REALISTIC HACKING FOR GAMES AND FICTION

Gen Con Online, September 16, 2021

Andrew Gronosky
Shewstone Publising LLC

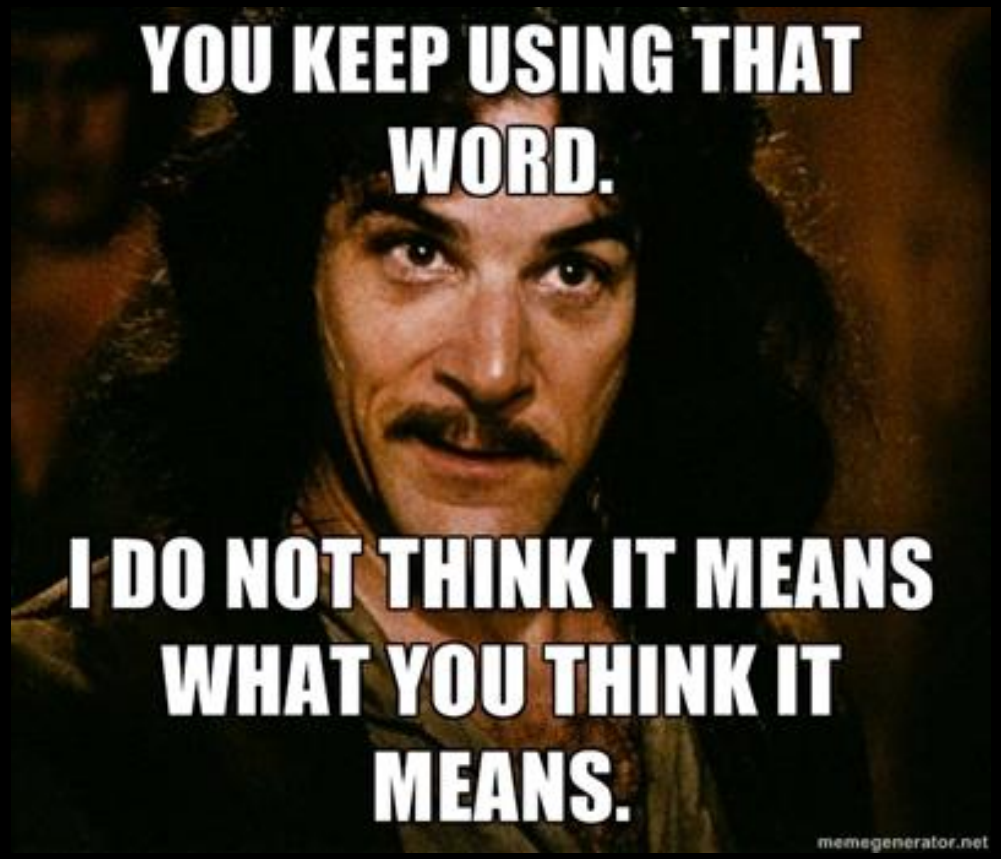
ABOUT ANDREW GRONOSKY

- By day, I lead a cybersecurity engineering team at a major enterprise software company.
- By night, I'm founder and owner of Shewstone Publishing.
  - Lead designer of **Magonomia®**, the RPG of Renaissance wizardry
  - Tabletop gamer and GM since 1980
- All opinions are my own.

AGENDA

- I'll describe general characteristics of several kinds of real-world attacks.
- I'll explain two interesting real-world attacks from 2017.
- We will use (and explain) real technical jargon.
- This presentation is non-technical: no details, code, or demonstrations.
- It will not tell you how to protect yourself or your company from attacks.
- Emphasis is on 21st century scenarios.

WHAT IS "HACKING" ANYWAY?



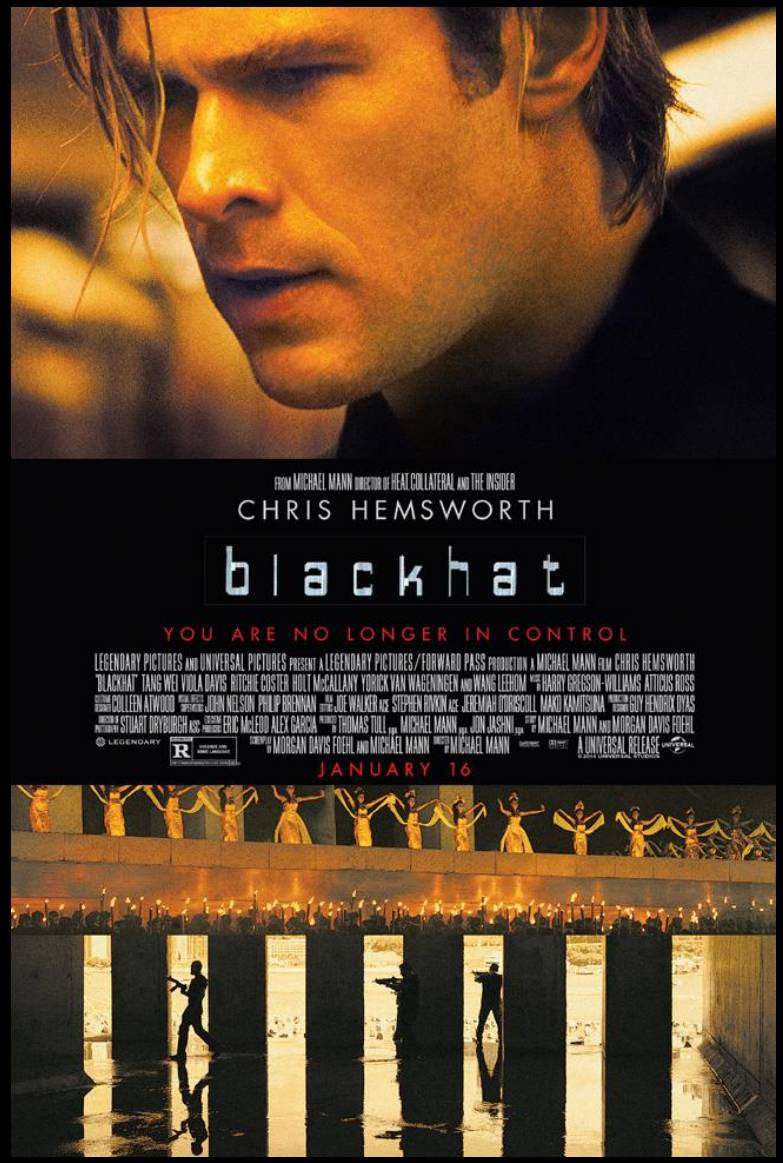
https://en.wikipedia.org/wiki/Hacker_culture

- "Hacking" has a different meaning to computer professionals than to news media.
- A "hack" is any simple solution to a complex problem, not necessarily related to security.
- Computer professionals call an attacker an "attacker" or "black hat (hacker)."

BLACKHAT (2015)

Why it's realistic:

- Describes an attack chain
- Multiple attack techniques
- Social engineering
- Target is a nuclear power plant
- Attacker didn't make their own tools
- Organized crime, organized response



SOCIAL ENGINEERING

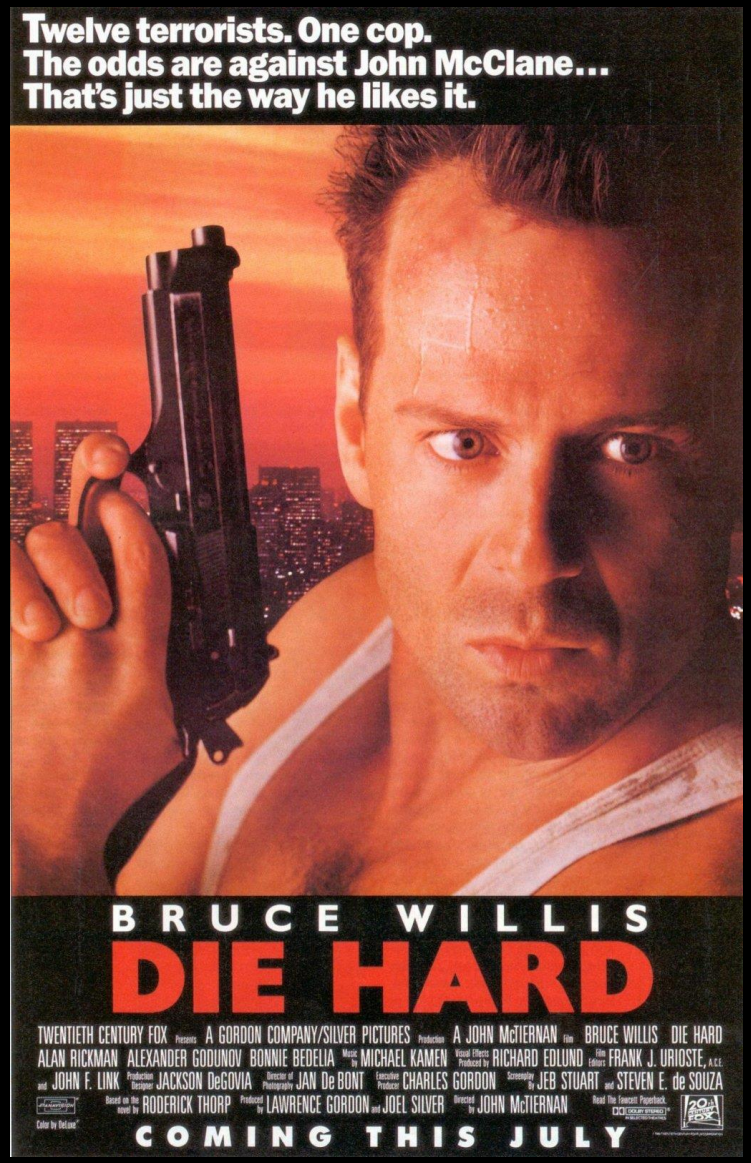
Social engineering means tricking a human into performing some action that helps the attacker.

- This blurs the lines between cyber-attacks, confidence scams, and espionage.
- In real life, about 80% of social engineering is by email (predictable, but it works).

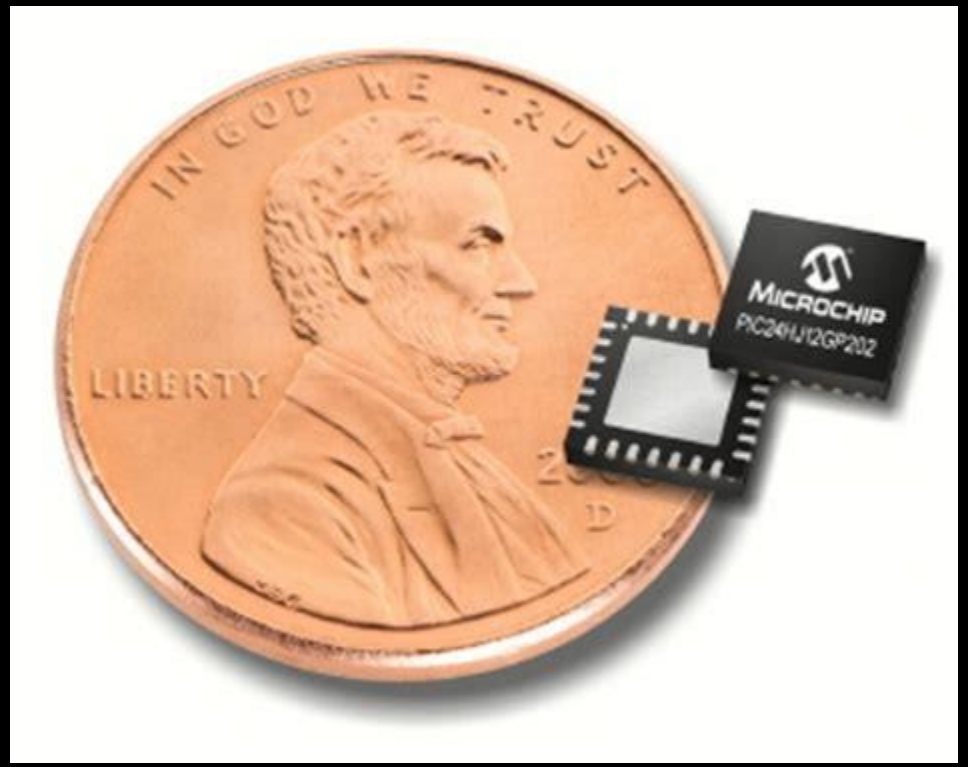
DIE HARD (1988)

Why it's realistic:

- Attacker's objective is to control physical systems
- The movie pre-dates the internet so local network access is required
- Organized crime with financial motivation



THE INTERNET OF THINGS



Everything that has a power cord [or battery] will be [wirelessly] connected to the internet, whether it makes sense or not.

- When every light bulb has an internet connection, every light bulb needs security updates.

CASE STUDY: CASINO FISH TANK (2017)

- Attackers used a smart aquarium as their entry and exit point to the casino's network.
- They exfiltrated the high-roller database.
- The attack was eventually detected by an unusual amount of outbound data from the fish tank.

https://www.forbes.com/sites/leemathews/2017/07/27/criminals-hacked-a-fish-tank-to-steal-data-from-a-casino

CASINO FISH TANK INSIGHTS

Why it's interesting

- You might think security isn't that important for a fish tank.
- Internet-connected sensors are already everywhere.
- Imagine if the attacker had to physically tamper with the device to exploit it.

Why it's representative

- 20% of attacks go undetected for months or years. Only 60% are detected within days.
- About 25% of attacks in 2020 used the target system only as a stepping stone.

VULNERABILITIES AND EXPLOITS

- A **vulnerability** is a security flaw or weakness that can accidentally or intentionally cause loss of confidentiality, integrity, or availability.
- An **exploit** is an intentional procedure for using the vulnerability to cause such an impact.

CHARACTER SHEET OF A VULNERABILITY

Common Vulnerability Scoring System (CVSS) v. 3.1 Base Score Metrics
https://www.first.org/cvss/calculator/3.1

IMPACT: THE CIA TRIAD

- **Confidentiality:** Read or copy data without permission.
- **Integrity:** Tamper with data.
- **Availability:** Prevent access to information or systems, temporarily or permanently.

INTEGRITY IMPACT

Real scenarios

- Tamper with system logs to conceal malicious activity.
- Install bitcoin mining software.
- Install key logger or network logger.
- Reprogram uranium refinement centrifuges (Stuxnet, 2010).

Imaginary scenarios

- Feed fake video into surveillance system or police body camera.
- Create a fake identity for a person or a company.
- Reprogram connected devices.
- Frame someone for cyber crime.

CASE STUDY: NOTPETYA (2017)

- It looked like ransomware but paying the ransom did not release the files.
- It destroyed data, backups, and network hardware.
- $10 billion economic damage.
  - Maersk, FedEx $300 million each
  - Ripple effect through supply chain

https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/notpetya-timeline-of-a-ransomworm/

NOTPETYA INSIGHTS

Why it's interesting

- Allegedly a Russian attack against Ukrainian transport infrastructure.
- Cyber-attack can be the cause of any man-made disaster you want to introduce in your story.
- You can make a great story about response to an attack.
  Containment and response are a race against the clock.

Why it's representative

- Ransomware is the third most common form of attack and rising fast.
- Technically, it's not that clever.
- Far-reaching, cascading impact.

REALISTIC ATTACKS

- Real attacks require a chain of exploits.
- Attackers aren't usually trying to impress anyone. If it's boring, but works, they'll do it.
- About 90% are financially motivated. Espionage is a distant second, and political motivation is interesting but rare.
- 85% of major attacks in 2020 involved a human element: social engineering or an insider.

SERIOUS READING

"Verizon: 2021 Data Breach Investigations Report." *Computer Fraud & Security*. 2021.6 (2021): 4-4. PDF.

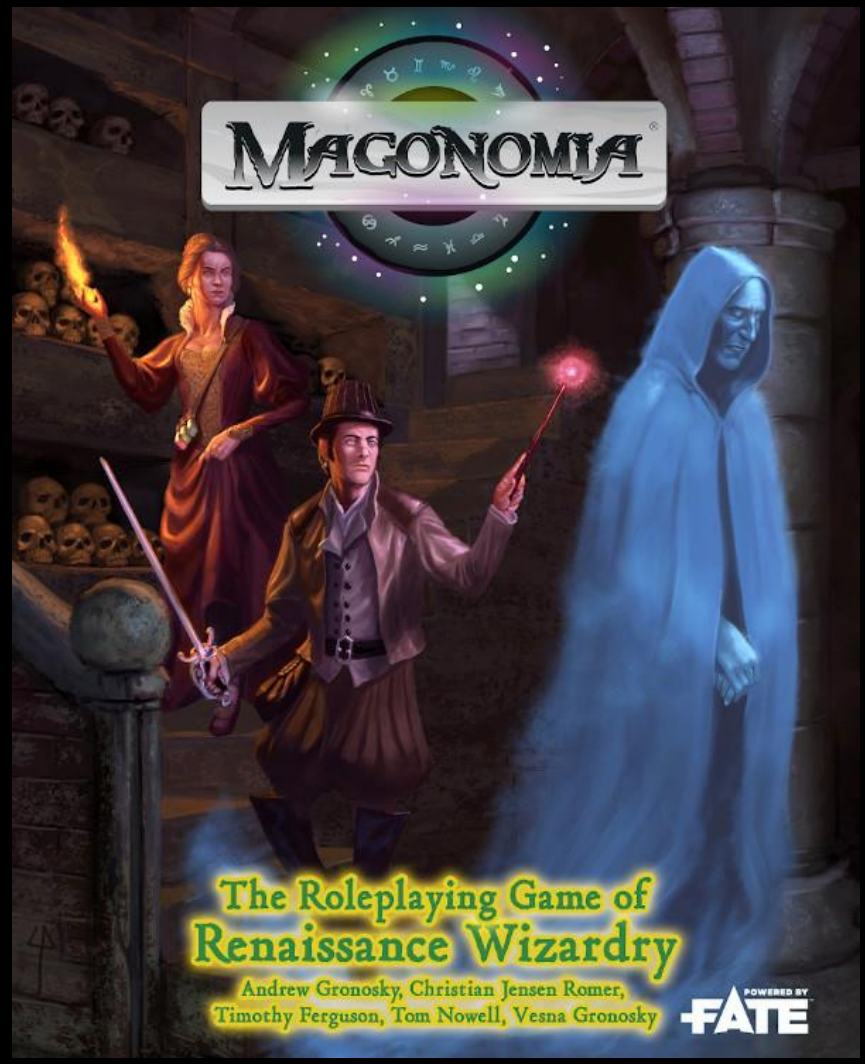
https://enterprise.verizon.com/resources/reports/2021/2021-data-breach-investigations-report.pdf

Schneier, Bruce. *Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World*. , 2019. Print.

YOU CAN BUY OUR GAME!

- *Magonomia®*, the RPG of Renaissance wizardry!
- Everyone plays a wizard using magic based on authentic Renaissance lore.
- If you buy the PDF before the print version comes out, we'll credit the PDF price toward your print purchase.

DriveThruRPG FIND OUR PRODUCTS @ DriveThruRPG.com



https://www.drivethrurpg.com/product/366281/Magonomia-the-RPG-of-Renaissance-Wizardry