EE260 Architecture/Hardware Support for Security

Nael Abu-Ghazaleh

Department of Computer Science and Engineering
Department of Electrical and Computer Engineering
University of California at Riverside
naelag@ucr.edu

September 27, 2018

Overview

- Why Architecture Support for Security? Two (and a half) stories

Overview

- Why Architecture Support for Security? Two (and a half) stories
  1. Computer system evolution

Overview

- Why Architecture Support for Security? Two (and a half) stories
  1. Computer system evolution
  2. Growing security and privacy threat

Overview

- Why Architecture Support for Security? Two (and a half) stories
  1. Computer system evolution
  2. Growing security and privacy threat
- What makes malware/attacks possible?

Overview

- Why Architecture Support for Security? Two (and a half) stories
  1. Computer system evolution
  2. Growing security and privacy threat
- What makes malware/attacks possible?
- So, what exactly is this course about?

Overview

- Why Architecture Support for Security? Two (and a half) stories
  1. Computer system evolution
  2. Growing security and privacy threat
- What makes malware/attacks possible?
- So, what exactly is this course about?
- Course mechanics: what work is required and how will I be graded?

Overview

- Why Architecture Support for Security? Two (and a half) stories
  1. Computer system evolution
  2. Growing security and privacy threat
- What makes malware/attacks possible?
- So, what exactly is this course about?
- Course mechanics: what work is required and how will I be graded?
- Reading (and writing!) papers

Trend 1: Architecture and Systems

- Moore's Law still with us for a while (transistor count increasing)
  - More cores?

Trend 1: Architecture and Systems

- Moore's Law still with us for a while (transistor count increasing)
  - More cores?
- Dennard's scaling made Moore's Law useful.

Device or Circuit Parameter	Scaling factor
Device dimension, t_{ox}, L, W	$1/\kappa$
Voltage, Current	$1/\kappa$
Capacitance	$1/\kappa$
Delay	$1/\kappa$
Power	$1/\kappa^2$
Power Density	1

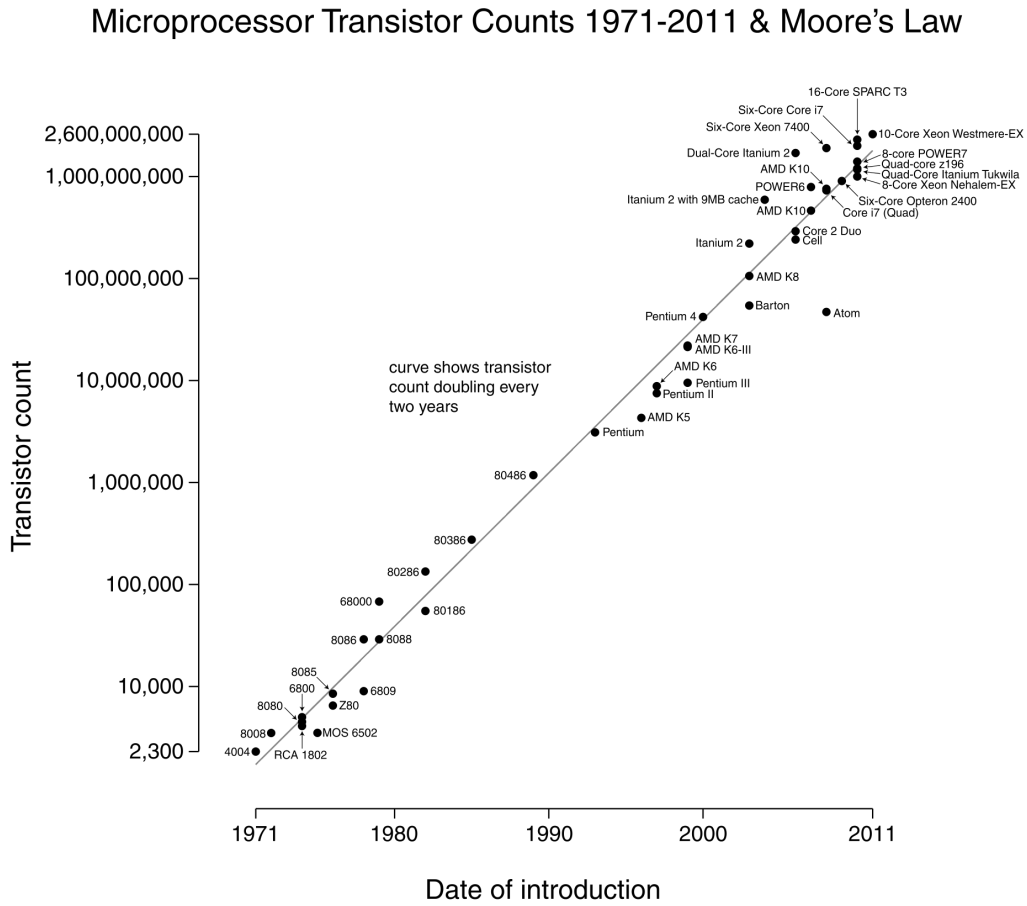
Trend 1: Architecture and Systems

- Moore's Law still with us for a while (transistor count increasing)
  - More cores?
- Dennard's scaling made Moore's Law useful.

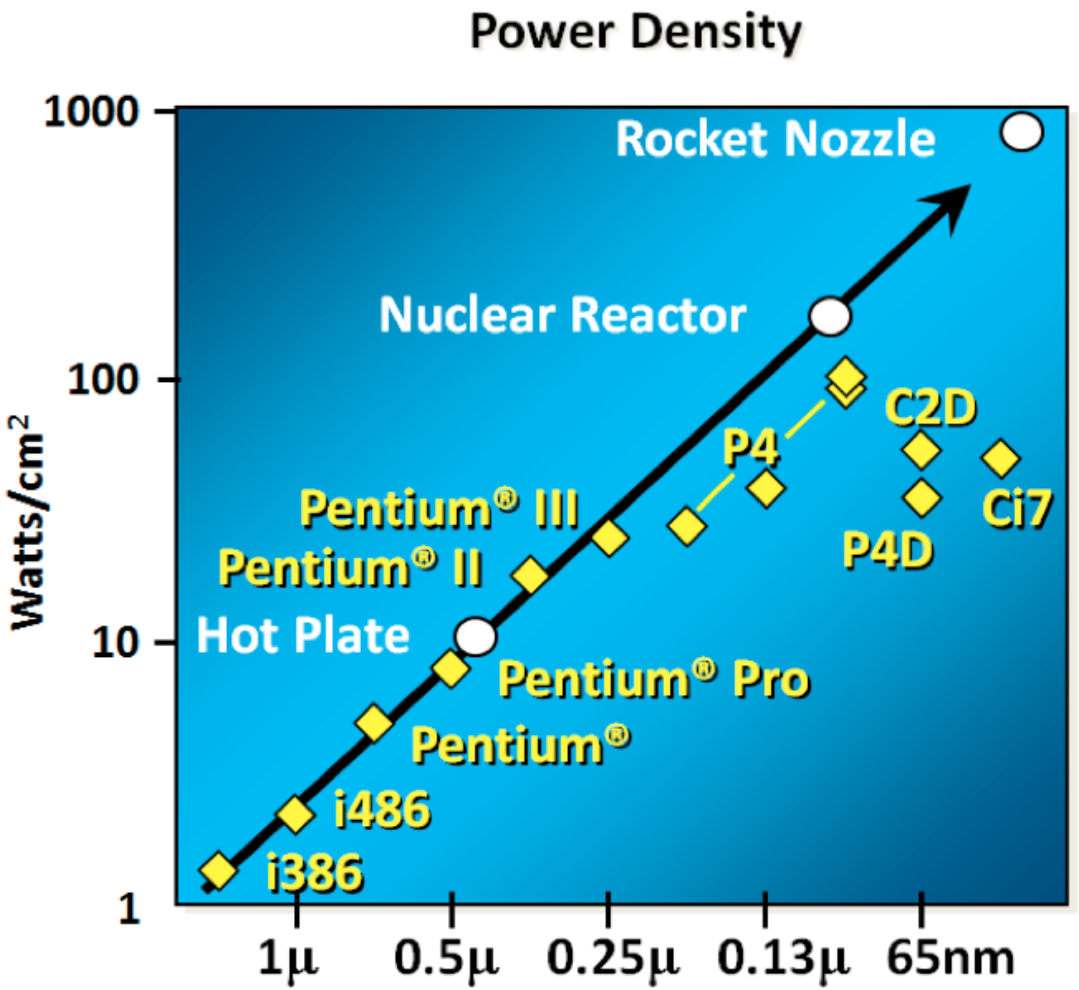
Device or Circuit Parameter	Scaling factor
Device dimension, t_{ox}, L, W	$1/\kappa$
Voltage, Current	$1/\kappa$
Capacitance	$1/\kappa$
Delay	$1/\kappa$
Power	$1/\kappa^2$
Power Density	1

- Unfortunately, Dennard's scaling stopped. Power wall is here.

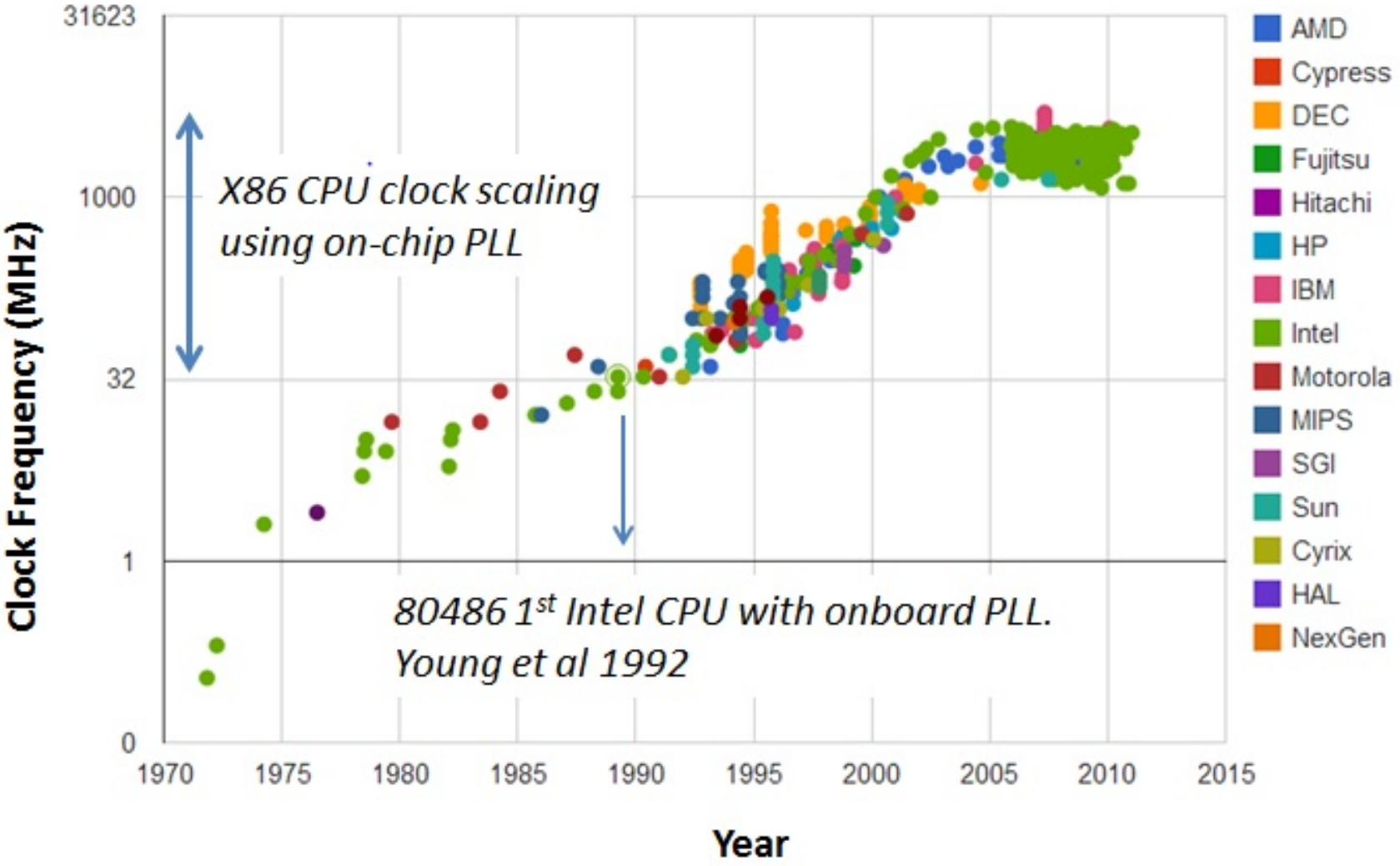
Transistor count still increasing



Power Wall


Power Density
1000
100
10
1
Watts/cm2
Rocket Nozzle
Nuclear Reactor
Hot Plate
Pentium® III
Pentium® II
Pentium® Pro
Pentium®
i486
i386
P4
C2D
P4D
Ci7
1µ
0.5µ
0.25µ
0.13µ
65nm

Power Wall (2)


31623
1000
32
1
0
Clock Frequency (MHz)
X86 CPU clock scaling
using on-chip PLL
80486 1st Intel CPU with onboard PLL.
Young et al 1992
1970
1975
1980
1985
1990
1995
2000
2005
2010
2015
Year
AMD
Cypress
DEC
Fujitsu
Hitachi
HP
IBM
Intel
Motorola
MIPS
SGI
Sun
Cyrix
HAL
NexGen

Implications–What to do with all the transistors?

Dark Silicon: at 8nm, only half the chip can be active at a time

Implications–What to do with all the transistors?

Dark Silicon: at 8nm, only half the chip can be active at a time

- Agressive power management needed: power=performance

Implications–What to do with all the transistors?

Dark Silicon: at 8nm, only half the chip can be active at a time

- Agressive power management needed: power=performance
- Specialized cores, turned on to match applications

Implications–What to do with all the transistors?

Dark Silicon: at 8nm, only half the chip can be active at a time

- Agressive power management needed: power=performance
- Specialized cores, turned on to match applications
- What to support in hardware?
  - "To achieve long battery life when playing video, mobile devices must decode the video in hardware; decoding it in software uses too much power." – Apple on Flash

Implications–What to do with all the transistors?

Dark Silicon: at 8nm, only half the chip can be active at a time

- Agressive power management needed: power=performance
- Specialized cores, turned on to match applications
- What to support in hardware?
  - "To achieve long battery life when playing video, mobile devices must decode the video in hardware; decoding it in software uses too much power." – Apple on Flash
- Innovation needed (not just in architecture–the whole system stack)

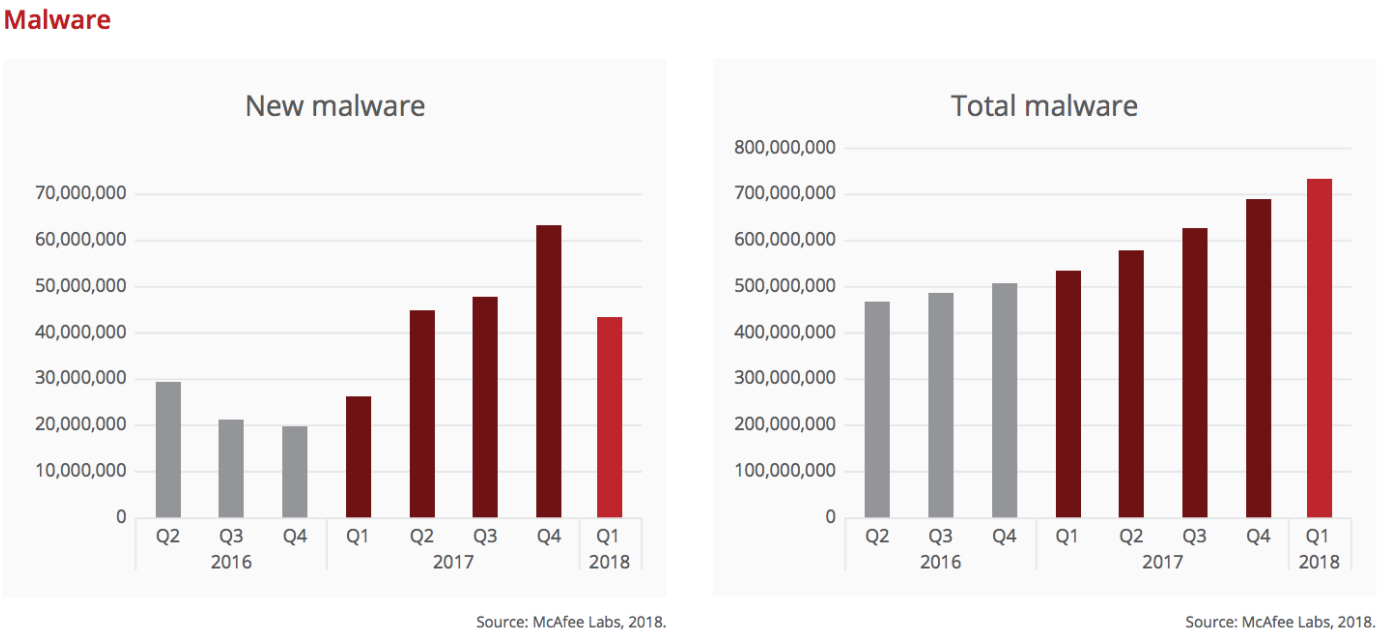
Systems are changing

- Rapid evolution in systems creating new tussle spaces
- Cloud computing, smart devices, smart grids, national infrastructure
  - New security and privacy concerns
  - New threat models and novel attacks

Systems are changing

- Rapid evolution in systems creating new tussle spaces
- Cloud computing, smart devices, smart grids, national infrastructure
  - New security and privacy concerns
  - New threat models and novel attacks
- CPU manufacturers investing in security
  - Trusted Platform Module (TPM)
  - No Execute bit (NX-bit)
  - Supervisor Mode Execution/Access Prevention (SMEP/SMAP)
  - AES Encryption Extensions
  - SHA Hash Extensions
  - MPX: Memory Protection Extensions
  - SGX –Software Guard Extensions (Isolated Execution)
  - IPT –Identity Protection Technology
  - ARM Trustzone; Amazon CloudHSM ...

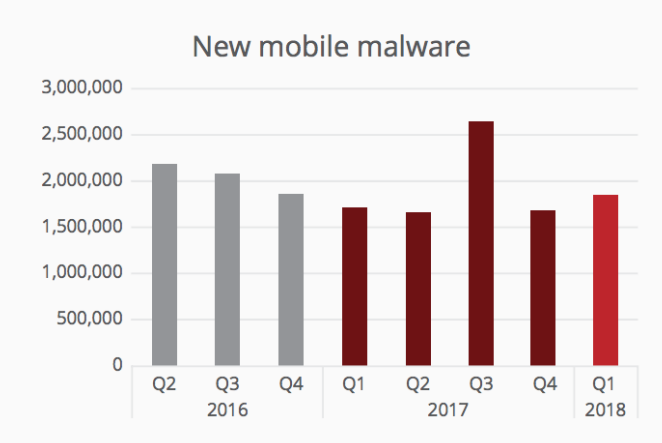
Trend 2: Malware is Brewing

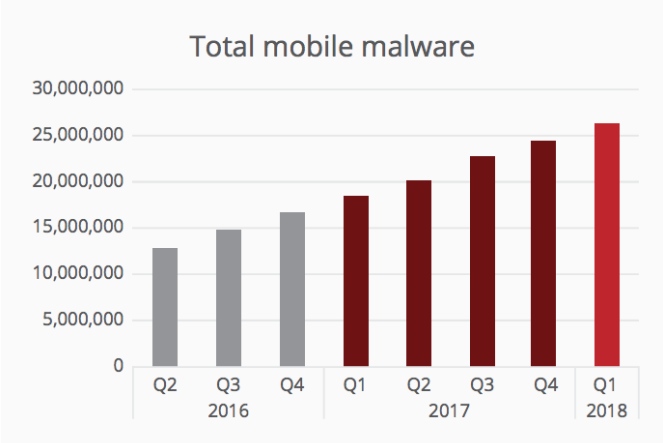


- McAfee malware "zoo" as of Q2 2018: 750 million samples
  - Over 40 mil new samples this period
  - Mobile malware arriving in earnest

Source: Mcafee Q2 2018 threat report

Trend 2: Malware is Brewing

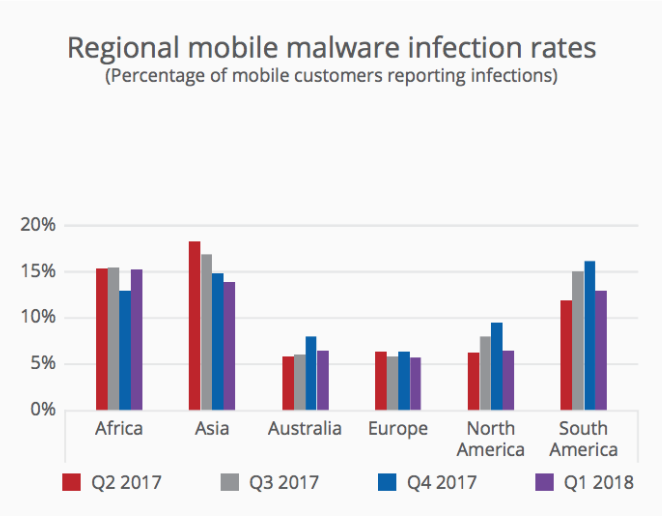




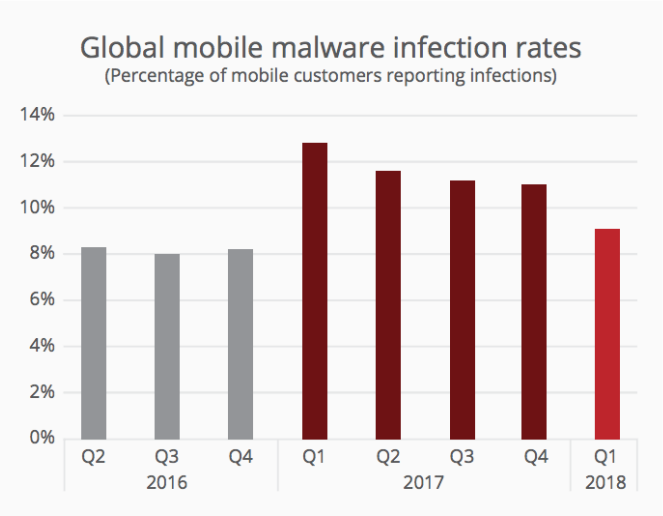
- McAfee malware "zoo" as of Q2 2018: 750 million samples
  - Over 40 mil new samples this period
  - Mobile malware arriving in earnest

Source: Mcafee Q2 2018 threat report

Trend 2: Malware is Brewing



Source: McAfee Labs, 2018.

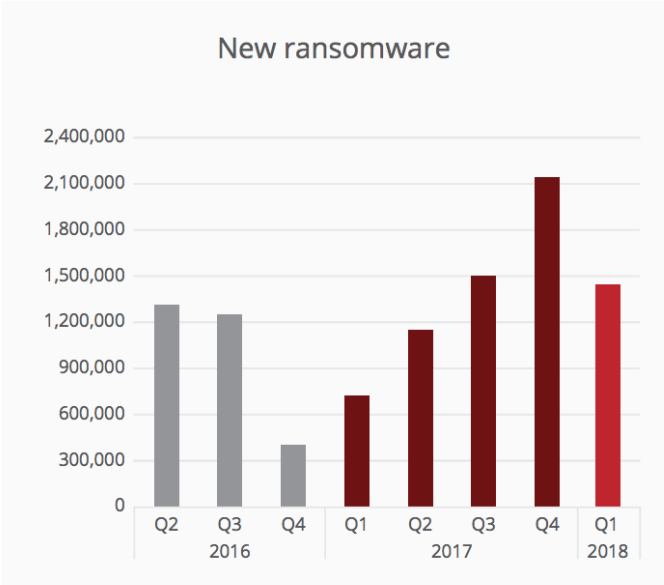


Source: McAfee Labs, 2018.

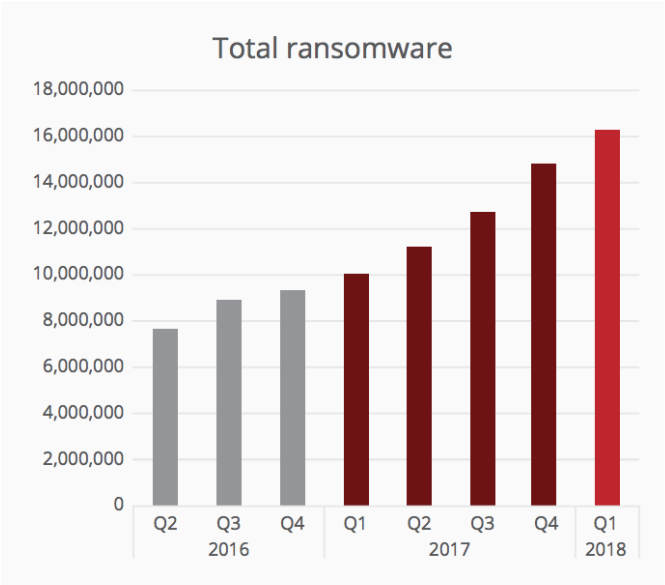
- McAfee malware "zoo" as of Q2 2018: 750 million samples
  - Over 40 mil new samples this period
  - Mobile malware arriving in earnest

Source: Mcafee Q2 2018 threat report

Trend 2: Malware is Brewing



Source: McAfee Labs, 2018.



Source: McAfee Labs, 2018.

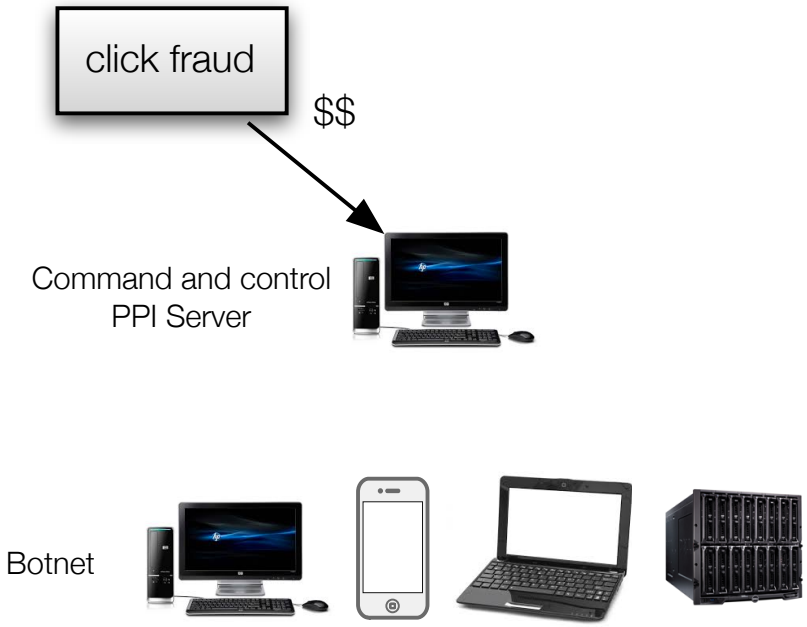
- McAfee malware "zoo" as of Q2 2018: 750 million samples
  - Over 40 mil new samples this period
  - Mobile malware arriving in earnest

Source: Mcafee Q2 2018 threat report

Underground Malware Economy: Pay-per-install

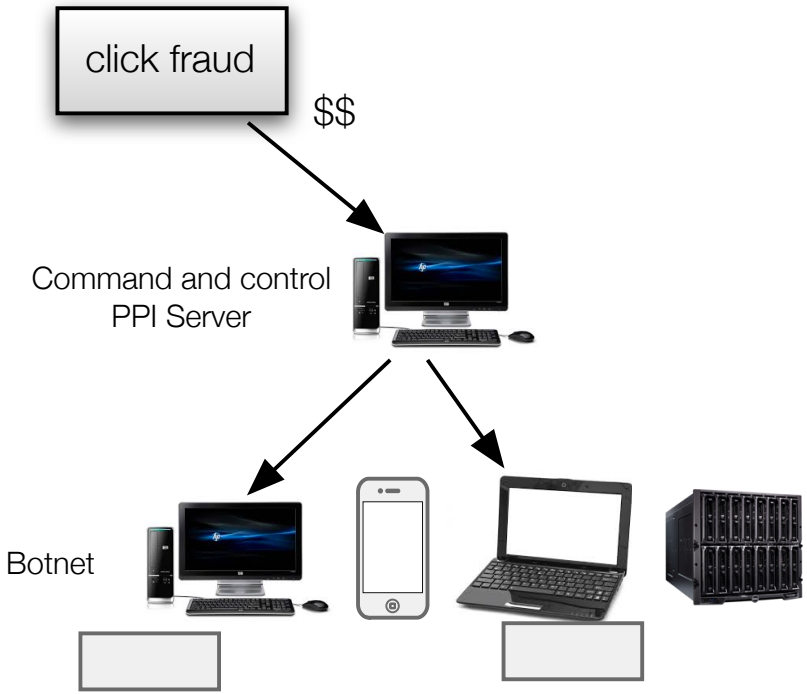
Source: Cabalerro et al. "Measuring pay-per-install..." Usenix 2011

Underground Malware Economy: Pay-per-install



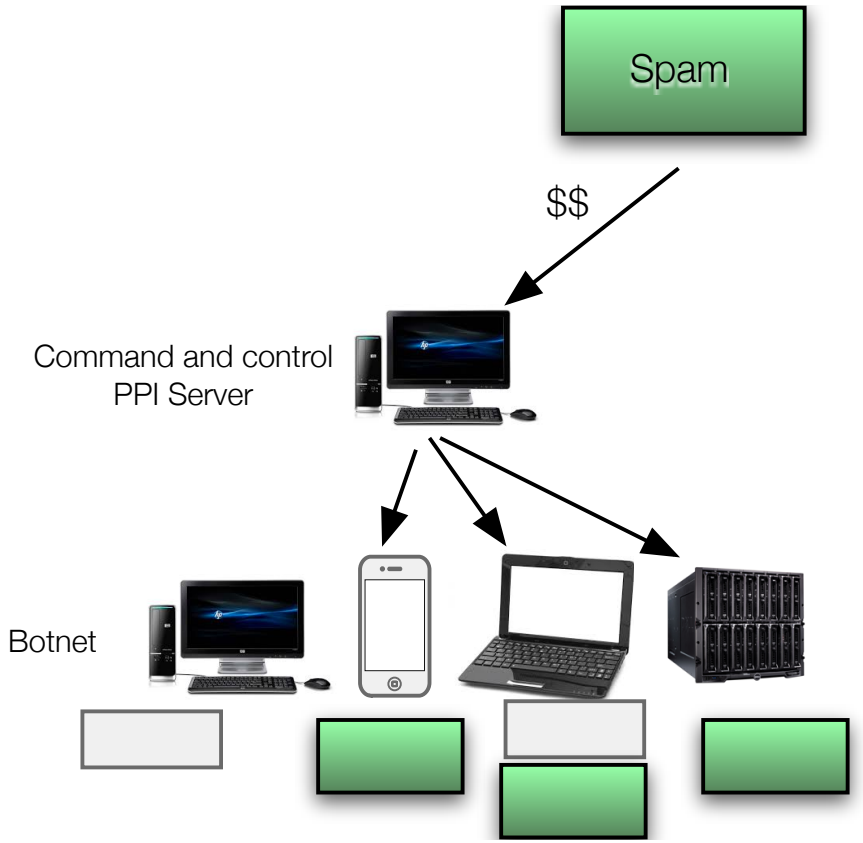
Source: Cabalerro et al. "Measuring pay-per-install..." Usenix 2011

Underground Malware Economy: Pay-per-install



Source: Cabalerro et al. "Measuring pay-per-install..." Usenix 2011

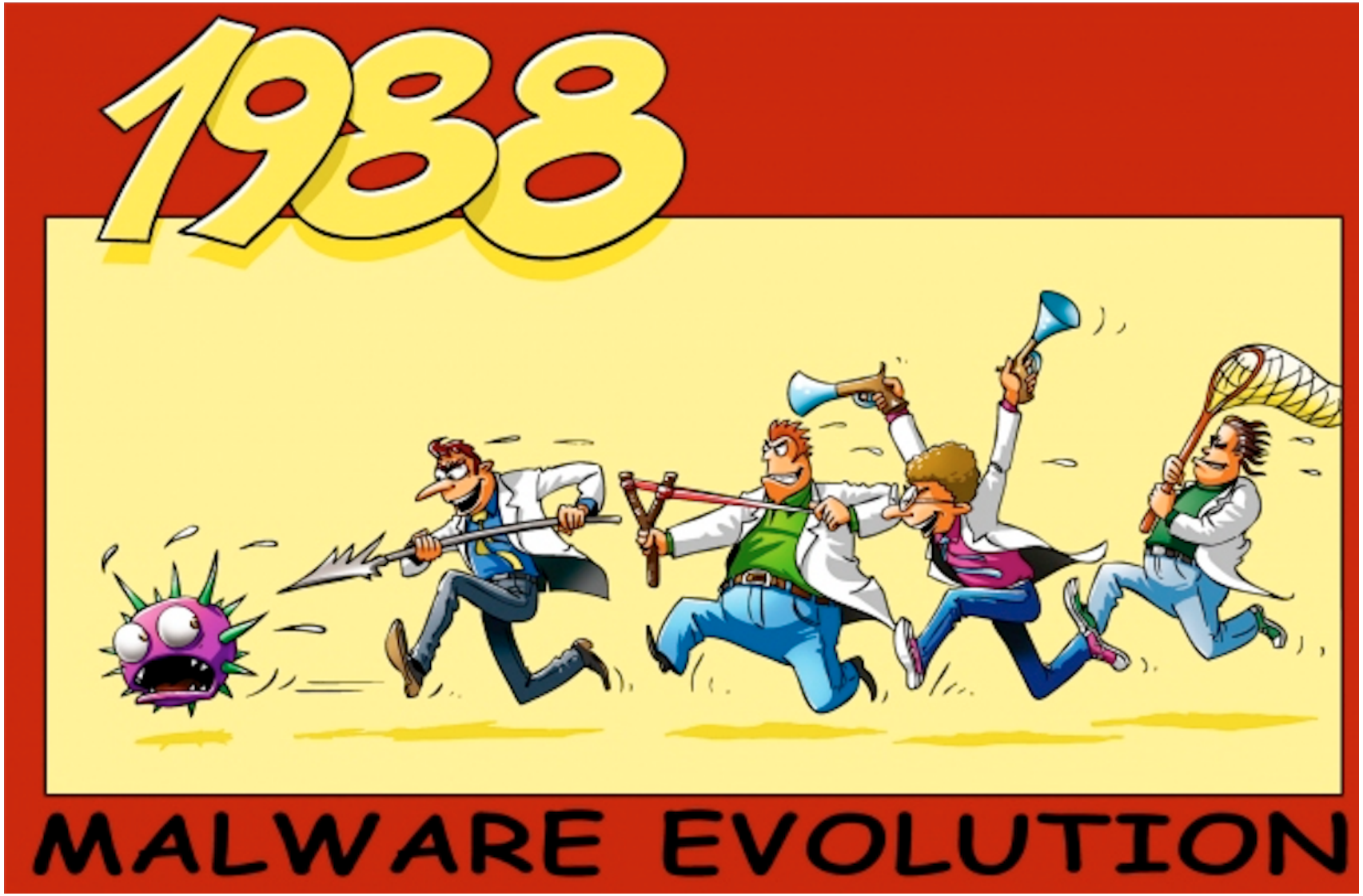
Underground Malware Economy: Pay-per-install



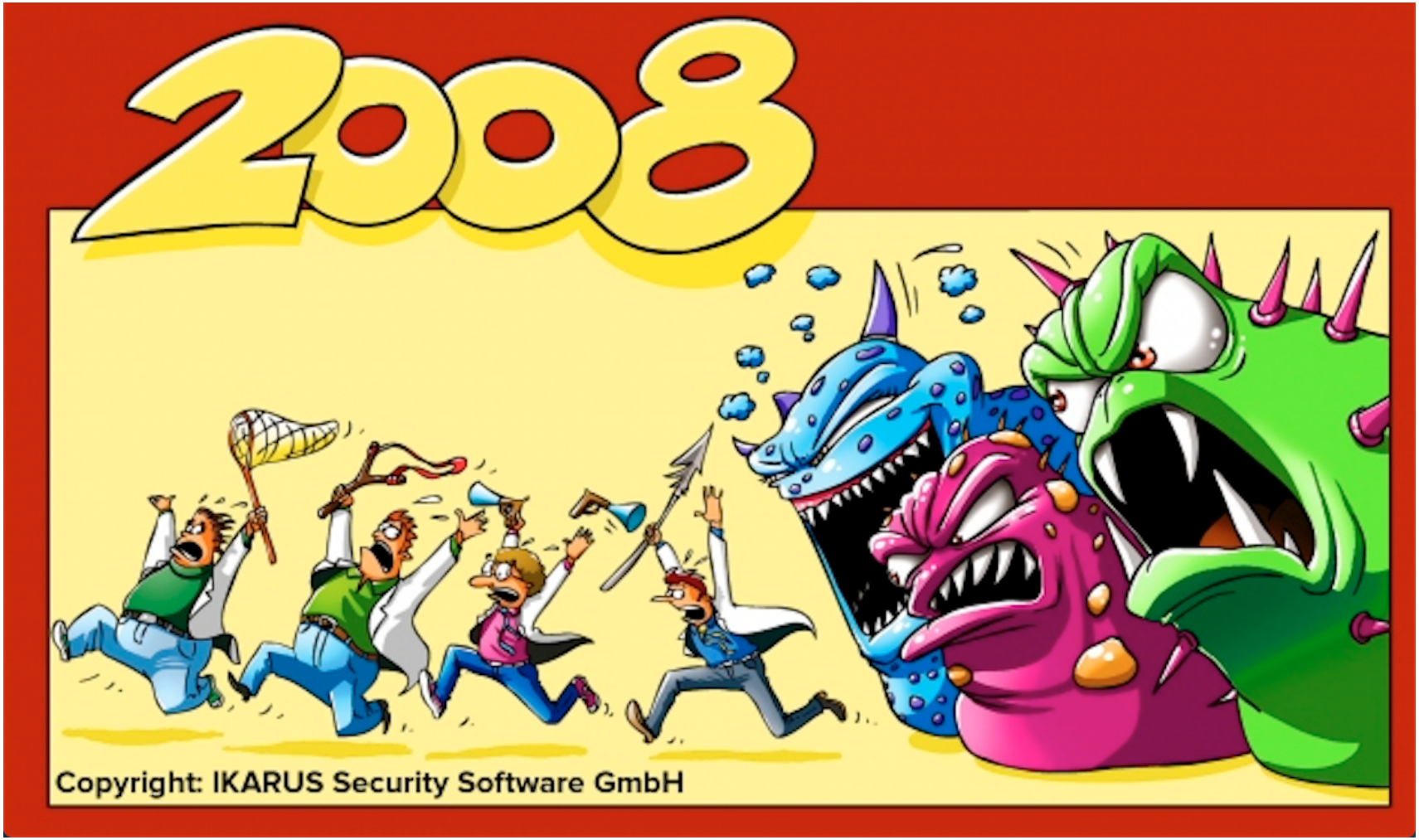
- Installs: 80-100 USD per 1000 machines (US); 7-8 USD per 1000 machines (Asia)

Source: Cabalerro et al. "Measuring pay-per-install..." Usenix 2011

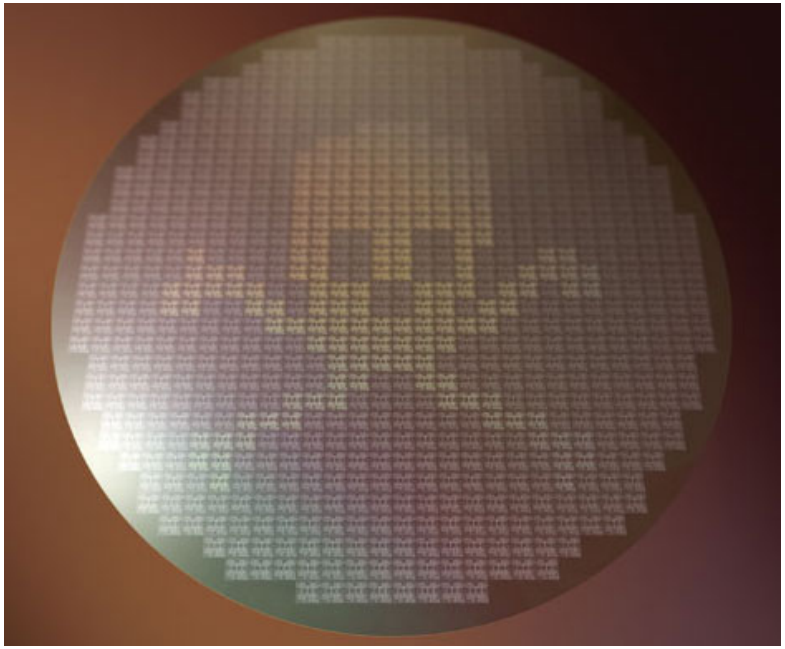
Malware: Summary



Malware: Summary

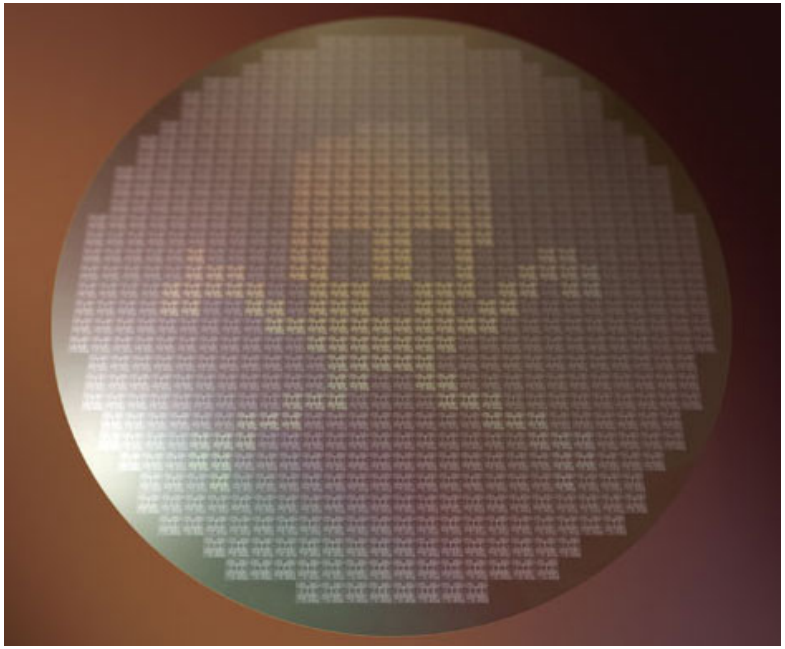


What about Hardware threats?



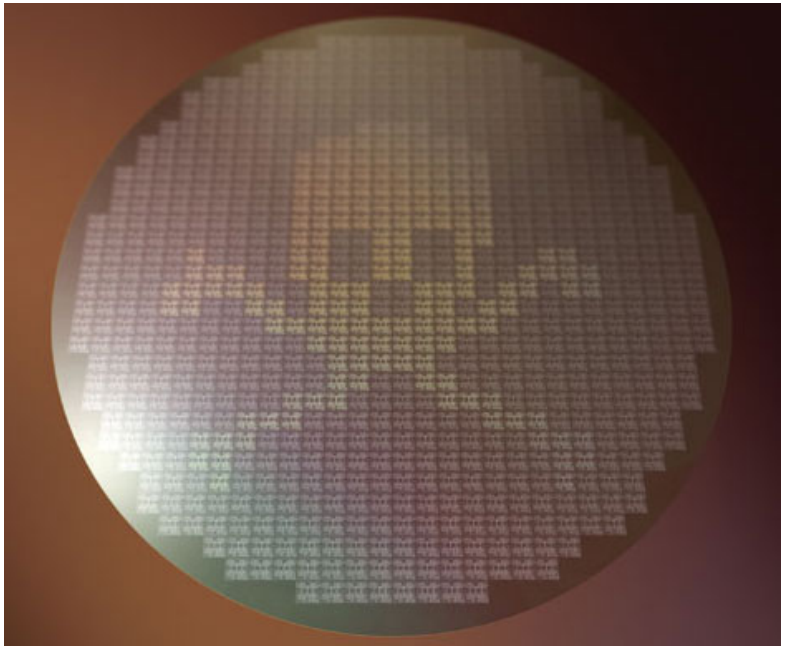
- September 2008: Israel bombs northeast Syria
  - State of the art Syrian radar system did not function–kill switch

What about Hardware threats?



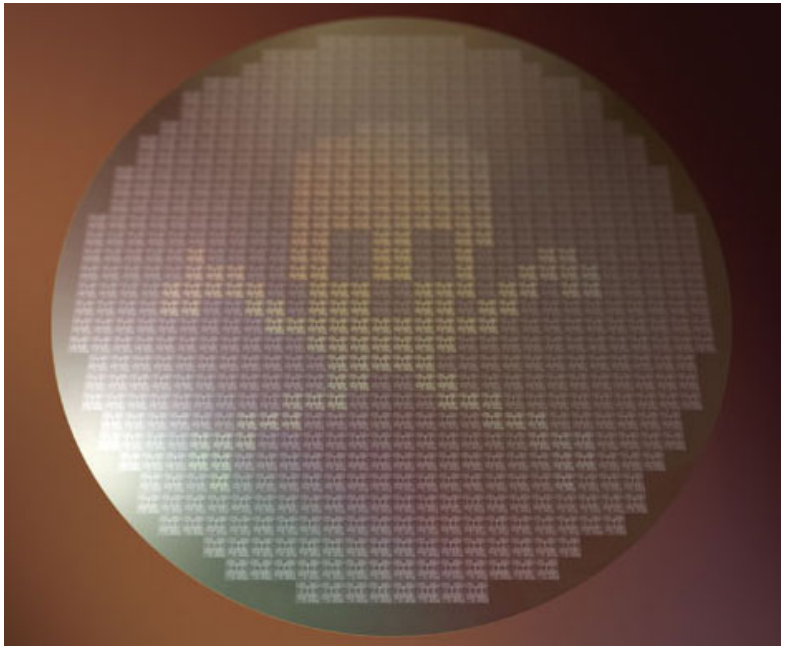
- September 2008: Israel bombs northeast Syria
  - State of the art Syrian radar system did not function–kill switch
  - Hardware Trojans: over 90% of chip foundaries are overseas

What about Hardware threats?



- September 2008: Israel bombs northeast Syria
  - State of the art Syrian radar system did not function–kill switch
  - Hardware Trojans: over 90% of chip foundaries are overseas
- Military CISCO routers discovered with many fake components from Chinese sources

What about Hardware threats?



- September 2008: Israel bombs northeast Syria
  - State of the art Syrian radar system did not function–kill switch
  - Hardware Trojans: over 90% of chip foundaries are overseas
- Military CISCO routers discovered with many fake components from Chinese sources
- How to solve this problem?

Hardware threats to security increasingly in the news!

- 2014: Rowhammer; exploited in 2015 to get root access

Hardware threats to security increasingly in the news!

- 2014: Rowhammer; exploited in 2015 to get root access
- 2017: CLOCKSCREW: fault injection through energy management

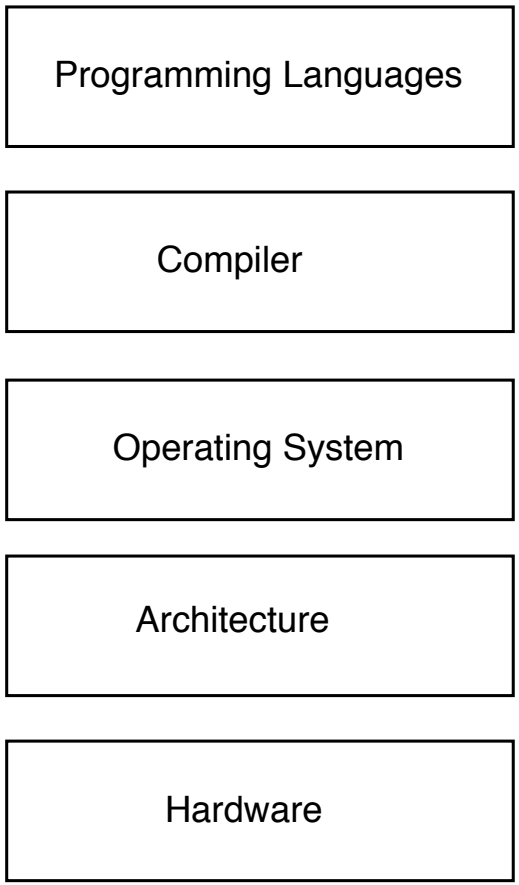
Hardware threats to security increasingly in the news!

- 2014: Rowhammer; exploited in 2015 to get root access
- 2017: CLOCKSCREW: fault injection through energy management
- 2018: Meltdown and specter

Hardware threats to security increasingly in the news!

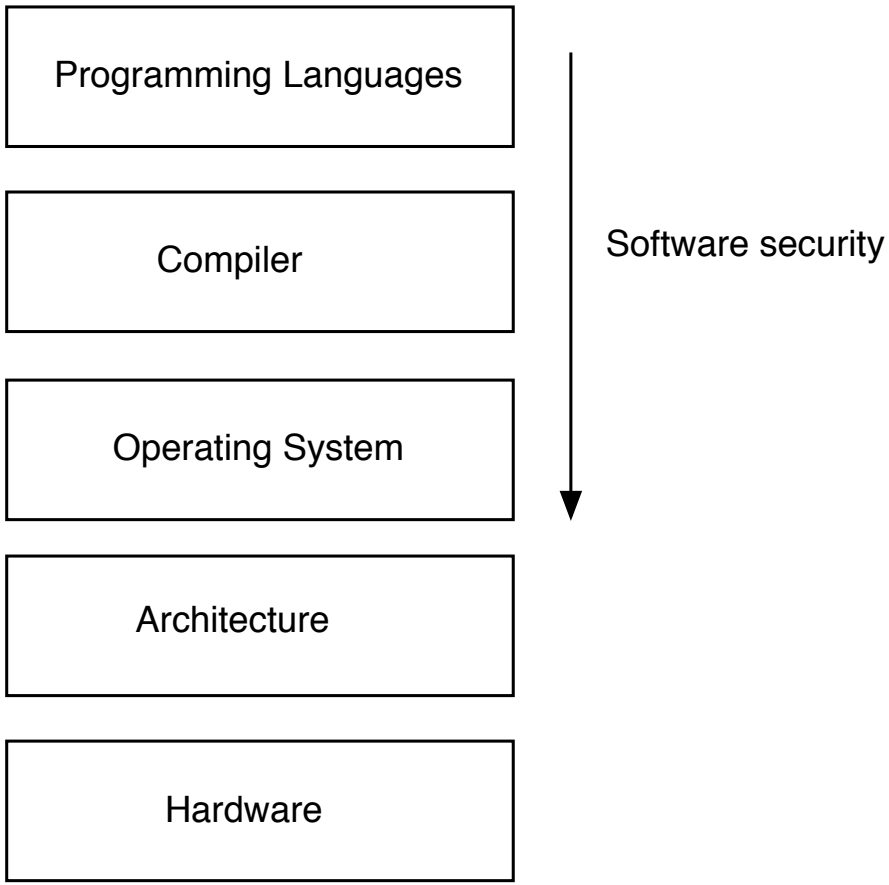
- 2014: Rowhammer; exploited in 2015 to get root access
- 2017: CLOCKSCREW: fault injection through energy management
- 2018: Meltdown and specter
- Many others...

What this course is about: HW Support for Security



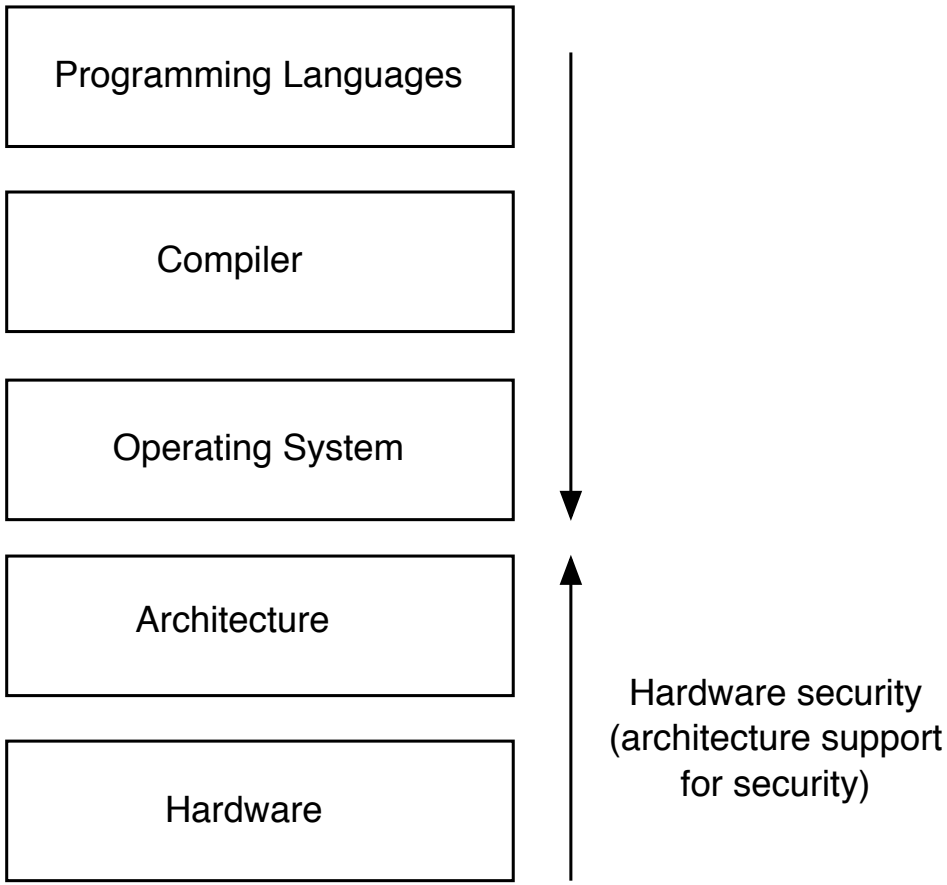
- Hardware vs. Architecture security; we'll do both
- Understand vulnerabilities – explore defenses

What this course is about: HW Support for Security



- Hardware vs. Architecture security; we'll do both
- Understand vulnerabilities – explore defenses

What this course is about: HW Support for Security



- Hardware vs. Architecture security; we'll do both
- Understand vulnerabilities – explore defenses

What are the Enablers for Software Based Attacks?

- Root causes of malware:

What are the Enablers for Software Based Attacks?

- Root causes of malware:
  1. Buggy software (how exactly? Next class)

Software	Lines of Code	Vulnerabilities
Xen	200K	59
Linux kernel	15M	228

What are the Enablers for Software Based Attacks?

- Root causes of malware:
  1. Buggy software (how exactly? Next class)

Software	Lines of Code	Vulnerabilities
Xen	200K	59
Linux kernel	15M	228

  2. Gullible/imperfect people
     - phishing; spear-phishing; repackaged applications; social engineering; insider attacks ...
     - Michigan county lost $1.2 mil to Nigerian Prince scam

What are the Enablers for Software Based Attacks?

- Root causes of malware:
  1. Buggy software (how exactly? Next class)

Software	Lines of Code	Vulnerabilities
Xen	200K	59
Linux kernel	15M	228

  2. Gullible/imperfect people
     - phishing; spear-phishing; repackaged applications; social engineering; insider attacks ...
     - Michigan county lost $1.2 mil to Nigerian Prince scam
  3. ...but also permissive systems

What are the Enablers for Software Based Attacks?

- Root causes of malware:
  1. Buggy software (how exactly? Next class)

Software	Lines of Code	Vulnerabilities
Xen	200K	59
Linux kernel	15M	228

  2. Gullible/imperfect people
     - phishing; spear-phishing; repackaged applications; social engineering; insider attacks ...
     - Michigan county lost $1.2 mil to Nigerian Prince scam
  3. ...but also permissive systems
     - Single vulnerability can compromise entire system

What are the Enablers for Software Based Attacks?

- Root causes of malware:
  1. Buggy software (how exactly? Next class)

Software	Lines of Code	Vulnerabilities
Xen	200K	59
Linux kernel	15M	228

  2. Gullible/imperfect people
     - phishing; spear-phishing; repackaged applications; social engineering; insider attacks ...
     - Michigan county lost $1.2 mil to Nigerian Prince scam
  3. ...but also permissive systems
     - Single vulnerability can compromise entire system
     - Same vulnerability can attack many machines with similar code base

What are the Enablers for Software Based Attacks?

- Root causes of malware:
  1. Buggy software (how exactly? Next class)

Software	Lines of Code	Vulnerabilities
Xen	200K	59
Linux kernel	15M	228

  2. Gullible/imperfect people
     - phishing; spear-phishing; repackaged applications; social engineering; insider attacks ...
     - Michigan county lost $1.2 mil to Nigerian Prince scam
  3. ...but also permissive systems
     - Single vulnerability can compromise entire system
     - Same vulnerability can attack many machines with similar code base
     - Privilege tussles: protection software can be disabled by attacker

What are the Enablers for Software Based Attacks?

- Root causes of malware:
  1. Buggy software (how exactly? Next class)

Software	Lines of Code	Vulnerabilities
Xen	200K	59
Linux kernel	15M	228

  2. Gullible/imperfect people
     - phishing; spear-phishing; repackaged applications; social engineering; insider attacks ...
     - Michigan county lost $1.2 mil to Nigerian Prince scam
  3. ...but also permissive systems
     - Single vulnerability can compromise entire system
     - Same vulnerability can attack many machines with similar code base
     - Privilege tussles: protection software can be disabled by attacker
     - Detection (and some prevention) is difficult (computational problem)

- Other attacks: physical attacks; hardware-sourced attacks; side-channel attacks; ...

Discussion: What role should hardware security play?

Discussion: What role should hardware security play?

- What is the advantage of hardware/architecture solutions vs. software ones?

Discussion: What role should hardware security play?

- What is the advantage of hardware/architecture solutions vs. software ones?
- What are the strengths of hardware vs. software?

Discussion: What role should hardware security play?

- What is the advantage of hardware/architecture solutions vs. software ones?
- What are the strengths of hardware vs. software?
- What are some weaknesses?

Discussion: What role should hardware security play?

- What is the advantage of hardware/architecture solutions vs. software ones?
- What are the strengths of hardware vs. software?
- What are some weaknesses?
- Confused: what is the difference?
  - Hardware is software? Hardware description languages
  - Hardware is software? FPGAs? Emulation

Intersection of Architecture and Security?

- Vulnerabilities originating in architecture
  - Side and covert channels
  - Speculation attacks
  - Fault injection
  - Exploitable bugs
  - Hardware trojans, ...

Intersection of Architecture and Security?

- Vulnerabilities originating in architecture
  - Side and covert channels
  - Speculation attacks
  - Fault injection
  - Exploitable bugs
  - Hardware trojans, ...
- Defenses rooted in architecture
  - Do no harm
    - Avoid vulnerabilities in architecture/HW
  - Help software
    - Security abstractions/mechanisms
    - Computational support for expensive defenses

Role of Hardware in Supporting Security

1. New models for supporting security; forget ambient authority
   - Access control models; capabilities; isolated execution
   - Trusted computing base
2. Computational Side of security
   - Support for reference monitors
   - Support for intrusion detection
   - Exploit new security primitives
3. Protection against Physical, Hardware and Microarchitecture based attacks
   - Hardware Trojans and counterfeit chips
   - Side channel attack, covert channel and denial of service
   - Physical attacks
4. Security support for emerging platforms
   - NVMs; embedded systems; cyberphysical systems

Role of Hardware in Supporting Security

1. New models for supporting security; forget ambient authority
   - Access control models; capabilities; isolated execution
   - Trusted computing base
2. Computational Side of security
   - Support for reference monitors
   - Support for intrusion detection
   - Exploit new security primitives
3. Protection against Physical, Hardware and Microarchitecture based attacks
   - Hardware Trojans and counterfeit chips
   - Side channel attack, covert channel and denial of service
   - Physical attacks
4. Security support for emerging platforms
   - NVMs; embedded systems; cyberphysical systems

Lets take a look at the tentative schedule

Course Mechanics: Overview

- Good news: no planned exams, homeworks, anything
  - Read, learn, discuss, enjoy

Course Mechanics: Overview

- Good news: no planned exams, homeworks, anything
  - Read, learn, discuss, enjoy
- Required work

Course Mechanics: Overview

- Good news: no planned exams, homeworks, anything
  - Read, learn, discuss, enjoy
- Required work
  - Required reading before class (more in a second)

Course Mechanics: Overview

- Good news: no planned exams, homeworks, anything
  - Read, learn, discuss, enjoy
- Required work
  - Required reading before class (more in a second)
    - Reading load, typically 1 paper for most classes

Course Mechanics: Overview

- Good news: no planned exams, homeworks, anything
  - Read, learn, discuss, enjoy
- Required work
  - Required reading before class (more in a second)
    - Reading load, typically 1 paper for most classes
    - Should spend about 2 hours to read before class and be ready to discuss

Course Mechanics: Overview

- Good news: no planned exams, homeworks, anything
  - Read, learn, discuss, enjoy
- Required work
  - Required reading before class (more in a second)
    - Reading load, typically 1 paper for most classes
    - Should spend about 2 hours to read before class and be ready to discuss
    - I'll ask you for a one page review for about half of the papers – you should try to do all

Course Mechanics: Overview

- Good news: no planned exams, homeworks, anything
  - Read, learn, discuss, enjoy
- Required work
  - Required reading before class (more in a second)
    - Reading load, typically 1 paper for most classes
    - Should spend about 2 hours to read before class and be ready to discuss
    - I'll ask you for a one page review for about half of the papers – you should try to do all
    - I (or one of you) will discuss other papers for each topic

Course Mechanics: Overview

- Good news: no planned exams, homeworks, anything
  - Read, learn, discuss, enjoy
- Required work
  - Required reading before class (more in a second)
    - Reading load, typically 1 paper for most classes
    - Should spend about 2 hours to read before class and be ready to discuss
    - I'll ask you for a one page review for about half of the papers – you should try to do all
    - I (or one of you) will discuss other papers for each topic
  - One or two presentations (i.e., you lead the discussion of a paper)
  - Could be on a topic that will become either a mini-survey or a project
  - Come up with discussion points

Course Mechanics: Survey or Project?

Course Mechanics: Survey or Project?

- Project is ambitious: have to identify a problem, learn tools, experiment, etc...
  - But could be very rewarding and you learn to do research in a new area
  - OK to repeat or slightly extend a paper you like; better if it is something new
  - Quarter is short: must have a proposal by end of week 4
  - Survey is significantly less work

Course Mechanics: Survey or Project?

- Project is ambitious: have to identify a problem, learn tools, experiment, etc...
  - But could be very rewarding and you learn to do research in a new area
  - OK to repeat or slightly extend a paper you like; better if it is something new
  - Quarter is short: must have a proposal by end of week 4
  - Survey is significantly less work
- What are the tools of the trade?
  - Simulators such as Gem5, MarSSx86, Wattch, GPGPUSim, DRAMSim, etc...
  - Hardware description languages and open cores; get your hardware to run on FPGA
  - Experimentation for attacks
  - Software analysis tools (PIN, IDAPro, ...)
  - Security analysis

How to read a research paper?

- Read Mitzenmacher and Keshav's advice (this class' reading!)

How to read a research paper?

- Read Mitzenmacher and Keshav's advice (this class' reading!)
- Mitzenmacher: Read critically; read creatively

How to read a research paper?

- Read Mitzenmacher and Keshav's advice (this class' reading!)
- Mitzenmacher: Read critically; read creatively
- Read in two passes (Keshav likes 3!)

How to read a research paper?

- Read Mitzenmacher and Keshav's advice (this class' reading!)
- Mitzenmacher: Read critically; read creatively
- Read in two passes (Keshav likes 3!)
- Writing Summary (Mitzenmacher):

How to read a research paper?

- Read Mitzenmacher and Keshav's advice (this class' reading!)
- Mitzenmacher: Read critically; read creatively
- Read in two passes (Keshav likes 3!)
- Writing Summary (Mitzenmacher):
  - a one or two sentence summary of the paper.

How to read a research paper?

- Read Mitzenmacher and Keshav's advice (this class' reading!)
- Mitzenmacher: Read critically; read creatively
- Read in two passes (Keshav likes 3!)
- Writing Summary (Mitzenmacher):
  - a one or two sentence summary of the paper.
  - a deeper, more extensive outline of the main points of the paper, including for example assumptions made, arguments presented, data analyzed, and conclusions drawn.

How to read a research paper?

- Read Mitzenmacher and Keshav's advice (this class' reading!)
- Mitzenmacher: Read critically; read creatively
- Read in two passes (Keshav likes 3!)
- Writing Summary (Mitzenmacher):
  - a one or two sentence summary of the paper.
  - a deeper, more extensive outline of the main points of the paper, including for example assumptions made, arguments presented, data analyzed, and conclusions drawn.
  - any limitations or extensions you see for the ideas in the paper.

How to read a research paper?

- Read Mitzenmacher and Keshav's advice (this class' reading!)
- Mitzenmacher: Read critically; read creatively
- Read in two passes (Keshav likes 3!)
- Writing Summary (Mitzenmacher):
  - a one or two sentence summary of the paper.
  - a deeper, more extensive outline of the main points of the paper, including for example assumptions made, arguments presented, data analyzed, and conclusions drawn.
  - any limitations or extensions you see for the ideas in the paper.
  - your opinion of the paper; primarily, the quality of the ideas and its potential impact.

How to read a research paper?

- Read Mitzenmacher and Keshav's advice (this class' reading!)
- Mitzenmacher: Read critically; read creatively
- Read in two passes (Keshav likes 3!)
- Writing Summary (Mitzenmacher):
  - a one or two sentence summary of the paper.
  - a deeper, more extensive outline of the main points of the paper, including for example assumptions made, arguments presented, data analyzed, and conclusions drawn.
  - any limitations or extensions you see for the ideas in the paper.
  - your opinion of the paper; primarily, the quality of the ideas and its potential impact.
- Specializing to security papers

How to read a research paper?

- Read Mitzenmacher and Keshav's advice (this class' reading!)
- Mitzenmacher: Read critically; read creatively
- Read in two passes (Keshav likes 3!)
- Writing Summary (Mitzenmacher):
  - a one or two sentence summary of the paper.
  - a deeper, more extensive outline of the main points of the paper, including for example assumptions made, arguments presented, data analyzed, and conclusions drawn.
  - any limitations or extensions you see for the ideas in the paper.
  - your opinion of the paper; primarily, the quality of the ideas and its potential impact.
- Specializing to security papers
  - Pay attention to the threat model

How to read a research paper?

- Read Mitzenmacher and Keshav's advice (this class' reading!)
- Mitzenmacher: Read critically; read creatively
- Read in two passes (Keshav likes 3!)
- Writing Summary (Mitzenmacher):
  - a one or two sentence summary of the paper.
  - a deeper, more extensive outline of the main points of the paper, including for example assumptions made, arguments presented, data analyzed, and conclusions drawn.
  - any limitations or extensions you see for the ideas in the paper.
  - your opinion of the paper; primarily, the quality of the ideas and its potential impact.
- Specializing to security papers
  - Pay attention to the threat model
  - Why hardware/architecture?

How to read a research paper?

- Read Mitzenmacher and Keshav's advice (this class' reading!)
- Mitzenmacher: Read critically; read creatively
- Read in two passes (Keshav likes 3!)
- Writing Summary (Mitzenmacher):
  - a one or two sentence summary of the paper.
  - a deeper, more extensive outline of the main points of the paper, including for example assumptions made, arguments presented, data analyzed, and conclusions drawn.
  - any limitations or extensions you see for the ideas in the paper.
  - your opinion of the paper; primarily, the quality of the ideas and its potential impact.
- Specializing to security papers
  - Pay attention to the threat model
  - Why hardware/architecture?
  - Evaluation: performance, complexity, practicality/deployment, security