Ghost Patches: Faux Patches for Faux Vulnerabilities
Jeff Avery, Eugene H. Spafford

Problem: Patch Based Exploit Generation

Fix: Deceptive Patches
Deception can be used in addition to traditional defenses to influence attackers’ decision making because of biases.\(^1\)

Traditional Patch
\[
a = b + c; \\
\text{If } (a < 0) \text{ return}
\]

Faux Patch
\[
a = b + c; \\
\text{If } (a < 0) \text{ return} \\
c = a + d; \\
\text{If } (c < 473) \\
e = c \\
e += 78
\]

Results\(^2\)

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.