TEE-aided Write Protection Against Privileged Data Tampering

Lianying Zhao, University of Toronto
Mohammad Mannan, Concordia University, Canada
Ransomware

+ 

Data destruction malware
WannaCry: ~4-8 billion
NotPetya: ~10 billion USD
Hackers wipe US servers of email provider VFEmail

Hackers did not ask for a ransom. VFEmail described the incident as "attack and destroy."

By Catalin Cimpanu for Zero Day | February 12, 2019 -- 10:59 GMT (02:59 PST) | Topic: Security
CIH virus

April, 1998
Current solutions

1. backup
2. anti-malware
3. monitor file I/O
4. save encryption keys
FlashGuard (CCS 2017)
✓ can handle privileged ransomware
✓ relies on intrinsic properties of SSD writes

➡ requires trusted clock, firmware modification
➡ cannot deal with data destruction malware
Data loss prevention against privileged malware
Infection

Existing data

New data

Time
We need trusted environments

**TEE-Disk**: Self-encrypting drives
**TEE-Host**: Intel TXT or AMD SVM
TEE-Disk with:

1. fine-grained **access control**
2. **programmable** control (lock-unlock)

Any SED drive
TEE-Host with:

1. dynamic root of trust, isolated
2. sealed secret (platform state binding)
3. device I/O access

Intel TXT or AMD SVM + a TPM
Design
Read/Recovery: any
Write/Update: authenticated
Inuksuk
Updater
Browser
OS kernel
Flicker
Inuksuk drivers

protected partition(s)

system/other partition(s)

Applications

...
Deployment modes
Stand-alone:
occasional interruptions (TXT exclusiveness)
Network-based:

any user device, no interruptions
Implementation challenges

Windows 7, 10, and Ubuntu (Intel and AMD)

1. Safely use I/O devices from the user OS
2. Programming the SED OPAL interface
3. DMA access in TEE
4. Porting Flicker to Windows 10 64-bit
## Performance
(file-transfer: mean MB/sec)

<table>
<thead>
<tr>
<th></th>
<th>Write/Existing</th>
<th>Write/New</th>
<th>Read</th>
</tr>
</thead>
<tbody>
<tr>
<td>50MB file</td>
<td>43.93</td>
<td>41.69</td>
<td>32.17</td>
</tr>
<tr>
<td>500KB file</td>
<td>26.46</td>
<td>8.09</td>
<td>16.67</td>
</tr>
</tbody>
</table>

OS and application **agnostic, zero penalty**
Inuksuk: summary

• Addresses: wiper + crypto ransomware
• Rootkit-capable attacks
• Multi-TEE design

Thank you
https://madiba.ensc.concordia.ca