Data Buddies Survey

UNC
DEPARTMENT OF
COMPUTER SCIENCE

CRA
Computing Research
Association

Undergraduate Survey
http://bit.ly/CSundergraduate

Graduate Survey
http://bit.ly/CSgraduate

What is it?
○ Anonymous survey provided by CRA open now through Oct. 31st

Why is it important?
○ Your feedback gives department real-time data on curriculum, pedagogy, student support and cultural climate from student POV

What's in it for you?
○ Completion of survey means raffle entry and chance to win Amazon gift card *(dept to raffle more than $1K in gift cards)*

Check your email for more details

Malware

COMP 435
Fall 2017
Prof. Cynthia Sturton

Spam

3

Monetizing Spam

- Advertising
- Phishing
- Scams
- Stock price manipulation
- New bots

4

Monetizing Spam

- 60% -- 90% of all email

- 10s of billions of spam messages

- Most spam is never delivered

- Success rates:
  - 1/200,000 (.0005%) malware hit rate
  - 1/12,000,000 (.0000083%) purchase

- Revenue: $1.5-2M/year

Phishing, Spear Phishing

Trick the recipient into taking unsafe action

Email Attack Countermeasures

- User vigilance

- Filtering by email providers

Denial of Service

Attacks on Availability

- Overload capacity

- Block access ransomware

- Component failure

Overloading Capacity
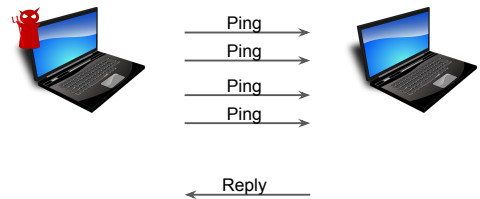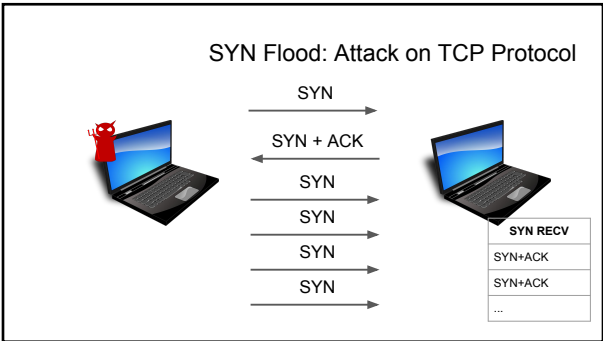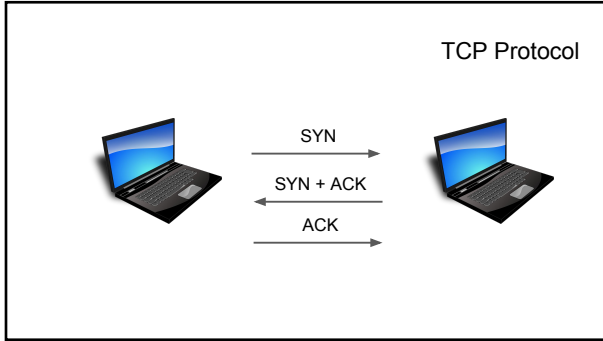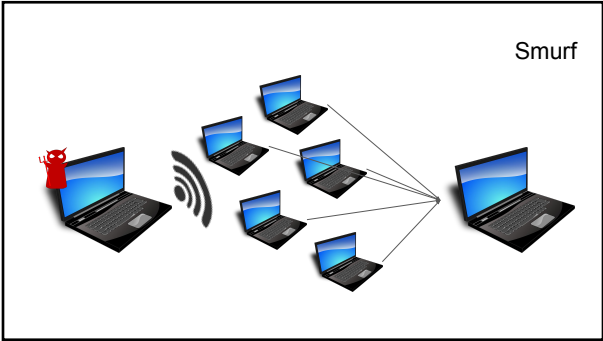
- Ping of Death

- Smurf

- SYN Flood

- DDOS

Ping

- Internet Control Message Protocol (ICMP)

- Send & Reply

- Tests reachability and availability of destination

Ping of Death

Ping
Ping
Ping
Ping

Reply

Smurf

TCP Protocol

SYN

SYN + ACK

ACK

SYN Flood: Attack on TCP Protocol

SYN

SYN + ACK
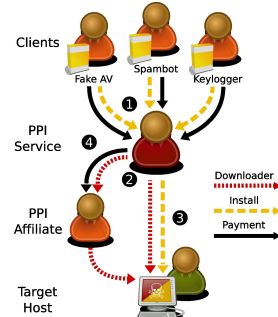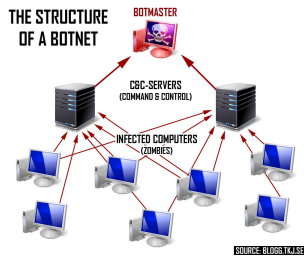
SYN

SYN

SYN

SYN

| SYN RECV |
| SYN+ACK |
| SYN+ACK |
| ... |

Underground Economy

Distributed Denial of Service

"Measuring Pay-per-Install: The Commoditization of Malware Distribution," Caballero et al. 2011

Threats to the Underground Economy

- Identification and authentication

- Single point of failure

- No honor among thieves