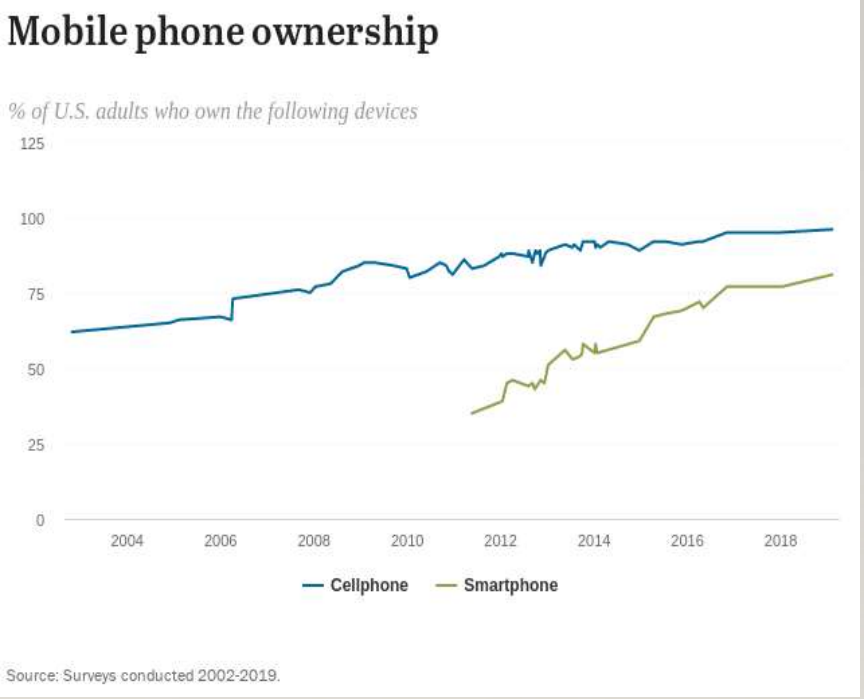
HOW TO COMPROMISE A CELL PHONE

BY

HAYDEN ACKERMAN

A TARGET-RICH ENVIRONMENT

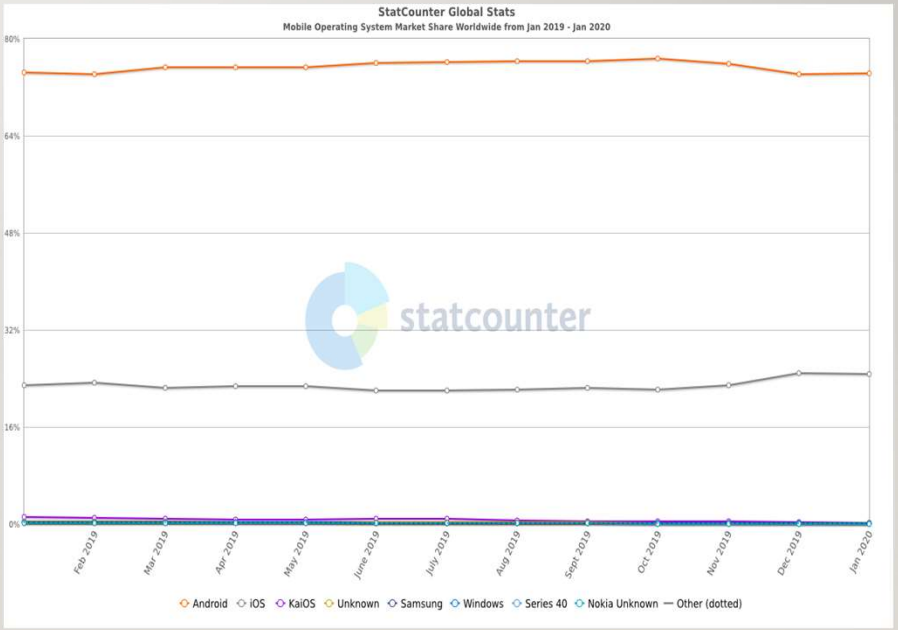
- The share of Americans that own smartphones is now 81%, up from just 35% in Pew Research Center's first survey of smartphone ownership conducted in 2011, up to around 96% (Pew Research Center, 2019).



https://www.pewresearch.org/internet/fact-sheet/mobile/

A TARGET RICH ENVIRONMENT(CONT.)

- Android has around a 74.3% market share, which translates to around two-and-a-half billion Android devices in the wild(Google, 2019).
- In contrast, according to Tim Cook, devices usage grew to around 1.5 billion(9to5Mac, 2020).



https://gs.statcounter.com/os-market-share/mobile/worldwide

SOCIAL ENGINEERING

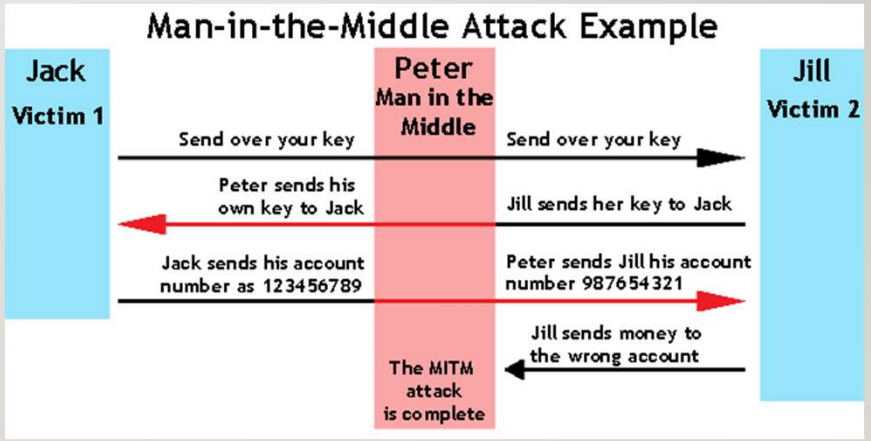
- Social engineering is the dark art of manipulating people (ExpressVPN, 2018).
- If I have your passcode, I have your phone. Let me install this sweet new app for you, it'll give me your banking information and everything!
- Do you need to charge your phone? Here, use my charging cable, an O.MG Cable which has a WIFI chip embedded in the USB header, allowing for remote commands ("O.MG Cable", 2019).

SIM SWAPPING

- A hacker contacts your wireless carrier (AT&T, T-Mobile, and so forth), wanting to transfer your phone number to his burner phone.
- Your phone number is stored on a SIM card in your phone, a little plastic chip. With personal information, the hacker could impersonate you and fool the support rep into installing your phone number on the hacker's own SIM card (Cipriani, 2020).
- Next thing you know, all 2-Factor authentication codes go to his phone and he wipes out your bank account.

MAN-IN-THE-MIDDLE ATTACKS

- Address Resolution Protocols (ARP) are used to find out identifying information about devices.
- ARP Poisoning is when an attacker falsifies ARP messages on a LAN and links your system's MAC address to his system (Libfeld, n.d.).
- I could choose to sniff your traffic or redirect you to the installation page for my malicious app.



https://www.veracode.com/sites/default/files/mitm-steps.gif

BLUETOOTH

- More devices have Bluetooth than WIFI, which makes a target-rich environment.
- Often exploits are used via the OBEX, or Object Exchange protocol, which allows devices to exchange files, business cards, and calendar information ("Bluetooth Hacking: A Case Study", 2009).
- Often Bluetooth is an easy drive-by attack vector, allowing attackers to siphon data without tremendous computing resources.

ACTIVE EXPLOITS

- StrandHogg – Uses a weakness in the multitasking system of Android to masquerade as a legitimate app
- Apple iMessage Exploit - Causes the phone to brick. The attacker sends a malformed message to the user's iMessage, and the malformed message is not interpreted correctly, bricking the phone.
- checkm8 – a bootrom vulnerability that will allow hackers to permanently jailbreak your system, giving them an insane amount of access to your phone. It's only available over a USB connection, but a hacker only needs physical access to your phone for a minute or two.

PROTECTING YOUR PHONE

- Don't let random strangers mess with your phone!!!!!! If you wouldn't trust someone with your wallet, why trust them with your phone?
- Don't plug into random USB ports all willy-nilly to charge. Purchase a USB condom. It only allows power to go through, no data whatsoever.
- Update your phone! Android vendors and Apple actively try to mitigate vulnerabilities and bugs.
- Use an antivirus.
- Be smart!

http://syncstop.com/usbcondom3.jpg

REFERENCES

- Browning, D., & Kessler, G. (2009). Bluetooth Hacking: A Case Study. *Journal of Digital Forensics, Security and Law*. doi: 10.15394/jdfsl.2009.1058
- Cipriani, J. (2020, February 9). SIM swapping is a scary form of phone number fraud. Here's how to detect it and what to do. Retrieved February 19, 2020, from https://www.cnet.com/how-to/everything-you-need-to-know-about-sim-swap-fraud-plus-one-thing-to-do-right-now/
- Demographics of Mobile Device Ownership and Adoption in the United States. (2019, June 12). Retrieved February 19, 2020, from https://www.pewresearch.org/internet/fact-sheet/mobile/
- Lexie. (2018, September 28). The Art of Social Engineering: Are You Being Conditioned? Retrieved February 19, 2020, from https://www.expressvpn.com/blog/the-art-of-social-engineering/

REFERENCES

- Libfeld, R. (n.d.). What is ARP Poisoning?: Security Wiki. Retrieved February 19, 2020, from https://doubleoctopus.com/security-wiki/threats-and-tools/address-resolution-protocol-poisoning/

Mg. (2020, January 2). O.MG Cable. Retrieved February 19, 2020, from https://mg.lol/blog/omg-cable/

Miller, C., & Apple. (2020, January 28). Apple announces record holiday Q1 2020 earnings: revenue of $91.8 billion, more. Retrieved February 19, 2020, from https://9to5mac.com/2020/01/28/apple-announces-record-holiday-q1-2020-earnings-revenue-of-91-8-billion-more/

Samat, S. (2019, August 22). A pop of color and more: updates to Android's brand. Retrieved February 19, 2020, from https://www.blog.google/products/android/evolving-android-brand/