# SD3 Secure Web Application Development

## ECommerce Security Issues

# Ecommerce Security Issues

- In this lecture …
  - Modification of Data
  - Denial of Service
  - Errors in Software
  - Repudiation

# Modification of Data

- Loss of data could be damaging, but modification could be worse.
  - What if someone gained access to your database and modified data?
- Wholesale deletion would be noticed but what about minor changes?
- Modifications could include changes to data or replacement of executable files.
- You can protect data from modification as it travels over a network by using digital signatures.
  - It doesn't stop the modification of data.
  - It alerts users to the modification of data.

# Modification of Data

- Files on servers should be protected by using the permission facilities your O/S provides.
- Detecting modification can be difficult.
  - By its very nature data is supposed to change.
- File integrity software can be used to verify if files have changed.
  - Tripwire – offer a suite of products, some of which are free.

# Denial of Service

- Occurs when somebody's actions make it difficult/impossible for users to access a service or delay their access to a time-critical service. Very difficult to defend against.
- The first DoS attacks were noticed in 2000 when a number of high profile sites were subject to DoS attacks.
  - Yahoo!
  - eBay
  - Amazon


- These sites are vulnerable to being shut for hours.

# Denial of Service

- Crackers have little to gain from shutting a site.
  - The site could lose money, time and its reputation.
- Some sites are susceptible to DoS because they have specific times when they expect to do most of their business.
  - Paddy Power – just before a big race/game.
- Crackers tried to extort money from online bookies in 2004 by threatening to attack during peak times.
- DoS is difficult to defend against.
  - It can be carried out in a large number of varied ways.

# Denial of Service

- Methods of attack include:
  - Installing software on the targets machine that uses most of its processor time.
  - Reverse spamming is where thousands of spam emails are sent out to the public with the target listed as the sender…..leads to lots of unhappy customers and angry replies.
  - Using an automated tool to scan the Internet looking for vulnerable machines and installing a tool on them. Once a large number of machines have been co-opted they are instructed to flood the target with network traffic all at once.

# Denial of Service

- Methods of defence?
  - Try to identify the port numbers used by common DoS tools and shut them.
  - Limit the percentage of traffic that uses particular protocols like ICMP.
  - Analyse packets entering the network.
    - The router samples packets and exports a datagram containing information about that packet.
    - This is commonly available technology, scales well, and is quite adequate to indicate trends in network traffic.

# Popularity of Denial of Service Attacks

- DDoS attacks are not only on the rise—they're also bigger and more devastating than ever before.
- From independent websites to multinational banks, it seems like no one is immune.
- In fact, a 2017 report from Cisco found that the number of DD0S attacks exceeding 1 gigabit per second of traffic will rise to 3.1 million by 2021, a 2.5-fold increase from 2016.

# What is a DDOS Attack?

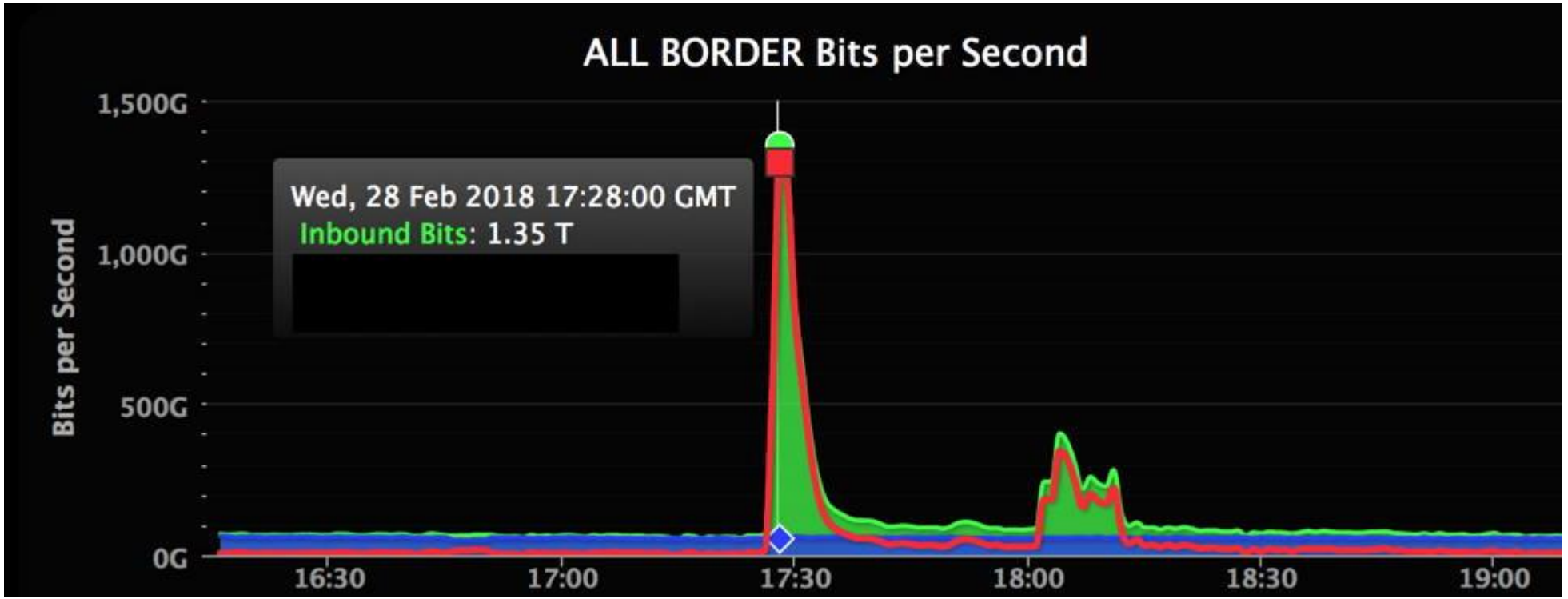
- DDoS stands for Distributed Denial of Service, which refers to the deployment of large numbers of internet bots—anywhere from hundreds to hundreds of thousands. These bots are designed to attack a single server, network or application with an overwhelming number of requests, packets or messages, thereby denying service to legitimate users such as employees or customers.
- Usually, attackers begin a DDoS attack by exploiting a vulnerability in a single computer system. The attacker's system then becomes the DDoS master and works to identify other vulnerable systems to turn them into bots.
- The perpetrator directs those computer bots to attack through the use of a command-and-control server, or botnet. At that point, all the attacker has to do is tell the bots who to target.

# Recent High Profile Denial of Service Attacks: GitHub

- On Feb. 28, 2018, GitHub was hit with a sudden onslaught of traffic that clocked in at 1.35 terabits per second. If that sounds like a lot, that's because it is—that amount of traffic is not only massive, it's record-breaking.
- According to GitHub, the traffic was traced back to "over a thousand different autonomous systems (ASNs) across tens of thousands of unique endpoints."
- What's worse is that GitHub was not entirely unprepared for a DDoS attack—they simply had no way of knowing that an attack of this scale would be launched.

# Recent High Profile Denial of Service Attacks: GitHub

- In this graph, you can see just how much of a difference there was between normal traffic levels and those of the attack:




- https://thehackernews.com/2018/03/biggest-ddos-attack-github.html

# Recent High Profile Denial of Service Attacks: The Carphone Warehouse

- The Carphone Warehouse was subjected to a DDoS attack on August 5th 2015.
- Hackers bombarded Carphone Warehouse with online traffic as a smokescreen while they stole the personal and banking details of 2.4 million people.
- Its online retail systems had come under bombardment before the major data theft was noticed.
- Hackers who steal personal data often sell

it in bulk on digital black markets to other

criminals who seek to use it to commit fraud.

# Recent High Profile Denial of Service Attacks: The Carphone Warehouse

- These types of frequent DDoS attacks are typically intended to distract corporate security teams.
  - They leave enough bandwidth available for a subsequent attack to infiltrate the victim's network.
  - This technique of DDoS as a smokescreen is becoming a more commonplace threat, especially for any internet-connected business that is housing sensitive data, such as credit card details or other personally identifiable information.
- http://news.sky.com/story/1532547/millions-hit-by-carphone-warehouse-cyber-attack

# Errors in Software

- All software could have serious errors in it.
- Web projects have short development times.
  - Higher likelihood of errors.


- Errors in software can lead to: Service unavailability.
  - Security breaches.
  - Financial losses.
  - Poor service to customers.
- Common causes include: Poor specification.
  - Bad assumptions made by developers.
  - Inadequate testing.

# Errors in Software


## Poor Specification.

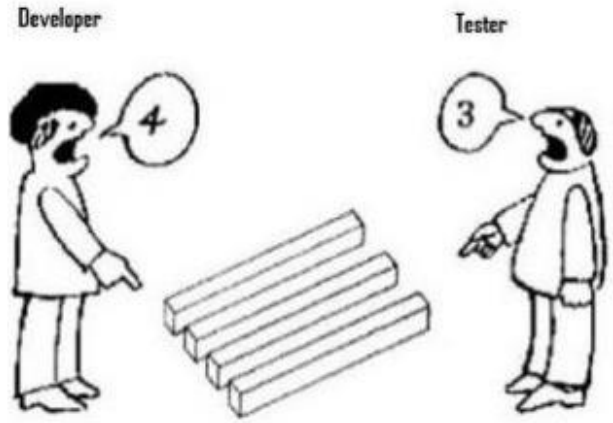
- The more ambiguous a design document the more likely your final product will end up with errors.
  - After a customers credit card is declined, the order should not be sent to the customer.
  - This has happened before.
- The less experience your developers have with a particular system the more precise your design has to be.

# Errors in Software


## Assumptions Made By Developers.

- System analysts and programmers often have to make assumptions.
  - Often these assumptions are incorrect.
  - Example 1: The likelihood that two conflicting actions might occur at the same time.
  - Example 2: Assuming that a users input will not contain any special characters or will be less than a particular size.
- Can be combated with good testing.
- Historically crackers have exploited weaknesses due to buffer overflow.

# Errors in Software




## Poor Testing

- Testing all possible conditions on all possible types of hardware, running all possible O/S with all possible user settings is rarely achievable.
  - A well designed test plan to test all functionality on a representative sample of common machine types is required.
- Every line of code should be tested at least once.
- Its important that people other than the original programmers are involved in testing.
  - Fresh people bring fresh assumptions.
  - Professionals are rarely keen to find flaws in their own work.

# Repudiation

- Occurs when once party involved in a transaction denies having taken part.
  - A person having ordered goods from a website then denying having authorised the charge on their card.
  - A person agreeing to something in email and then claiming that the email was forged.
- Authentication provides surety about who you are dealing with.
  - If issued by a trusted organisation, digital signatures of authentication can provide assurances.

# Repudiation

- Messages sent by both parties need to be tamperproof.
  - Signing or encrypting messages makes them difficult to surreptitiously alter.
- In ecommerce company should be willing to hand over proof of its identity and a few hundred Euro to a certifying authority such as Verisign.