## From the "Analysis of a Denial of Service Attack on TCP" paper:

1. **In a SYN flooding attack, attackers usually would use spoofed source IP address(es), choosing what kind of address(es) would make the attack more effective?**

- Spoofing IP addresses that belong to hosts that are not reachable by the victim would work best as the connection will never be established.

## From the "A Classification of SQL Injection Attacks and Countermeasures" paper:

2. **Besides user inputs, as we have discussed during the lecture, what other mechanisms can be used to inject malicious SQL queries?**

- Injection through Cookies
- Injection through server variables
- Second order injection

## From the "Cross-Site Scripting Prevention with Dynamic Data Tainting and Static Analysis" paper:

3. **The proposed method uses a combination of dynamic and static taint analysis to prevent attacks. Generally, a taint-based system has three main components: sources (when tainted data is introduced), sinks (when we should check whether a piece of data is tainted), and optional, sanitizers (where tainted data can become untainted). Based on this modeling, what are the taint sources and sinks in this attack prevention system?**

- Taint sources are the places where tainted data is introduced into the system. This could be cookies, forms, URL, path etc. Taint sinks are the places where that tainted data is used in a potentially dangerous way. This could be value assignment, Arithmetic operations, control structures and loops, function calls and function call evaluations.

## From the "A Practical Approach to Identifying Storage and Timing Channels" paper:

4. **This paper proposed a method called the "Shared Resource Matrix Methodology" to detect storage and timing side-channels. Using the criteria proposed by this work, explain how FLUSH+RELOAD attack discussed in the lecture meets the criteria.**

- A flush+reload attack is a type of side-channel attack that involves monitoring the cache behavior of a system to extract sensitive information. The attacker first flushes a memory location from the cache, then performs an operation that accesses the same memory location. By measuring the time it takes for the operation to complete, the attacker can determine whether the memory location was accessed from the cache or from main memory. This meets the criteria as we can know by looking at the SRM table which components are accessing cache in an insecure manner. Using the timing channels we can apply lock on read and access operations.

## From the "Outside the Closed World" paper:

5. **Machine learning, especially deep learning seems to be a magical and powerful technology (hammer) that can solve any problem (nail). However, the authors of this paper strongly against starting with the premise to use machine-learning (or, worse, a particular machine-learning approach) and then looking for a problem to solve. Instead, what is the most important question one should answer when trying to decide whether to use ML to solve a security problem?**

- One should have an answer for '**why**' the particular choice promises to perform well in the intended setting—not only on strictly mathematical grounds, but considering domain-specific properties.

## From the "Making Machine Learning Robust Against Adversarial Inputs" paper:

6. **Please explain what formula (1) means:**

(1)

- The formula describes an optimization problem where the objective is to minimize the norm of the variable (z) subject to the constraint that the function f(x+z) equals some value (t). In other words, the goal is to find the optimal value of z that minimizes the norm while satisfying the constraint that f(x+z) = t. This is done to get a perturbed image x* which is given by the original image x + adding some noise that is generated by the constrained optimization.

## From the article "Security Mindset"
https://cubist.cs.washington.edu/Security/2007/11/22/why-a-computer-security-course-blog/

Links to an external site.

7. **We say the biggest difference in security research (from other domains) is the existence of adversarial. What kind of question would be interesting to an adversarial?**

- Questions that would be interesting to an adversarial in the context of computer security mindset would likely focus on finding vulnerabilities or weaknesses in systems or networks, and developing strategies for exploiting those vulnerabilities to gain unauthorized access or disrupt normal operations. The question would be something like, the product foo seems nice, but can someone exploit it by doing blah attacks(buffer overflow attacks, return to libc attacks, sniffing and spoofing attacks etc.)

## Takeaway

8. **What is the most useful thing you learnt from this class?**

- Main takeaway is to prepare for unthinkable attacks and inputs from user and to not trust any library or piece of code that is not written by self. We should have regular security updates, patches and strong password policies.
-