CERIAS

The Center for Education and Research in Information Assurance and Security

Ghost Patches: Faux Patches for Faux Vulnerabilities

Jeff Avery, Eugene H. Spafford

Problem: Patch Based Exploit Generation

Half of Android Devices **Unpatched** Last Year

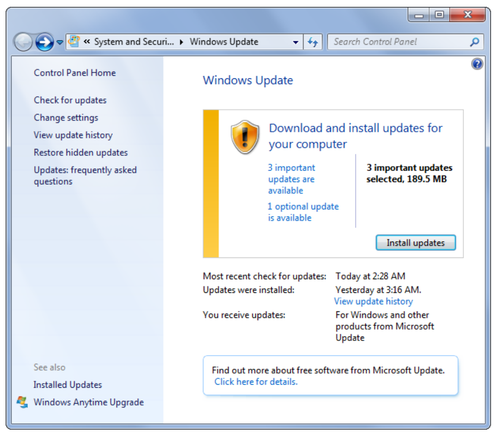
Threatpost - Mar 23, 2017

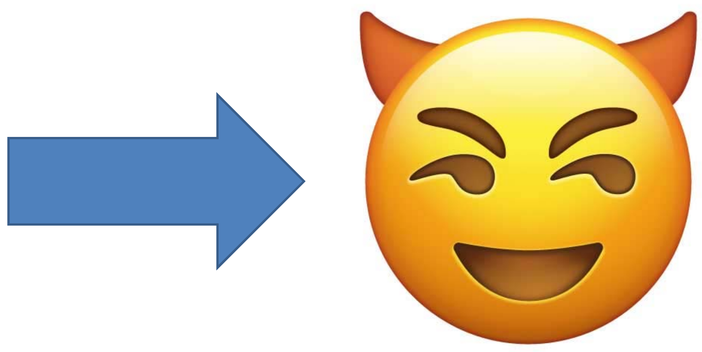
In that timeframe, Google touted its work with wireless carriers, **system** on chip manufacturers and device makers to release security patches at a faster pace. “Several manufacturers, including Samsung, LG and OnePlus, regularly deliver security updates **...**

How misaligned incentives give hackers an advantage over IT ...

TechRepublic - Mar 20, 2017

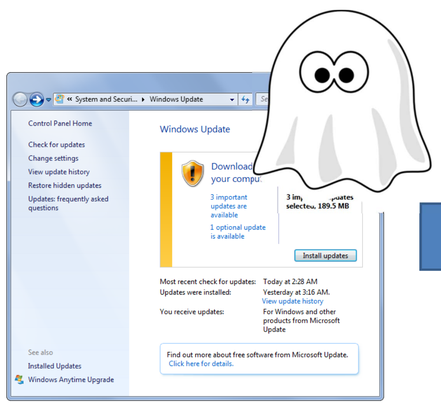
... costly vulnerability research and exploit development, they take advantage of publicly disclosed vulnerabilities to exploit **unpatched systems**." ...

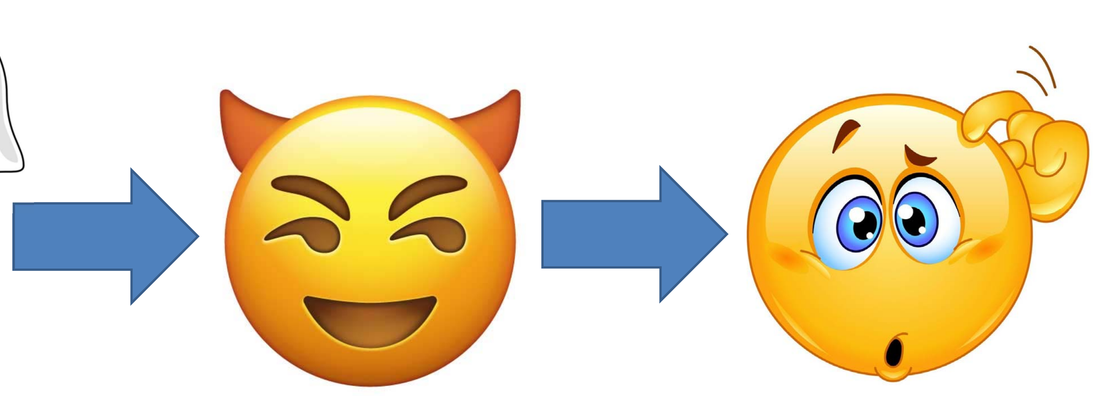




Fix: Deceptive Patches

Deception can be used in addition to traditional defenses to influence attackers’ decision making because of biases.[1]





Traditional Patch

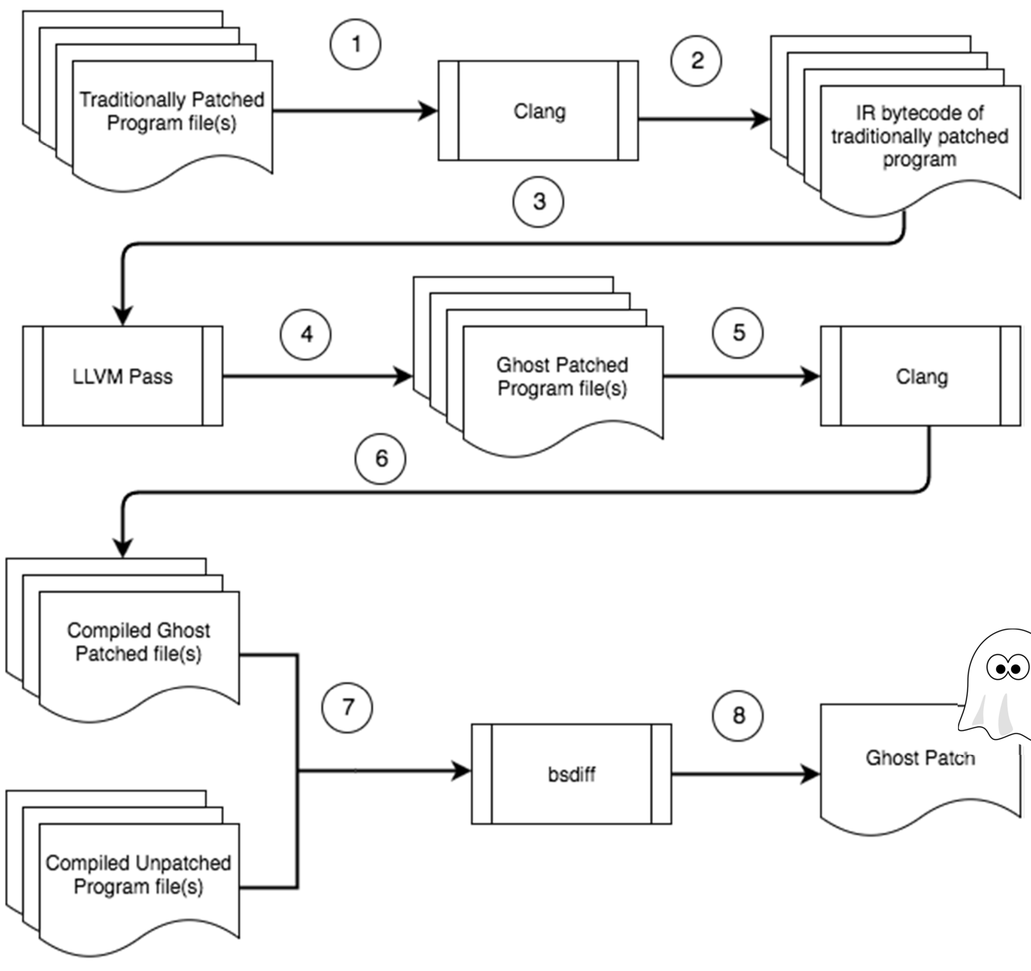
```
a = b + c;
If (a < 0)
    return
```

Faux Patch

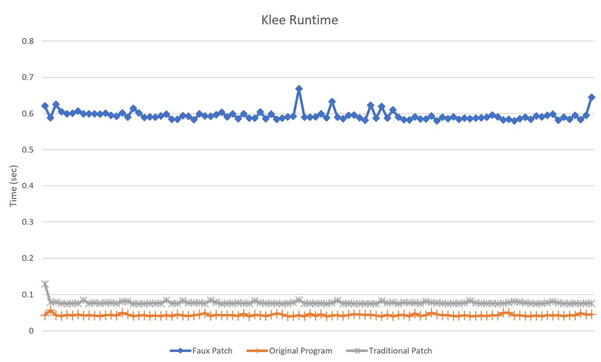
```
a = b + c;
If (a < 0)
    return

c = a + d;
If (c < 473)
    e = c
    e += 78
```

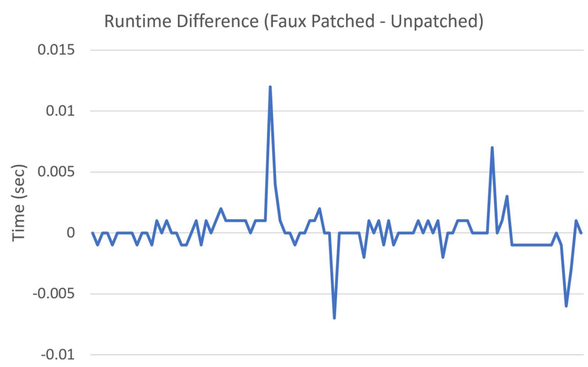
Results[2]



Dynamic Analysis Time



Runtime



Conclusion

- Ghost patch dynamic analysis time is significantly higher compared to traditional patches
- No statistically significant difference in program runtime between faux and unpatched programs
- Deception can be used to increase patch analysis time and exploit development by attackers while only trivially impacting program runtime

The National Science Foundation supported this research under award number 1548114.

1. Avery, Jeffrey. Almeshekah, Mohammed H.. Spafford, Eugene H.. Offensive Deception in Computing. In 12th International Conference on Cyber Warfare and Security (ICCWS 2017).
2. Avery, Jeffrey. Spafford, Eugene. Ghost Patches: Faux Patches for Faux Vulnerabilities. To appear in 32nd International Conference on ICT Systems Security and Privacy Protection (IFIP SEC 2017).

CERIAS

PURDUE UNIVERSITY