Kathleen Fisher

Program Manager, Information Innovation Office

High Assurance Systems

DARPA Cyber Colloquium
Arlington, VA

November 7, 2011

Physical systems vulnerable to cyber attacks

Falsified speedometer reading:
140 mph in [P]ark!

K. Koscher, et al. "Experimental Security Analysis of a Modern Automobile," in Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, May 16-19, 2010.

Many remote attack vectors

Long-range wireless

Indirect physical

Entertainment

Short-range wireless

Mechanic

Image sources: www.autoblog.com, www.journalofamnangler.com, www.1800pocketpc.com, en.wikipedia.org/wiki/Compact_Disc www.thedigitalbus.com, coolmaterial.com, www.laptopsarena.com, www.elec-intro.com, mybluetoothearbuds.blogspot.com, www.diytrade.com

Pervasive vulnerability

SCADA Systems

Computer Peripherals

Vehicles

Sources:
en.wikipedia.org/wiki/File:Gas_centrifuge_cascade.jpg, gis-rci.montpellier.cemagref.fr, cyberseecure.com, www.ourestatesale.com, www.eweek.com, pastorron7.wordpress.com, landsat.gsfc.nasa.gov, www.tech2date.com, www.militaryaerospace.com, www.naval-technology.com, www.chinacartimes.com

Medical Devices

Communication Devices

We need a fundamentally different approach

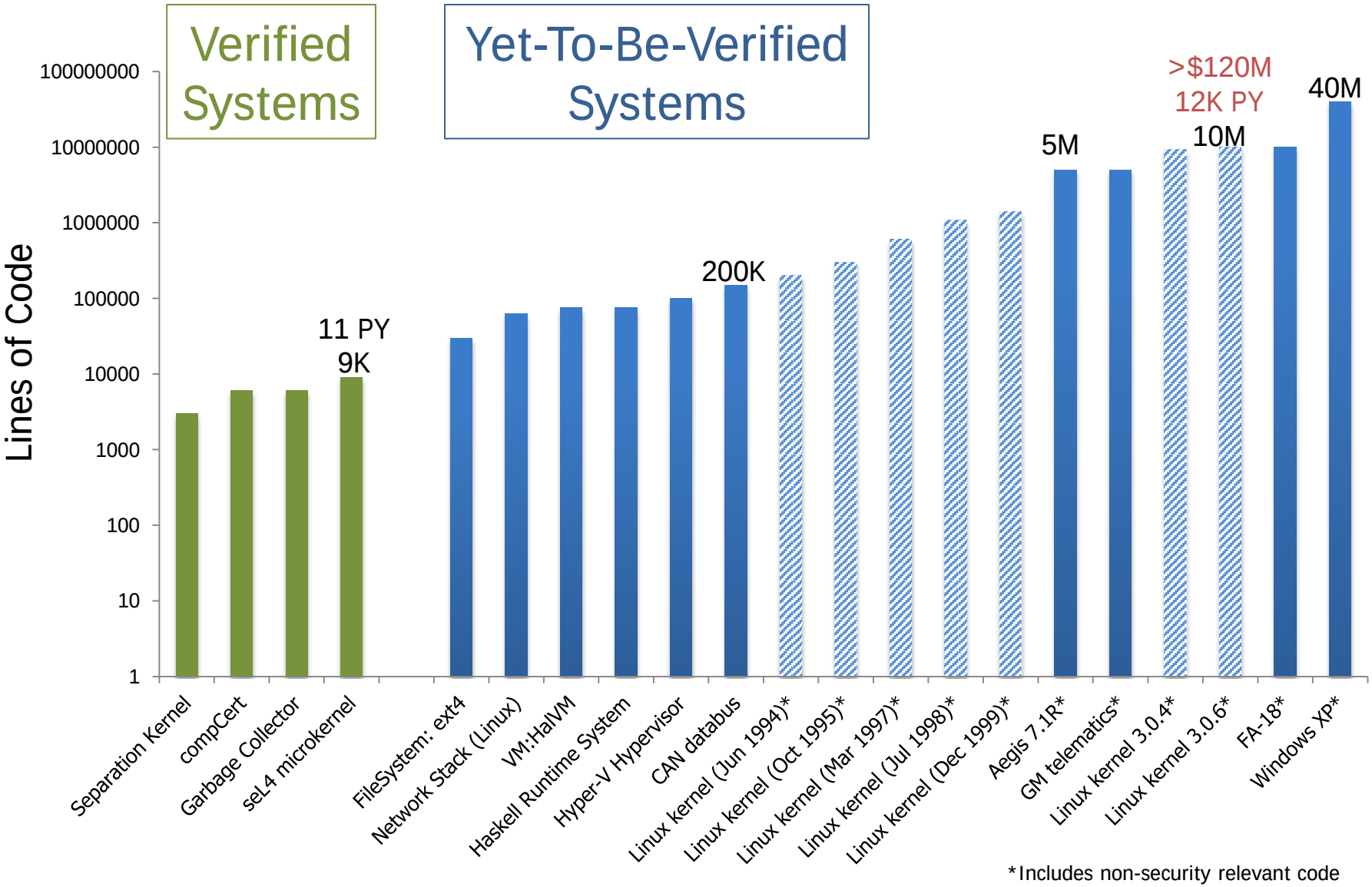
- State of the art:
  - Anti-virus scanning, intrusion detection systems, patching infrastructure
- This approach *cannot* solve the problem.
  - Focused on known vulnerabilities; can miss zero-day exploits
  - Can introduce new vulnerabilities and privilege escalation opportunities

October 2010 Vulnerability Watchlist

Vulnerability Title	Fix Avail?	Date Added
XXXXXXXXXXX XXXXXXXXXXX Local Privilege Escalation Vulnerability	No	8/25/2010
XXXXXXXXXXX XXXXXXXXXXX Denial of Service Vulnerability	Yes	8/24/2010
XXXXXXXXXXX XXXXXXXXXXX Buffer Overflow Vulnerability	No	8/20/2010
XXXXXXXXXXX XXXXXXXXXXX Sanitization Bypass Weakness	No	8/18/2010
XXXXXXXXXXX XXXXXXXXXXX Security Bypass Vulnerability	No	8/17/2010
XXXXXXXXXXX XXXXXXXXXXX Multiple Security Vulnerabilities	Yes	8/16/2010
XXXXXXXXXXX XXXXXXXXXXX Remote Code Execution Vulnerability	No	8/16/2010
XXXXXXXXXXX XXXXXXXXXXX Use-After-Free Memory Corruption Vulnerability	No	8/12/2010
XXXXXXXXXXX XXXXXXXXXXX Remote Code Execution Vulnerability	No	8/10/2010
XXXXXXXXXXX XXXXXXXXXXX Multiple Buffer Overflow Vulnerabilities	No	8/10/2010
XXXXXXXXXXX XXXXXXXXXXX Stack Buffer Overflow Vulnerability	Yes	8/09/2010
XXXXXXXXXXX XXXXXXXXXXX Security-Bypass Vulnerability	No	8/06/2010
XXXXXXXXXXX XXXXXXXXXXX Multiple Security Vulnerabilities	No	8/05/2010
XXXXXXXXXXX XXXXXXXXXXX Buffer Overflow Vulnerability	No	7/29/2010
XXXXXXXXXXX XXXXXXXXXXX Remote Privilege Escalation Vulnerability	No	7/28/2010
XXXXXXXXXXX XXXXXXXXXXX Cross Site Request Forgery Vulnerability	No	7/26/2010
XXXXXXXXXXX XXXXXXXXXXX Multiple Denial Of Service Vulnerabilities	No	7/22/2010

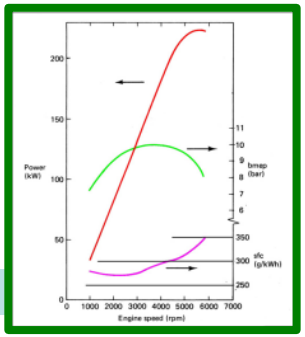
1/3 of the vulnerabilities are in security software!

Critical Components within Reach of Formal Methods



High-Assurance Component Factory

Cyber



Physical

Key Challenges

- Reusable components
- Composition
- Increasing automation
- Scaling
- Concurrency
- Cyber-physical integration

Sources: en.wikipedia.org/wiki/File:Gas_centrifuge_cascade.jpg, gis-rci.montpellier.cemagref.fr, cyberseecure.com, www.ourestatesale.com, www.tech2date.com, www.eweek.com, dronewarsuk.wordpress.com

High Assurance: Correctness, Safety, Security

Feedback welcome!

- Promising research directions?
- Additional challenges?
- Other things you think I should know?

Contact Information: Kathleen.Fisher@darpa.mil