1 | What are we protecting?

The Intel Management Engine (also abbreviated to Intel ME or even just IME) is an embedded microcontroller located on the Platform Controller Hub of modern Intel CPUs that runs a modified version of MINIX. It is outside the scope of the operating system, is always on while the computer is connected to power (even if the computer is turned off). It has more complete access to the system and all hardware than even the kernel itself and as a result is an appealing target.

1.1 | Sources

See here and here.

2 | Who are we protecting it from, and what are their motivations?

- Because of its notable status, hackers trying to find exploits as a challenge or for acclaim
- Large scale foreign attacks that want complete control of a system: Intel is a pervasive chip vendor so foreign governments are all but guaranteed to be using it
- Corporations interested in corporate esponiage or sabotage: Intel pervasiveness works here too
- Disgruntled employees wanting to get revenge on Intel
- Those looking to attack major corporations for data leaks, etc (see above)
  - Evidenced by `https://www.youtube.com/watch?v=iffTJ1vPCSo`: Google particularly interested in removing this.
- Profiteers: there is market for selling rootkits because of their general utility
- Government-pressured backdoors from entities like the NSA
- Anyone trying to write more generic yet hard-to-remove malware like ransomware for a profit motive

3 | What methods of attacks do we prevent?

3.1 | Potential Attack Vectors

- Rogue Intel engineer pushes a malicious firmware update

- Researcher finds exploit
  - MINIX vulnerability
  - Web server exploit
- Foreign agent gains physical access to a user's machine

3.2 | Preventative Measures

- Security by Obscurity
  - Intel is very close-lipped about details surrounding Intel ME and all of the firmware is proprietary
  - Argument in favor of security by obscurity is that it is harder to find exploits when there is less information available
  - Argument against is that it makes it harder for community to safely address exploits and usually leads to less security than public believes there is
- Rapid firmware updates in response to expoits
  - Example: `https://www.intel.com/content/www/us/en/support/articles/000025619/software.html`
- Disabling most of Intel ME for sale to government entities
  - Booting directly into HAP
  - Evidenced by `https://www.theregister.com/2017/08/29/intel_management_engine_can_be_disabled/`
- Proper access control systems at Intel
  - Having IDs
  - Requiring authentication to push to a repository
  - Mandatory code review

3.3 | External Preventative Measures

- Third party tools for disabling ME
  - MECleaner

4 | What are the possible effects of these attacks?

- Most major desktop computers would be vulnerable to a very hard to remove rootkit not visible to the OS
- Financial Wellbeing of Intel customers
  - Exploits could allow for major profit losses for large companies
  - PR damage for companies that are victims of exploit: i.e were there to be a data breach at Google due to this they would also recieve backlash despite it being Intel's fault
- Financial Wellbeing of Intel
  - Large scale exploit would lead to serious customer backlash and PR issues
  - Likely decrease in Intel sales vs AMD (even though AMD has an equivalent feature any exploit would likely be different)
- Emotional Wellbeing of Intel customers
  - Any data breaches could reveal sensitive information
  - Things like Ransomware target normal people and cause distress
- Physical Wellbeing of Intel customers
  - Foreign governments targeting utilities (like the U.S. did with Iran) could indirectly cause physical harm to U.S. citizens.

5 | What are their resources?

5.1 | Foreign powers

- Large amounts of money and time
- Access to talent

5.2 | Researchers

- Little funding
- Experience with finding exploits

5.3 | Rogue Intel engineer

- Access to proprietary information
  - Deeper knowledge of Intel ME
- Access to systems required to update firmware

5.4 | Profiteers

- Potentially money?
- Little resources.

5.5 | Individual people

- Time

5.6 | Corporations

- Large amounts of funding
- Access to talent

5.7 | Government

- Legal pressure
- Large amounts of funding

5.8 | Malware engineers

- Little to no resources

6 | What are our resources?

- Large company with lots of funding
- Most knowledge of how the Intel ME works due to the obscurity strategy
- Manpower enables a fast reaction time

7 | **What should we do?**

- Reduce the featureset of the Intel ME so as to remove attack vectors
- Sell chips without the ME to large companies to minimize damage on that front
- Add extra authentication and eyes into the pipeline for shipping firmware to prevent rogue employees from pushing malicious updates.