Trustwave®
SpiderLabs®

DEF CON 19:
Getting SSLizzard

Nicholas J. Percoco – Trustwave SpiderLabs
Paul Kehrer – Trustwave SSL

Agenda

- Introductions
- Primer / History: SSL and MITM Attacks
- Mobile SSL User Experience
- Research Motivations
- Research Implications
- Data Transmission Assault Course Components
- Introducing SSLizzard
- Mobile App Test Results
- Conclusions

Introductions

Who are we?

Nicholas J. Percoco (c7five)

- Head of SpiderLabs at Trustwave
- Started my InfoSec career in the 90s

Paul Kehrer (reaperhulk)

- Lead SSL Developer at Trustwave
- Enjoys baking cakes in spare time.

Introductions

What's this talk about?

- **De-evolution** of User **Security Experience** (in Mobile Devices)
- **History** and Types of **SSL Attacks**
- **Lack** of Testing **Tools** for Mobile Applications
- How Various App and Devices **Perform Under "SSL Stress"**
- A **Tool Release** to Help Solve this Problem

Primer / History: SSL and MITM Attacks

What is SSL?

- Stands for **"Secure Sockets Layer"**
- Developed by **Netscape** in 1994
  - Implemented in Netscape Navigator 1.0
- A protocol to secure a **client->server data transmission**
- Uses **Asymmetric Keys** to establish a **Symmetric Key**
  - This happens during a "handshake" before actual data is transmitted

Primer / History: SSL and MITM Attacks

- **Where is SSL (certs) Used?**
  - To Establish **Secure Client to Server** Communication
  - Client Identity (**User Authentication**)
  - Application **Signing**
  - Log **File Integrity**

Primer / History: SSL and MITM Attacks

- **How is SSL used in Mobile Devices?**
  - To Secure Communication Over **Public Networks**
  - To Establish "App" to **Server Communication**
  - "App" **Code Signing** (Android, IOS, BlackBerryOS)
  - Mobile Device Management **Profiles** (Signed)

Primer / History: SSL and MITM Attacks

- **What is a Man-in-the-Middle Attack?**
  - Injecting an "Attacker" between a Client and a Server Session.
  - "Attacker" intercepts Client request to Server
  - "Attacker" established a SECURE Session with Server
  - "Attacker" established a UNTRUSTED Session with Client
  - "Attacker" can then view / modified data between Client and Server

Primer / History: SSL and MITM Attacks

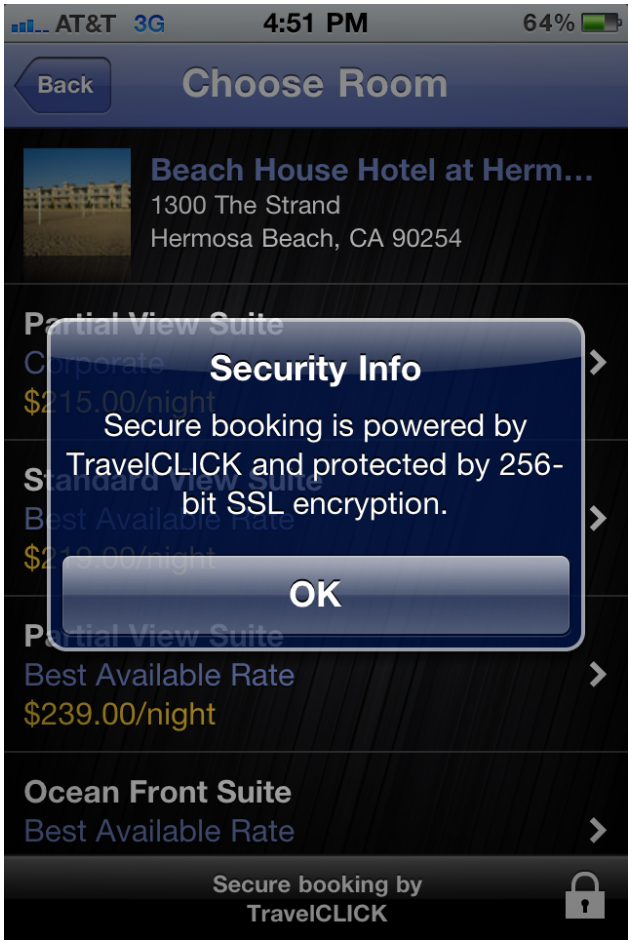
- **What tools exist to help w/ MITM Attacks?**
  - **thicknet** – MITM framework developed by Steve Ocepek (SpiderLabs)
  - **ettercap** – "is a suite for man in the middle attacks on LAN"
  - **arpspoof** – facilitates "arp poising"
  - **mitmproxy** – "is an SSL-capable, intercepting HTTP proxy"
  - **sslstrip** – relies on arpspoof then"strips" the SSL session to force Client to talk HTTP to attacker

Primer / History: SSL and MITM Attacks

- **Why is true SSL MITM difficult?**
  - SSL certificates have a **"chain of trust"**
  - Attacking public CAs not impossible, but **not practical**
  - Self-Signed Certs throw **Client errors**
  - Malformed Certs are **difficult to generate**

Mobile SSL User Experience

- **No Standard UI**
- **Most Cases -> No UI At ALL!**
- **Cryptic Warming Messages**
- **Users Don't Know the Difference**
- **Pop-up could be BS**



Trustwave SpiderLabs

Research Motivations

- The **Browser Community** spent almost **two decades tweaking the UI behavior** when it comes to SSL
- The **Mobile Device** market **destroyed** that in **less than five years**
- There are **no standards** that today's mobile users **expect to see** when their data is transmitted via SSL

Research Motivations

- Most apps **completely ignore** the UI aspect of security
- There is **zero functionality difference** between an app that sends data in the **clear vs. encrypted**
- App developers need to pay attention to this, but also **need tools to help them test SSL behavior** easily and consistently

Research Implications

- Attackers are focusing **more mobile app weaknesses**
- If a popular app mishandles SSL, their users are more susceptible to attacks
  - **Credential Stealing**
  - **Data Interception**
  - **Response Manipulation**
- These attacks will go unnoticed due to:
  - **Lack of User Awareness of the Risks**
  - **Lack of UI Cues within Apps**

Data Transmission Assault Course Components

- **How do you build a test lab?**
  - **Wireless Switch**
    - WRT-54GL running Tomato Firmware
  - **Attacker System**
    - Linux (must be connect via Ethernet to Switch)
      - ettercapNG-0.7.3 (w/ SpiderLabs patch)
  - **Victim Clients**
    - Android (Nexus S – v2.3.4)
    - iPod Touch 4th Gen (v4.3.3)

Data Transmission Assault Course Components

What types of SSL certs do you need?

1. **Valid for Target Domain (i.e. www.myapp.com)**

2. **Various Malformed SSL Certificates:**
   - Null Prefix (big news in 2010)
   - CRLF
   - Self-Signed
   - Signed by Parent Cert (set CA:FALSE)
   - Invalid ASN.1 Structures (Fuzzing)
   - Broken Encodings

3. **A Method to Generate the Above Easily…**

Introducing SSLizzard - About

- **SSLizzard** is an open source toolkit to easily generate multiple types of invalid SSL certs **for ANY given domain**.
- The output is then **used in various MITM frameworks** to perform the SSL attack
- Successfully tested with **ettercap** (see patch on DVD)
- A **thicknet** module is being developed by **Steve Ocepek**.
- Can be used **against any OS, Application or Browser**.

Introducing SSLizzard – Uses / Usage

- **Command Line**
  - ruby sslizzard.rb mydomain.com
- **Generates a key and a number of certificates with various invalid structures for testing.**
- **Output is written in the current working directory**

Introducing SSLizzard – Setup a Test

- Execute **SSLizzard** to **generate certs**
- Set up **ettercap** (patched) with **–x** flag to specify cert type you want to test
- Use your app as normal and see if you get error msgs
  - If you don't get errors, check ettercap to see if **data was intercepted**
- You will need to **execute** ettercap **once per cert type** generated by **SSLizzard** to comprehensively test

Introducing SSLizzard - Demo

- **Generating a collection of certs**
- **Using the certs in ettercap (SpiderLabs patch)**
- **Video of interception of traffic**
- **Video of victim devices throwing errors/not throwing errors**

Mobile App Test Results

TO BE RELEASED AT DEF CON 19

Conclusions

We need a world where:

- **Developers use SSL for all data transmission**
- **Consistent, simple, UI that users can understand**
- **Apps and Devices that fail closed when there is a secure transmission problem**

Trustwave's SpiderLabs®

SpiderLabs is an elite team of ethical hackers at Trustwave advancing the security capabilities of leading businesses and organizations throughout the world.

More Information:

Web: https://www.trustwave.com/spiderlabs

Blog: http://blog.spiderlabs.com

Twitter: @SpiderLabs

Trustwave®

SpiderLabs®

Questions?