Cybersecurity Overview – supplementary slides

Dr Dan Kim

Associate Professor in Cybersecurity,
School of EECS
The University of Queensland, Australia
Homepage: https://researchers.uq.edu.au/researcher/23703

Availability - CrowdStrike outage

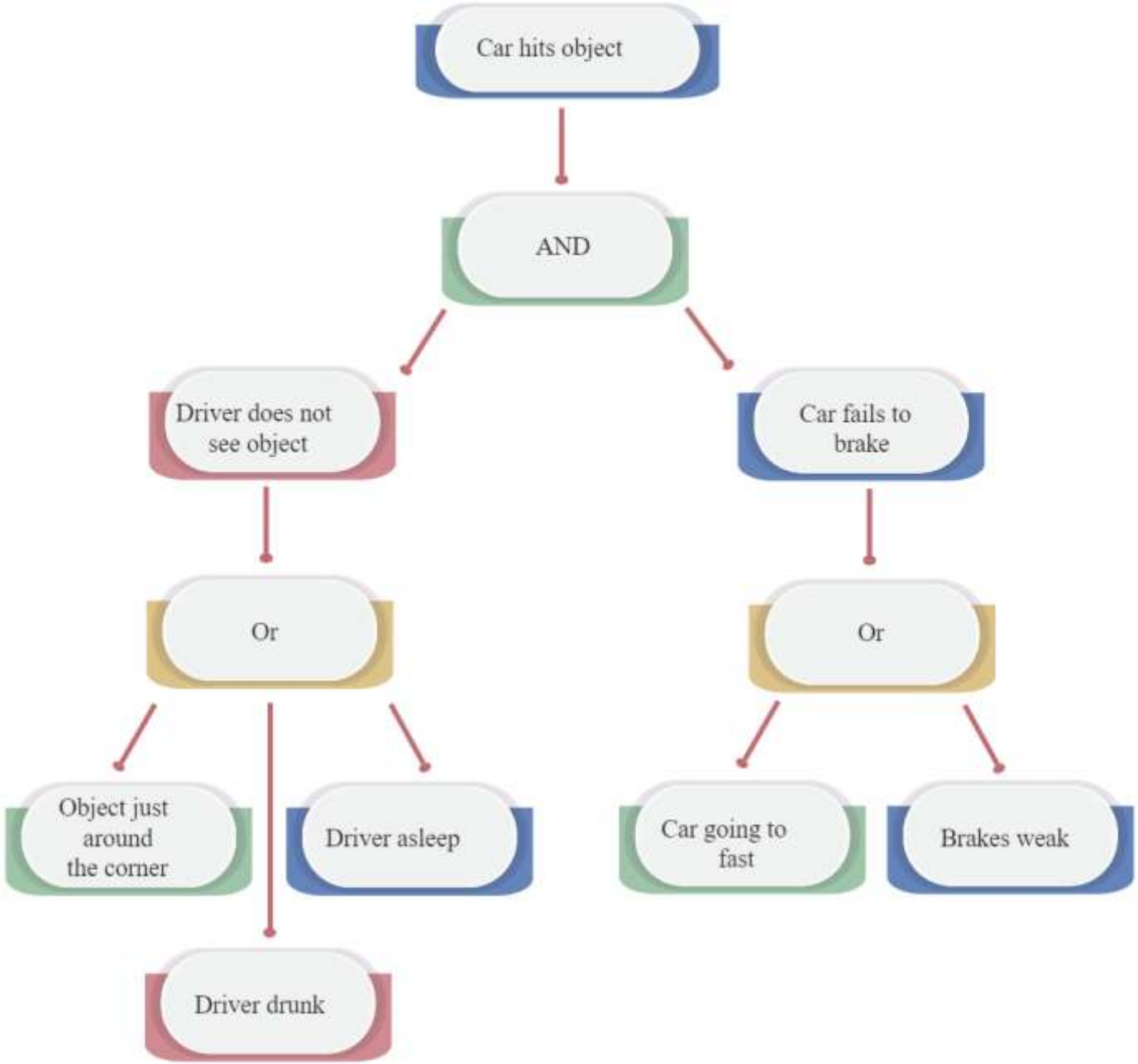
- considered the largest IT outage in history affecting millions of Windows systems around the world.
- occurred July 19, 2024, with millions of Windows systems failing and showing the infamous blue screen of death (BSOD).
- The flaw in CrowdStrike Falcon was inside of a sensor configuration update. The sensor is regularly updated -- sometimes multiple times daily -- to provide users with mitigation and threat protection.
- Microsoft estimated that approximately 8.5 million Windows devices were directly affected by the CrowdStrike logic error flaw. That's less than 1% of Microsoft's global Windows install base.
- Services affected include the following.
  - **Airlines and airports:** The outage grounded thousands of flights worldwide, leading to significant delays and cancellations of more than 10,000 flights around the world. In the United States, affected airlines included Delta, United and American Airlines. These airlines were forced to cancel hundreds of flights until systems were restored. Globally, multiple airlines and airports were affected, including KLM, Porter Airlines, Toronto Pearson International Airport, Zurich Airport and Amsterdam Schiphol Airport.
  - **Public transit:** Public transit in multiple cities was affected, including Chicago, Cincinnati, Minneapolis, New York City and Washington, D.C.
  - **Healthcare:** Hospitals and healthcare clinics around the world faced significant disruptions in appointment systems, leading to delays and cancellations. Some states also reported 911 emergency services being affected, including Alaska, Indiana and New Hampshire.
  - **Financial services:** Online banking systems and financial institutions around the world were affected by the outage. Multiple payment platforms were directly affected, and there were individuals who did not get their paychecks when expected.

https://www.techtarget.com/whatis/feature/Explaining-the-largest-IT-outage-in-history-and-what-it-involved

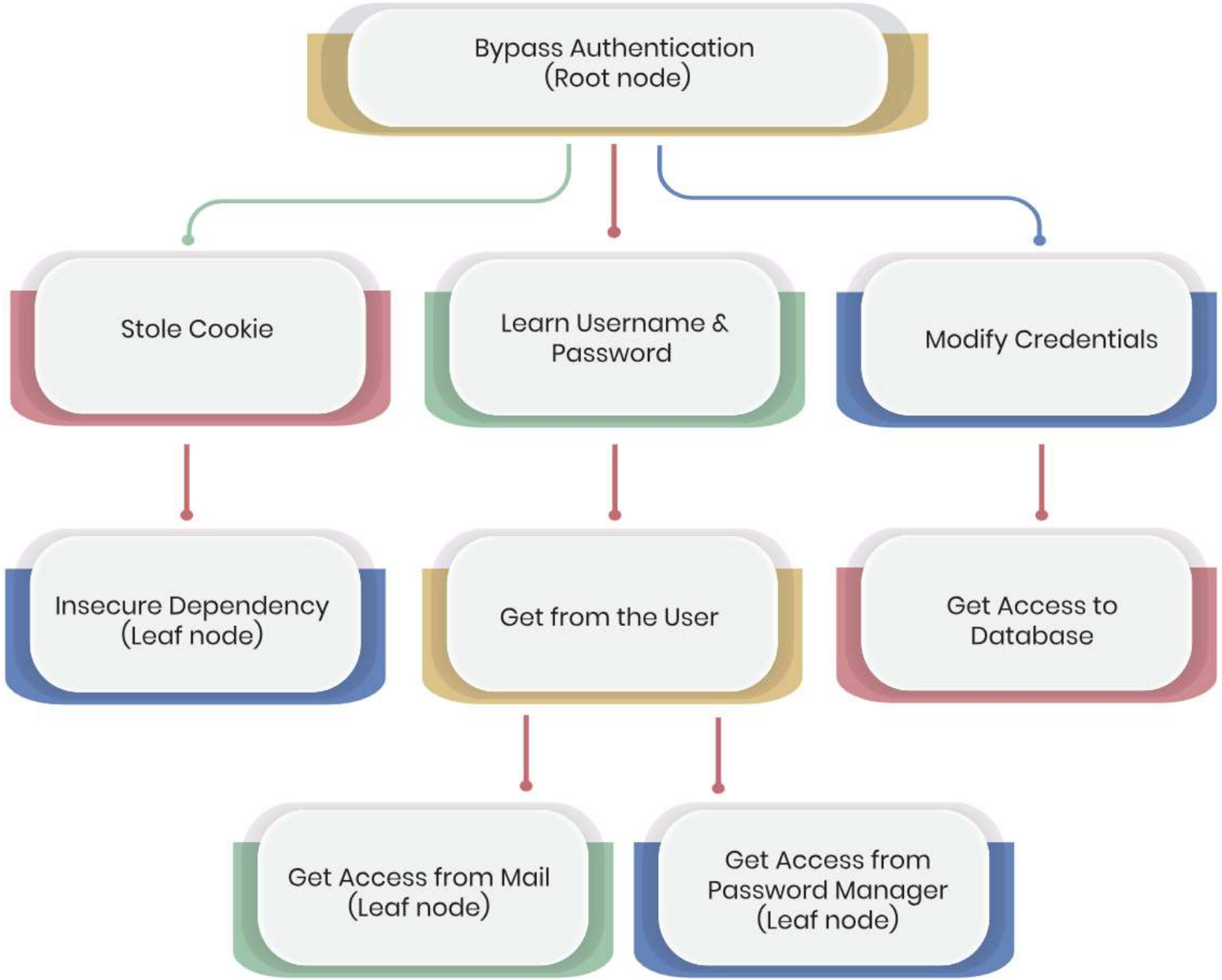
Attack Trees? How practical?

- National Cyber Security Centre (NCSC) in UK used attack trees to **identify cyber security risks** in their security analysis for the UK telecoms sector.
- This involved identifying higher level impacts or outcomes, and linking these to lower level methods or exploitation routes that could contribute to such events occurring.

https://www.ncsc.gov.uk/collection/risk-management/using-attack-trees-to-understand-cyber-security-risk



https://www.ncsc.gov.uk/collection/risk-management/using-attack-trees-to-



https://www.ncsc.gov.uk/collection/risk-management/using-attack-trees-to-