# PROJECT 2035
# MAKE HACKING GREAT AGAIN

## CAN WE GO BACK TO PLAYING DOOM ON FRIDGES?

DEFCON908, OCTOBER 24TH, 2024

STEVE BECKER, LINKEDIN: /IN/STEVEJBECKER

# WHAT IS A HACK ANYWAYS?

- Used by MIT students for technology-based practical jokes
- The first modern appearance of the word was in MIT's The Tech on November 20, 1963
  - 'Hackers' tied up phone lines
  - Placed long distance calls, but charged them to a local radar base
  - Used a computer to search lines for an open dial tone

# HACKS VS SAFETY & RESOURCE LOSS

- A practical joke shouldn't cause a loss of money or resources
- Jokes don't cause damages to people or property
- That includes people's sense of self and privacy
- This becomes an eventual core piece of hacking groups:

  Don't Do Crimes & Don't Hurt or Harass People

# IN THE BEGINNING, THERE WERE SECRETS

- Sometime around 100 BC Caesar created a rotating cipher
- Fast forward to the 1500s and Vigenère used a key in a similar cipher
- 400 years later and the Germans used Enigma, cracked by Turing
- Then in the 1970s, IBM started work on Data Encryption Standard

# PRIVACY AND PROTECTION

- Aristotle wrote of two spheres of life – public and private
- Two Englishmen, Locke and Mill, stressed the rights of individuals between the 17th and 19th Centuries, with many peers in between
  - John Locke with natural rights of life, liberty, and property
  - John Stuart Mill with the importance protection from state interference
- The Internet then was invented…
  - This has made a lot of people very angry and been widely regarded as a bad move.

# HACKER EVOLUTION

- First hackers were playing pranks, then stealing phone cycles, then banks…
- The Mentor published the Hacker's Manifesto January 8, 1986
  - The acknowledgement of the criminal element is clear
  - But the intent is clear; curiosity is not a crime
  - Hacking is using curiosity to have a system work in an unintended way
  - Ergo, hacking =/= crime.

# IMPACT OF TECHNOLOGY ADOPTION RATES

- More businesses move to using technology
- Technology becomes more available
- Technology can be abused, both for fun and profit
- Two distinct branches of 'hacking' emerge

# COSTS OF HACKING

- Rough costs in 1990 was about $500 million
- In 2000, that rose to $17 billion
- In 2010, that rose to $1 trillion
- What will the cost end up being in 2035?

- This was according to documentation from Forbes and Washington Post

# REDUCING THE IMPACT OF HACKING

- Can we create applications with low to no risk?
- Can we train people to reduce risk from low to no?
- What other options are available?

# REDUCING RISK – FIRST IDEA

- Better application security
- Removal of client-side execution / processing
- Radical redesign of protocols and legacy integrations

# REDUCING RISK – SECOND IDEA

- Additional server side protections
- Use of homomorphic encryption techniques
- Quantum-resistant encryption techniques
- Removal of intentional weakening of security and encryption

# REDUCING RISK – THIRD IDEA

- Open source software must be maintained and audited
- Profit cannot be extracted without returning investment
- SBOM and other similar initiatives must be ramped up, fast
- If we can't roll our own, we need to make sure we're rolling something…

# REDUCING RISK – SOME QUESTIONS

- What can risk assessments reveal about the ‘unknown unknowns’ that will occur?
- Can the Internet be both compatible and secure? Do we need to have radical changes to backwards compatibility?
- What does that do to current economies and the global marketplace – will reduced equity lead to more criminal hacking?

# REDUCING RISKS – MORE QUESTIONS

- What impacts will increased knowledge and awareness of technology itself have on personal security and risk?
- Will we need evolutionary leaps in technology and not incremental, linear change?

# REDUCING RISKS –GOVERNMENT QUESTIONS

- Can additional regulations protect people appropriately?
- Will Bitcoin or other non-fiat currency be the problem or a solution?
- Can we reduce criminality through regulation? Through UBI? What other unexpected options do we have at our disposal?

# REDUCING RISKS – MORE GOV'T QUESTIONS

- Will nation-state sponsored attackers, or similarly resourced groups, disrupt reductions to risk and other changes?
- What does legal or physical-security based surveillance require of privacy and personal security? What trade-offs are we willing to make as a society?
- When will the average citizen vote with these things in mind? Will we have the option to vote at all?

# REDUCING RISKS – THE AI QUESTION

- What does AI do the future of security – both offensively and defensively?
- Will the data models reduce privacy, or will the tradeoffs brought by the power of knowledge tip the scales?

# IDDQD

- Can we go back to hacking meaning changing your Start Menu?
- Can we go back to just having fun exploring interesting things?
- But mostly, can we just go play Doom?