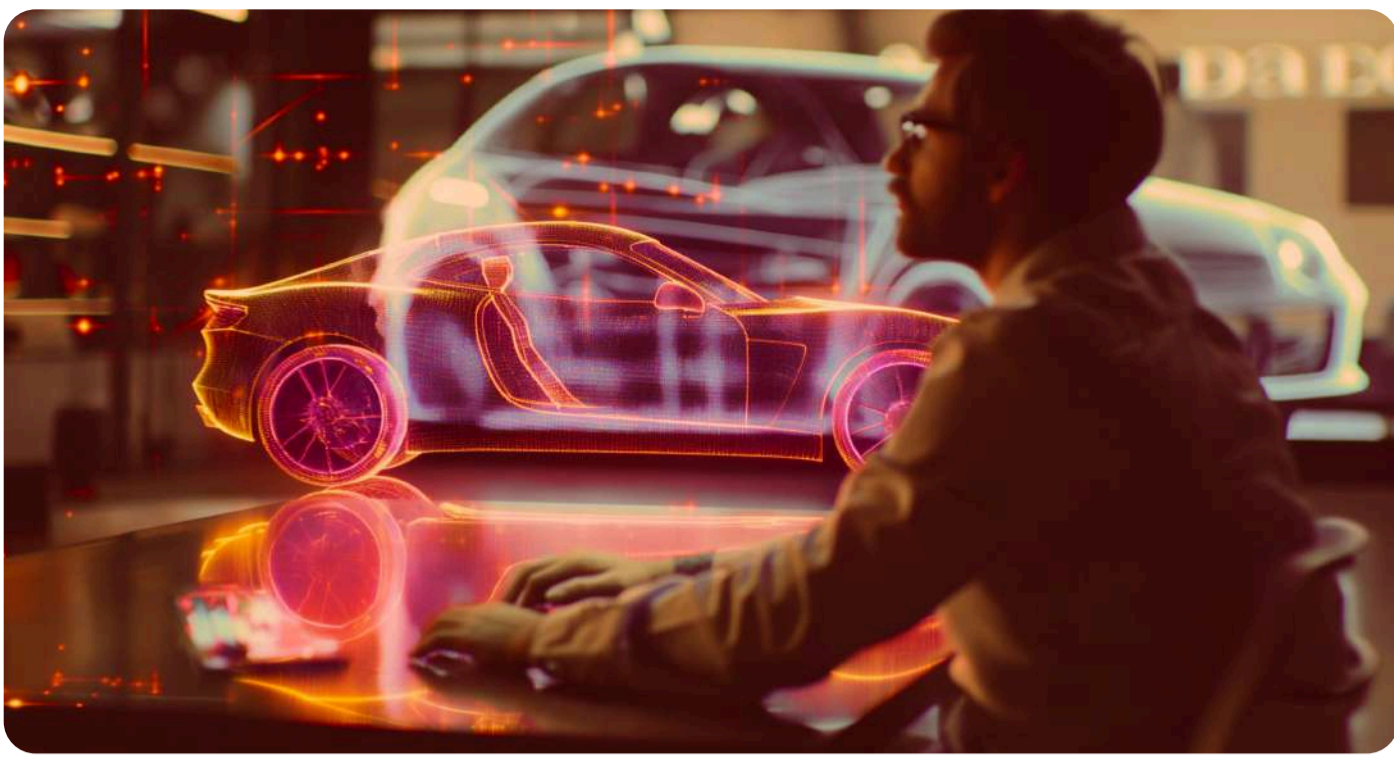


How System Prior art saved us in the Final Hour!

CASE STUDY

Definition

- ▶ Ever stumbled upon the term "**system prior art**"? If not, no worries—chances are, it's new to you too.
Recently, during our invalidation journey, we stumbled upon this intriguing method of exploring non-patent literature: **System Prior Art**. But before we delve into our invalidation search journey, let's unravel the mystery of System Prior Art first, shall we?
- ▶ Imagine stumbling upon evidence from the real world that proves a technology existed before a certain date. That's the essence of System Prior Art—a tangible gadget, software, or tool that mirrors the claimed technology, predating the cut-off date. It's like finding a hidden treasure trove of proof-of-concept hidden in non-patent literature.
- ▶ But how does System Prior Art differ from your normal Prior Art? Well, while any document before the cut-off date can serve as Prior Art, System Prior Art goes a step further. It showcases functioning models, offering compelling evidence of technology in action.
- ▶ The avenues for finding system prior art are endless!
- ▶ From scouring YouTube for product reviews and teardown videos to exploring trade shows like CES, there's a wealth of information waiting to be unearthed. And if the digital realm doesn't yield results, search offline havens like libraries and printed tech magazines to find relevant system prior art.



Introduction To The Case

🔍 We've been tasked with an intriguing invalidation challenge: cybersecurity testing for vehicle systems. With every vehicle now connected to the internet, they essentially function as mobile IoT devices. However, this connectivity also exposes them to cyber threats. A thorough cybersecurity testing approach is imperative to safeguard these vehicles from potential hackers who can infiltrate their communication networks.

🔍 Enter "penetration testing," also known as "pen testing."

🔍 This method involves utilizing the vehicle's CAN bus—the communication network within the vehicle—to assess its vulnerability. The process unfolds by first receiving and defining a penetration test instruction for the target vehicle. Then, utilizing specialized CAN communication equipment, the pen test is executed to gather CAN bus test data. This data is subsequently analyzed and processed according to the test scheme to yield a penetration test result.

🔍 In essence, penetration testing serves as a crucial defense mechanism, ensuring the security and integrity of vehicles in an increasingly connected world.

Phase 1 Conventional Approach

▶ Our journey began with a targeted search strategy. We narrowed our focus to key concepts: "Cybersecurity Testing," "Penetration Testing," and "Autonomous Vehicle Cyberattacks" utilizing the CAN bus. In our quest through patent literature, we stumbled upon a treasure trove of valuable classes like "H04L63/1433," "H04L63/1441," "G06F11/3692," "G06F21/577," and "G06F2221/034" - all shedding light on vulnerabilities and countermeasures against malicious traffic, particularly in vehicle security.

H04L63/1433-41

H04L63/1441



G06F11/3692

G06F2221/034

▶ Despite our conventional approach yielding less than anticipated, we remained optimistic about our direction. While we uncovered a few patents, they fell short of the features we required, particularly in simulating penetration testing of the CAN bus for a car emulator. But our spirits remained high - we knew we were on the right path.

Phase 2 The Brainstorming, New Leads, Assignees, Inventors

▶ In our initial analysis, we uncovered promising leads from various entities such as IBM, Siemens, Boeing Co., Beihang University, and several automotive giants like BMW, Toyota, Nissan Motor, and General Electric Company. These organizations are actively involved in safeguarding autonomous vehicles from cyber threats.

Contact Us :



Phase 3 Unconventional Way, Using Leads Exhibition, Consumer Show & YouTube

▶ Picture this: the annual Consumer Electronics Show (CES) in Las Vegas—a dazzling spectacle where tech titans unveil their latest innovations, from futuristic gadgets to cutting-edge cars and beyond. It's the ultimate showcase of tomorrow's technology, and we had a hunch that somewhere within its halls lay the answer to our quest.

▶ With our cut-off date looming in the past, CES editions before 2020 held the promise of revealing demonstrations of cyberattack software in cars. It was a shot in the dark, but sometimes fortune favors the brave.

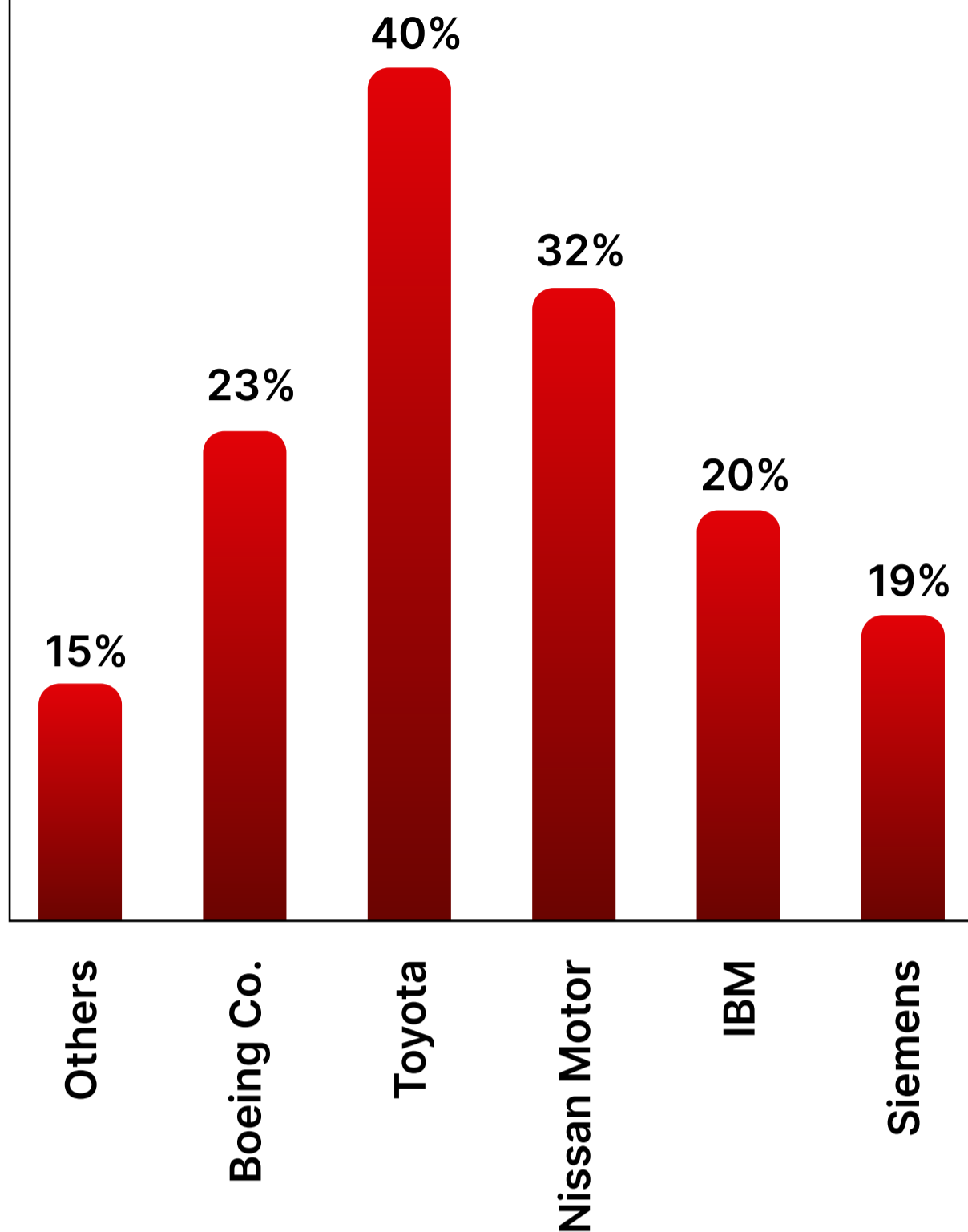
▶ After hours of tireless exploration, our efforts bore fruit. We found a video from CES 2017 showcasing connected cars. In it, a salesperson demonstrated the unsettling reality of hacking a real car using remote cyber-hacking software. It was a thrilling discovery, bringing us one step closer to our goal.



Connected Car at CES 2017: Harman cyber security demo

[Video1 – “**Connected Car at CES 2017: Harman cyber security demo**”, Credit: [Source](#)]

Their Contribution >>>





▶ During the brainstorming session, we explored diverse avenues to achieve our goal. Some suggested searching for demonstration videos on YouTube showcasing cyberattacks, while others proposed exploring the work of third-party software companies. There were also mentions of hacking competitions resembling gaming events, where participants attempt to hack into cars. Lastly, trade shows, exhibitions, or consumer shows were highlighted as potential sources of futuristic software yet to hit the market.

▶ Our objective was clear: to find a working demo or live tutorial of cybersecurity testing before the cut-off date. While this lead was new territory for us, it represented our last hope in this pursuit.

Contact Us :

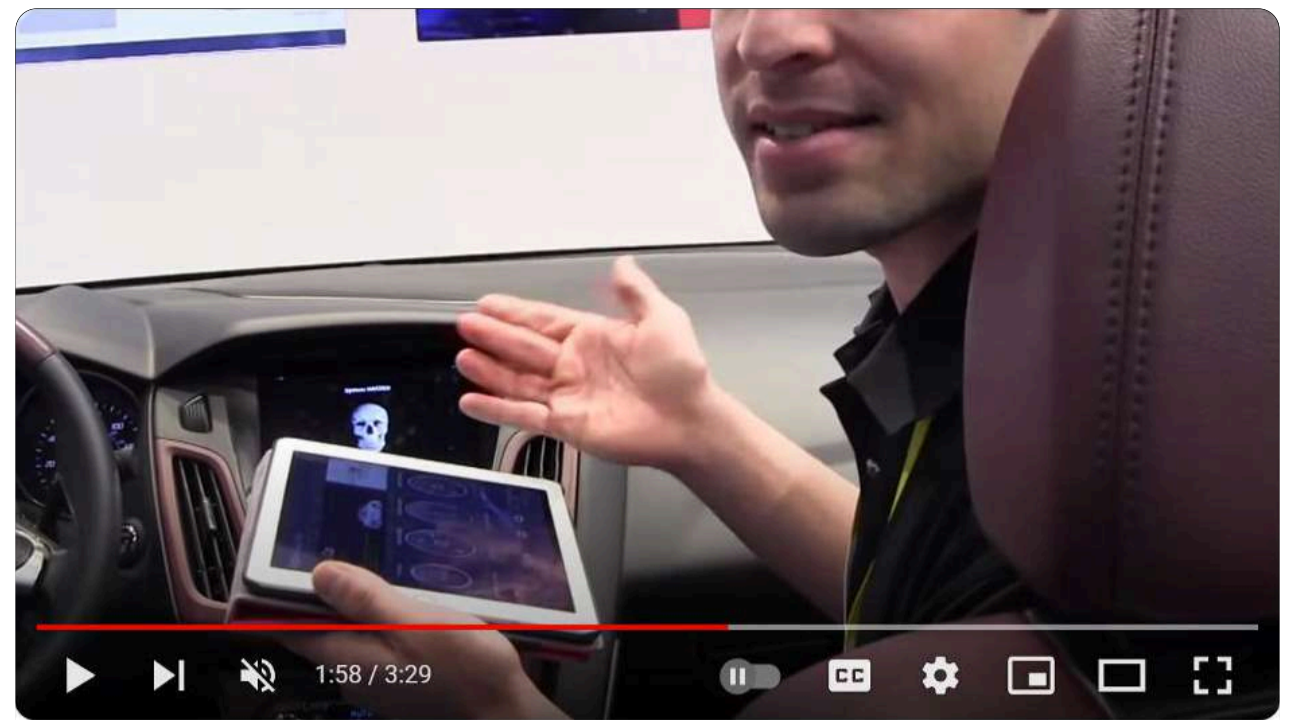


 We were making progress. We delved deeper into YouTube, searching videos with titles like "Cyber Hacking," "Penetration Testing," "CAN bus hacking," "How to hack your Car," "Cybersecurity demo," "Testing Automobiles against cyber-attacks," or "Decoding CAN message."

 Beyond videos, we broadened our search to include software companies offering similar solutions. Several names emerged: dSPACE Group, Argus Cyber Security, Connected Car, Continental Automotive Vehicle, DEFCON Conference, and BMW Group Careers.

HIT THE JACKPOT !

Exciting news! We hit the jackpot when we stumbled upon a video showcasing cyber security testing on a real car.



Argus Cyber Security Demo: Stops Car Hacking

[Video2 – “**Argus Cyber Security Demo: Stops Car Hacking**”, Credit: [Source](#)]

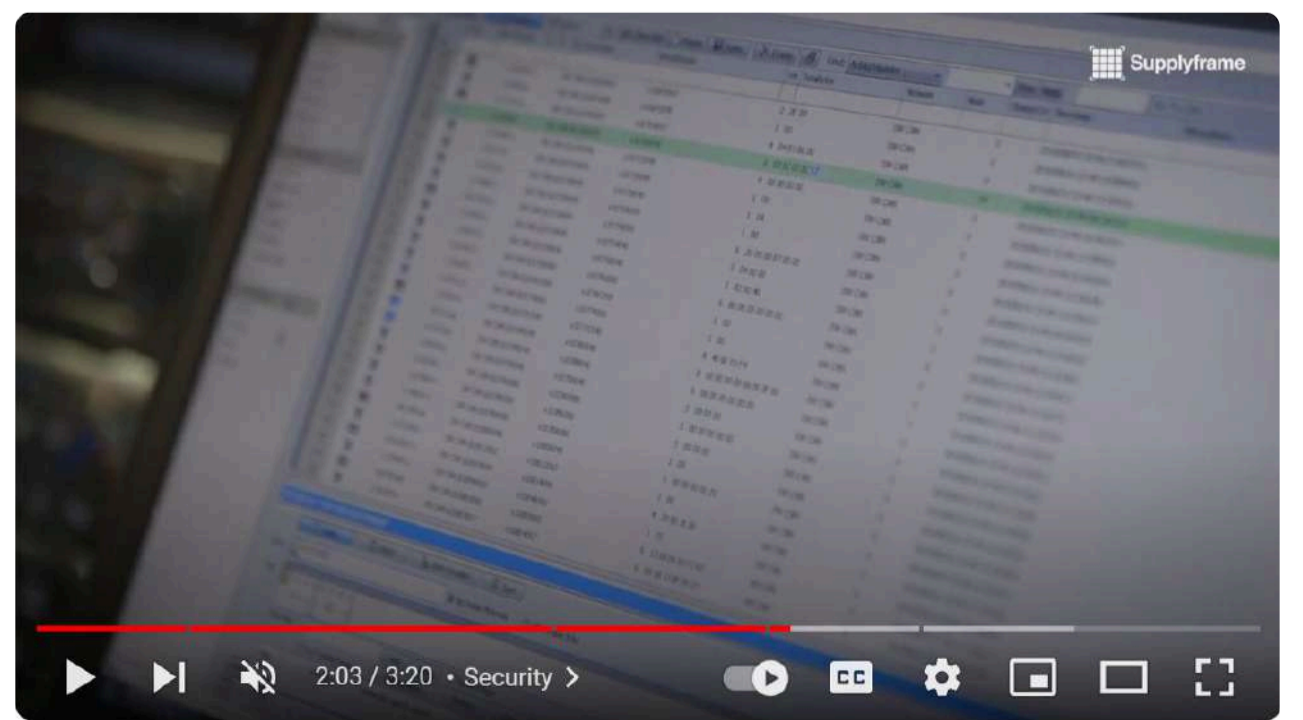
But the surprises didn't end there – another video surfaced, revealing a hacking competition in action.



DEF CON 27: Car Hacking Deconstructed



DEF CON 27: Car Hacking Deconstructed



DEF CON 27: Car Hacking Deconstructed

[Video3 – “**DEF CON 27: Car Hacking Deconstructed**”, Credit: [Source](#)]



Argus Cyber Security Demo: Stops Car Hacking



Argus Cyber Security Demo: Stops Car Hacking




Contact Us :



Who would've guessed our leads would guide us to such riveting real-world testing footage before our cut-off date? These videos provide undeniable proof that our claimed invention was indeed in use before the deadline. And just like that, we uncovered system prior art.



Here Are Some Tips We Learned Along The Way:

-  Don't wait around! By broadening our search beyond traditional NPL literature, we unearthed valuable system prior art that might have otherwise been missed.
-  Another effective method is to check teardown videos on the FCC database, especially for US products.
-  Remember, thorough research is key. Taking the time to explore all available avenues ensures a successful invalidation process every time!

Expert

He is a leading tech analyst with a curiosity for groundbreaking inventions. With an engineering degree in Electronics and Communications from UIET, Chandigarh, Ankush holds over 6 years of hands-on experience in the field. Leading a skilled team, he excels in conducting accurate prior art searches, comprehensive portfolio analyses, and crafting strategies tailored to client's unique needs. His expertise spans a wide spectrum of cutting-edge technologies including 3G/4G/5G, Wifi, IoT, AI/ML, smart and power electronics, and beyond.



Contact Us :

