Introduction to Information Security

Theory vs. Practice
Administration

• Exercises
• Exam
• Feedback
  • https://www.ims.tau.ac.il/Tal/
  • https://www.guerrillamail.com/
The Ken Thompson Hack

- Reflections on Trusting Trust

The compiler translates source code into "opaque" binaries

- What if we changed the compiler to insert a backdoor?
- Yeah, but then we wouldn't use the compiler...
  - But how would we know? – Source code!
  - What if we changed the compiler's compiler, to insert a backdoor which causes the compiled compiler to insert a backdoor? – That wouldn't show in its source code!

Conclusion: Trust No One
TPM

• What if someone tampered with my application?
  • Let the OS verify it!
  • But what if someone tampered with my OS?
    • Let the bootloader verify it!
    • But what if someone tampered with my bootloader?
      • Let dedicated hardware verify it! – TMP
      • Tampering with dedicated hardware is hard
Theory vs. Practice

- Decidability vs. Computability
- In theory, theory and practice are the same; in practice, they're not
- For example, are air-gapped system secure?
  - Yes, if you implement everything yourself (remember the Ken Thompson Hack?)
  - Discovering Python – David Beazley
  - But if you move anything at all between the air-gapped system and the outside world...
    - USBs
    - CD-ROMs (!)
    - Sound, Electromagnetic Radiation, etc.
- Usability vs. Security – think "Your password has expired"
Interesting Communication Schemes

• **NOT:**
  • **TOR**
    • It's for anonymity
    • Except maybe hidden services...
    • Anyway, it's fishy
  • **Private Cloud Services**
    • Basically a meeting point
    • Connecting via proxy usually doesn't work
  • **Social Networks (+ Wikipedia)**
    • I can barely maintain my own Facebook Page
    • Detecting is much easier than mimicking
Interesting Communication Schemes

- **Tunnels**
  - Don't really solve the problem, but provide a safety net

- **MITM / MOTS**
  - Perfect, but extremely hard to achieve

- **File Sharing / Torrents**
  - Not a meeting place like a private cloud service
  - Not as hard to maintain as a social profile
  - But it must be synchronized!
    - That's just moving the problem elsewhere (i.e., communicating key instead of message)
Interesting Communication Schemes

• Reduction
  • Given that we can synchronize the URL / torrent, we can do the rest
  • That's already easier than downloading a payload or uploading a product

• Synchronization schemes
  • External
    • Weather forecast at a given place
    • Number of characters in a News website at a given time
  • Internal: PRG
    • Synchronize seed
      • Hardcoding
      • One time communication (≠ rare communications!)
Conclusions

• Information Security is not solvable*
  • * SAI / other singularity notwithstanding
• You must know practice theory
  • Especially to make abstractions and reductions well
• You must know practice
  • To get things done, obviously
  • To not hinder your thought process
    • Familiarize yourself with tools and frameworks
    • Spend time mastering the tools you use often
      • Special case: if you do it more than twice, write a script
شبירת דיסנגוס
Dan Gittik
דנ גיטיק
dan.gittik@gmail.com
050-3734176