TRACKING THE PERFORMANCE OF INTRUSION PREVENTION SYSTEMS

Jeffrey Stuckman

James Purtilo

University of Maryland, College Park

The performance measurement problem

- Intrusion prevention systems prevent vulnerabilities from being exploited (known or unknown)
  - Web application firewalls (prevent SQL injection, etc)
  - Anomaly detectors
  - Data execution prevention
- Hundreds of IDS/IPS algorithms from academia and industry
- How do we know which defenses are worth deploying?
- Performance measurement is ad-hoc at best
  - A few standard benchmarks exist (1999 DARPA IDS evaluation, etc)
- Even if we could benchmark an IPS at one point in time, would it really be useful?

The questions we really want to answer

- Vaccine analogy – Flu virus antigens shift over time so revaccination is required
- Software counterpart – vulnerabilities are continuously discovered, patched, and created
- How did my defense work against the exploits of its era?
- How does my defense work against today's exploits?
- How will my defense work against future exploits?
  - How does my defense mitigate my vulnerabilities which are currently unknown?

Defense performance tracking

- This is a work in progress and part of our research into intrusion prevention systems
- Use available threat intelligence to choose a representative mixture of top exploits every month
  - Internet telescopes / honeypots
  - Popular exploit toolkits
  - Field reports
- Use an automated testbed to test each IPS against all monthly threat mixtures – past and present.

April 2011

SecureNet	April 2011			
CVE-2009-1483	☑			
CVE-2009-1684	☑			
CVE-2009-1933	☑			
CVE-2009-2031	☑			
CVE-2009-2054	☒			
CVE-2010-0478	☑			
CVE-2010-1573	☑			
CVE-2010-1893	☒			
CVE-2011-0183	☑			
CVE-2011-1021	☒			
CVS-2011-1301	☒			

(Hypothetical)

May 2011

SecureNet	April 2011	May 2011		
CVE-2009-1483	☑	☑		
CVE-2009-1933	☑	☑		
CVE-2009-2031	☑	☑		
CVE-2009-2054	☑	☑		
CVE-2010-0478	☒	☒		
CVE-2010-1573	☑	☒		
CVE-2010-2100	☑	☑		
CVE-2011-0183	☒	☑		
CVE-2011-1021	☑	☑		
CVE-2011-1301	☒	☒		
CVE-2011-1439	☒	☒		

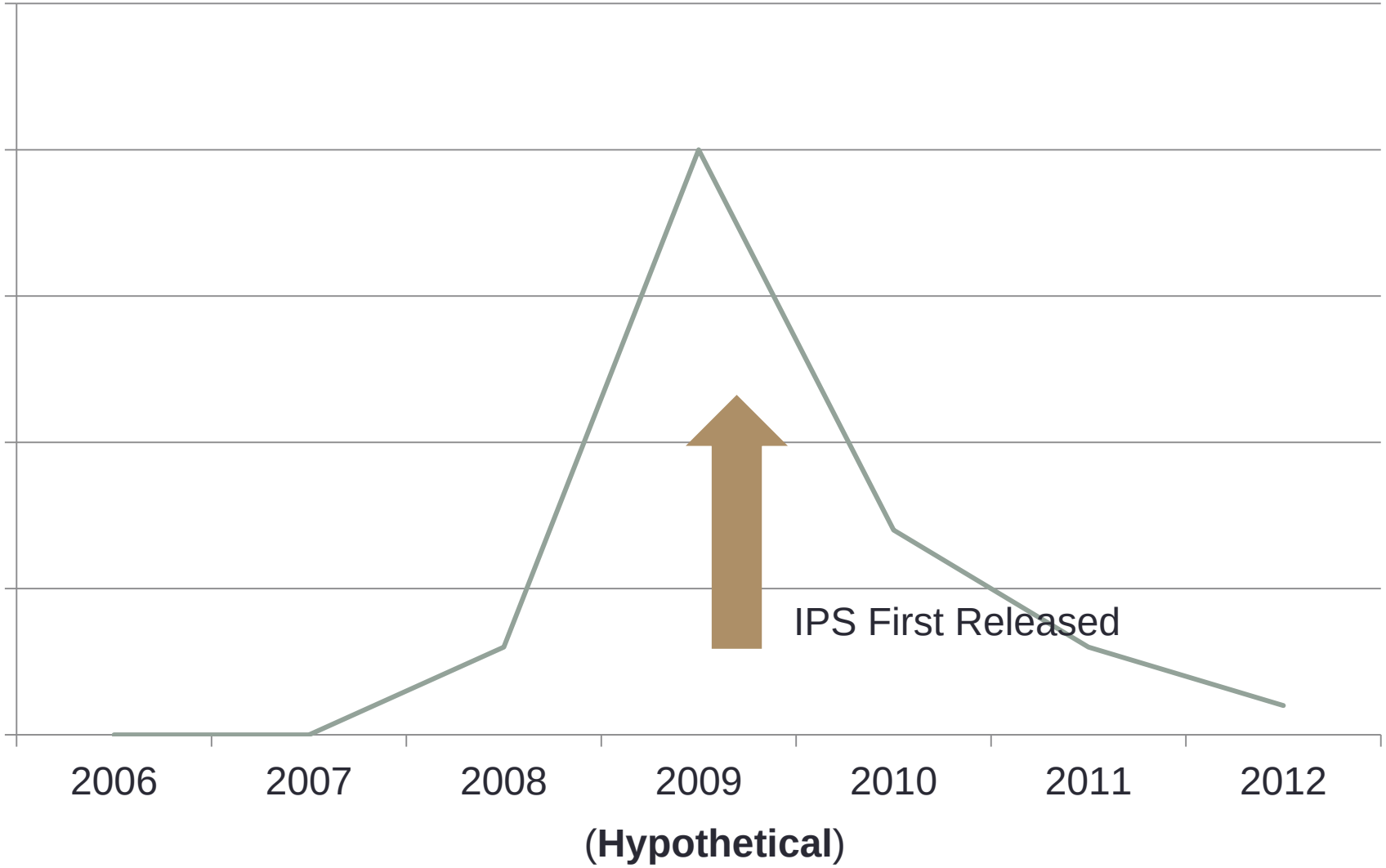
(Hypothetical)

July 2011

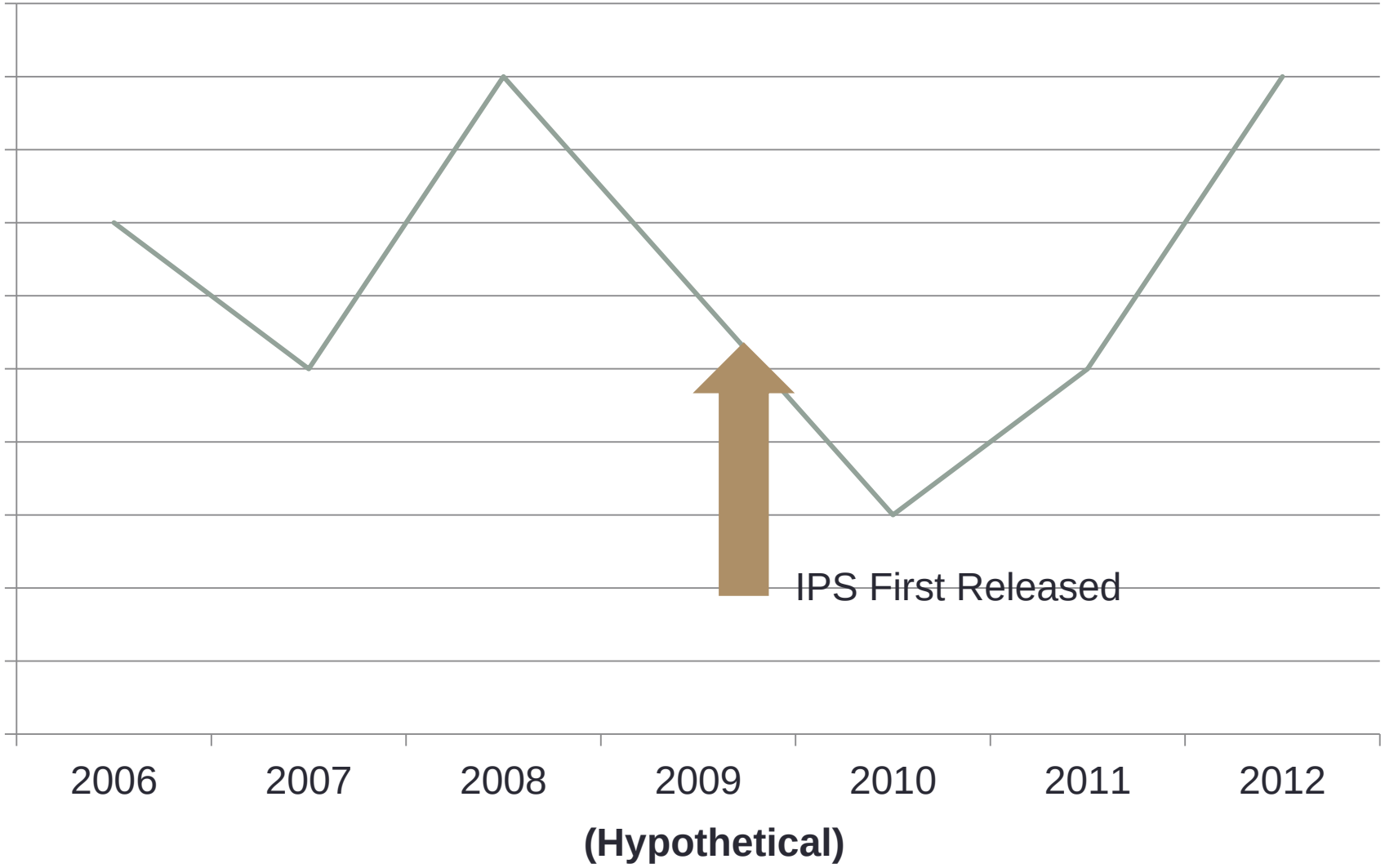
SecureNet	April 2011	May 2011	June 2011	July 2011
CVE-2009-1483	☑	☑	☑	☑
CVE-2009-2031	☑	☑	☑	☑
CVE-2010-0478	☑	☑	☒	☒
CVE-2010-2100	☑	☑	☑	☑
CVE-2010-2310	☒	☒	☒	☒
CVE-2011-1021	☑	☒	☒	☑
CVE-2011-1301	☑	☑	☑	☑
CVE-2011-1439	☒	☑	☑	☒
CVE-2011-1583	☑	☑	☒	☒
CVE-2011-1638	☒	☒	☒	☒
CVE-2011-1975	☒	☒	☒	☒

(Hypothetical)

Defense performance tracking – Signature-based IPS



Defense performance tracking – Anomaly detection



Several open questions remain

- How to choose a representative mix of exploits?
- How to score exploit variants?
- How to score systems that disrupt legitimate workloads?

Questions or comments?

Our scope

- In scope:
  - Intrusion prevention systems (and anomaly detectors which can be used for intrusion prevention)
  - Systems that mitigate vulnerabilities in outward-facing applications due to bugs or misconfigurations
- Not in scope:
  - Penetration testing tools
  - Virus/attachment scanners
  - Pure intrusion detection systems

Testbed architecture