Network Security:

New Essentials for Safeguarding Network Systems

June 13th, 2007

Dr. Kevin Kahn
Intel Senior Fellow
Director
Communications Technology Lab

Security Concerns are Impacting Business

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

"50% of consumers are concerned about their financial information being safe online. 24% performed fewer transactions online as a result."[2]

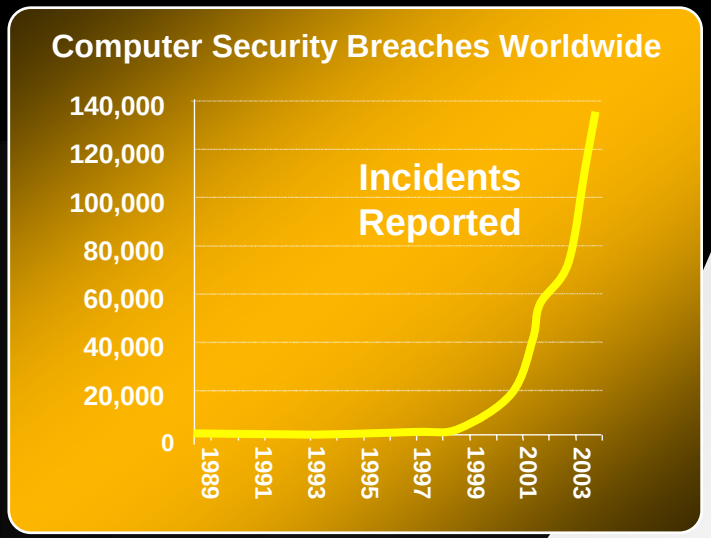
Time to exploit vulnerability ~6.8 days. Time from exposure of vulnerability to patch availability ~49 days.[3]

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

1 McAfee, 2006
2 Consumer affairs poll, May 2006
3 Symantec Internet Security Threat Report Trends for July 05 – December 05 Volume IX, Published March 2006
4 http://www.technologynewsdaily.com/node/7032

And are the Top IT Concern

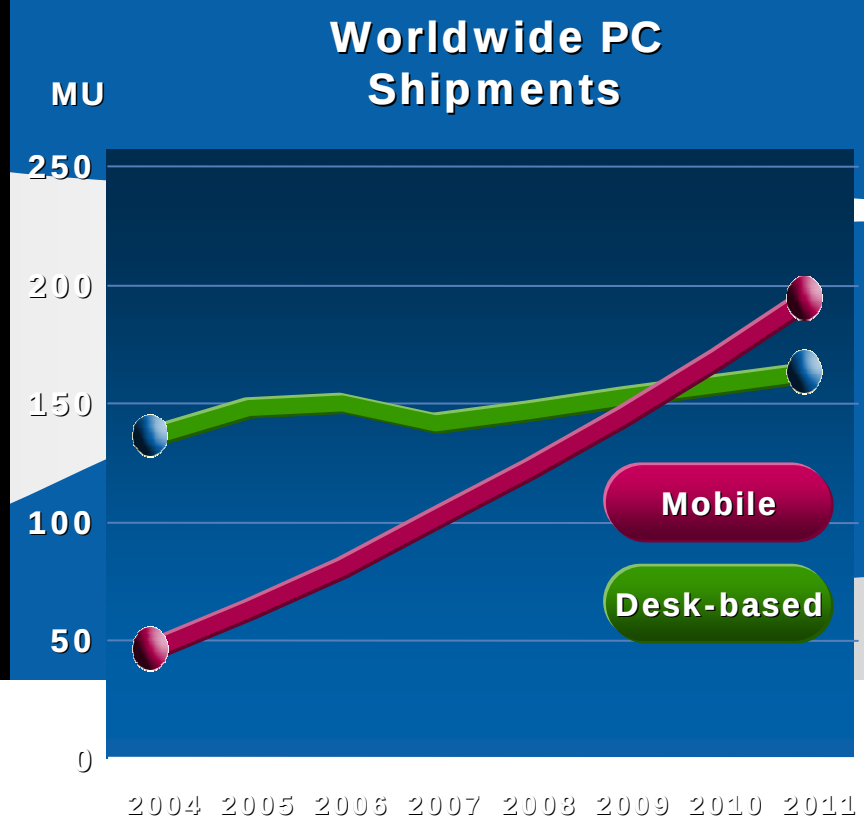
- New security challenges
  - Not just fast spreading worms
  - Rising stealthy attacks
  - Rootkits & system bots
- Software patch management alone is insufficient
- Attack virulence makes manual



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

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



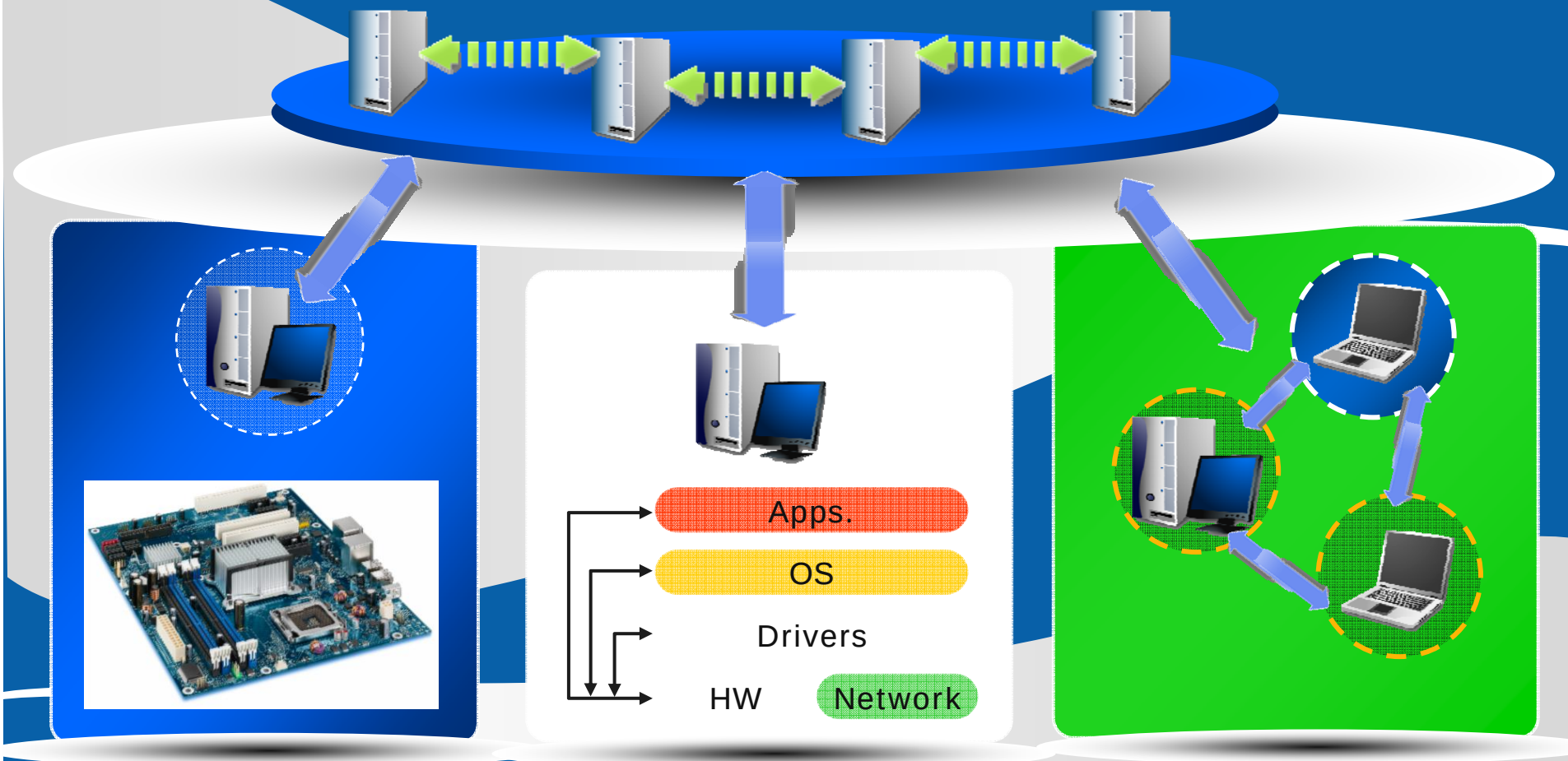
New Security Paradigms Needed

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

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

Layers Provide Scaleable Performance



Harden the Platforms

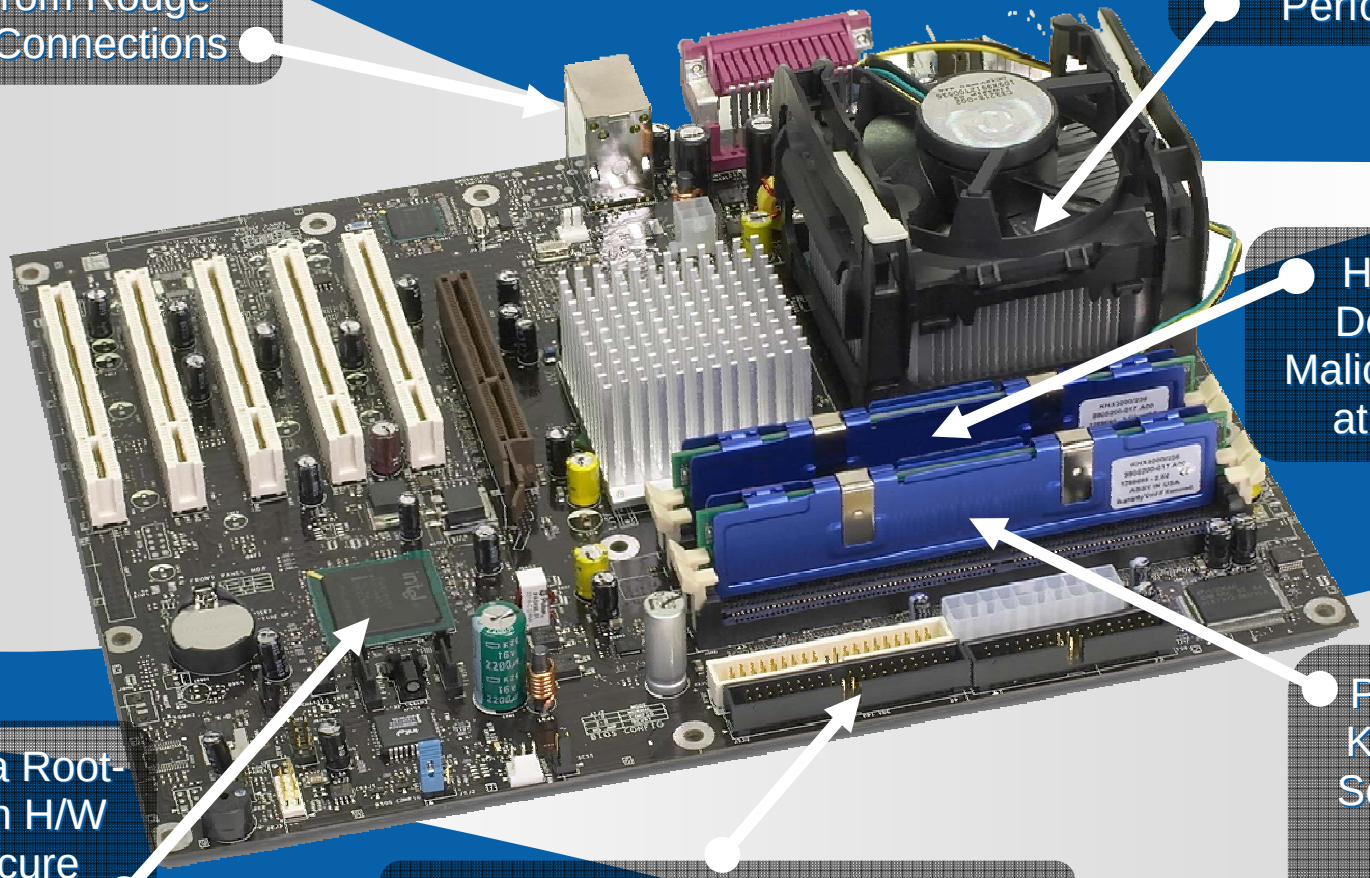
Leave Nowhere to Hide & Secure the Links

Collaboration

Harden the Platform

Access Controls to Protect from Rouge Network Connections

New Instructions for Cryptography Performance



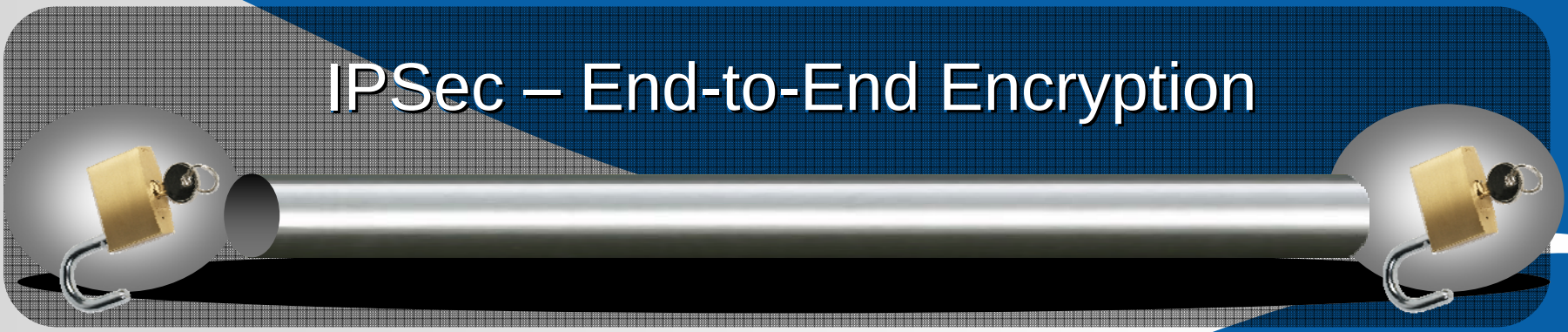
H/W-based Detection of Malicious Attacks at Run Time

Protection of Known-Good Software from Run Time Attacks

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

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

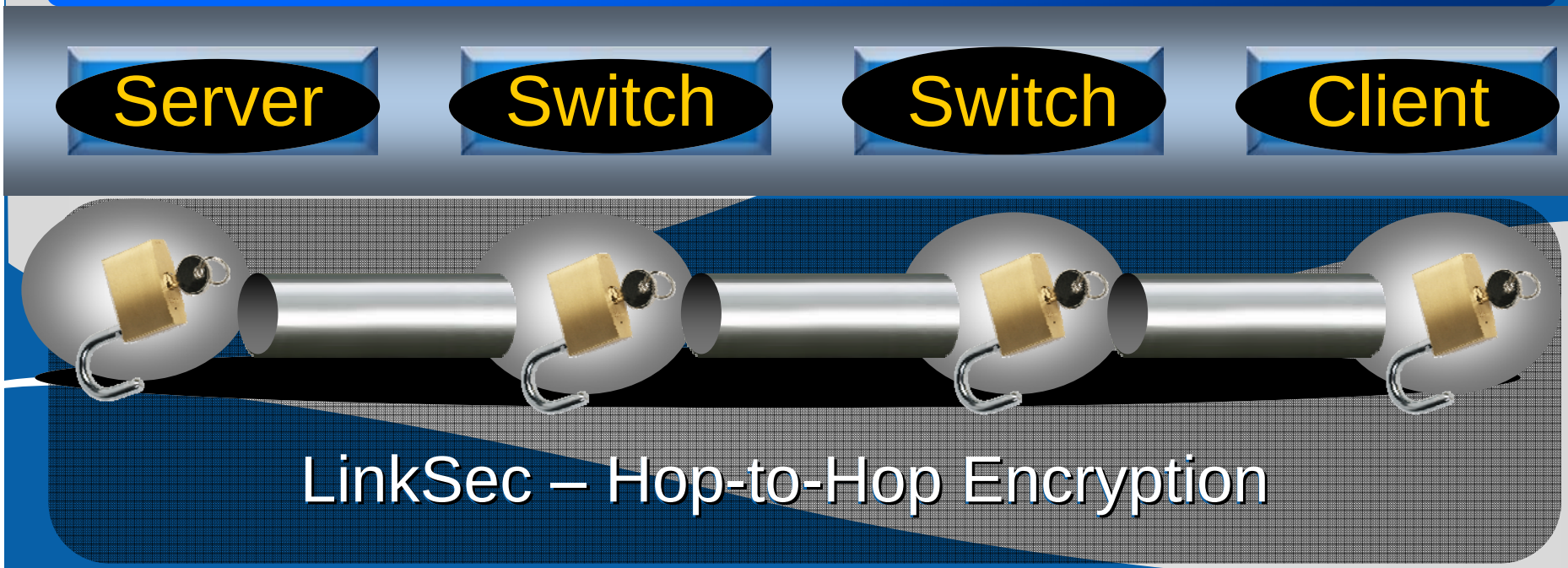
Securing the Links: End-to-End Confidentiality



- End to end solution
- Issues with scalability and manageability
- Alternative solutions:
  - LinkSec
    - Converts end-to-end protection into link-by-link protection
  - Enclaves
    - Builds on LinkSec
    - 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 Demo

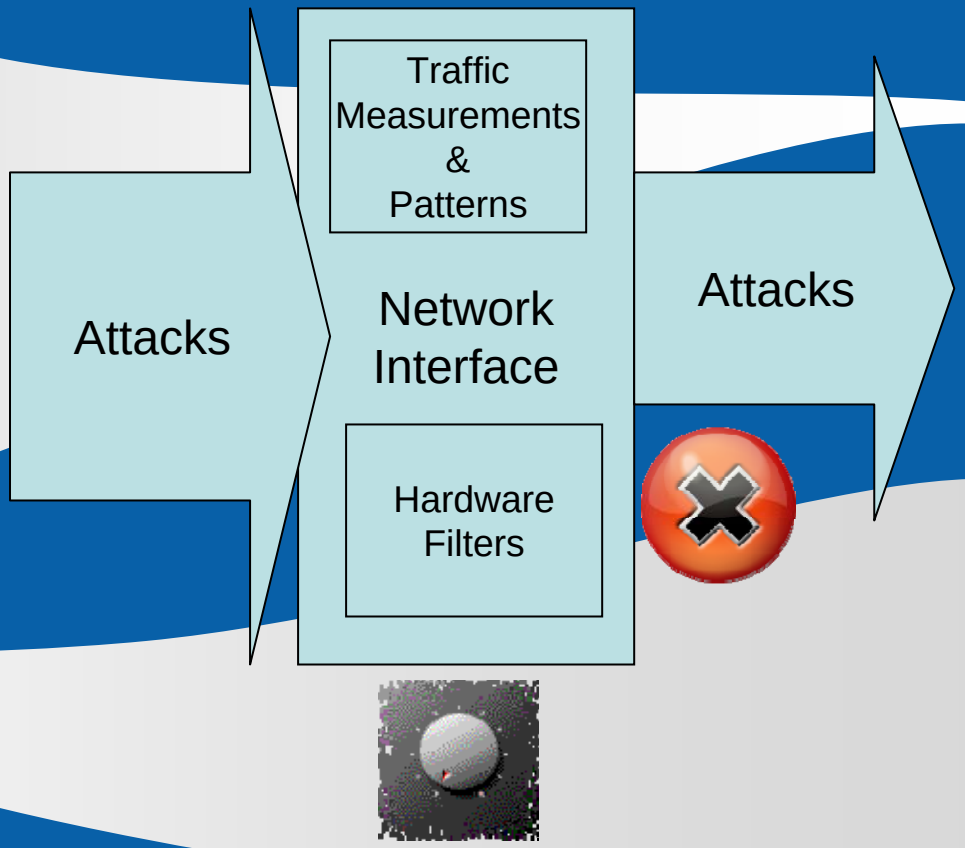
Secure Network Enclaves:
Current Research Emphasis

- 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

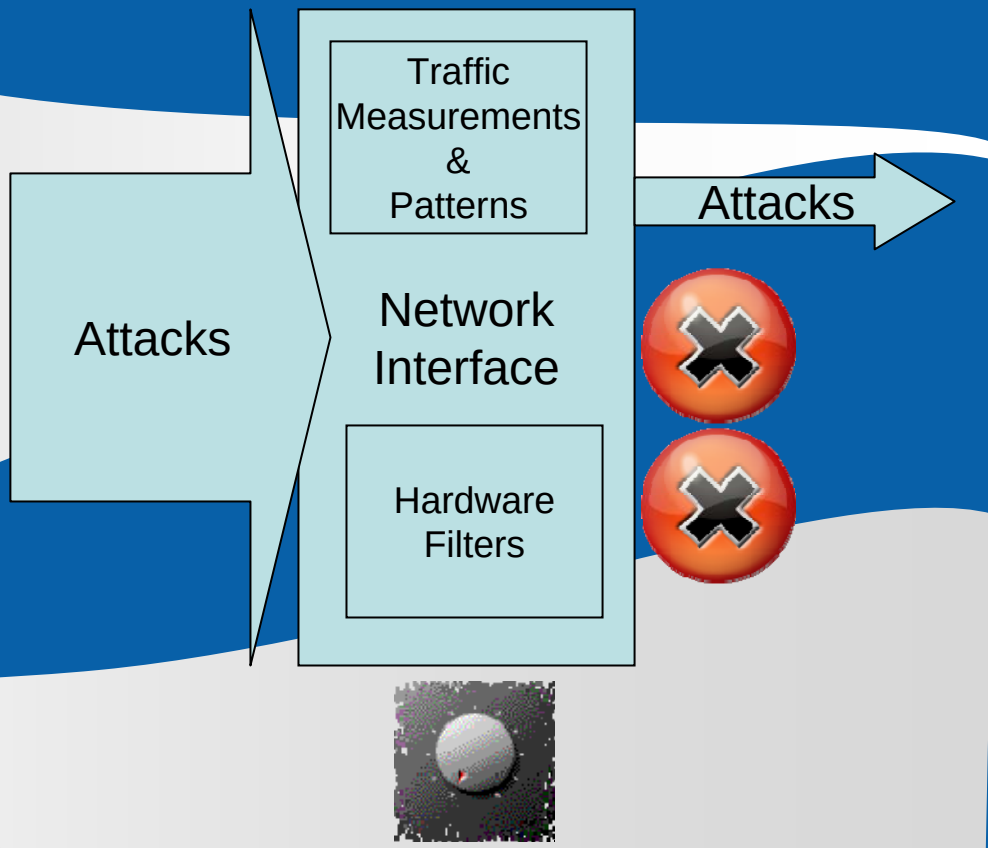
Collaborative Defense:
Step 1: Hardware Filters

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

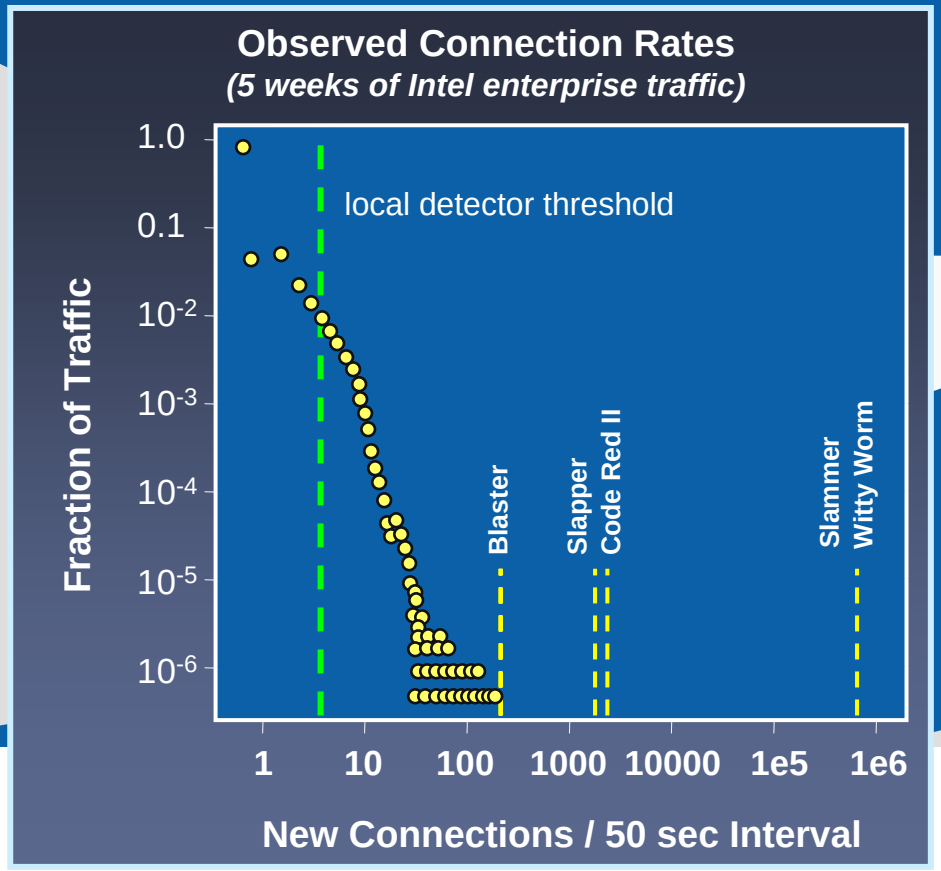


Collaborative Defense:
Step 2: Heuristics

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



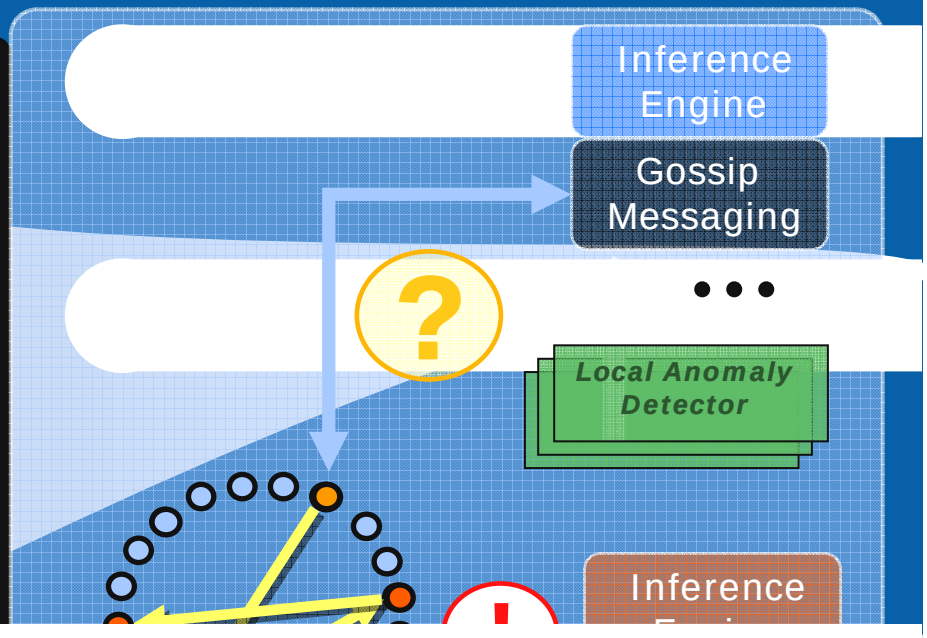
Rules are not Enough – Attacks are Evolving



Challenge is to reduce threshold of detection without increasing false alarms

Collaborative Defense:
Step 3: Inference and Gossip

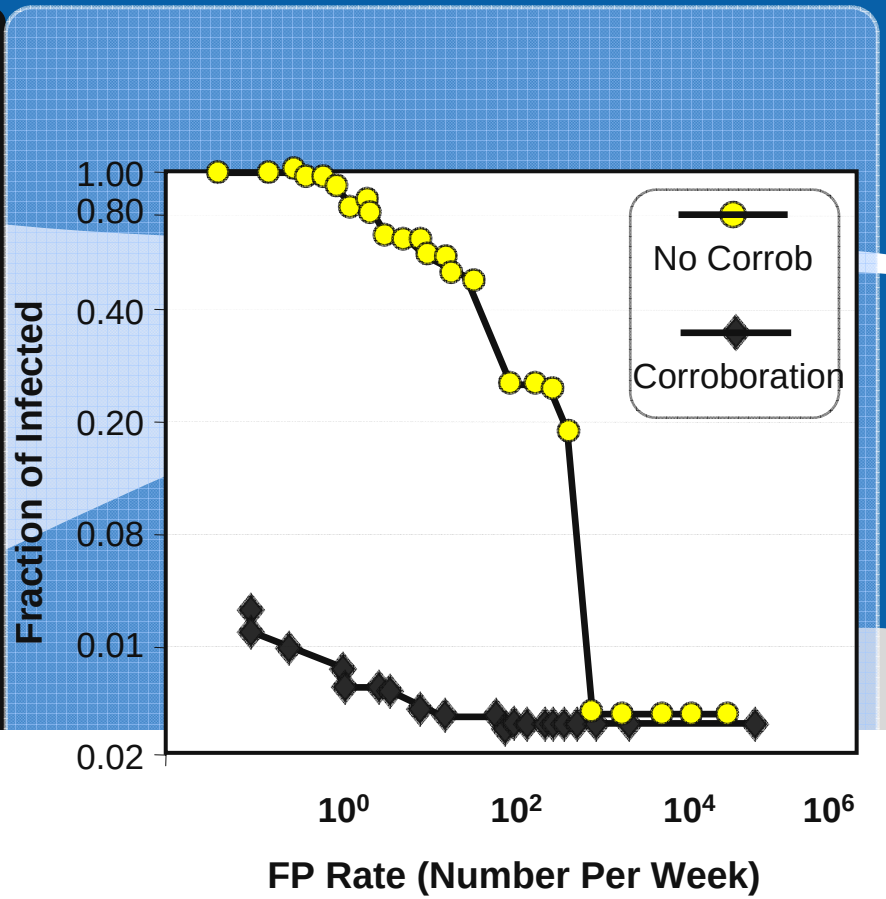
- Employ probabilistic inference
  - Correlate events across multiple machines
  - Combine weak hypotheses into strong evidence
  - Dramatically cut false positives
- Implement scalable, robust



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

The Results: Gossip is Good

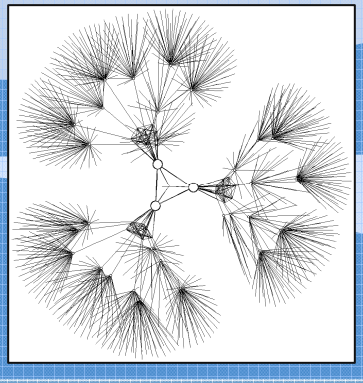
- Collaboration drives false alarms down
  - Allows many simple, but imperfect detectors
- Collaboration roots out stealthy attacks
  - Collect concise local data
  - Put in global correlation framework
- Scalability works in our favor
  - The more participating nodes,

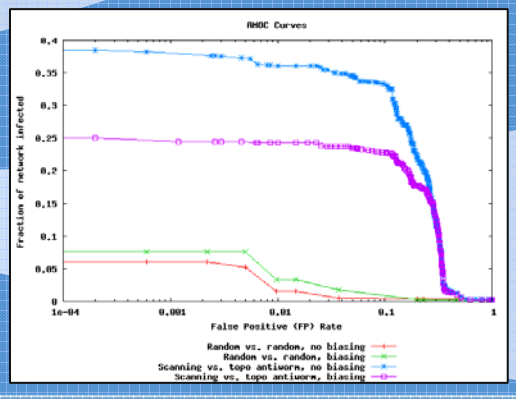


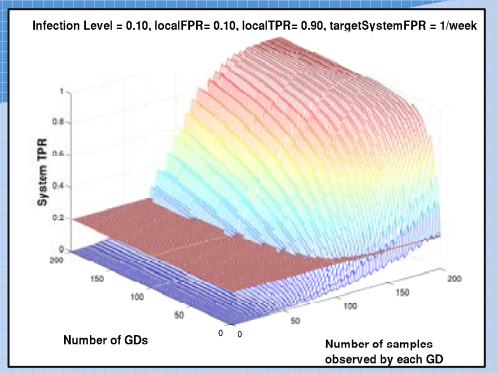
Speculation: There is a class of algorithms that have the property that leads to improvement with increasing scale

Future Directions

- **Adaptation and Learning**
  - end-hosts are dynamical systems
- **Messaging optimizations**
  - bias to send “bad news” faster
  - parameterize so distributed outperforms centralized
- **Reaction strategies**
  - exploit topological & historical knowledge
- **Architectural Robustness**
  - security







Summary

- Security is the #1 IT problem
- Complex problem mandates system level solutions
- No single solution to fix all problems
  - Competing tradeoffs: Performance and Scalability
- Intel is innovating across multiple layers
  - Harden the platform
  - Leave nowhere to hide
  - Secure the links
  - Collaborative Defense


intel
Leap ahead™