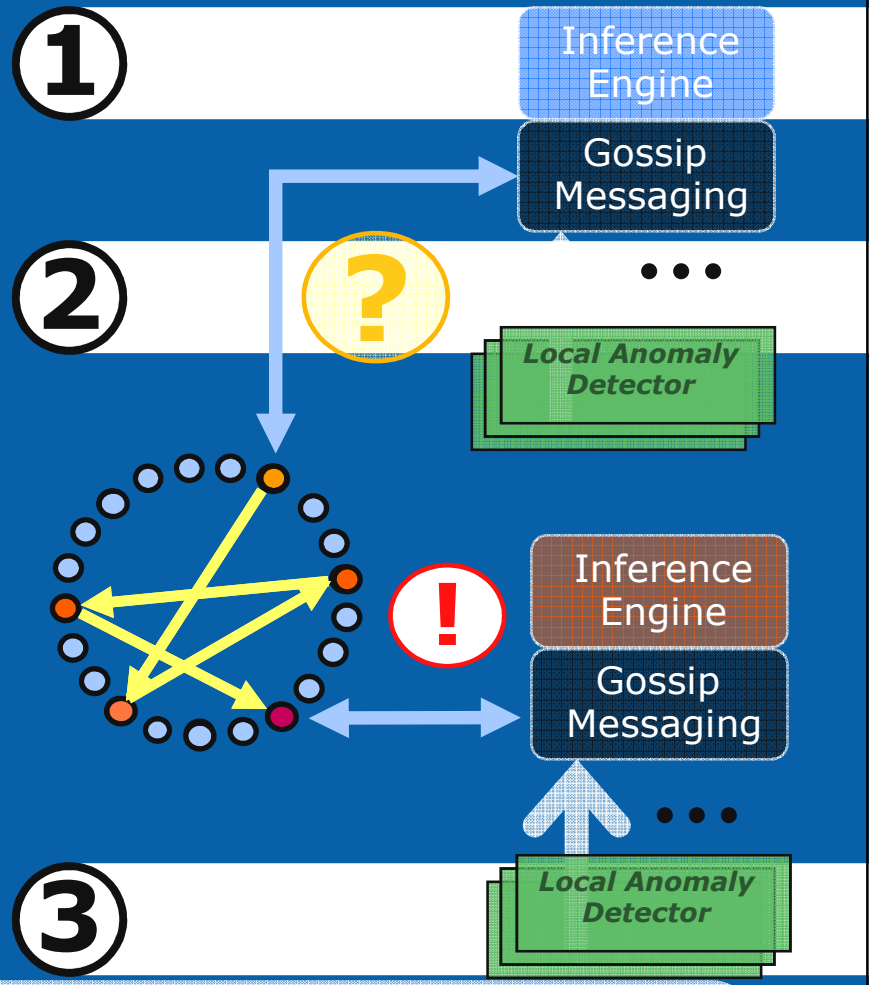
Rules are not Enough – Attacks are Evolving



Challenge is to reduce threshold of detection without increasing false alarms

Collaborative Defense: Step 3: Inference and Gossip

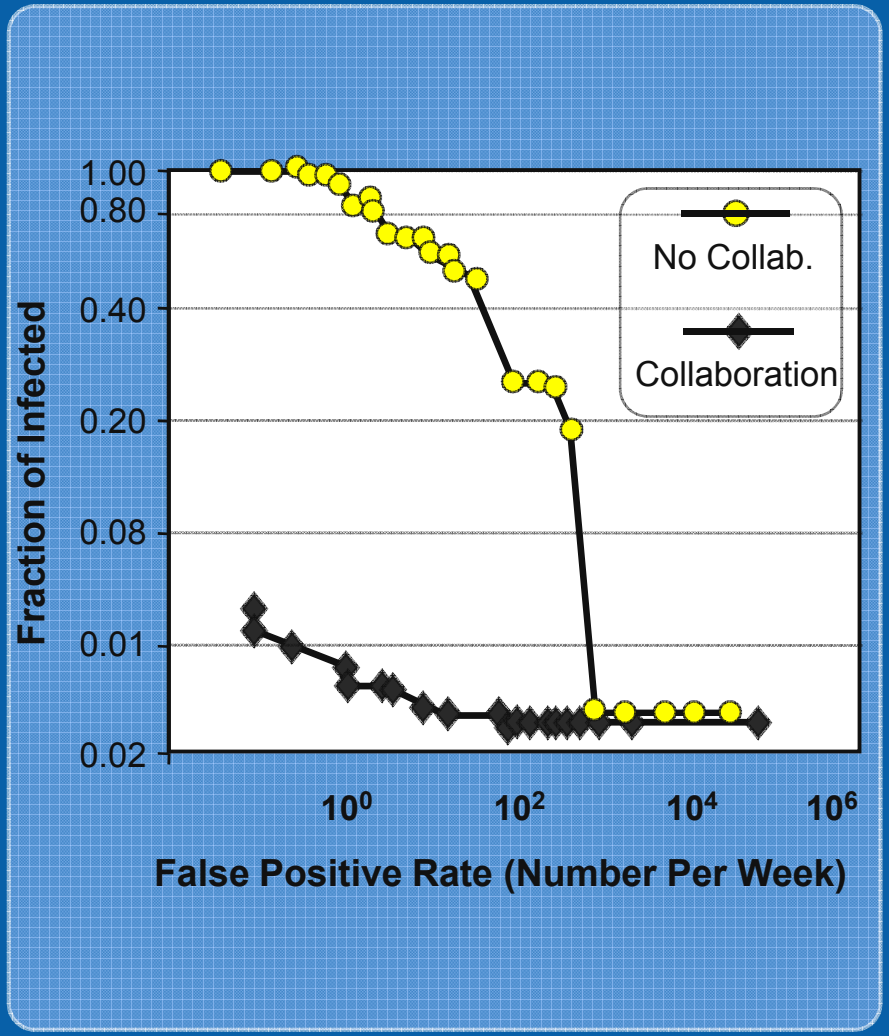
- Employ probabilistic inference
  - Correlate events across multiple machines
  - Combine weak hypotheses into strong evidence
  - Dramatically cut false positives
- Implement scalable, robust messaging protocols
- Design self-configuring local anomaly detectors



Exploiting the power of scale – Making Scale work to our benefit

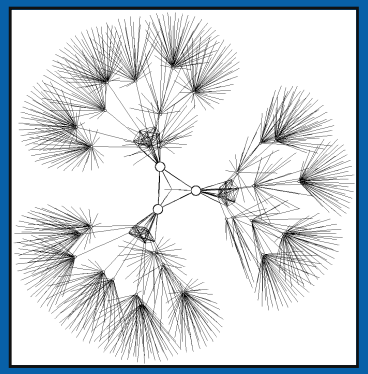
The Results: Gossip is Good

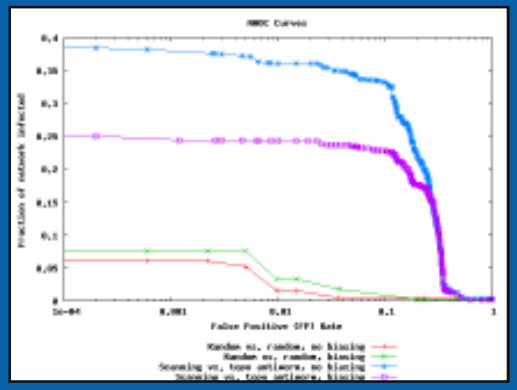
- Collaboration drives false alarms down
  - Allows many simple, but imperfect detectors
- Collaboration roots out stealthy attacks
  - Collect concise local data
  - Put in global correlation framework
- Scalability works in our favor
  - The more participating nodes, the better the performance

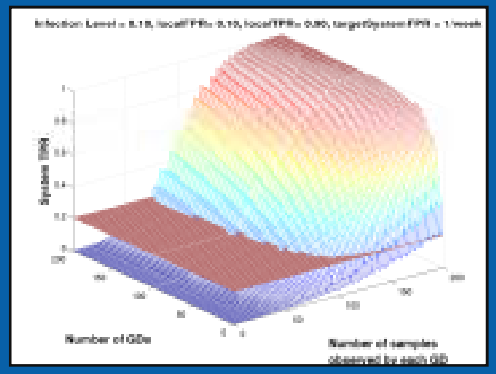


Future Directions

- **Adaptation and Learning**
  - end-hosts and networks are dynamic systems
- **Messaging optimizations**
  - bias to send "bad news" faster
- **Pinpointing suspect systems**
  - exploit topological & historical knowledge







Collaboration between distributed platforms provides major advantages in detecting intrusions

Summary

- **Security remains a top IT problem**
  - Device Proliferation, Mobility, new LCN classes pose major challenges
- **Think about the networked system of platforms**
  - when you consider security vulnerabilities
- **No single solution to rapidly evolving threats**
  - Competing tradeoffs: Performance, Scalability, Simplicity
  - Opportunity: use scalability to our advantage while maintaining performance and simplicity
- **New Essentials for safeguarding LCN systems:** *innovate across multiple layers*
  - 1 Harden the platform
  - 2 Secure the links
  - 3 Leave nowhere to hide
  - 4 Collaborative defense

Let's work together in the LCN research community to create the secure local networks of tomorrow!


intel®
Leap ahead™