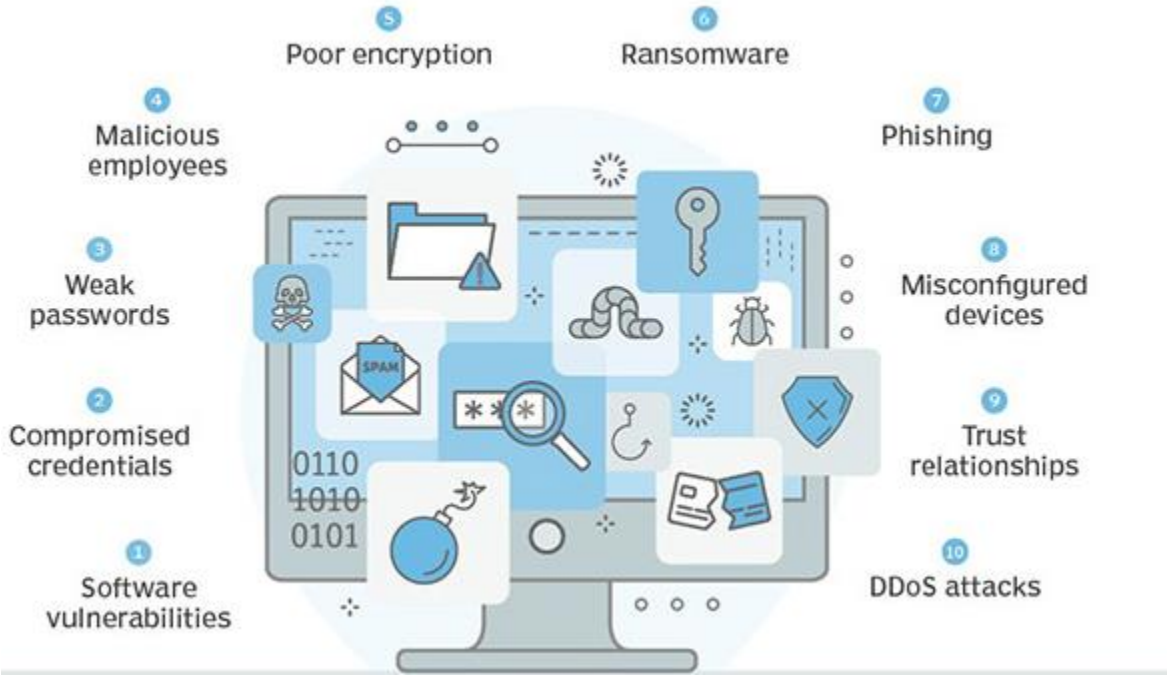
Universidad de Alcalá

Seguridad en Sistemas Distribuidos:
Vectores de ataque



Carlos Javier Hellín Asensio

carlos.hellin@edu.uah.es

Grado en Ingeniería Informática

Curso: 2021-2022

Contenido

Introducción

En este trabajo se ha documentado varios vectores de ataque con el que se pueda entender su funcionamiento con noticias, vídeos, herramientas, etc.… y en algunos casos con papers que profundizan aún más. Con esta memoria se quiere hacer un pequeño resumen de los distintos ataques, además de proporcionar los enlaces de dónde se ha obtenido la información de los distintos ataques para su consulta.

Deepface Attack

Uno de los ataques más usados con la llegada de los “fake news” y también como una mejora del conocido ataque fraude del CEO. En esta ocasión se encuentran bastante casos de estos ataques incluyendo uno que forma parte de la guerra de Ucrania con un vídeo falso de Zelenskyy. Existe una herramienta llamada DeepFaceLab que siguiendo el tutorial (disponible en las carpetas del ataque) se puede llegar a realizar un deepface de forma fácil, aunque he realizado algunas pruebas y para llegar a unos buenos resultados requiere tener muy buenas tarjetas gráficas.

Enlaces:

https://www.theguardian.com/world/2021/apr/22/european-mps-targeted-by-deepfake-video-calls-imitating-russian-opposition

https://twitter.com/RihardsKols/status/1385155498979348481

https://i.blackhat.com/USA21/Wednesday-Handouts/us-21-Deepfake-Social-Engineering-Creating-A-Framework-For-Synthetic-Media-Social-Engineering-wp.pdf

https://arxiv.org/ftp/arxiv/papers/2012/2012.07989.pdf

https://arxiv.org/ftp/arxiv/papers/2103/2103.00484.pdf

https://www.ic3.gov/Media/News/2021/210310-2.pdf

https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-war-report-hacked-news-program-and-deepfake-video-spread-false-zelenskyy-claims/

https://www.youtube.com/watch?v=X17yrEV5sl4

https://www.youtube.com/watch?v=cQ54GDm1eL0

https://www.youtube.com/watch?v=IFXLhoUNrw8

https://www.youtube.com/watch?v=EGEID-_XWCM

https://mrdeepfakes.com/forums/thread-guide-deepfacelab-2-0-guide

Eavesdropping Attack

Con la llegada de los asistentes virtuales se han creado dispositivos inteligentes que escuchan cuando les hablamos como Amazon Echo y Google Home. Esto ha hecho que salgan ataques de escucha, aprovechando que muchos de ellos permiten a los desarrolladores crear sus propias aplicaciones para estos dispositivos. Es cierto, que muchos de estos ataques son solucionados rápidamente por las empresas en cuestión, pero eso no quiere decir que siga existiendo la posibilidad de hacer este ataque de otra manera o que haya una vulnerabilidad que lo permita.

Enlaces:

https://www.srlabs.de/bites/smart-spies

https://www.youtube.com/watch?v=A3n-0AbXznc

https://www.youtube.com/watch?v=X2gddqD1wUI

https://www.investopedia.com/terms/e/eavesdropping-attack.asp

https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-kumar.pdf

Fake Broker Attack

El auge de las criptomonedas ha hecho que salgan falsos brókers que, mediante grupos de Telegram, se anime a inversiones donde supuestamente se consigue ganancias. Este ataque no es necesario de un software en concreto sino más bien requiere de ingeniería social. Últimamente aparece más en las noticias este tipo de casos, en el que muchas veces se realizan certificaciones falsas para convencer más de la inversión y en ocasiones se desconocen que si se consulta a la Comisión Nacional del Mercado de Valores se puede saber si esa empresa opera legamente en España.

Enlaces:

https://maldita.es/malditobulo/20220425/estafa-facebook-telegram-criptomonedas-timo/

https://www.osi.es/es/actualidad/avisos/2022/03/detectadas-distintas-modalidades-de-fraude-traves-de-plataformas-de

https://maldita.es/malditatecnologia/20220420/grupos-inversion-criptomonedas-telegram-timo/

https://www.tuparaisonline.com/novafx-de-philbrandon/

https://www.youtube.com/watch?v=j1Y_ST4oR7M&t=26s

Keystroke Inference Attack

A partir del COVID-19 se empezó a dar un mayor uso a las videoconferencias y con ello, distintos ataques se fueron conocieron. En este caso, es un ataque bastante peculiar, ya que, a partir del movimiento de los hombros, brazos, ojos, etc… se puede saber lo que está escribiendo la persona a través de una videollamada y, por lo tanto, si estuviera escribiendo contraseñas, PIN o información confidencial se podría conocer. Es un ataque que sobre todo se trata en el ámbito académico y científico, y no se ha encontrado noticias de ataques reales, pero no deja de ser interesante además de las posibilidades que pueda tener.

Enlaces:

https://www.researchgate.net/profile/Ahmed-Al-Haiqi/publication/266088297_Keystrokes_Inference_Attack_on_Android_A_Comparative_Evaluation_of_Sensors_and_Their_Fusion/links/542543810cf26120b7ac8784/Keystrokes-Inference-Attack-on-Android-A-Comparative-Evaluation-of-Sensors-and-Their-Fusion.pdf?origin=publication_detail

https://link.springer.com/chapter/10.1007/978-3-642-30921-2_16

https://arxiv.org/abs/2010.12078

https://www.youtube.com/watch?v=UFOhM1E-UvQ

https://www.semana.com/tecnologia/articulo/ojo-con-el-zoom-snooping-la-tecnica-con-la-que-descifran-contrasenas-por-videollamada/202003/

https://web.asu.edu/sites/default/files/cnsg/files/c41.pdf

https://www.youtube.com/watch?v=qFPZQ0t3-GM

log4jshell

La vulnerabilidad de log4jshell a finales de 2021 fue bastante notorio por ser una librería usada bastante por empresas y que permitiese la ejecución remota de código. Desde una máquina virtual con Kali se ha probado la vulnerabilidad con el código que está en las carpetas.

Enlaces:

https://www.xataka.com/seguridad/log4shell-vulnerabilidad-critica-proporciones-catastroficas-que-amenaza-destrozar-internet

https://github.com/kozmer/log4j-shell-poc

https://www.youtube.com/watch?v=tJW204uZWPU

https://arstechnica.com/information-technology/2021/12/minecraft-and-other-apps-face-serious-threat-from-new-code-execution-bug/

https://www.incibe-cert.es/blog/log4shell-analisis-vulnerabilidades-log4j

Reentrancy Attack

Los Smart Contracts, que hacen uso de la tecnología Blockchain, son unos contratos que se parece a lo que sería un contrato en la vida real, excepto que se han programado con un lenguaje determinado para establecer las directrices del contrato. Aunque los ataques de Reentrancy puedan parecer una vulnerabilidad del pasado, que afecto a muchos contratos y fueron robados millones de dólares (como se puede ver en la carpeta de noticias), sigue siendo una vulnerabilidad para tener cuenta a la hora de programar.

Enlaces:

https://www.youtube.com/watch?v=4Mm3BCyHtDY

https://www.youtube.com/watch?v=3sIwIYfeOD8

https://valid.network/post/the-reentrancy-strikes-again-the-case-of-lendf-me

https://www.securing.pl/pl/reentrancy-attack-in-smart-contracts-is-it-still-a-problem/

https://halborn.com/explained-the-burgerswap-hack-may-2021/

https://rekt.news/cream-rekt/

https://medium.com/siren/siren-incident-report-264e57f16d7

https://hackernoon.com/hack-solidity-reentrancy-attack

https://www.securing.pl/en/reentrancy-attack-in-smart-contracts-is-it-still-a-problem/

https://arxiv.org/pdf/2105.02881.pdf

Ryuk

Ryk fue uno de los ransomware más conocidos, junto a WannyCry, y más usado para ataques a instituciones públicas durante el año 2021. Fue usado para atacar el SEPE, el Ministerio de Trabajo y empresas privadas como Everis.

Enlaces:

https://www.businessinsider.es/vivio-ciberataque-sepe-dentro-19000-horas-extra-973861

https://www.businessinsider.es/ryuk-ransomware-detras-ataque-sepe-ha-fallado-826459

https://www.20minutos.es/tecnologia/ciberseguridad/asi-es-ryuk-el-virus-que-tiene-en-jaque-al-ministerio-de-trabajo-este-malware-ya-fue-responsable-del-ciberataque-al-sepe-4724171/

https://elpais.com/economia/2021-06-09/everis-revela-que-el-ciberataque-de-finales-de-2019-le-costo-15-millones-de-euros.html

https://www.youtube.com/watch?v=CRCL9zma_ac

https://www.youtube.com/watch?v=PZqM8pwrLdQ

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-006.pdf

Supply Chain Attack

Los ataques de cadena de suministro son aquellos capaces de comprometer a los proveedores de servicios digitales (los ISP, proveedores de software, etc.) para así afectar a un mayor número de usuarios que utilizan o tienen contratado dichos servicios.

Algunos de estos ataques se han realizado contra empresas de EEUU y organizaciones gubernamentales como la NASA o el Pentágono.

Enlaces:

https://protecciondatos-lopd.com/empresas/ataques-cadena-de-suministro/

https://www.xataka.com/pro/ataque-a-solarwinds-explicado-que-ataque-a-esta-empresa-desconocida-trae-cabeza-a-grandes-corporaciones-gobiernos-mundo

https://www.xataka.com/seguridad/sofisticado-ciberataque-solarwinds-enciende-alarmas-proveedor-pentagono-decenas-grandes-companias-ha-sido-comprometido

https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html

https://www.youtube.com/watch?v=jxTxGlE9X5s

https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

Vehicular Sensors Attack

Los coches autónomos ya son una realidad, y con ello, llegan también los ataques. En este caso a los sensores que llevan estos coches, haciendo creer que existen obstáculos falsos o generando el dilema del tranvía. Todos estos ataques todavía están dentro de entorno de investigación, pero se deberá tener en cuenta para su futuro.

Enlaces:

https://www.osti.gov/pages/servlets/purl/1763654

https://cosmosmagazine.com/news/tricking-driverless-car-sensors/

https://hackercar.com/ciberataques-coches-autonomos/

https://www.mdpi.com/1424-8220/22/1/360/htm

https://www.wevolver.com/article/new.attack.on.autonomous.vehicle.sensors.creates.fake.obstacles

https://www.youtube.com/watch?v=hYuvmwzqmsY

Voice Spoofing Attack

Parecido al ataque de deepfake y también como una mejora del fraude del CEO. Existe la tecnología y el uso de inteligencia artificial con el aprendizaje automático para, a partir de audios de una persona relevante, pueda ser imitada para realizar acciones fraudulentas o ciberdelitos como hacerse pasar por un CEO y que ya ha ocurrido si se ve en la carpeta de noticias.

Enlaces:

https://nakedsecurity.sophos.com/2019/09/05/scammers-deepfake-ceos-voice-to-talk-underling-into-243000-transfer/

https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402

https://blog.knowbe4.com/ceo-fraud-attacks-now-use-deepfake-audio-and-ai-to-mimic-executives-over-the-phone

https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/?sh=e7b249275591

Conclusiones

Como conclusiones de este trabajo es que se ha querido aprender de diferentes ataques más o menos actuales o que en un futuro puedan ser relevantes. También se ha “jugado” con algunos de ellos que fuesen fácil de realizar como el de deepfake y log4jshell para conocer y entender mejor su funcionamiento.

Está claro, que según se va avanzando en la tecnología van a surgir nuevos y mejores vectores de ataque para realizar ciberdelitos, y que, será necesario disponer de una defensa por cada ataque que se conozca. Muchos de estos ataques ya han sido corregidos, pero hay otros que todavía no hay un ningún sistema de defensa o serán difíciles de detectar.