WHEN GOOD TECHNOLOGY GOES BAD

The Evolution of Mobile Technology

CSID
A part of Experian

MARCH 2014

INTRODUCTION

A GREAT IMPACT ON SOCIETY

Mobile hardware is evolving at an unbelievable rate. Think about it: the cell phone you are using right now has more computing power than the computers that sent Neil Armstrong into space a few decades ago. And not only has mobile technology been advancing so impressively, but the costs associated with the technology have been decreasing, making it more widely available and adopted.

Such advancements in technology and reduction in costs have drastically changed the way we live and lead to more conveniences in our lives. We can send important files no matter where we are in the world, communicate more easily with family and friends, and even work outside of the home and office. We have more information at our fingertips than any time in history. Not only that, but advancements in mobile technologies have even provided Internet access to those who may not have had it before. Everyone now has a voice.

Clearly, the evolution of mobile technology has had a great impact on our lives – but it's not all positive. As we develop more sophisticated mobile devices like cell phones, tablets, and routers, others are devising ways to use them for harm.

We have more information at our fingertips than any time in history.

ENTER EXPLOITATION

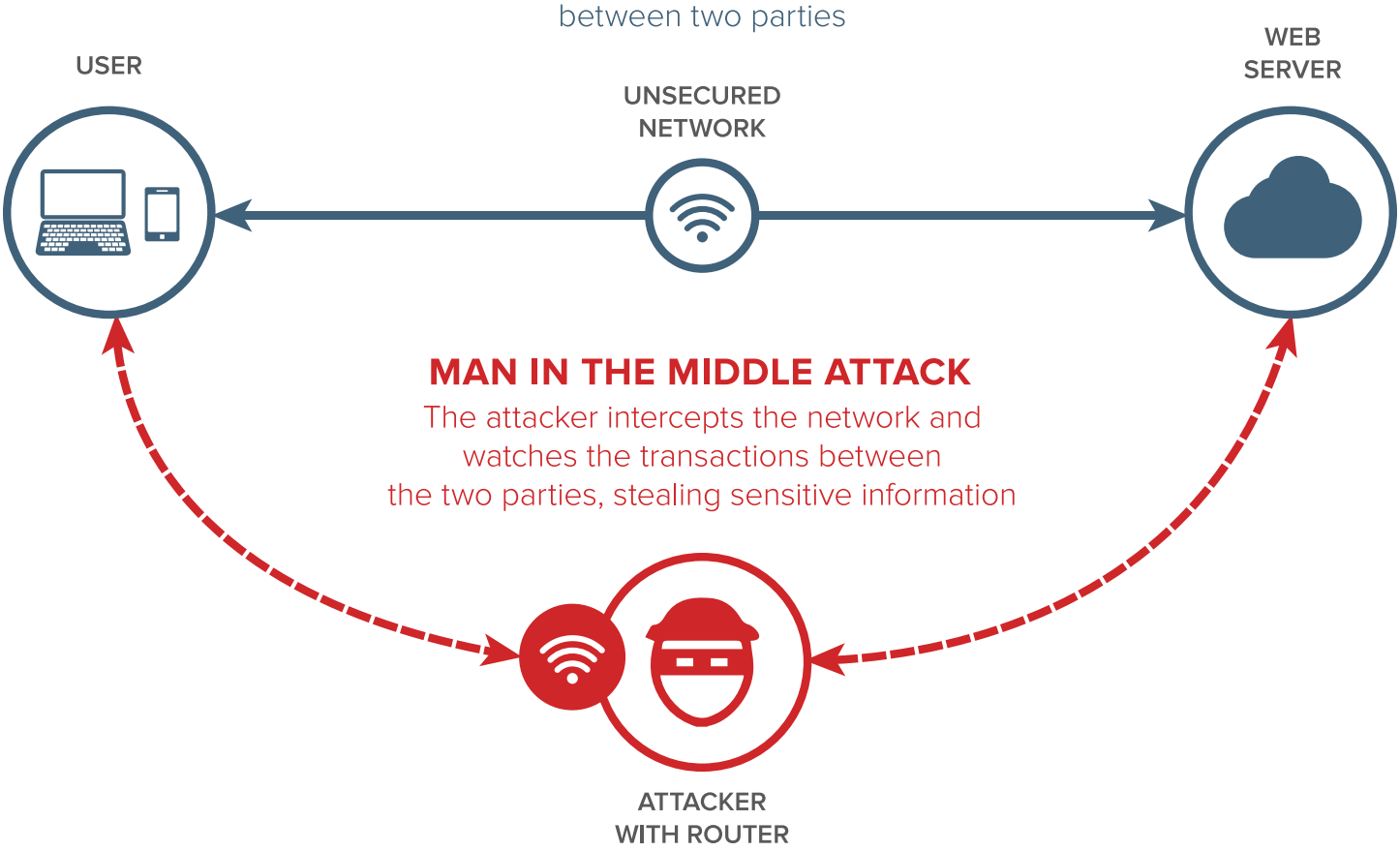
Man-in-the-middle (MITM) attacks are a type of cyber attack in which a malicious individual inserts himself into a conversation between two devices, impersonates both devices and gains access to information that the two devices were trying to send to each other. With just a $20 router and an ordinary computer, anyone can conduct a man-in-the-middle attack.

You can most often find MITM attacks taking place on unsecured networks like public WiFi hotspots. Why are these hotspots targeted? First of all, they are popular. According to the Wireless Broadband Alliance, the number of public WiFi hotspots is expected to reach 5.8 million by 2015, up from 1.3 million in 2011 – a 350% increase in just four years. They are also vulnerable. The 2013 Kaspersky Consumer Security Risks Survey found that 34% of public WiFi users said they took no special measures to protect online activity while using a hotspot and only 13% took the time to check the encryption standard of any given access point.

Because of its hub-and-spoke architecture, any WiFi access point is a window to the Internet for all the devices attached to it. Every request from a device goes via an access point, and only then reaches the sites that users want to visit. Without any encryption of communications between the device and the access point, it's a simple task to intercept all the data a user enters. So if you conduct a sensitive transaction while on public WiFi (i.e. purchase something in an online store or logging into your online bank account) this data can be intercepted and used for fraud and identity theft.

If your communication is encrypted, you are still vulnerable – a MITM attack also allows the attacker to effectively re-route users to malicious versions of requested sites. At these malicious sites, they can capture data in plaintext as well as attempt to capture additional details.

WI-FI PLATFORM EXPLOITATION HACK



TAKEAWAYS

While technology makes our lives convenient, it also introduces new security risks and holes. It is time to stop sacrificing security for convenience. We need to use technology in the right way to stay secure. You wouldn't leave your car unlocked, so why do the same for your mobile devices?

If you must use unsecured or public WiFi, keep your data secure with these tips:

• Be aware – Know that new types of attacks are developed and carried out each day. Stay smart and always use your common sense when on the Internet.

• Treat all WiFi links with suspicion – Malicious links go in disguise and often look valid.

• Verify you are using a legitimate link – Ask yourself, where did this link come from? Have you been to that URL before? Do you trust the source?

• Use a VPN – Virtual Private Networks (VPNs) enable your computer to access and share information across a public network as if it were connected to a private one. This is a good solution if you must use public WiFi.

• Avoid sharing sensitive information on websites – Keep activities like online shopping, banking and email to private networks, as they typically house a good deal of sensitive, private information that is valuable to cyber criminals.

• Protect your device against cyber attacks with antivirus solutions – Antivirus software can certainly help protect your device, but it is not foolproof. Use it in combination with other smart tactics like those listed here.

• Consider identity protection and monitoring services – As a business you can have a third party company monitor your business domain, IP addresses, and employee credentials for signs of fraud or compromise. As a consumer, you can protect you and your family through credit and identity protection monitoring.

ABOUT CSID

CSID

CSID, a part of Experian, is a leading provider of global identity protection and fraud detection technologies for businesses, their employees, and consumers. With CSID's enterprise-level solutions, businesses can take a proactive approach to protecting the identities of their consumers all around the world. CSID's comprehensive identity protection services extend beyond credit monitoring to include a full suite of identity monitoring and fraud detection services; identity theft insurance provided under policies issued to CSID; full-service restoration services; and proactive data breach services.

Methodology

CSID and digital data collection firm Research Now teamed up to survey a demographically representative sample of 150 owners of small businesses in the U.S. with 1-10 employees from the Research Now Small Business Owners Panel. The sample framework is balanced based on industry, vertical, number of employees, annual revenue, years in business, legal entity type and personal service business types.

Contact Us

Join CSID on Facebook at facebook.com/CSID and on Twitter at @CSIdentity.

For more information, please contact Director of Marketing, Cody Gredler at cgredler@csid.com.

Sources: NASA | Wifi hotspots set to more than triple by 2015, Informa, 2011 | Public WiFi Hotspots Ripe for MITM Attacks, Info Security, 2013

©2016 CSID

LEARN MORE AT

CSID.COM