WEARABLE SECURITY

MARKUS JAKOBSSON
MAJAKOBSSON@PAYPAL.COM
MARKUS@FATSKUNK.COM
TAKE POWER...
... BEHAVIOR
... USER INTERFACES
... AND PATCHES
WEARABLE TAKES IT A STEP FURTHER
HOW DOES **THAT** MAKE ME FEEL?
USE EXAMPLE: GOOGLE GLASS
Not a lot
* ok glass *
EXAMPLE: PIN INPUT

INSTRUCTIONS: CHANGE PIN TO YOURS!
* ok glass *
EXAMPLE: PIN INPUT
EXAMPLE: PIN INPUT
EXAMPLE: PIN INPUT
EXAMPLE: PIN INPUT
EXAMPLE: PIN INPUT
EXAMPLE: PIN INPUT
EXAMPLE: PIN INPUT
EXAMPLE: PIN INPUT
EXAMPLE: PIN INPUT
EXAMPLE: PIN INPUT
EXAMPLE: PIN INPUT

1234
Welcome back
EXAMPLE: SPAM FILTERING

Your email won $1 Million in Microsoft lottery
My name is Dr. Yousef, I have big news for you. Wealthy widow, wants to invest in your country. Check V1AGRA. Your email won $1 Million in Microsoft lottery. Will pay extra to ship to son in Africa? Can you ship to son in Africa? I will pay extra.
My name is Dr. Yousef, I have big news for you. Wealthy widow wants to invest in your country. Your email won $1 Million in Microsoft lottery. Will pay extra. Can you ship to son in Africa? Cheap V1AGRA.
ADVERSARY

1. DATA MINING SPAMMER
2. END USER
EXAMPLE: SPAM FILTERING

Wealthy widow, wants to invest $ in your country
EXAMPLE: SPAM FILTERING

Wealthy widow, wants to invest $ in your country

(widow, invest, $, your country)
Wealthy widow, wants to invest $ in your country

EQUIV: ($, USD, US$, Pounds, Euro)
Wealthy widow, wants to invest $\text{in your country.}$ Please!
EXAMPLE: SPAM FILTERING

- Fraud schemes have pitches (= story lines)
- Represent each pitch as one or more rules, using normalization & equivalence classes.

Build rules using combinations of cues:

**Stranger**: “my name”, “I am”, “know me”

**Money**: “USD”, “huge sum”, “,000,”

**Lottery**: “email has won”, “drawing”, “lottery”
EXAMPLE: JAILBREAKING
EXAMPLE: JAILBREAKING

Who is attacking whom?
And how?
And why?
WHOM, HOW AND WHY?

Rootkits

Jailbreaks

Trojans
Whom = user

Rootkits

Whom = service provider

Jailbreaks

Trojans
Rootkits

Jailbreaks

Trojans

How = privilege escalation

How = user actions; social engineering, marketplace.
Rootkits

Jailbreaks

Trojans

Why = money, espionage

Why = control, piracy

Why = snooping (contacts, location).
Worst case: sniff SMS
JBAILBREAKING: THE NEGLECTED CHILD

(Because we are so used to thinking of content providers as the enemy?)
MALWARE DEFENSES

- Harden the device
  - Data Execution Prevention
  - Address Space Layout Randomization
  - Code Signing, Code Obfuscation
- Filter in the marketplace
  - Code Analysis, Forbidden API calls, Reputation
- Filter during runtime
  - On Device: Signatures, Behavioral
  - On Backend: Signatures, Velocity, C&C detection
- Patch
- Audit before sensitive events
  - Software Based Attestation
JAILBREAK DEFENSES

• Harden the device
  • Data Execution Prevention
    Address Space Layout Randomization
    Code Signing, Code Obfuscation
• Filter in the marketplace
  • Code Analysis, Forbidden API calls, Reputation
• Filter during runtime
  • On Device: Signatures, Behavioral
    On Backend: Signatures, Velocity, C&C detection
• Patch
• Audit before sensitive events
  • Software Based Attestation
- Harden the device
  - Data Execution Prevention
  - Address Space Layout Randomization
  - Code Signing, Code Obfuscation
- Filter in the marketplace
  - Code Analysis, Forbidden API calls, Reputation
- Filter during runtime
  - On Device: Signatures, Behavioral
  - On Backend: Signatures, Velocity, C&C detection
- Patch
- Audit before sensitive events
  - Software Based Attestation
MADE

JAILBREAK DEFENSES

• Harden the device
• Data Execution Prevention
  Address Space Layout Randomization
  Code Signing, Code Obfuscation

• Filter in the marketplace
  Code Analysis, Forbidden API calls, Reputation

• Filter during runtime
  On Device: Signatures, Behavioral
  On Backend: Signatures, Velocity, C&C detection

• Patch

• Audit before sensitive events
  Software Based Attestation
Jailbreak Defenses

- Harden the device
  - Data Execution Prevention
  - Address Space Layout Randomization
  - Code Signing, Code Obfuscation
- Filter in the marketplace
  - Code Analysis, Forbidden API calls, Reputation
- Filter during runtime
  - On Device: Signatures, Behavioral
  - On Backend: Signatures, Velocity, C&C detection
- Patch
- Audit before sensitive events

Software Based Attestation

Malware Defenses

- Only hampers development –
- Not in marketplace –
- Has root, no propagation, no C&C –
JAILBREAK DEFENSES

- Harden the device
- Data Execution Prevention
- Address Space Layout Randomization
- Code Signing, Code Obfuscation
- Filter in the marketplace
- Code Analysis, Forbidden API calls, Reputation
- Filter during runtime
- On Device: Signatures, Behavioral
- On Backend: Signatures, Velocity, C&C detection
- Patch
- Audit before sensitive events

Software Based Attestation

- ONLY HAMPERS DEVELOPMENT –
- NOT IN MARKETPLACE –
- HAS ROOT, NO PROPAGATION, NO C&C –
- VOLUNTARY –
DEVICE ID

- HTML Cookies
- Flash Cookies
- User Agent
DEVICE ID

HTML Cookies
Flash Cookies
User Agent
DEVICE ID

HTML Cookies
Flash Cookies
User Agent
DEVICE ID

- HTML Cookies
- Flash Cookies
- User-Agent
DEVICE ID: 301 COOKIES

visible page ➔ Same-name
DEVICE ID: 301 COOKIES

visible page ➔ Same-name ➔ unique-name

301 moved permanently
DEVICE ID: 301 COOKIES

visible page
DEVICE ID: 301 COOKIES

visible page -> Same-name

I want Unique-name
WEARABLE SECURITY