CS 183AG
Lecture 14

Current Topics: Vehicular Networking + Security

Arthi Padmanabhan

Oct 19, 2022

Recap

- Vehicle communicate with each other and with nearby infrastructure
- They can exchange messages about accidents, traffic, etc
- This communication is subject to threats to security and privacy of drivers

Today’s Goal

- Identify, understand, and categorize various types of threats
  - Common threats to internet traffic
  - Specific effects on VANETs

Importance of VANETs

- Vehicle Adhoc Network
- Expected to be extremely prevalent, especially with emergence of autonomous vehicles
- Specific type of MANET (Mobile Adhoc Network)

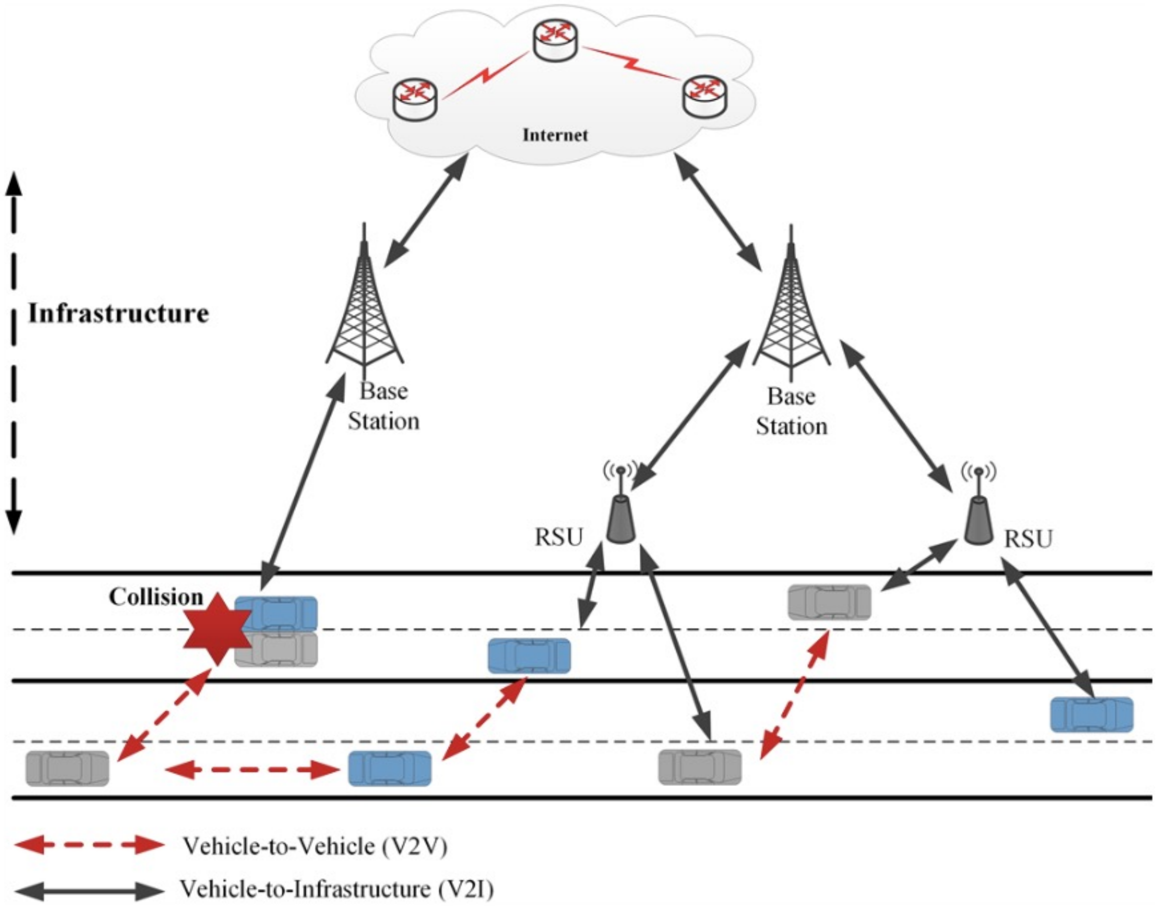
VANET Background

- Vehicles are equipped with several sensors (camera, GPS, etc)
- Sensors collect information (speed, location, etc) and share with neighboring vehicles (V2V) and roadside infrastructure units, RSUs (V2I)
  - RSUs are often speed cameras or mobile communication base station
- Message exchange uses standard mobile communication (4G, LTE, etc)

Goals

- Ensure traffic safety and efficiency
- Assist drivers in critical situations such as accidents
- Provide drivers with info such as weather and traffic
- Monitor fleet of vehicles remotely (e.g., truck company)

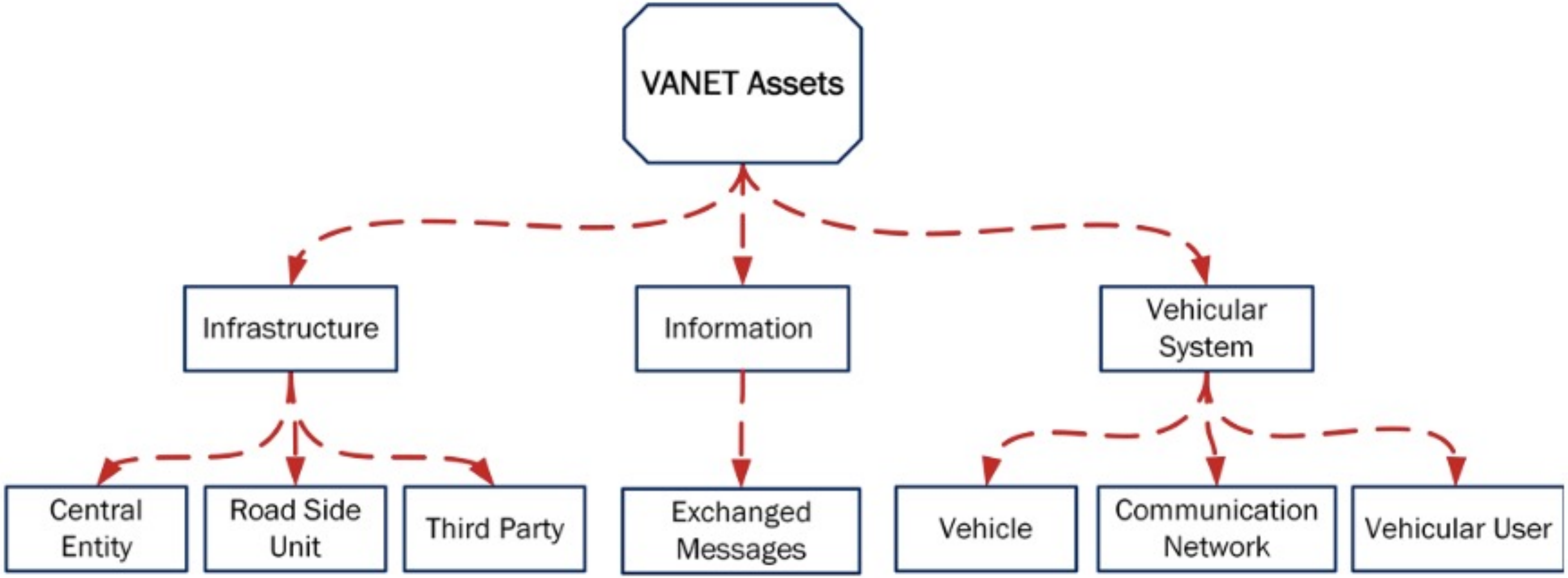
Goals


Internet
Infrastructure
Base Station
Base Station
RSU
RSU
Collision
Vehicle-to-Vehicle (V2V)
Vehicle-to-Infrastructure (V2I)

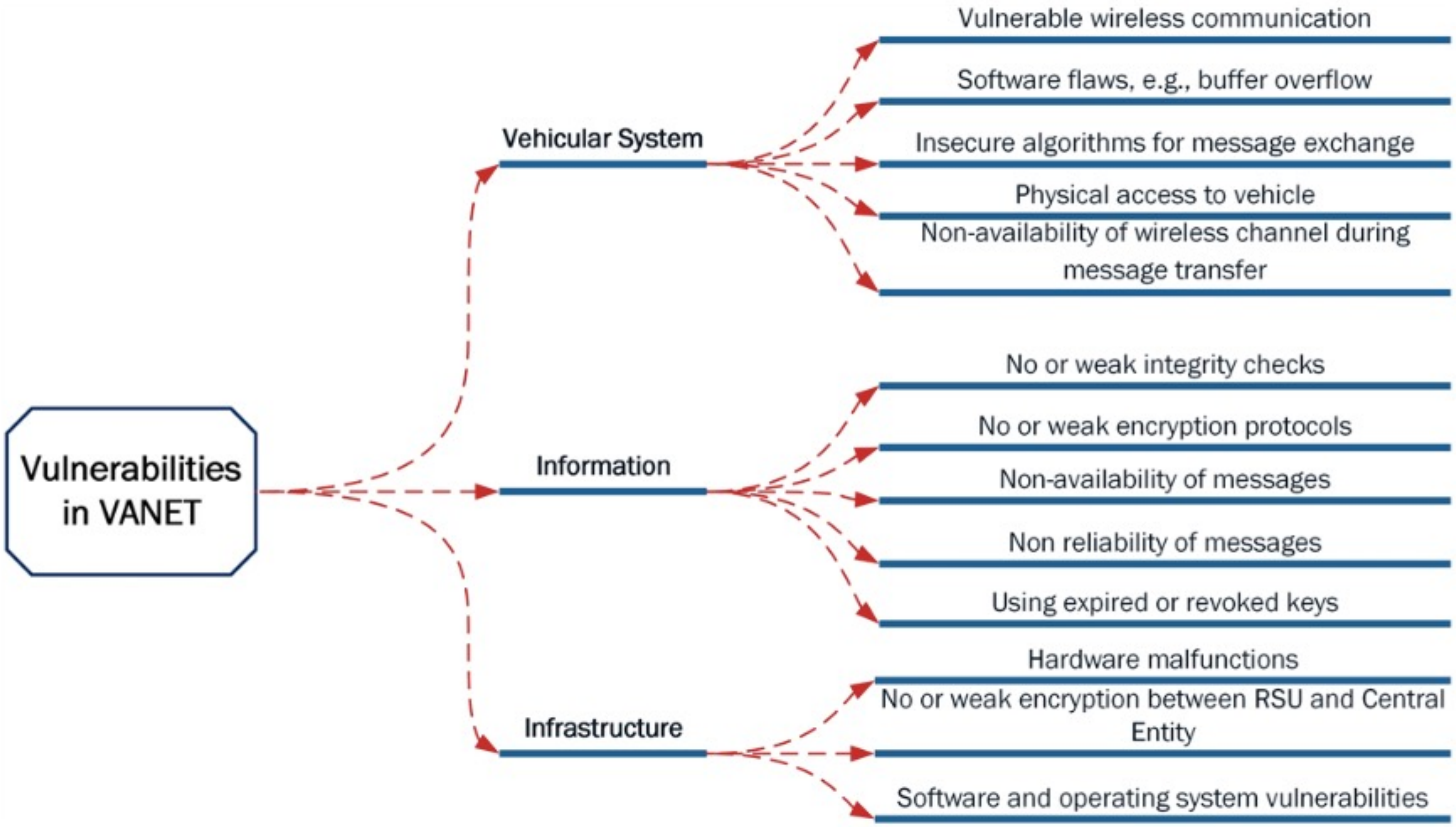
Vulnerabilities

- VANETs are large decentralized networks with legitimate and potentially malicious nodes
- VANET communication heavily relies on nodes cooperating
- Many vulnerabilities are shared with traffic on the rest of the internet but get more attention because of the severity of impact

Entities that Need Protection

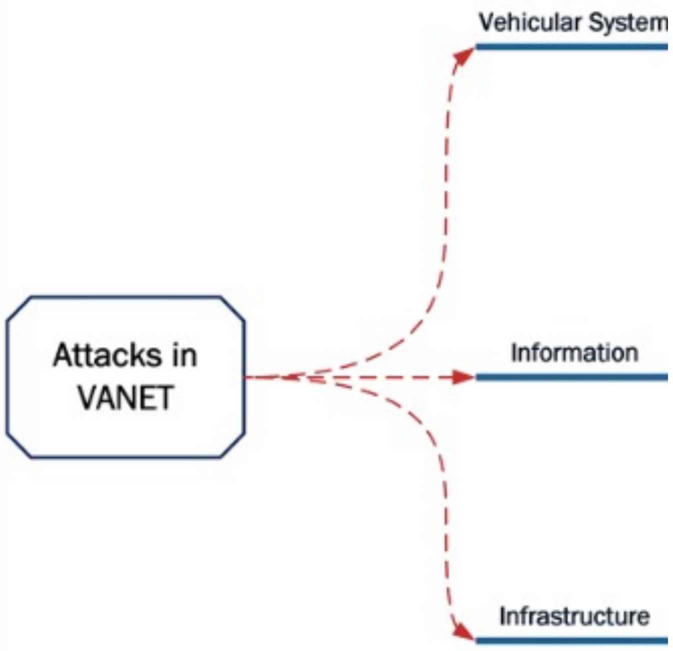


Categorization of Threats

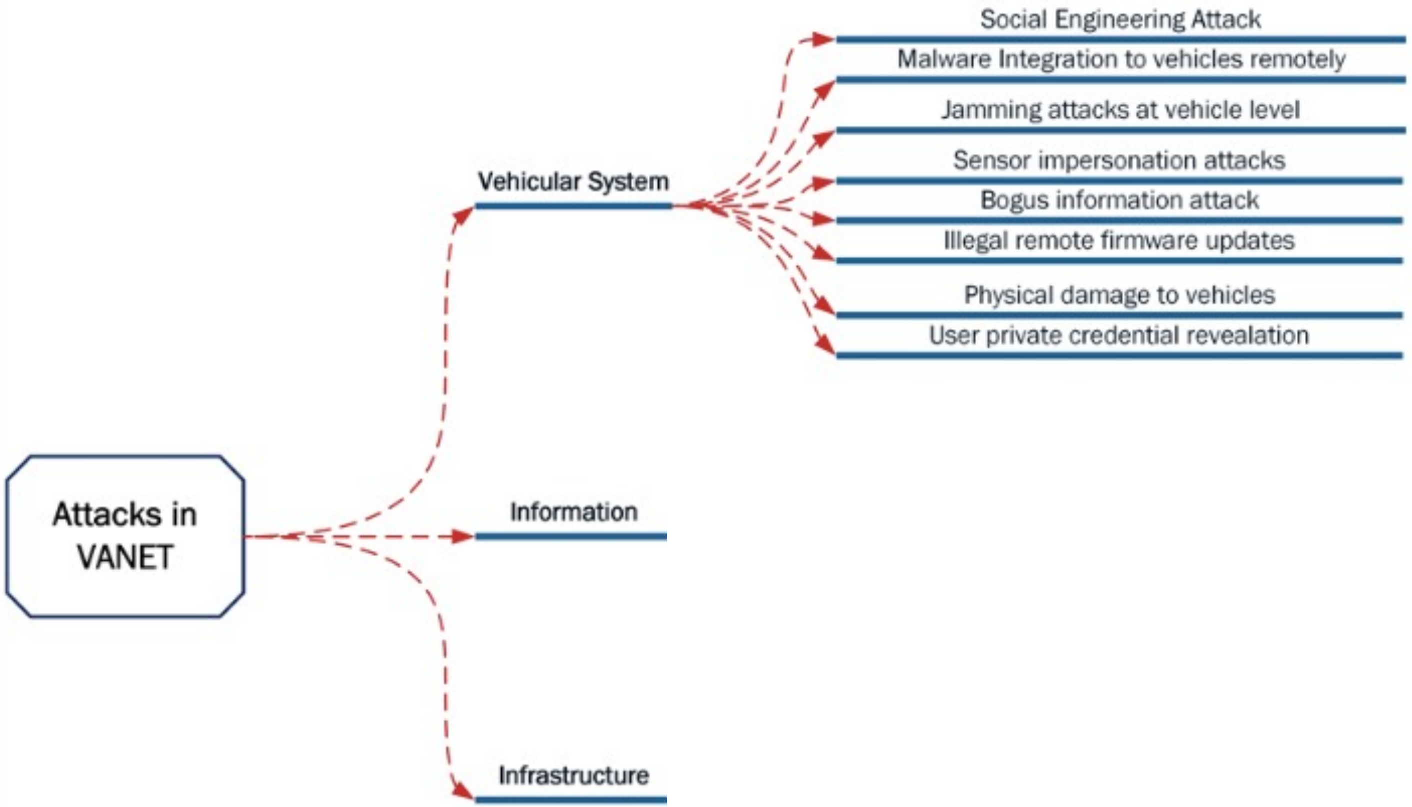


Vulnerabilities in VANET
Vehicular System
Vulnerable wireless communication
Software flaws, e.g., buffer overflow
Insecure algorithms for message exchange
Physical access to vehicle
Non-availability of wireless channel during message transfer
Information
No or weak integrity checks
No or weak encryption protocols
Non-availability of messages
Non reliability of messages
Using expired or revoked keys
Infrastructure
Hardware malfunctions
No or weak encryption between RSU and Central Entity
Software and operating system vulnerabilities

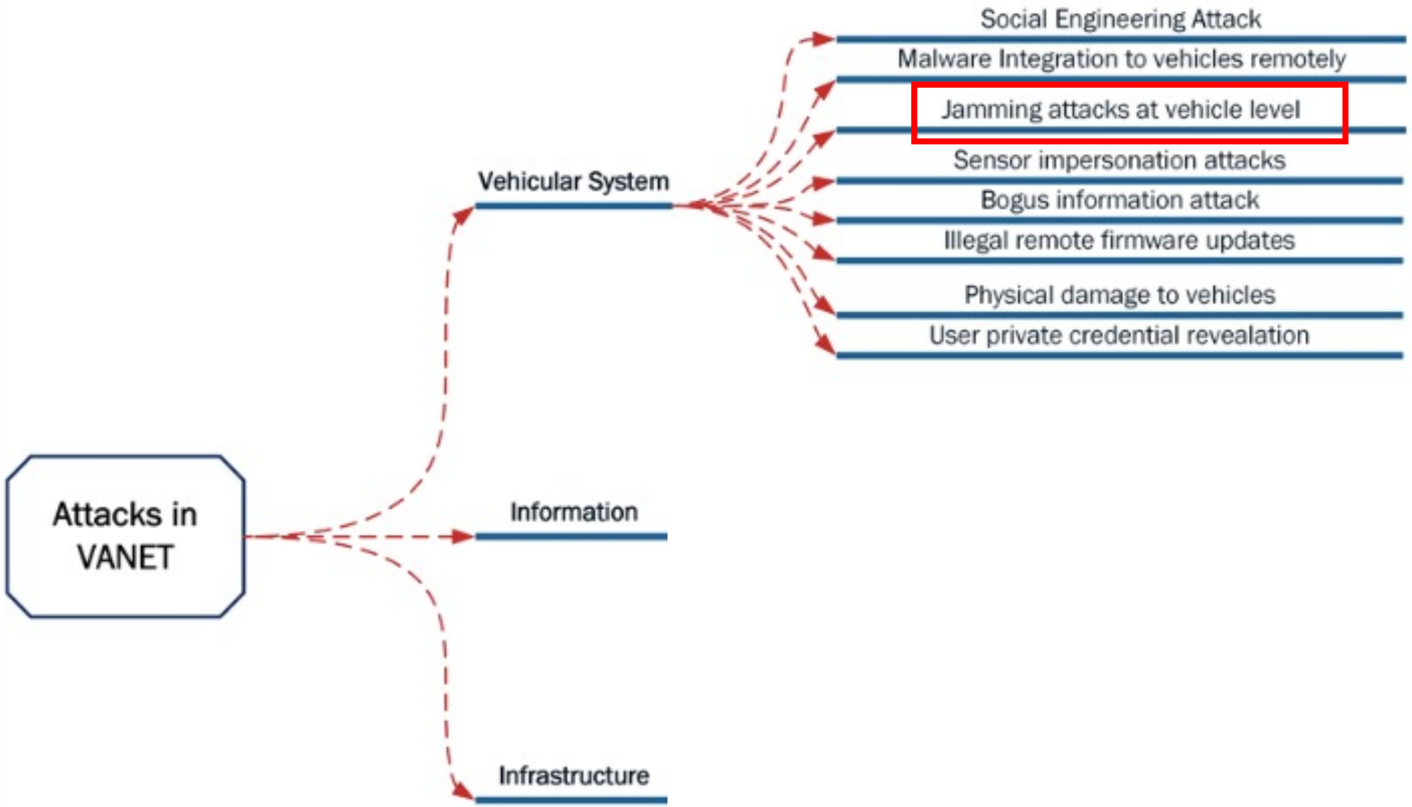
Types of Attacks in VANETs



Attacks on Vehicular Systems


Attacks in VANET
Vehicular System
Information
Infrastructure
Social Engineering Attack
Malware Integration to vehicles remotely
Jamming attacks at vehicle level
Sensor impersonation attacks
Bogus information attack
Illegal remote firmware updates
Physical damage to vehicles
User private credential revealation

Attacks on Vehicular Systems



Attacks in VANET

Vehicular System

Social Engineering Attack

Malware Integration to vehicles remotely

Jamming attacks at vehicle level

Sensor impersonation attacks

Bogus information attack

Illegal remote firmware updates

Physical damage to vehicles

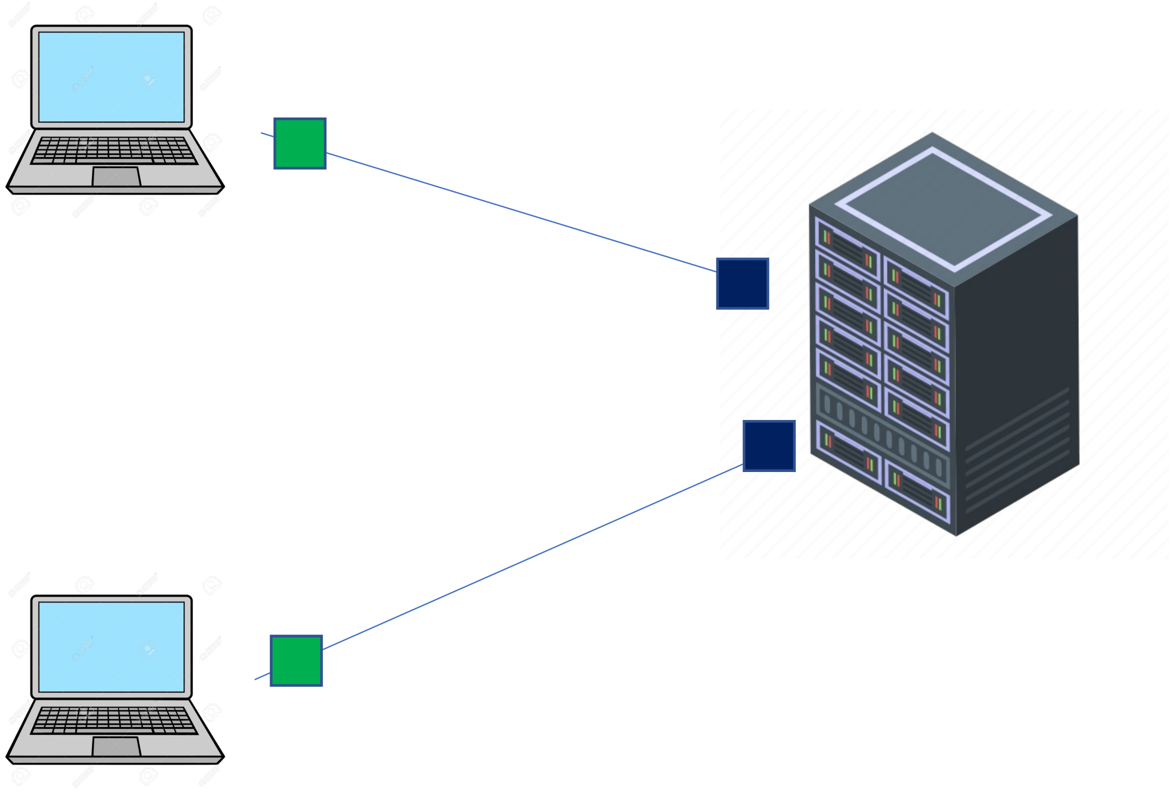
User private credential revealation

Information

Infrastructure

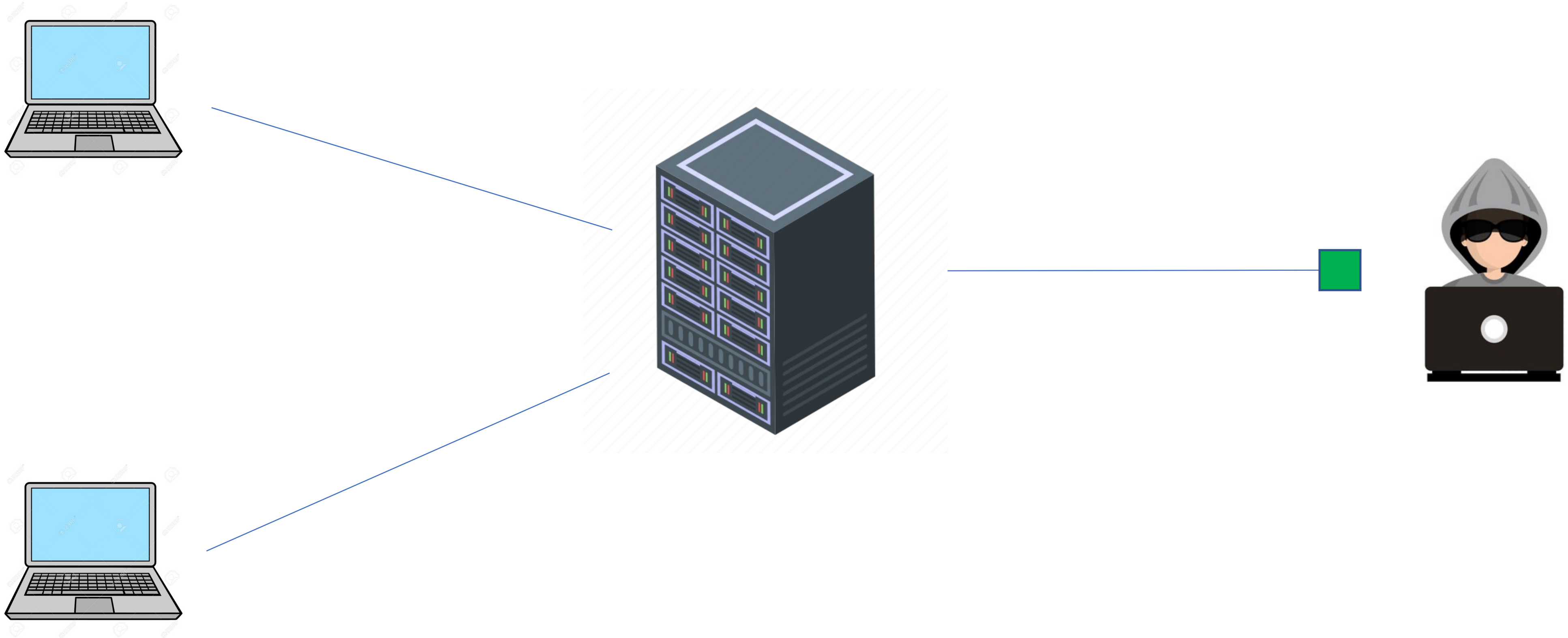
DoS Attacks

- Server that hosts website responds to requests for website content



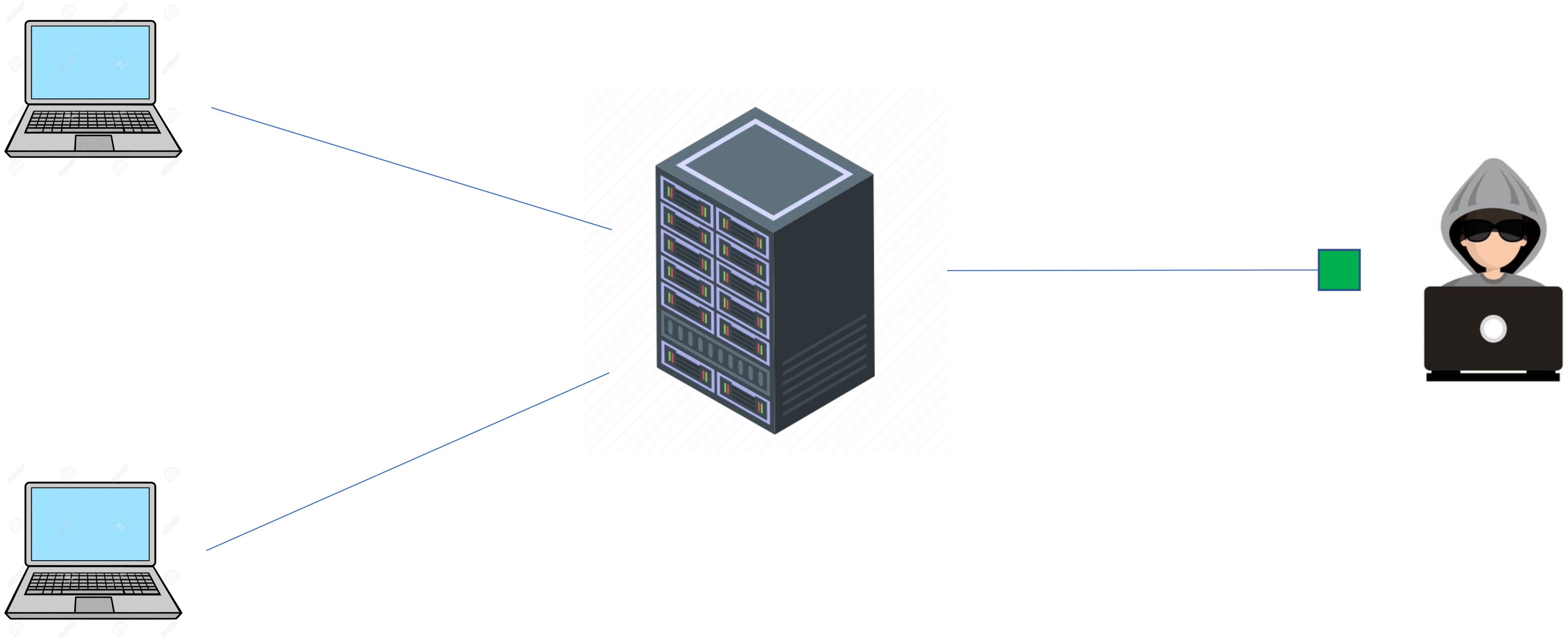
DoS Attacks

- Attacker can flood the server and saturate its ability to respond to requests



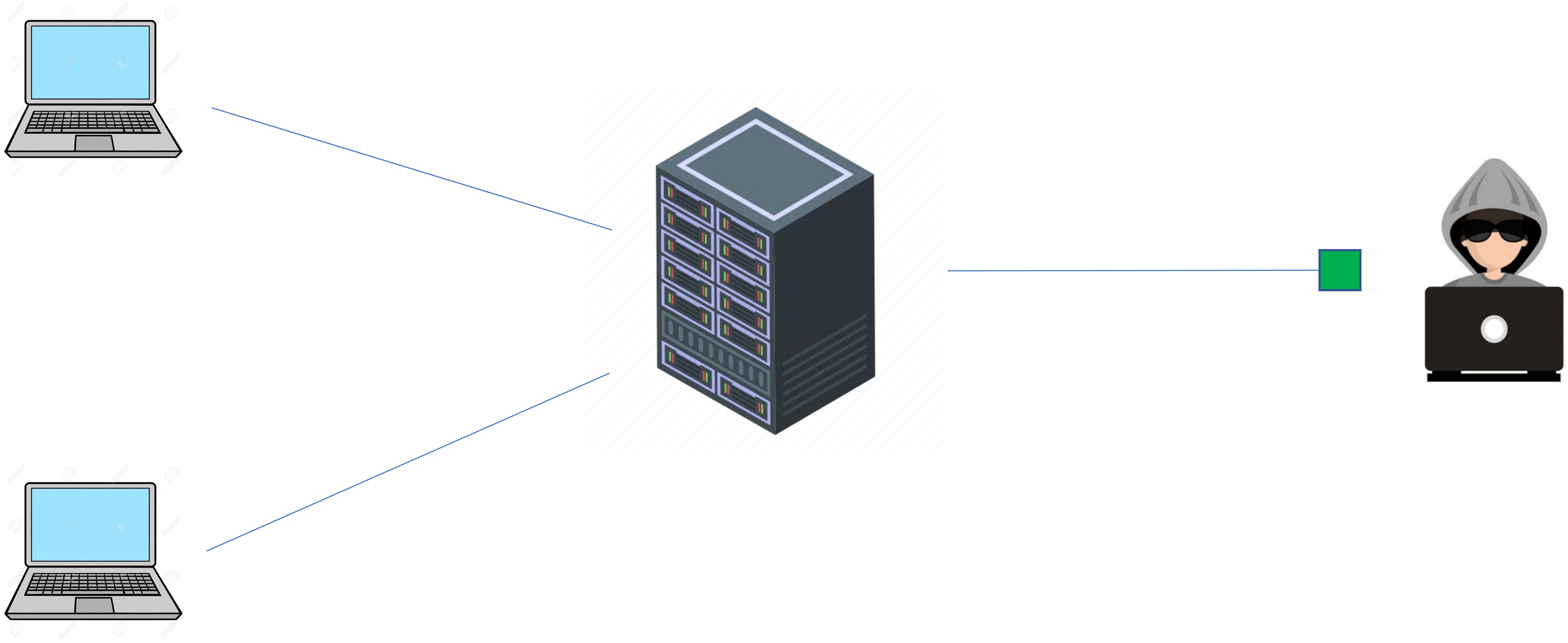
DoS Attacks

- This eats up the server's resources: CPU, memory, and network bandwidth and makes responses to other requests very slow (or stop)



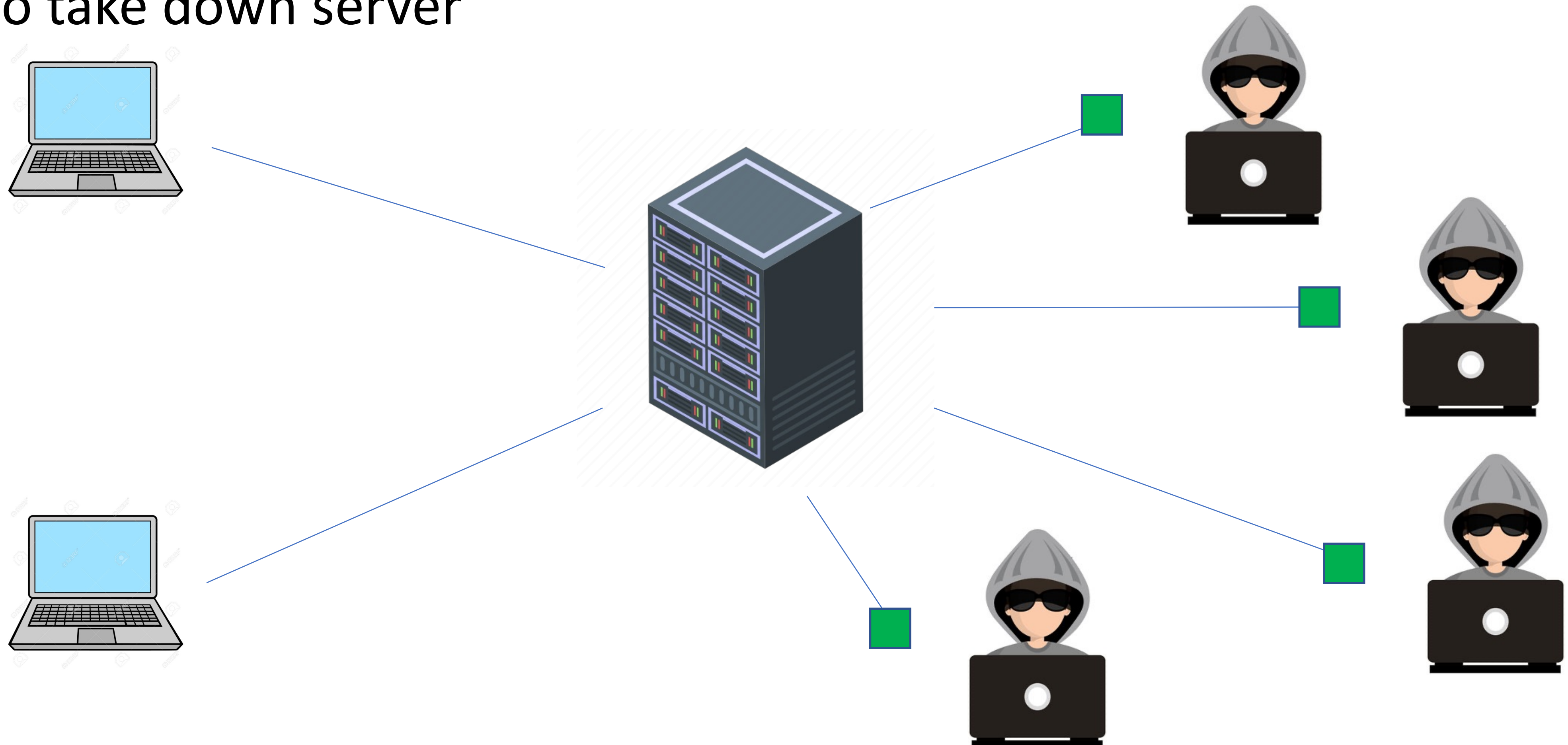
DoS Attacks

- It’s fairly easy to identify a single source sending many requests



DDoS Attacks

- Multiple senders join the attack -> harder to identify and stop, quicker to take down server



DDoS Attacks

- Use a large army of computers to launch a flooding attack
- Members are called “bots” or “zombies”
- Army is called botnet

DDoS Attacks

- How does initial hacker recruit others to its botnet?
- Malware!
  - User opens an email attachment or website – then their computer is part of the army of infected computers
  - Attacker can then tell them all to attack at the same time

DDoS Attack

- What is being sent?
  - Depends on the type of attack, but all will request some sort of action or response from server
- Could send simple ping message, ICMP (error handling), UDP
- Could be more complicated, such as sending compressed files, knowing that the server try to open them
  - Takes resources to open that many files
  - Takes memory each time a file is opened

DDoS Attacks: Types + Responses

- Volume attack: massive amounts of bogus messages, all of which warrant a reply
- Protocol-level attack: receiver expects certain packet types and knows how to respond; take advantage of that by sending specific packet types – ex/ ping of death, Smurf DDoS

DDoS Attacks: Types + Responses

- Volume attack: massive amounts of bogus messages, all of which warrant a reply
- Protocol-level attack: receiver expects certain packet types and knows how to respond; take advantage of that by sending specific packet types – ex/ ping of death, Smurf DDoS
  - Ping of death: send malformed packets that cause buffer overflow error
  - Smurf DDoS: send messages to the broadcast address, spoofing the source address to be the server; every device on the network will keep sending replies to the server and saturate it

DDoS Attacks: Types + Responses

- Volume attack: massive amounts of bogus messages, all of which warrant a reply
- Protocol-level attack: receiver expects certain packet types and knows how to respond; take advantage of that by sending specific packet types – ex/ ping of death, Smurf DDoS
  - Ping of death: send malformed packets
  - Smurf DDoS: send messages to the broadcast address where the source is the server; every device on the network will keep sending replies to the server and saturate it
- Application-level attack: sophisticated attacks that target a certain application to exploit application and OS-level vulnerabilities
  - HTTP flooding: send stream of GET and POST requests that trigger high level of system processing; harder to detect

DDoS Attacks: Reasons

- Attack a competitor
  - Affects their reputation
- Money: ransom
- Political
- For fun

DDoS Attack Responses

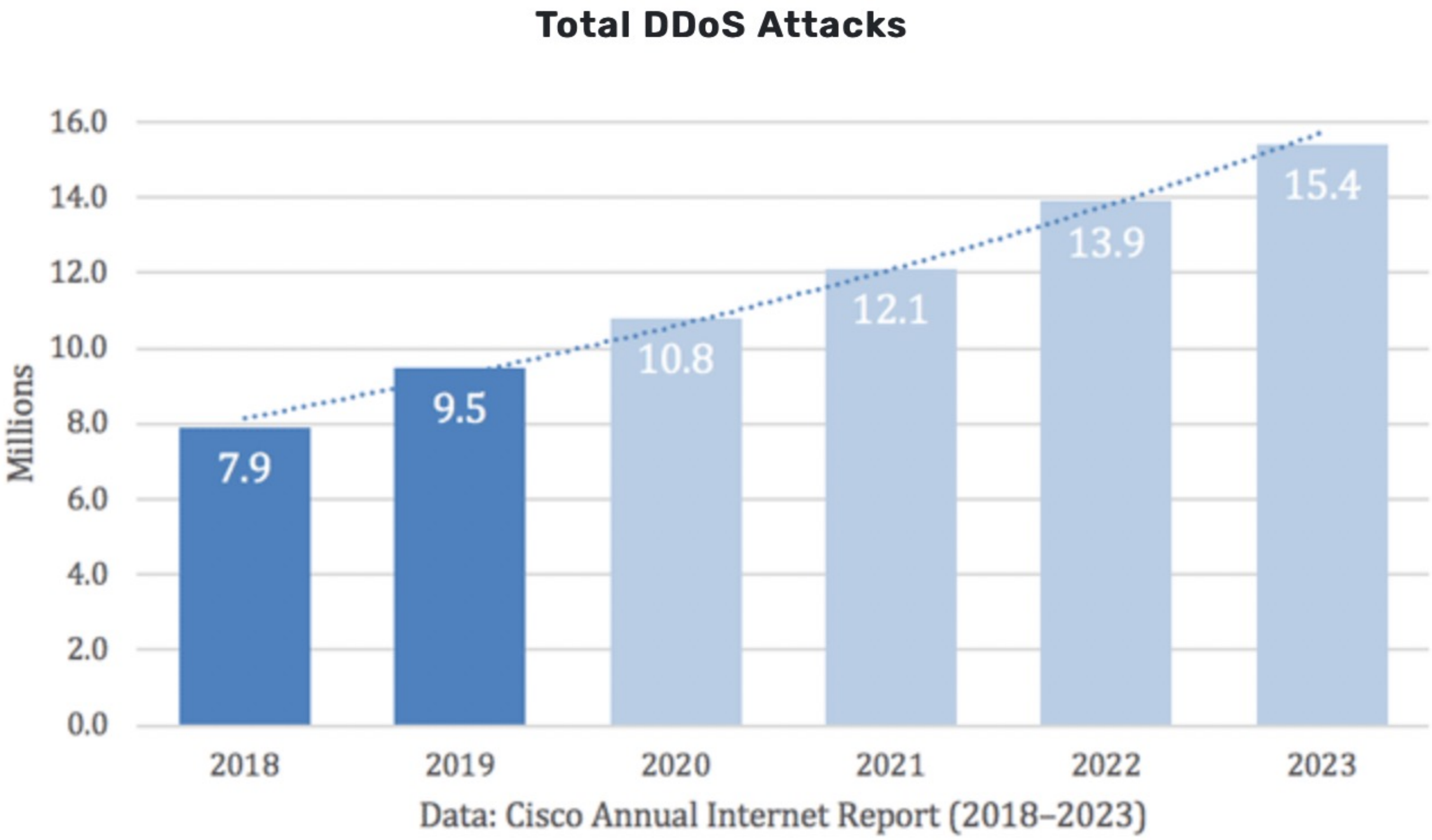
- Firewalls + load balancers
  - Firewalls can detect too much traffic from one source and block it
  - Protocol level attacks target firewalls though – how?
  - Load balancers reroute traffic from one server to another
- Look for patterns

DDoS Attack Prevention

- Easiest to host on cloud service provider -> more bandwidth, checks in place to detect suspicious patterns, they back up your data and can serve out of a different server
- CDN (content delivery network): redundant servers keep a cached version of site (for purpose of bringing it closer to user) -> causes multiple copies and avoids single point of failure
  - Cloudfare
  - Akamai

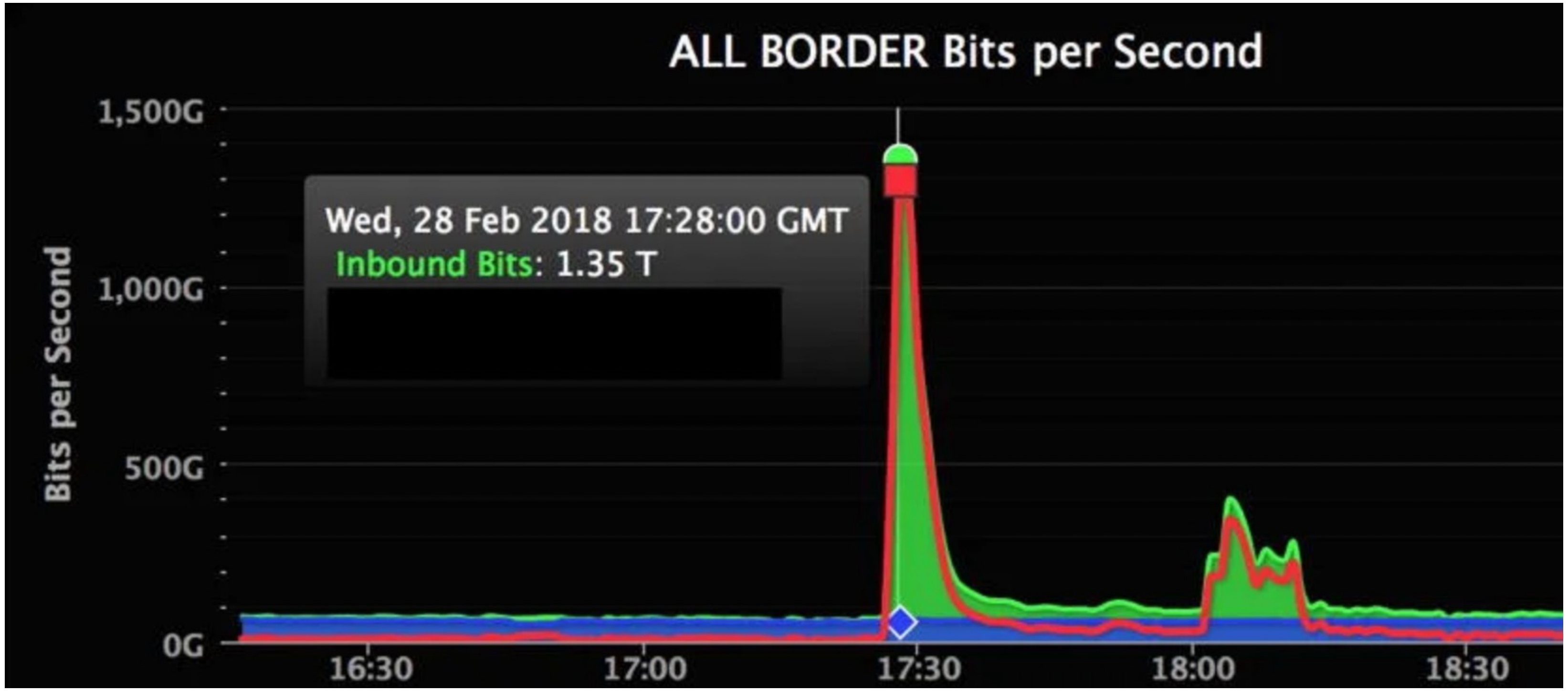
Famous DDoS Attacks

- Google, 2020
- AWS, 2020
- Mirai, 2016



Famous DDoS Attacks

- Google, 2020
- AWS, 2020
- Mirai, 2016
- GitHub, 2018



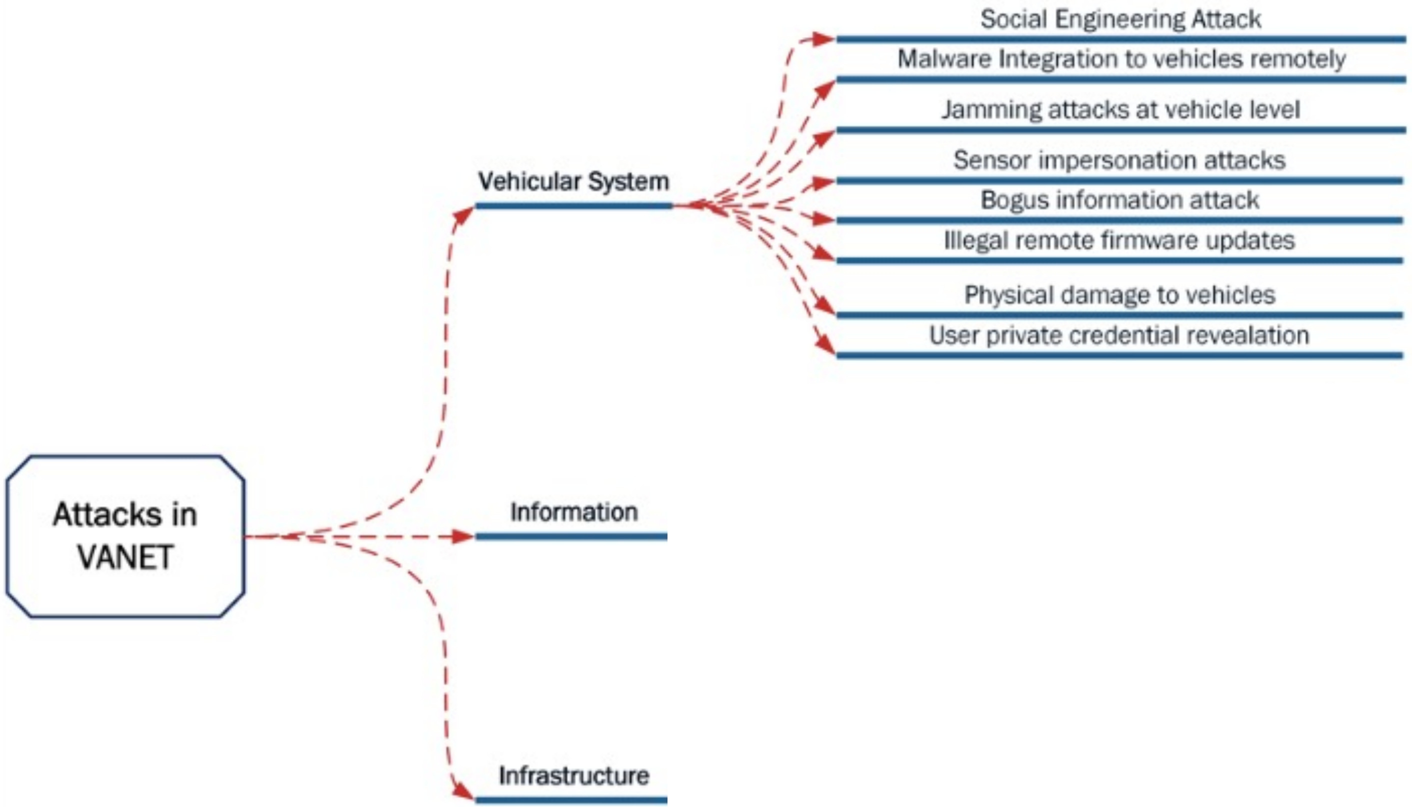
DDoS in VANETs

- Cars can become zombies and DDoS cars around it
- Can lead to jamming – car stops being able to respond to any requests, including from within the car

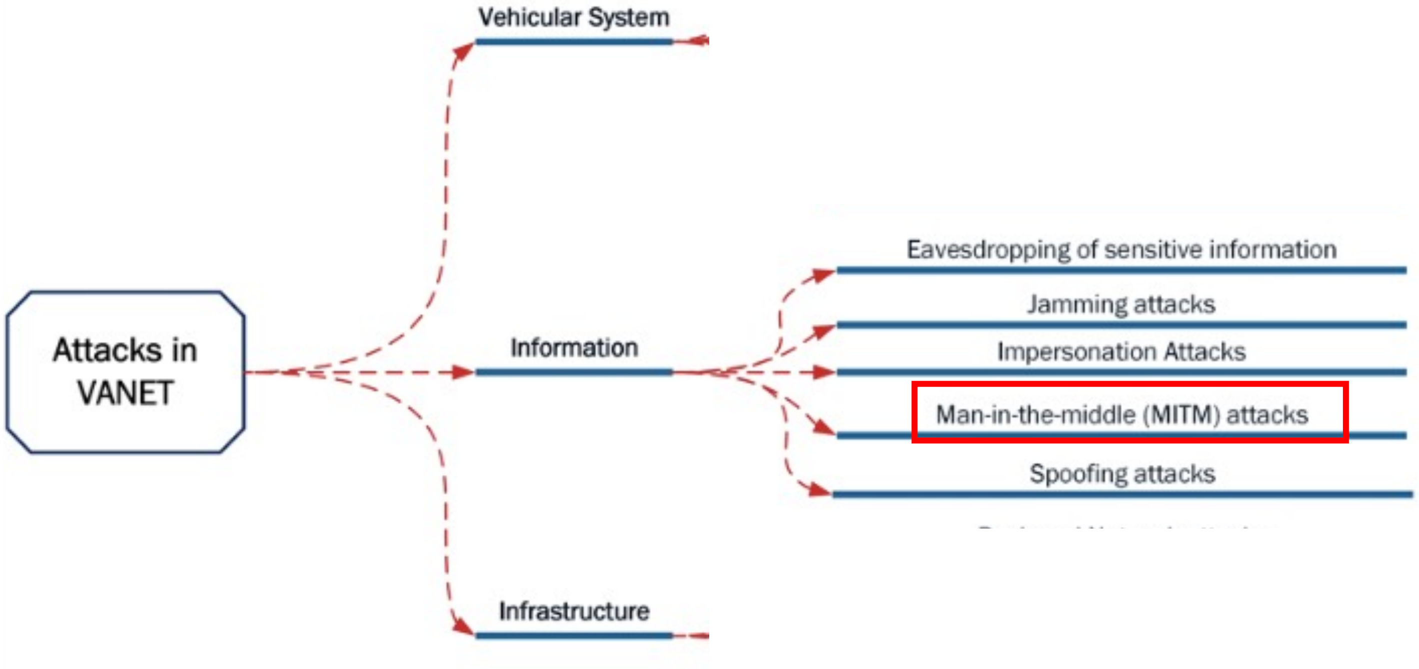
DDoS in VANETs: Trust Building

- One paper: Frequency of positive interactions can be used to build trust. Can assess whether to respond to request based on other vehicle’s trust index
- Only simulated, not in real world – hard to test on real world results

Attacks on Vehicular Systems


Attacks in VANET
Vehicular System
Information
Infrastructure
Social Engineering Attack
Malware Integration to vehicles remotely
Jamming attacks at vehicle level
Sensor impersonation attacks
Bogus information attack
Illegal remote firmware updates
Physical damage to vehicles
User private credential revealation

Attacks on Vehicular Systems



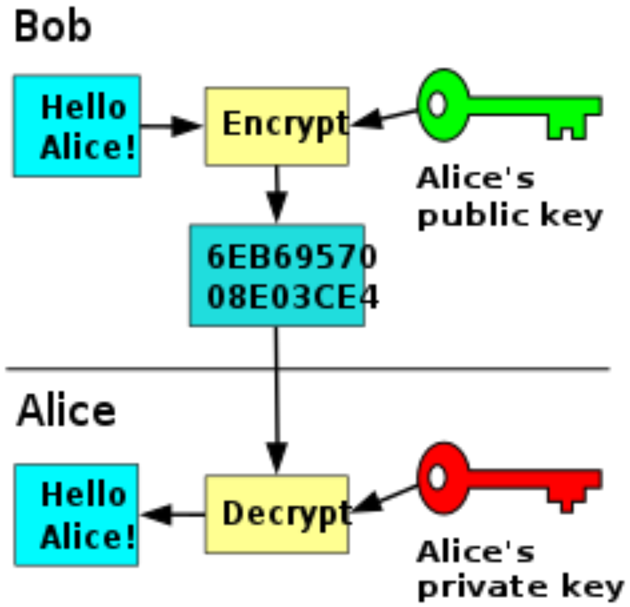
Man in the Middle Attacks

- 10-15 years ago, all data was in plain text so anyone who heard it could read the message
- Solution: use public and private keys

Secure Sockets Layer (SSL)

- Computer: I would like to talk securely
- Server: Sure, here is my public key
- Computer uses server’s public key to encrypt message. Only server has private key to decrypt it

Secure Sockets Layer (SSL)



Problem Solved?

- Someone in the middle can change first message exchange (“I would like to talk securely”, “Sure, here is my public key”)
- Each party think the public key they are using to encrypt is each others but it’s actually the attackers

Signed Certificates

- Solution: there is a third party vouching for the set of public keys you’re exchanging
- Server: here is public key – it’s been signed by those trusted people.
    - If attacker changes 1 bit, the math doesn’t add up anymore

Trust Certificate Authorities?

- How do you know which authorities to trust?
  - Depends on known trust
- A Dutch certificate authority got conned/coerced into generating valid signed certificate the for whole of Google
  - Someone managed a massive Man in the Middle attack and was able to look at all of Google's exchanges
  - Found because someone realized that the Google certificate was signed by entity in Netherlands
- Concern that governments can coerce?

Trusted Authority on Devices

- Each device keeps a list of trusted authorities
- Root authority must be signed by known authority, others can be signed by root, or authority that root has signed, etc –> chain of certificates
- What if you could insert yourself into that list?

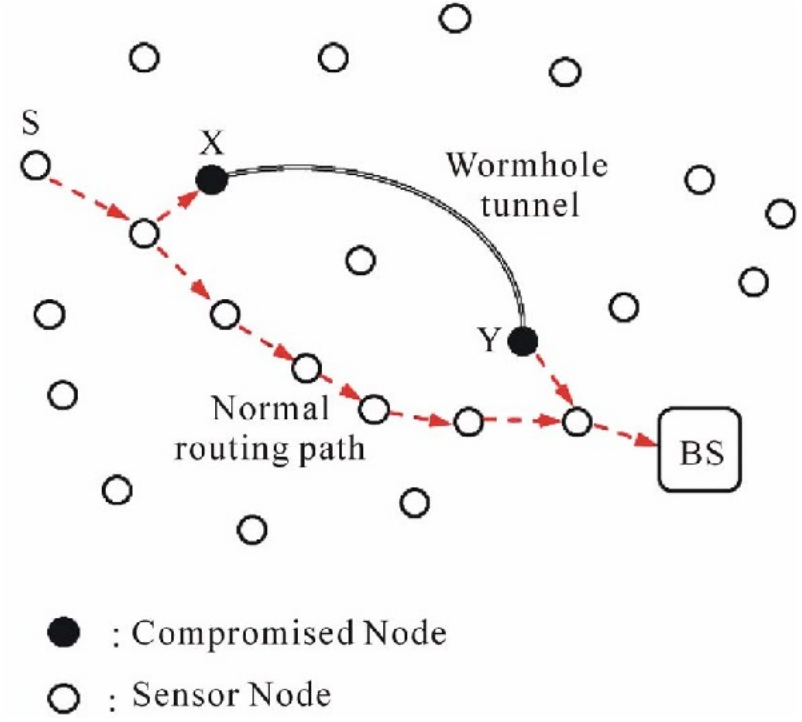
Famous MitM Attacks

- Lenovo used company called Superfish for ads
- Superfish installed themselves into list of trusted devices on every Lenovo laptop – single self-signed root certificate
- Ran a little program sitting on computer looking at all traffic and inserting ads
- Really bad idea! Why?
- Hundreds of thousands made vulnerable. Dept of Homeland Security had to get involved

Man in the Middle Attacks in VANETS

- Attacker can alter and forward messages between vehicles or between vehicle and RSU

Wormhole Attacks



References

- https://www.scirp.org/journal/paperinformation.aspx?paperid=73220

Upcoming

- Midterm released next Tuesday morning, due following Sunday evening
- Study guide will be posted to course webpage by tomorrow afternoon
- Please go through it and send me anything you’d like to go over in more detail - through email, Slack, or feedback form on webpage