Characterizing Security and Privacy Practices in Emerging Digital Credit Applications

Jasmine Bowers, Imani N. Sherman, Kevin Butler, and Patrick Traynor

Florida Institute for Cybersecurity
University of Florida
In The News

Africa News

Making access to credit and loan repayment available to anyone, anywhere

Entrepreneur India

Digital and Paperless Personal Loans: The Future of Consumer Lending
There can not be a more lucid and safe way to get a personal loan, hence, let’s explore

Forbes

Chinese Social Credit Score: Utopian Big Data Bliss Or Black Mirror On Steroids?

The Philadelphia Inquirer

Fintech lenders are tracking and judging your digital trail
by Joseph N. DiStefano, Posted: July 3, 2018
What Is Digital Credit?

You're approved!

You're approved!

You're approved!

You're approved!
What Is Digital Credit?
What Is Digital Credit?
What Is Digital Credit?

Data, Data, Data!

Data, Data, Data!

Data, Data, Data!

Data, Data, Data!
Access to Credit
Access to Credit
Timeline

- **Goals**
- Methodology
- Results
- Takeaways
Goals

• Perform the first “industry-wide” security and privacy analysis of online credit providers.
  • Evaluate privacy policies for coverage
  • Measure security of applications
  • Characterize security of web servers
Timeline

• Goals

• **Methodology**

• Results

• Takeaways
Methodology

• Examine both the readability and content of privacy policies

• Measure the data types collected

• Evaluate the configuration of mobile applications and web servers
Timeline

• Goals

• Methodology

• **Results**

• Takeaways
The median of the international policies is higher than the median of both sets of U.S. policies.
While policies with lower word count covered less, we cannot conclusively say that longer policies are fully comprehensive.
Significant mismatches between data types mentioned in privacy policies and what is taken.
public class EncryptionHelper {
    private Context a;
    private static String b;
    private static byte[] c;
    private static EncryptionHelper d;
    private static final String e;

    static {
        EncryptionHelper.b = "AES";
        EncryptionHelper.c = new byte[]{-52, 51, -68, -121, -44, -114, -59, -20, -79, 22, 34, -77, -48, -75, 45, 93};
        EncryptionHelper.e = EncryptionHelper.class.getName();
    }

    private String decryptPassword(String arg9) {
        try {
            SecretKey v2 = SecretKeyFactory.getInstance("DES").generateSecret(new DESKeySpec("I-cry-when-angles-deserve-to-die".getBytes("UTF-8")));
            byte[] v1 = Base64.decode(arg9, 0);
            Cipher v0 = Cipher.getInstance("DES");
            v0.init(2, ((Key)v2));
            arg9 = new String(v0.doFinal(v1));
        }
    }

    public String getApiKey() {
        String v1 = this.settings.getString("api_key", "");
        String v2 = !TextUtils.isEmpty(((CharSequence)v1)) ? new DesDecrypter("KO0KOP0W0RLD0DOMINATION").decrypt(v1) : "";
        return v2;
    }
}
Audit of Transport Security Practices

- Best and worst Qualys SSL Server test score of all URLs found in the assessed apps

- Key:
  - Best
  - Worst
  - Best / Worst
Aftermath

• This work started two years ago as a partnership with the Center for Financial Inclusion (CFI) at Accion

• As a result, this work has caused significant changes in the community with lenders large and small beginning to talk more realistically about the protections they provide and must provide as an industry.

• This work has already had significant impact in the financial inclusion space, and has forced industry-wide discussion about security and regulation (which is difficult across borders).
Timeline

• Goals

• Methodology

• Results

• Takeaways
Take-Aways

• Privacy policies and code need to match.

• Even financial companies are getting security horribly wrong.

• The real risk of continuing to get this wrong is that the world’s most vulnerable (5 billion people) are at risk!
Thank you!

Jasmine Bowers  @JasmineDBowers
Imani Sherman  @SoulfulSherman
Kevin Butler  @kevinrbbbutler
Patrick Traynor  @patrickgtraynor