Computer Security and Privacy and the Human Factors Behind It

Daniela Oliveira

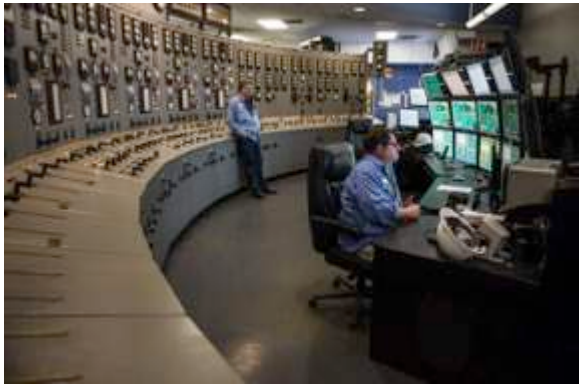
Associate Professor

Department of Electrical and Computer Engineering

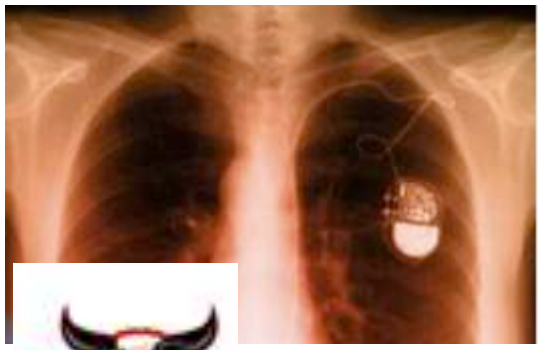
University of Florida

Florida Institute for Cyber Security

A Society Dependent on Networked Computer Systems



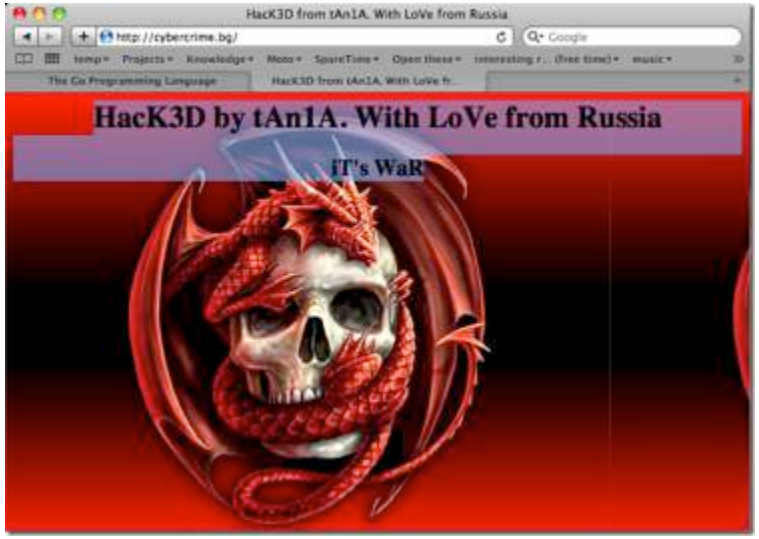
Computer Systems Target of a Never-Ending War



Who are the new attackers?

Nation states

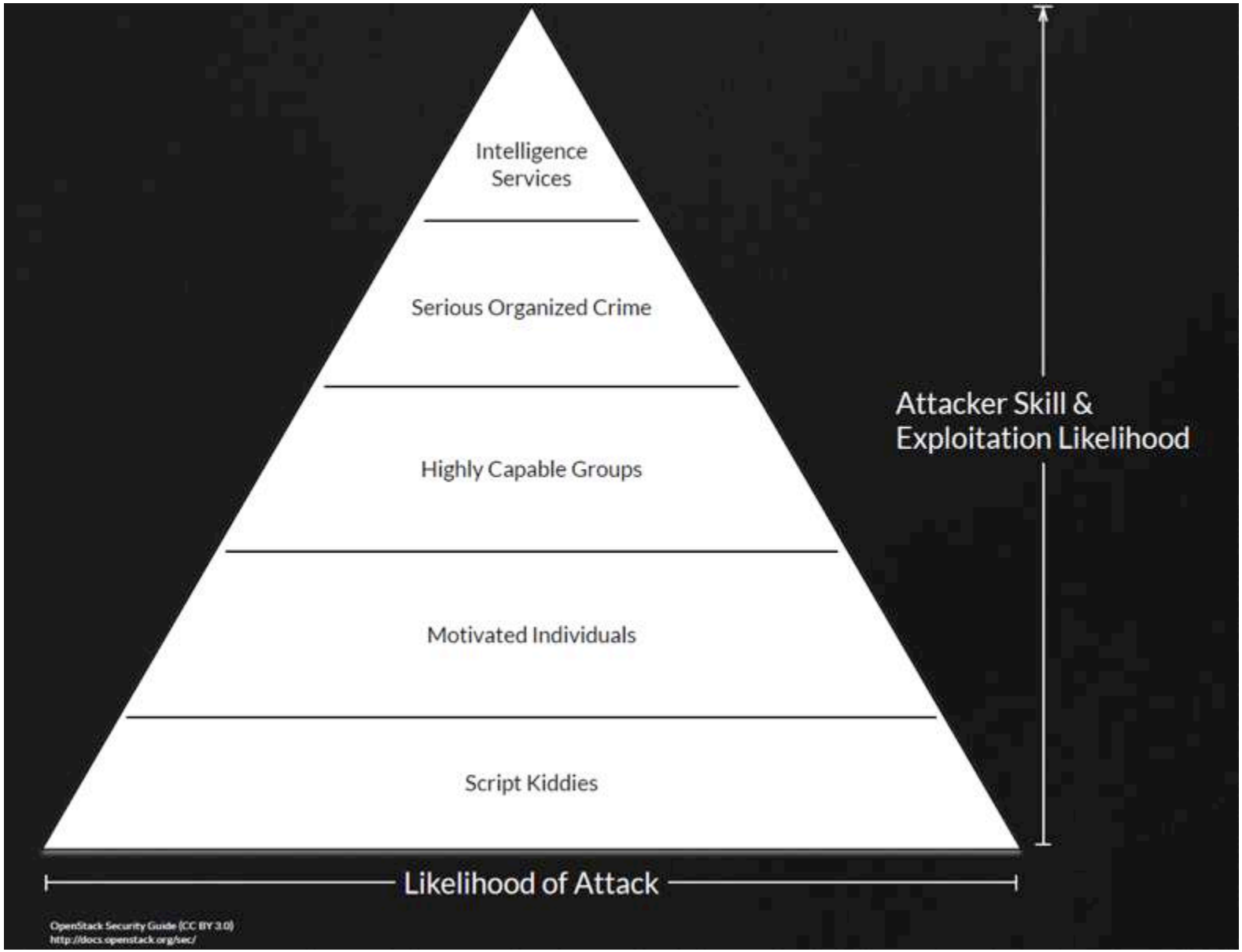
Cyber espionage



Organized crime

Insiders

Who are the new attackers?



Devastating Consequences

Billions of dollars in cyber security spending

Does Cybercrime Really Cost $1 Trillion?

National Security Agency Director Gen. Keith Alexander speaks about cybersecurity and the new threats posed to the U.S. economy and military at the American Enterprise Institute in Washington, D.C., on July 9, 2012. (Chip Somodevilla/Getty Images)

Devastating Consequences

U.S.

The New York Times

Hacking of Government Computers Exposed 21.5 Million People

By JULIE HIRSCHFELD DAVIS JULY 9, 2015

Devastating Consequences

WAR STORIES | MILITARY ANALYSIS. | AUG. 18 2015 5:00 PM

Losing Control of the Vehicle

You should be at least a little scared of car hacking.

By Fred Kaplan

Slate

HEALTH

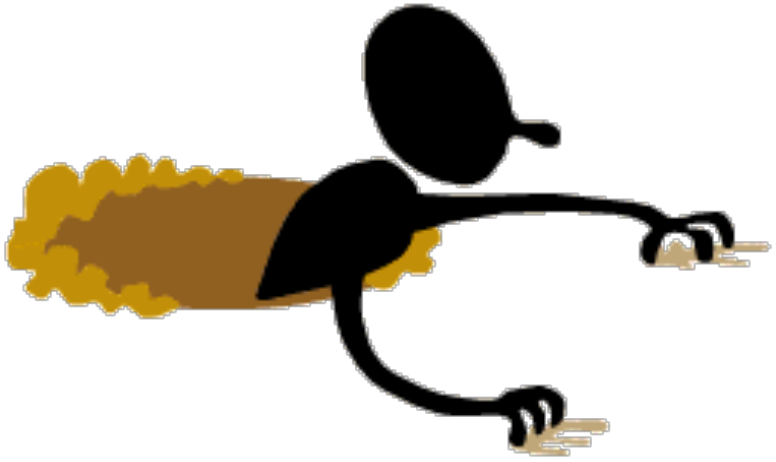
FDA ISSUES WARNING ABOUT HACKABLE MEDICAL DEVICES

DRUG PUMP MAY BE THE FIRST TO RECEIVE SUCH A WARNING, BUT IT WON'T BE THE LAST

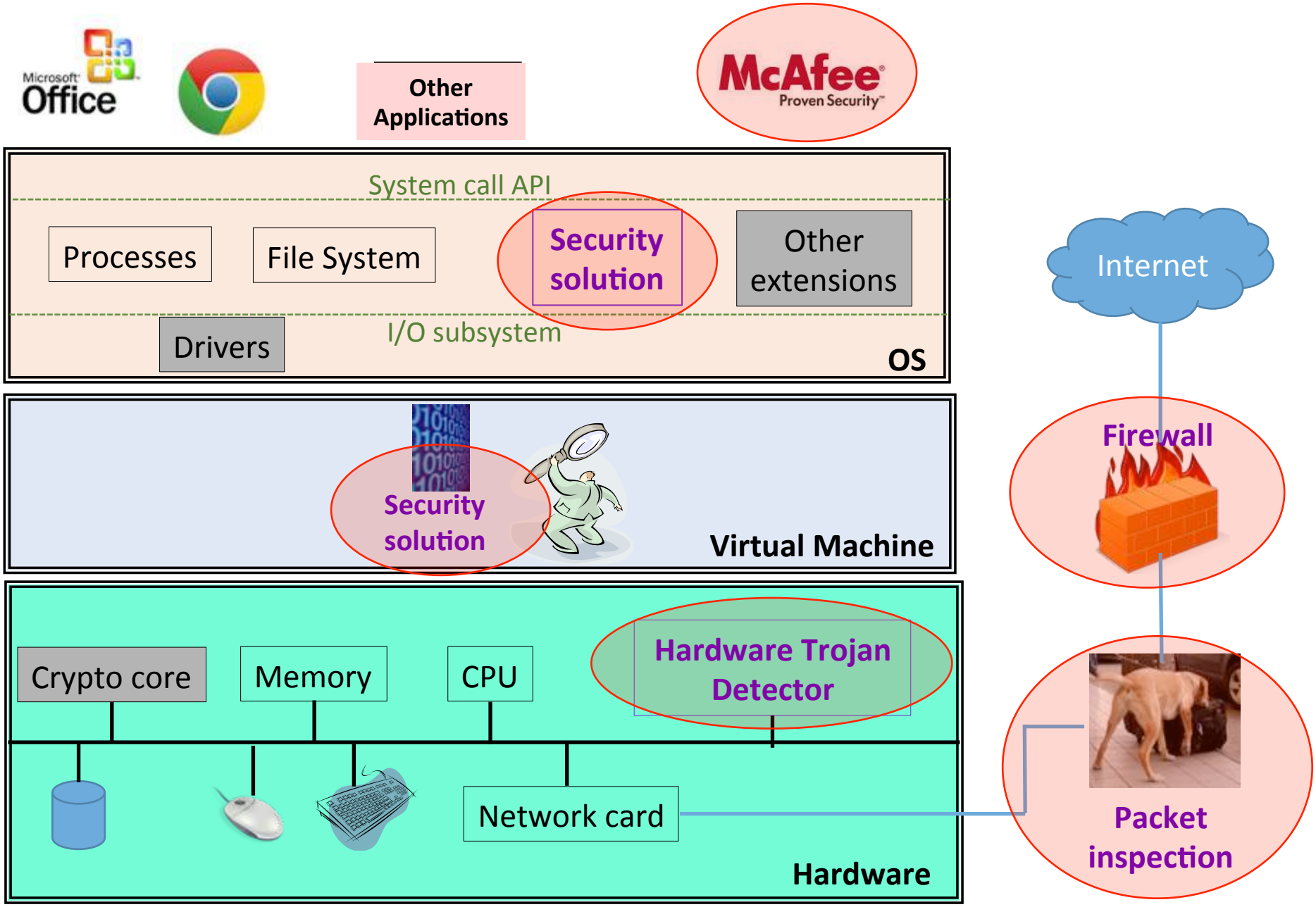
By Alexandra Ossola Posted August 5, 2015

POPULAR SCIENCE

Defense Solutions Not Keeping Up



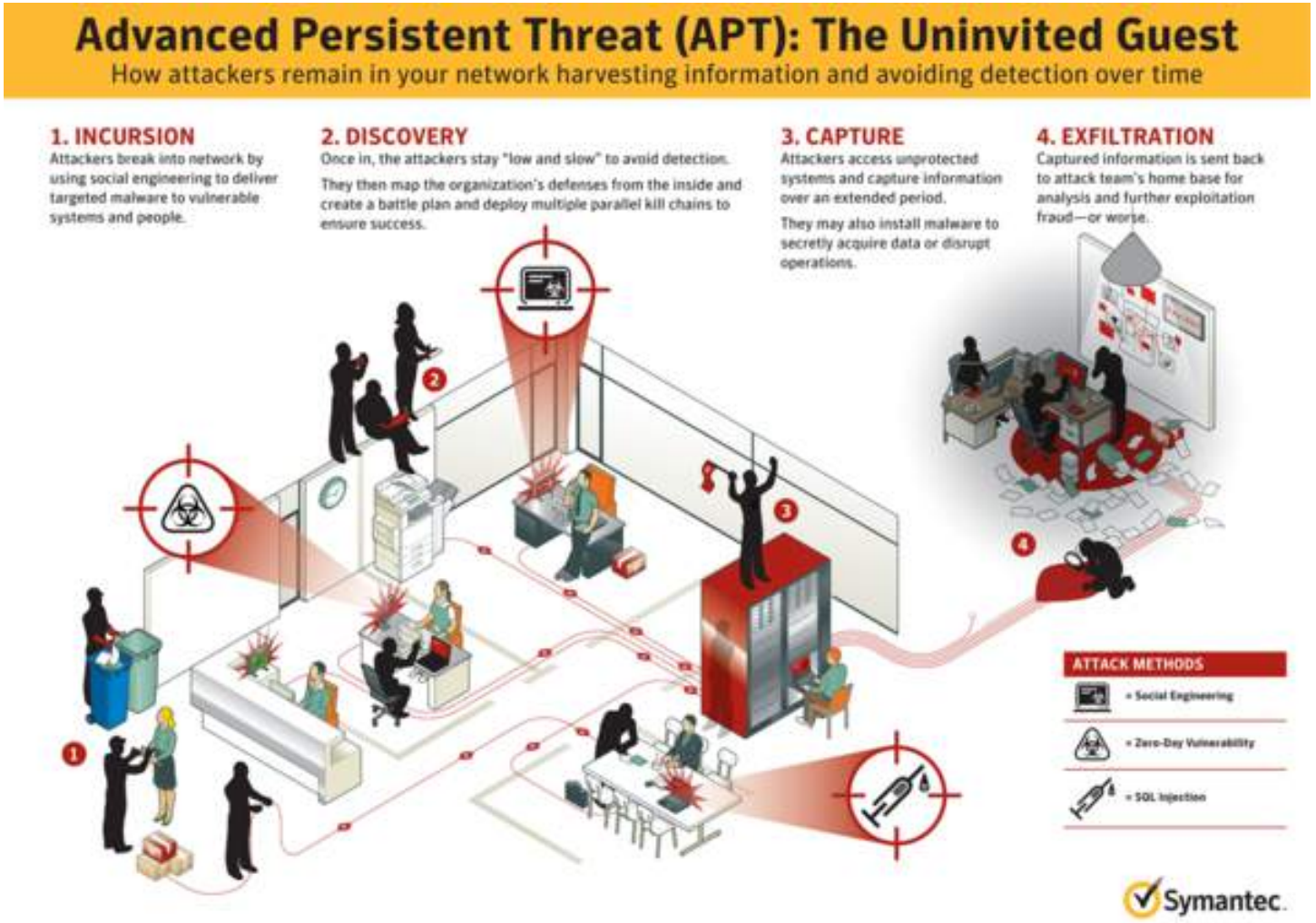
The State-of-The-Art



The Social, Behavioral, and Economics Aspects

It is not all about technical solutions!

Advanced Persistent Threats



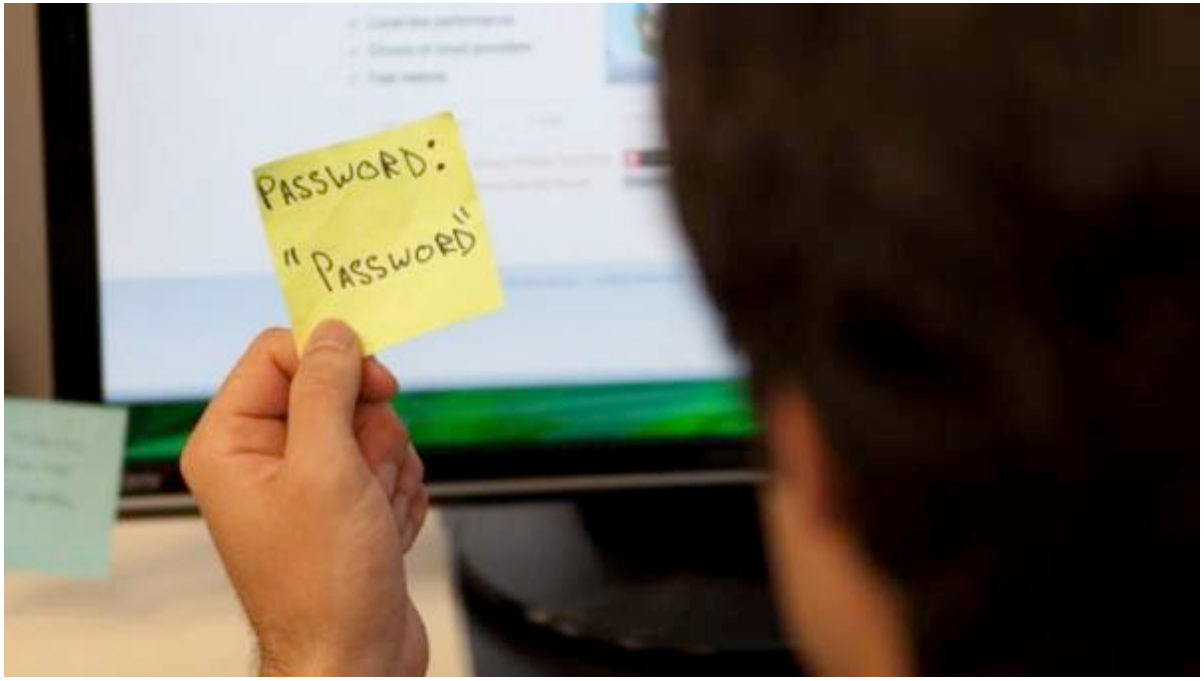
Google and Facebook are Attacker's Best Friends

Chinese spies used fake Facebook profile to friend NATO officials

Chinese spies created a fake Facebook profile of U.S. Navy admiral James Stavridis, friended various NATO officials, and gained access to their personal data. The fake profile has since been taken down.

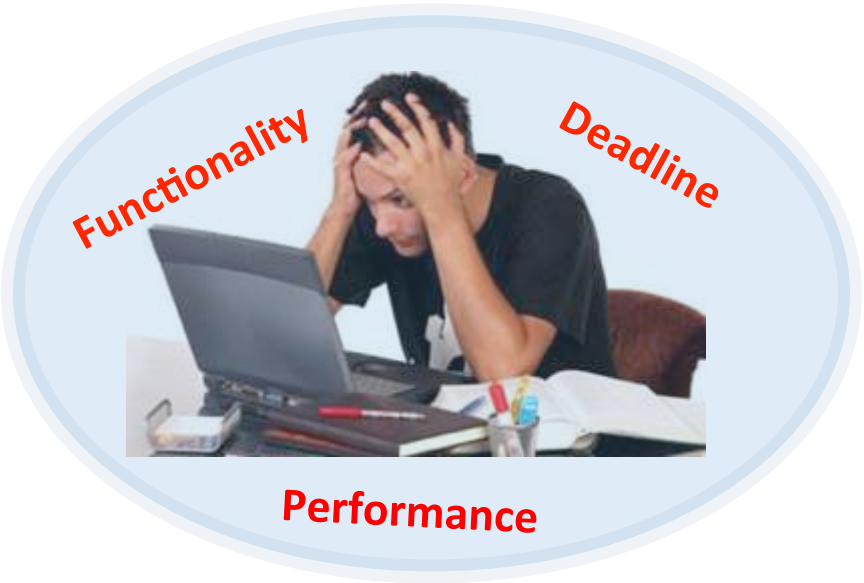
By Emil Protalinski for Friending Facebook | March 11, 2012 -- 22:58 GMT (15:58 PDT) | Topic: Social Enterprise

Economics/Psychology: Security is a Daily Burden to Users



Economics/Psychology: Security is not a Priority in Software Development

Developers do not seek security information while coding



Security

Vulnerabilities hidden in corner cases

Our work

How Can We Overcome the Problems of Computer System Monoculture?

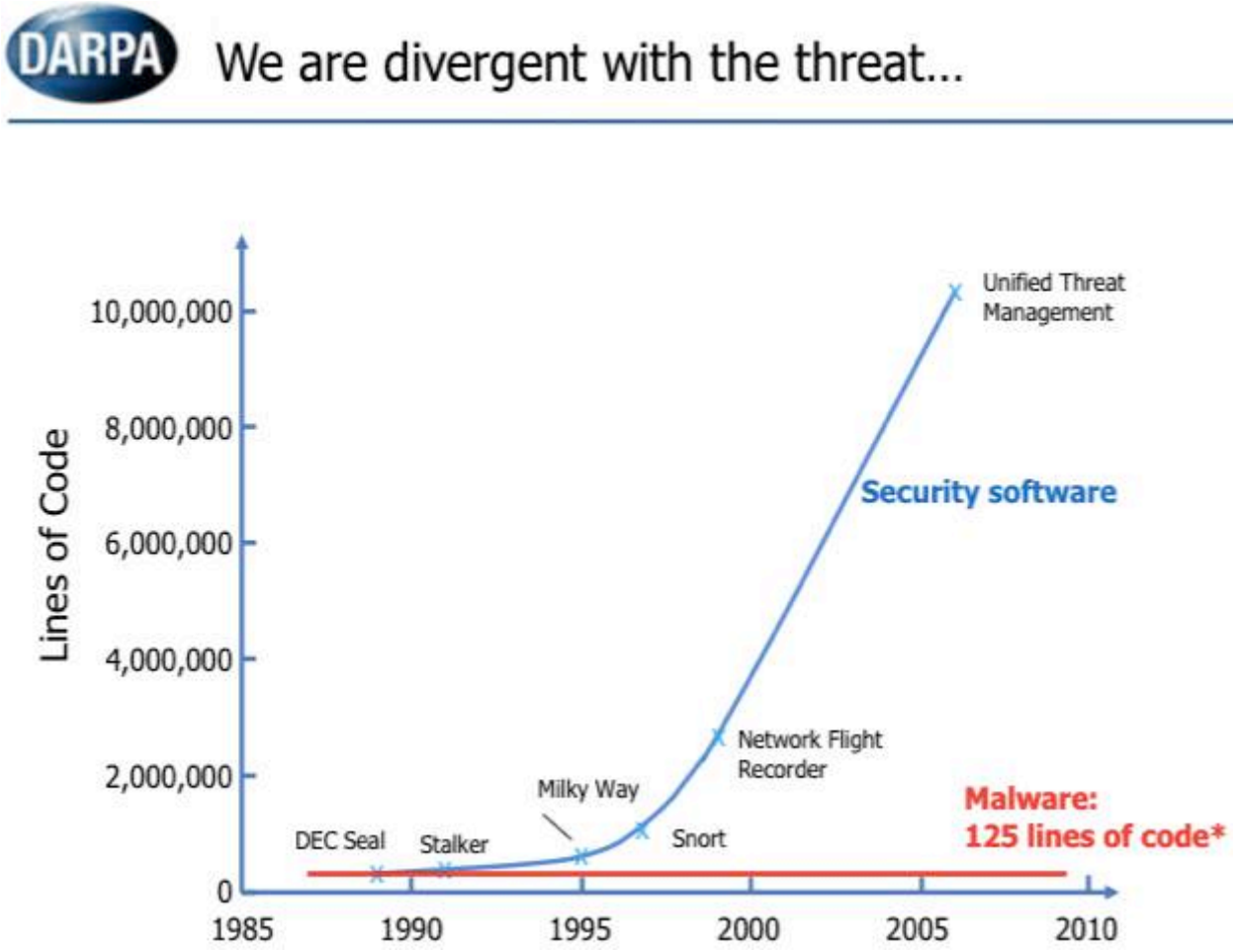
Predictability poses security problems…

- Vulnerabilities exploitable on all systems of same type

Code Red 2001: 359,000 hosts infected

$2 billion in losses

Predictability Makes Attacker's Life Easier



Peiter "Mudge": DARPA Framework for Cyber Security 2011

What If Operating Systems Were ***Trustworthy Unpredictable***?

Unpredictability "Trends"

- Address Space Layout Randomization (ASLR)
- ISA Randomization
- Compiler Specialization
- Diverse implementation
  - N-version programming, library OSes

Still residual certainty that benefits attackers!

Variation without unpredictability is not enough!

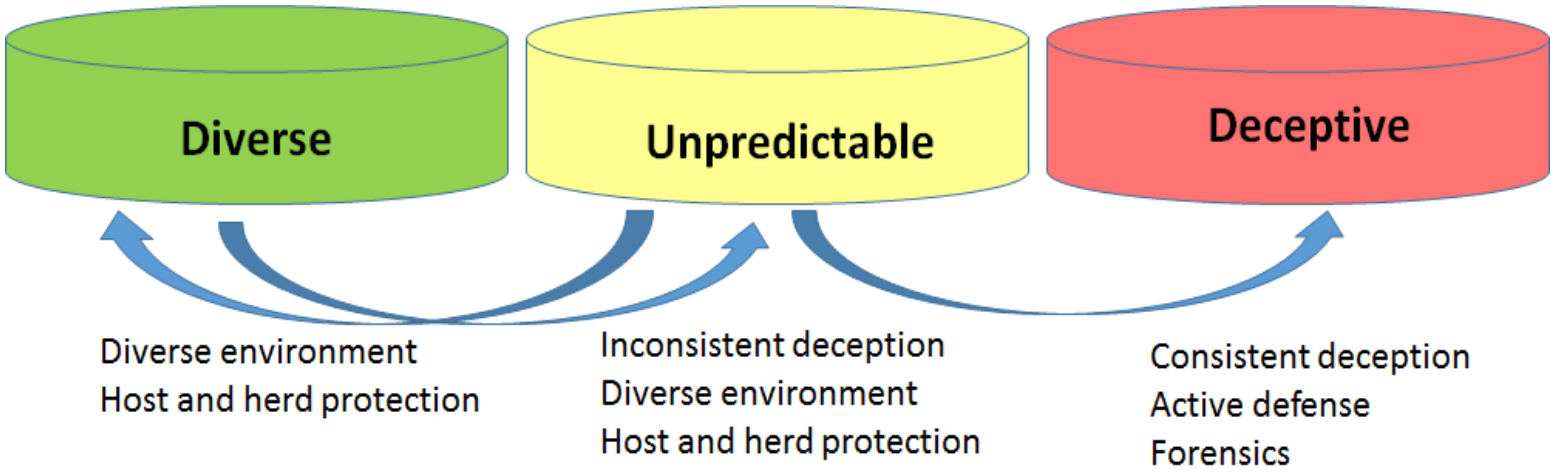
Trustworthy Unpredictability at OS Level

- For “good” uses: OS is predictable -> efficiency and reliability
- For “unknown” uses: OS inefficient and unreliable

Selective Unpredictability for Stealthy Malware

Spectrum Behavior OS

Chameleon



Typical Scenario

- Bob, 78, living in a retirement community in Florida



  - not computer savvy, clicks in links from phishing email, installing malware
  - Malware engage in later DDoS attacks
  - Bob never notices: malware is active only after 1am.

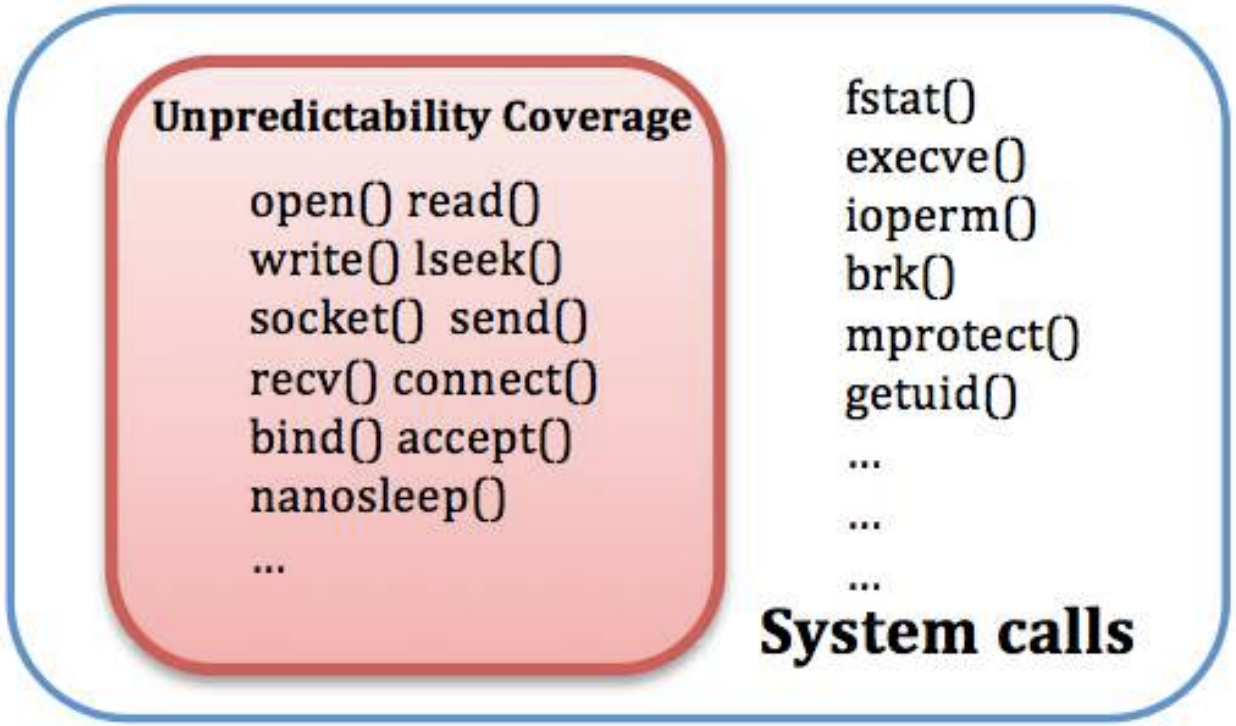
Chameleon Scenario

Strategies

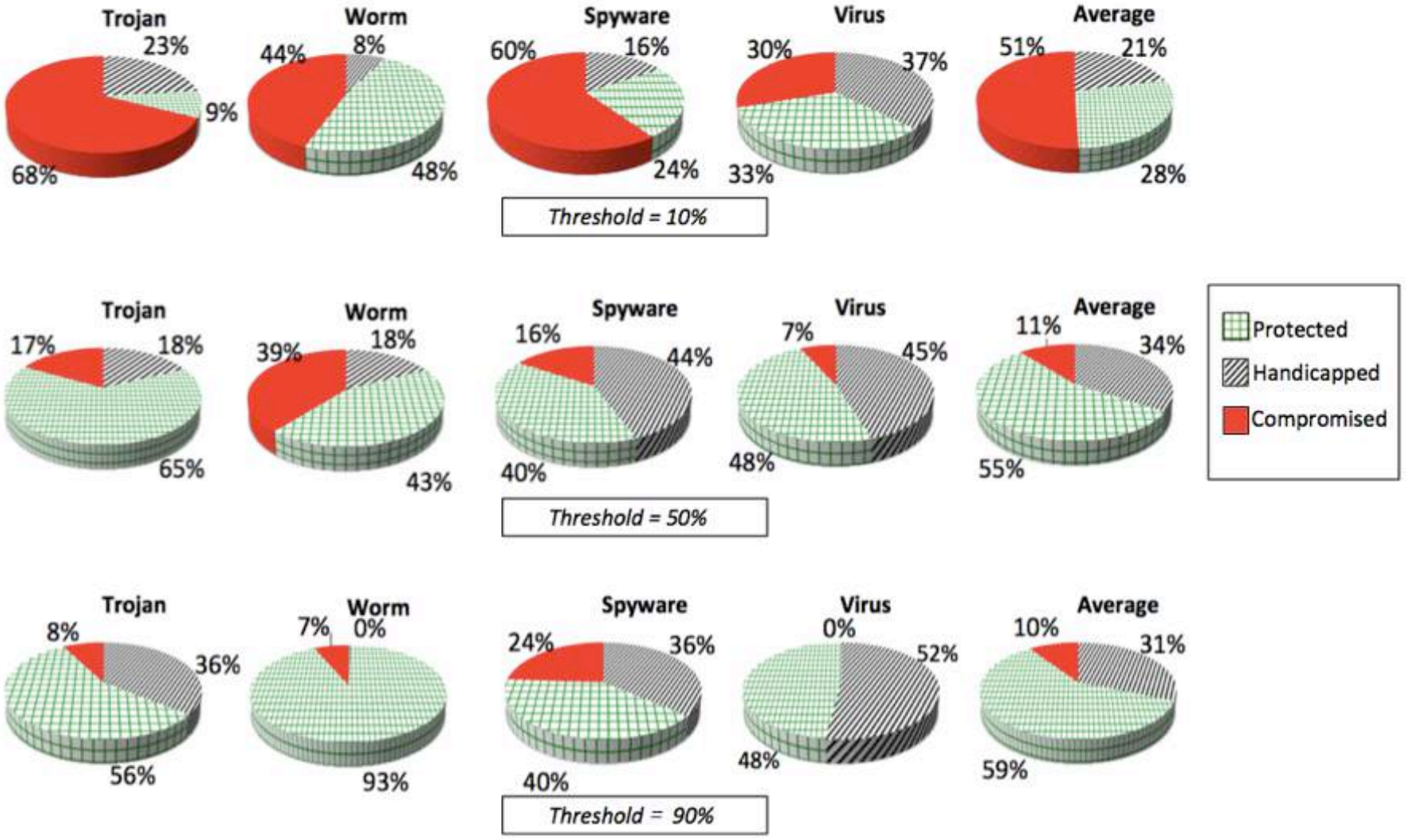
- Strategy 1: Silence the system call
- Strategy 2: Change buffer bytes
- Strategy 3: Add more wait time
- Strategy 4: Connection Restriction
- Strategy 4: Change file pointer

Unpredictability Coverage

Only for system calls not critical to process start-up



Security Analysis



Keylogger with Unpredictability

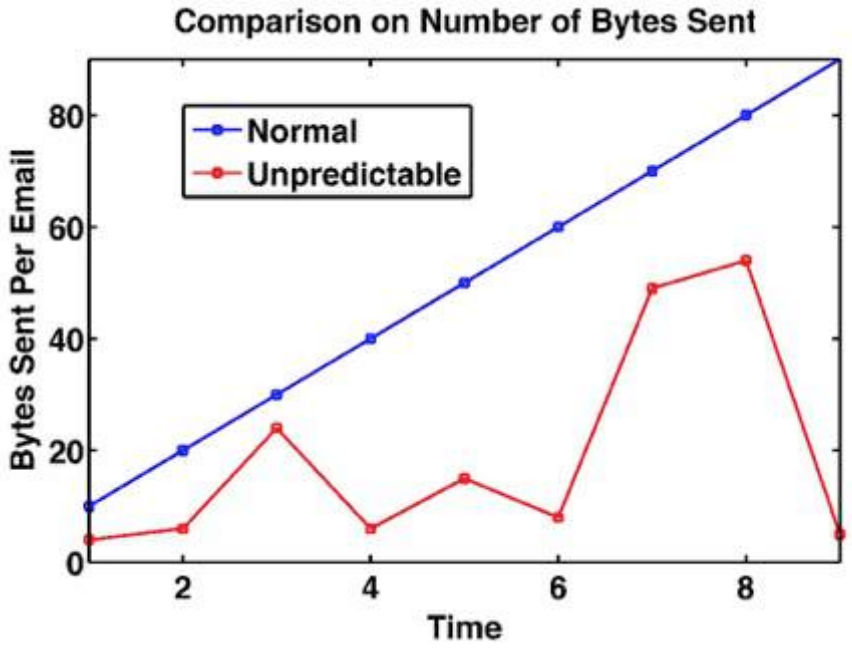
- Strategies:
  - Change `write( fd, *buf, size)` buffer;
  - Change `lseek( fd, offset, whence)` pointer;

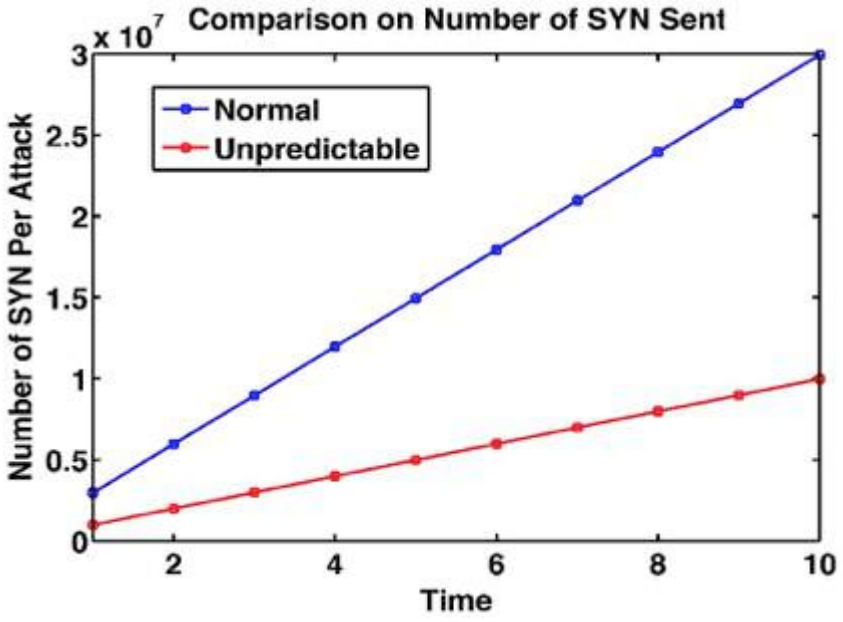
Keylogger with Unpredictability

- Strategies:
  - Change `write( fd, *buf, size)` buffer;
  - Change `lseek( fd, offset, whence)` pointer;

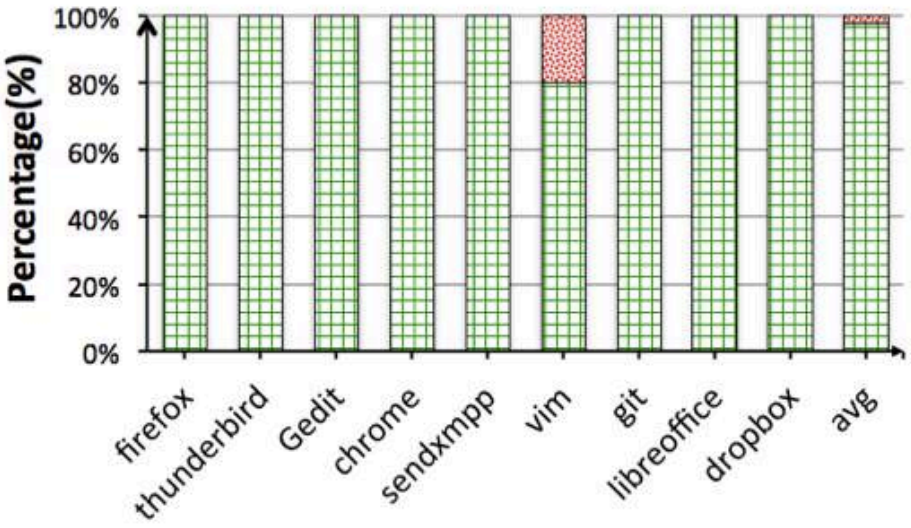
Botnet with Unpredictability

- Strategies:
  - Silence `read( fd, *buf, size);`
  - Silence or reduce len in `sendto( sockfd, *buf, len, …);`

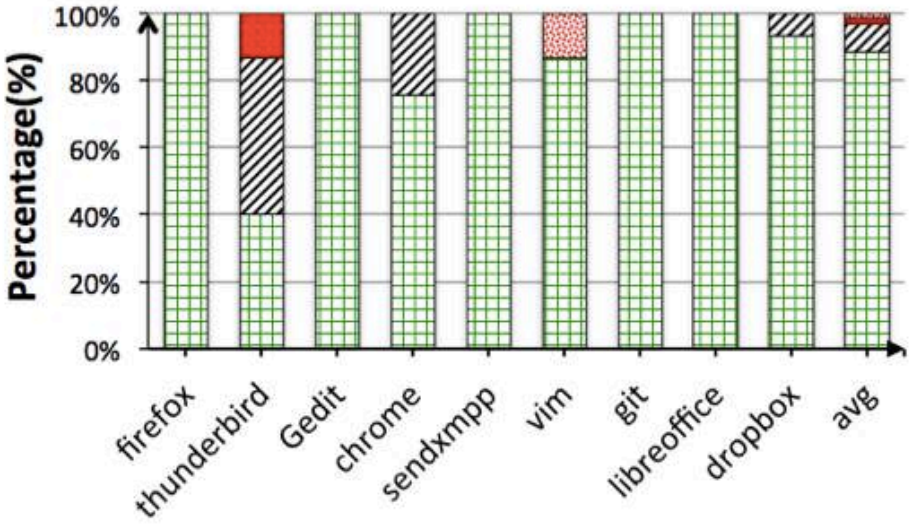




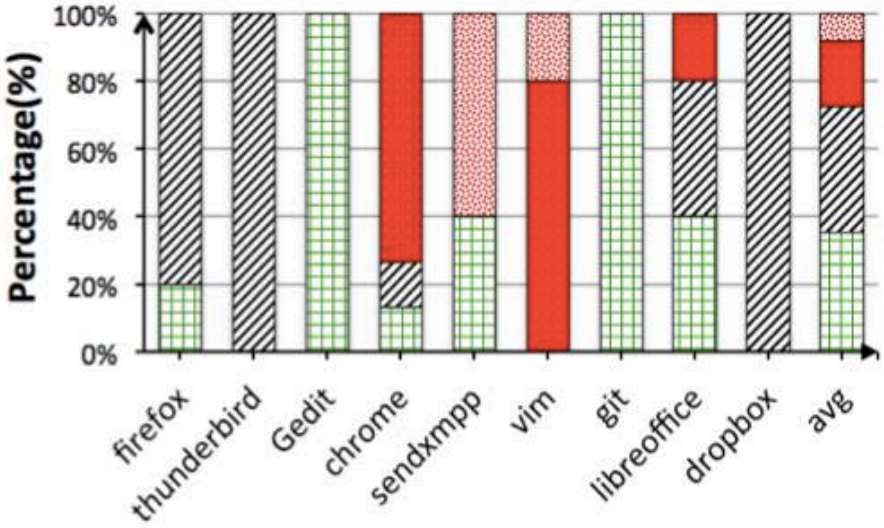
What About Benign Software?



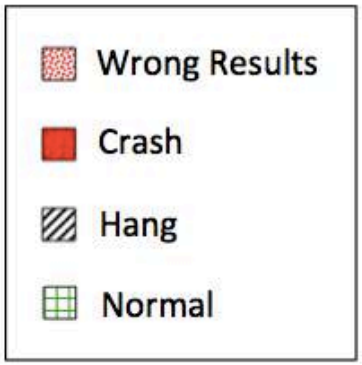
threshold = 10%



threshold = 50%

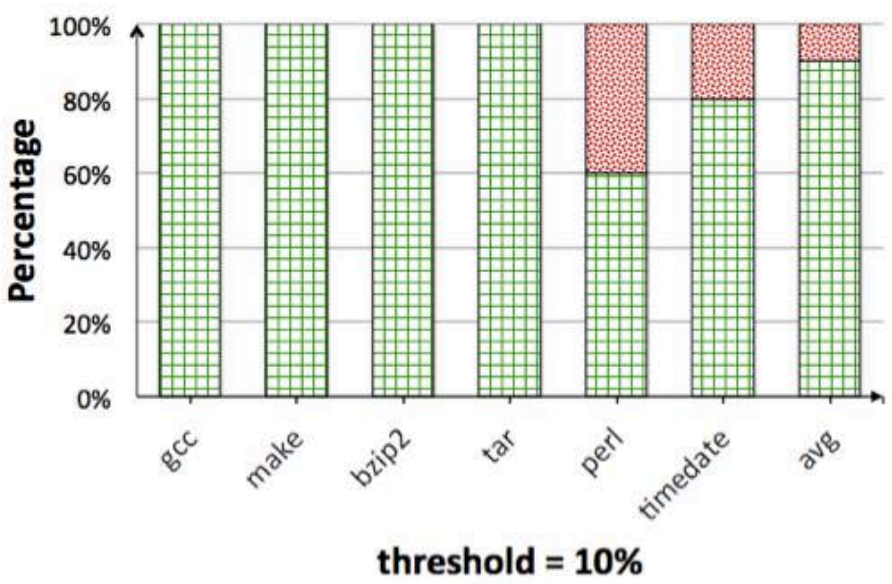


threshold = 90%

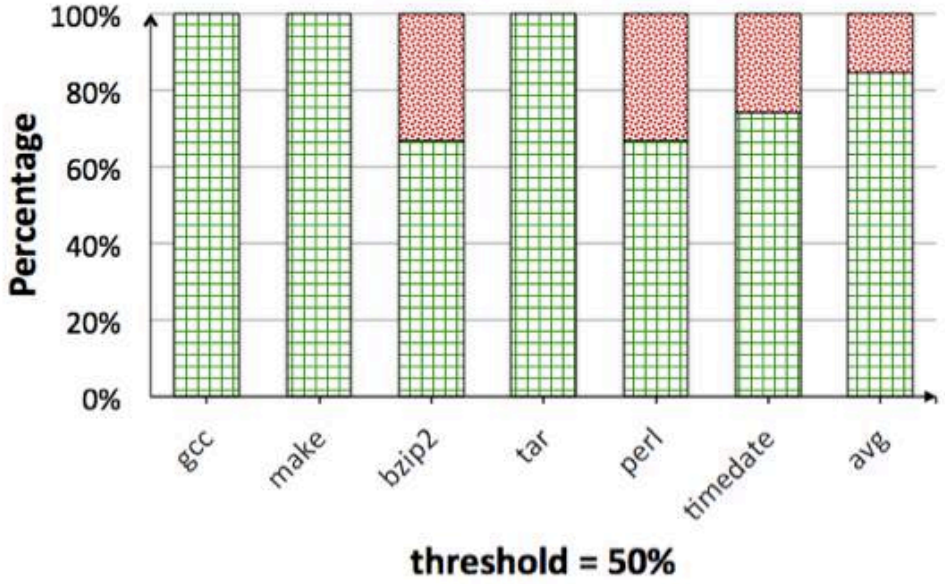


IO Bound

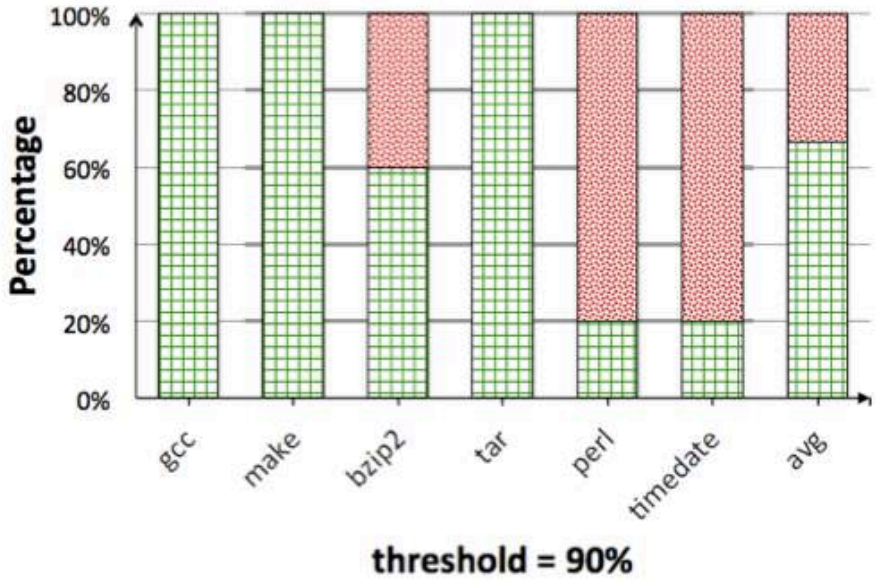
What About Benign Software?



threshold = 10%



threshold = 50%



threshold = 90%

CPU Bound

Concluding Remarks

- Holy grail of system design: thwart attacker with less effort than generating attacks
- Chameleon makes systems diverse by design and actively secure:
  - Diverse + Unpredictable: every instance of system behaves differently
  - Deceptive: lures adversaries into revealing their strategies

Unpredictability is promising!

Thank you!

daniela@ece.ufl.edu