Cybersecurity Digest

Bi-Weekly update by the CISO Section of Meghalaya Rural Bank

Volume 2 Issue 12 **Date: 16.09.2025**

Your employees are using AI. But are they using it safely?

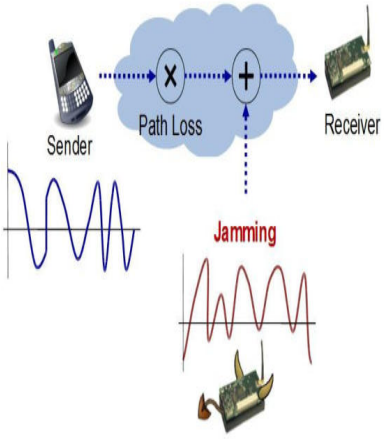
"Shadow AI", the use of unapproved AI tools at work, is more common than you think. New research reveals that 80% of companies are showing signs of this risky behaviour. From sales teams entering customer data into ChatGPT to HR uploading resumes into Claude, the potential for data leaks is massive.

Jamming– The Rising Cyber Threat

Jamming attacks are the use of malicious interference on wireless communication systems, including Wi-Fi, Bluetooth, and cell phone networks. GPS systems can also be the target of jamming attacks. In 2020, for example, 85% of cargo truck thefts in Mexico reportedly involved GPS jamming.

The intention of a jamming attack is to "jam" a network, preventing devices from communicating, disrupting essential services, or even bringing down a network altogether in a denial of service (DOS) attack.

Jamming attacks generally use physical devices to overload a network with strong signals, disrupting usual operations. Fraudsters can also take advantage of the service disruption, and therefore the confusion to callers, by committing telecommunications fraud attacks such as call spoofing.



Jamming attacks can happen on both a small and large scale. They can be weaponized as a wartime tactic or in terrorist attacks, or used for relatively superficial purposes. For example, jamming attacks can be used to cut off sound to Bluetooth speakers if the music is too loud at a neighborhood party

GPS Jamming

GPS jamming became a common part of vehicle theft from around 2010. An inexpensive device is used to disrupt signals to and from GPS satellite devices, essentially allowing a stolen and tracked vehicle to "disappear off the radar". Such devices have been used both for car thefts and for thefts of lorries with valuable cargo.

The same jamming devices can also be used to evade road tolls that use automated systems.

Wi-Fi Jamming

Wireless jamming attacks can use dedicated jamming devices or specially configured or compromised Wi-Fi-enabled devices such as laptops or smartphones.

A Wi-Fi jamming attack could be used to flood a wireless network with a constant disruption signal, resulting in slow speeds or a total lack of access for legitimate users. For example, security firms warn that wireless jammers can be used to disable Wi-Fi security cameras, by robbing them of the bandwidth they need to operate.

Consequences of Jamming Attacks

Disruption of Communication

Jamming attacks have the ability to disrupt or completely disable communication on networks such as Wi-Fi and Bluetooth. This can result in a loss of internet connectivity and the failure of the systems relying on it.

Data such as passwords and card details can also potentially be intercepted by a malicious actor as part of a jamming attack.

Inaccurate Navigation and Positioning

Above, we described how a GPS jamming attack can play a part in car theft or evading detection for traffic offenses. Various jamming attacks can also be used in modern military conflicts.

For example, it's been reported that GPS jamming attacks have taken place in Eastern Ukraine on a regular basis since Russia annexed Crimea in 2014. In war scenarios, jamming techniques can impact everything from unit positioning to the flow of information.

Financial Losses

Businesses of all kinds are increasingly reliant on wireless technology, for everything from service provision to payment processing. A retail store or restaurant that's unable to process card transactions due to a lack of internet access will immediately begin to lose money.

Jamming attacks can also play a part in other incidences of cybercrime, such as masquerade attacks, in which the interception of communications can lead to costly data leaks that compromise people's financial security.

How to Detect and Protect Against Jamming Attacks

a. Establish a way to monitor the strength of the wireless signal on the network. A sudden inconsistency in signal strength, or an increase in interference could be signs of a jamming attack in progress.

b. Use an intrusion detection system (IDS). Such a system can identify unusual traffic on the network and sometimes also take automatic steps to thwart an attack in progress. For example, an IDS can be used to shut down a frequency channel where suspicious activity is detected.

c. Educate yourself and other device users on cybersecurity principles. Encourage the use of virtual private networks (VPNs) and advise caution when using public Wi-Fi networks, such as those in cafes and hotels.

d. Use the strongest encryption available and practice good password hygiene.

Alongside these steps, remember that the best practices in cybersecurity may change over time, especially given the developing technology involved in jamming attacks. As such, point number c above bears repeating: Educate yourself about how to stay safe online with the most up-to-date research on jamming attacks and countermeasures.