Mobile Application Security

Promises and Pitfalls in the New Computing Model

Alex Stamos
Partner

iSEC PARTNERS

https://www.isecpartners.com

Agenda

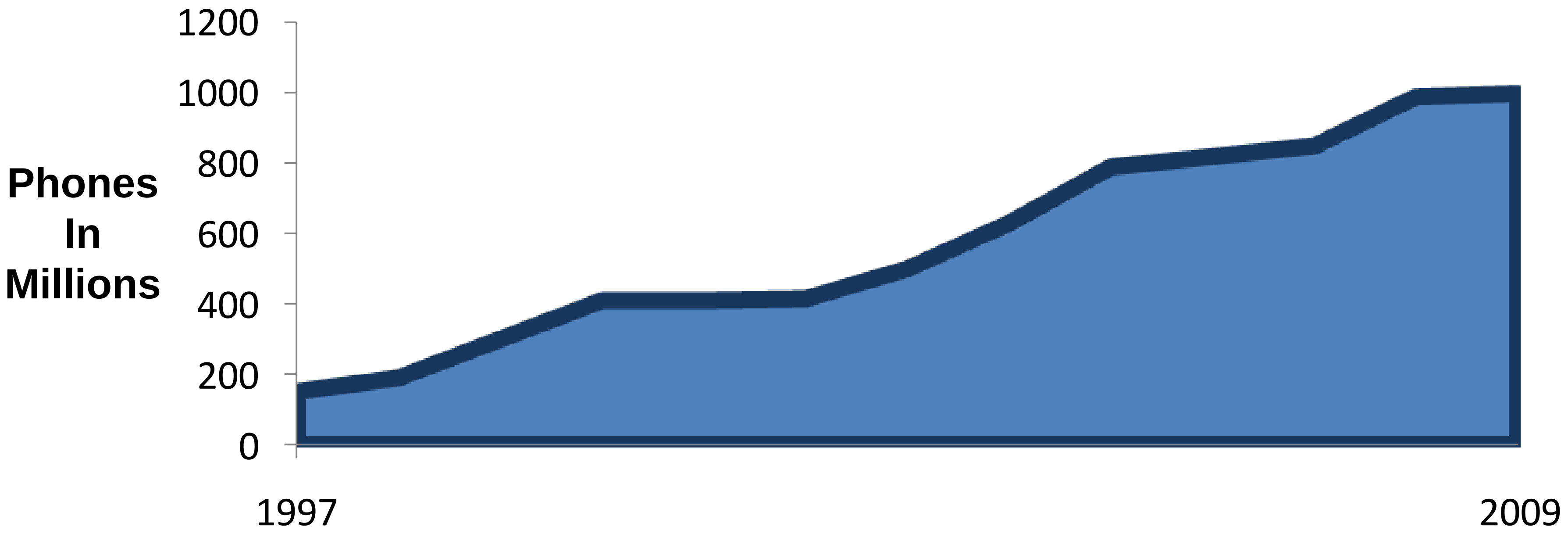
- Mobile Computing Today
- Security Challenges
- Supporting Security
- Mobile Web Security
- Actions

Mobile Computing Today

Trends

Attack Surfaces

Mobile Phone Sales Per Year



Data from Tomi Ahonen Almanac 2009

Wi Fi™

EDGE/ 3G

CUSTOM APPS

Bluetooth®

DESKTOP SYNCH

FLASH MEMORY

AT&T 3G
9:42 AM
SMS
Text
Tuesday 9
Calendar
Photos
Camera
YouTube
Stocks
280
Maps
73°
Weather
Clock
Calculator
Notes
Settings
iTunes
App Store
Phone
Mail
Safari
iPod
$
%
}
?

Major Smartphone Platforms

- Symbian
- Windows Mobile
- iPhone
- RIM (Blackberry)
- Android
- Palm Pre?

NOKIA
Eee PC
The New York Times
LATEST NEWS
amazonkindle

Trend Catalysts

- Sexier Devices
- Younger Generation
- F500 Acceptance
- Multi-Environment Phones

- Unlimited Data Plans
- Provider App Stores

Security Challenges

Defining Security

Challenges

Defining the Customer

What is Security?

- Not the PC or Server Model
  - Single User
  - High-Value Information
  - Low-Value Applications
- Availability and Power
- Local Attacker Resistance

The Airline Pocket

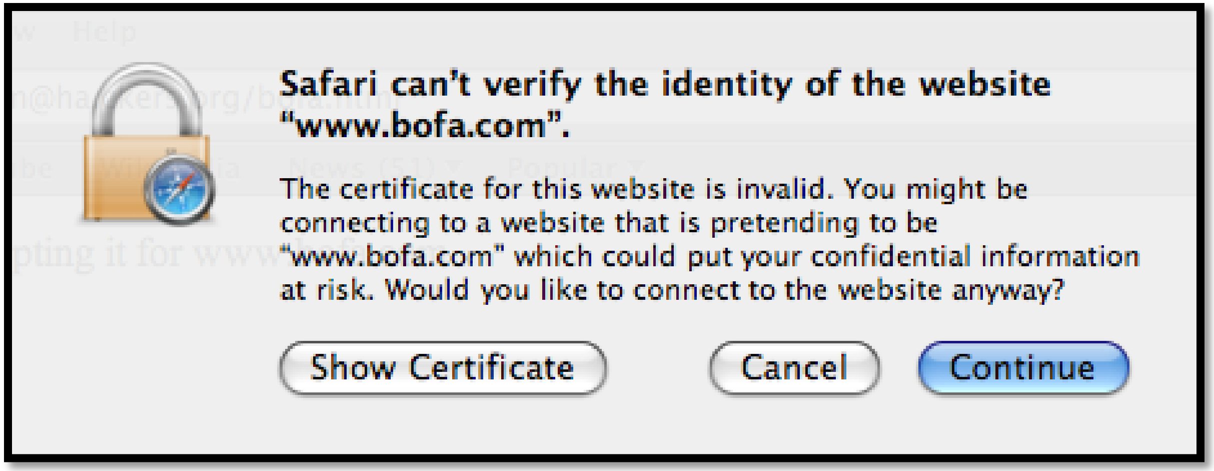
- Physical Security Just Doesn’t Exist
- Phones will Be Lost
- Need Ways of Protecting Data
  - Local encryption
  - Cloud storage

Hardware Limitations

- Limited Bandwidth
- Power
- CPU
- Size

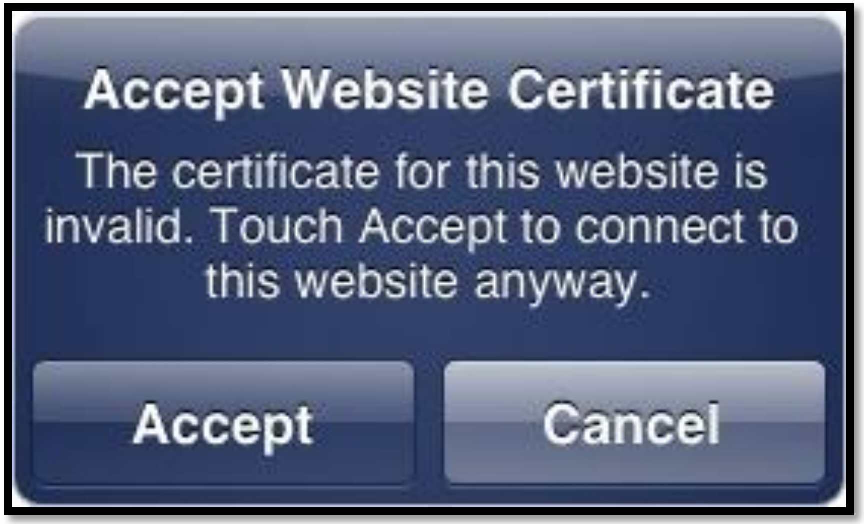
Technology Will Solve These

Screen Size



Safari can't verify the identity of the website "www.bofa.com".

The certificate for this website is invalid. You might be connecting to a website that is pretending to be "www.bofa.com" which could put your confidential information at risk. Would you like to connect to the website anyway?



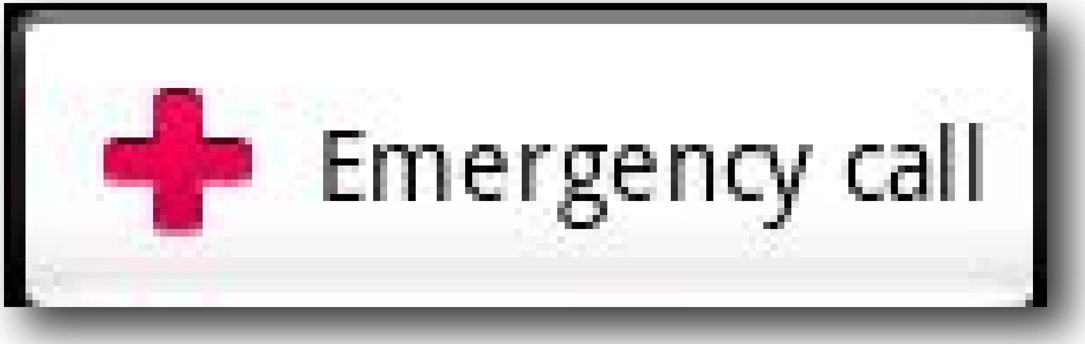
Accept Website Certificate

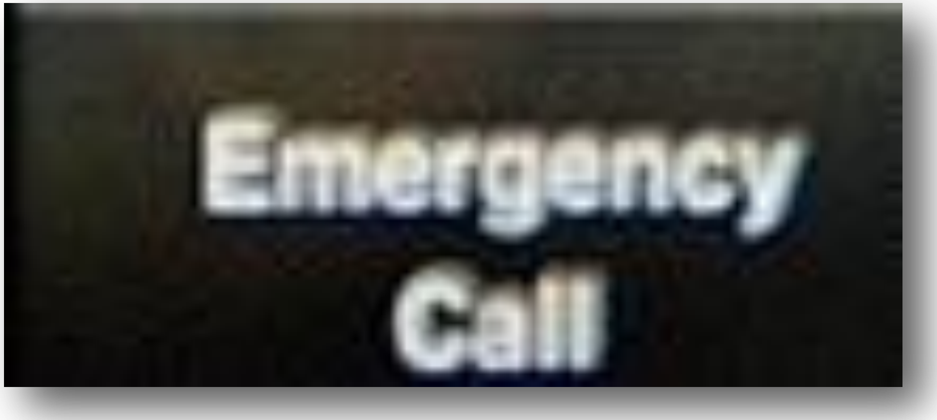
The certificate for this website is invalid. Touch Accept to connect to this website anyway.

Poor Keyboards

C)sOz*ao1pdn

Regulations





User Identification

- Real Time
- Must be Available Immediately
- One Handed Interface
- More Prompts than PC

“Ownership”

- OS Vendor
- Carrier

- User
- Application Developer

All “Own” the Phone and Have Differing Objectives

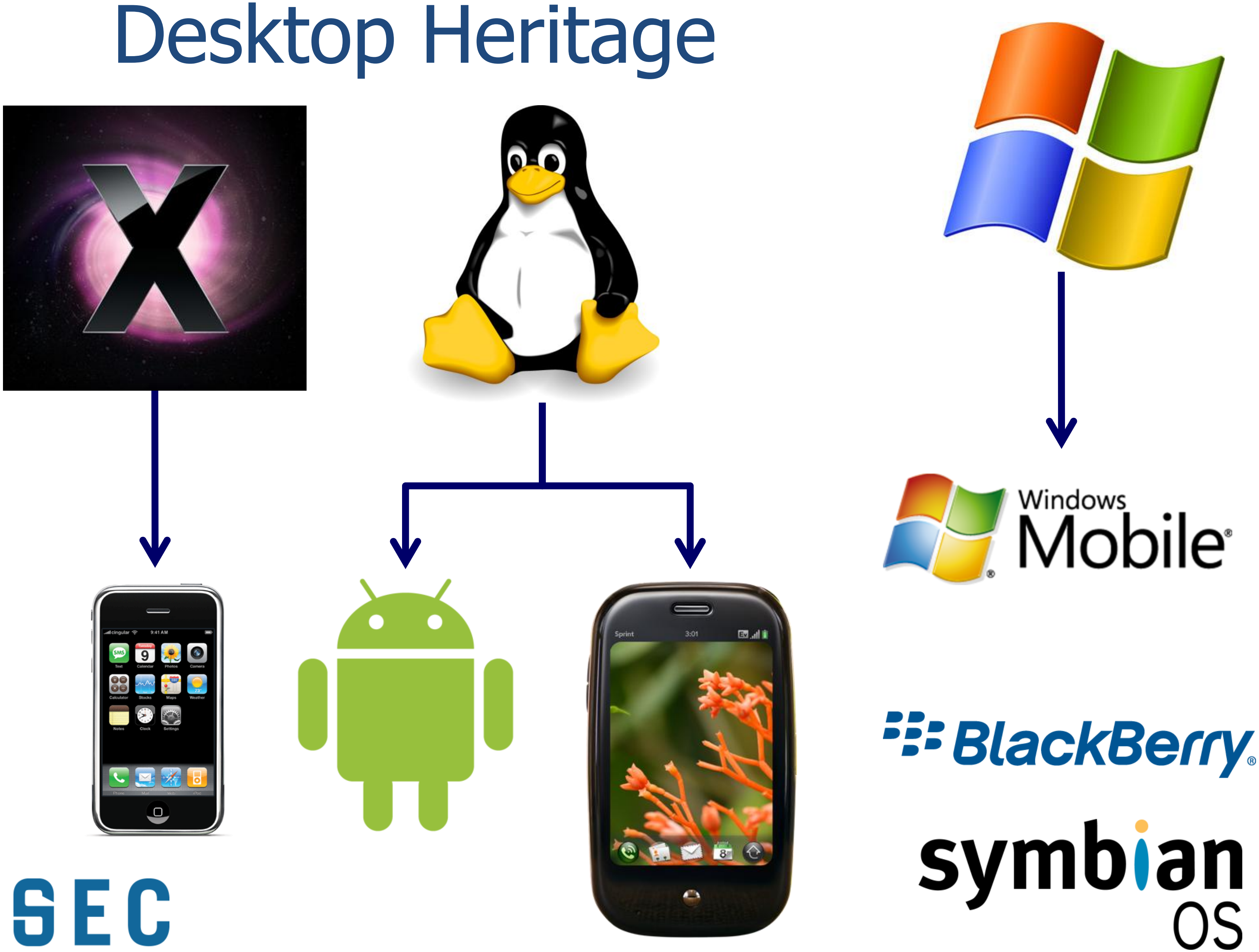
Distribution Challenges

- Indirect Customer Relationship
- Patching Difficulties
  - Carriers are anti-patch
- Long Update Lag
- Multiple Hardware Platforms

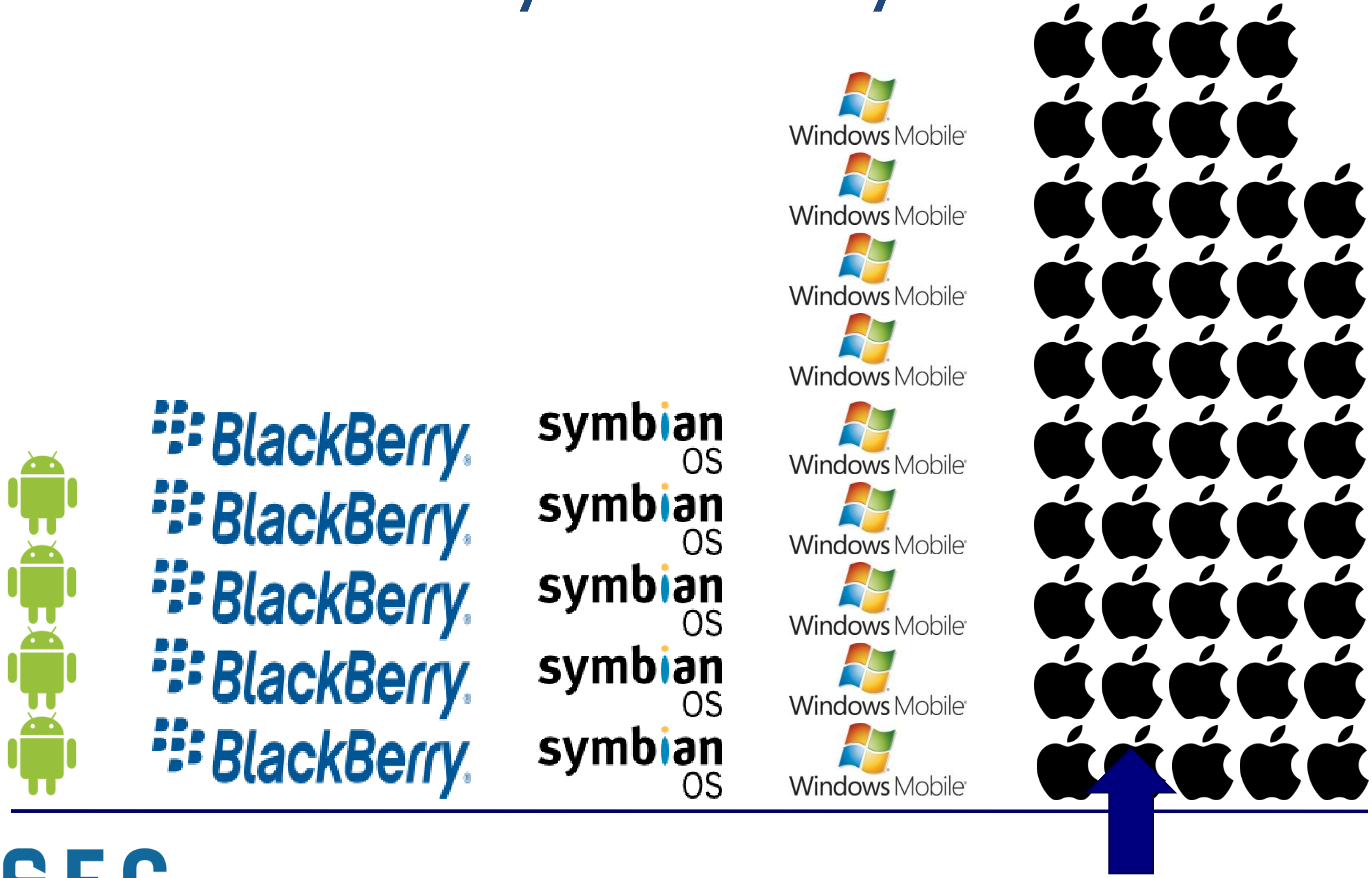
Unsafe Languages

- Windows Mobile (C/C++)
  - .Net Mobile Framework (safe)
  - /GS, SafeCRT
- iPhone (Objective-C)
  - Has C Constructs
  - NX Stack/Heap
- Symbian (Symbian C++)
  - C++ with more Complex Memory Management

Desktop Heritage



Vulnerability Count by Platform



Need to add 46 more

Growing Security Activity

- Targeted by Security Community
- CanSecWest
- Asian & European Research
- Commercial Spy Products

Supporting Security

Security Goals

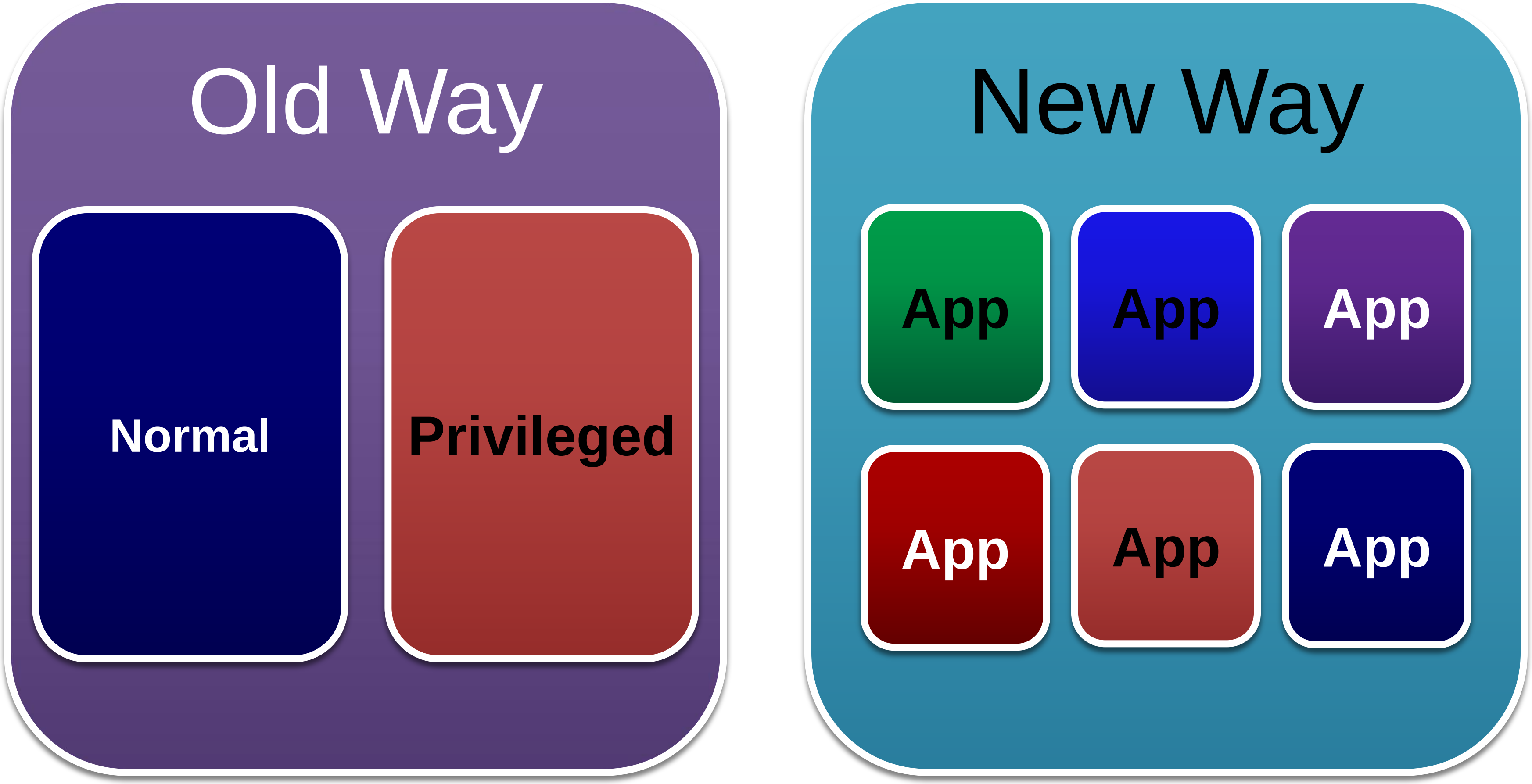
Shift in Computing Models

Platform Comparison

Security Goals

- Users can Safely Run Applications
- OS Protected from Applications
  - A.K.A. Steal Carrier Revenue
- Per-Application Private Data
- Contain Vulnerabilities

Two Models



Old Way

Normal

Privileged

New Way

App

App

App

App

App

App

Old Way

- Windows Mobile
- All or Nothing
- Signatures Defines Permission Level
- No or Limited File Permission Systems
- No “users”
    - Good, because it doesn’t make sense

Pros/Cons

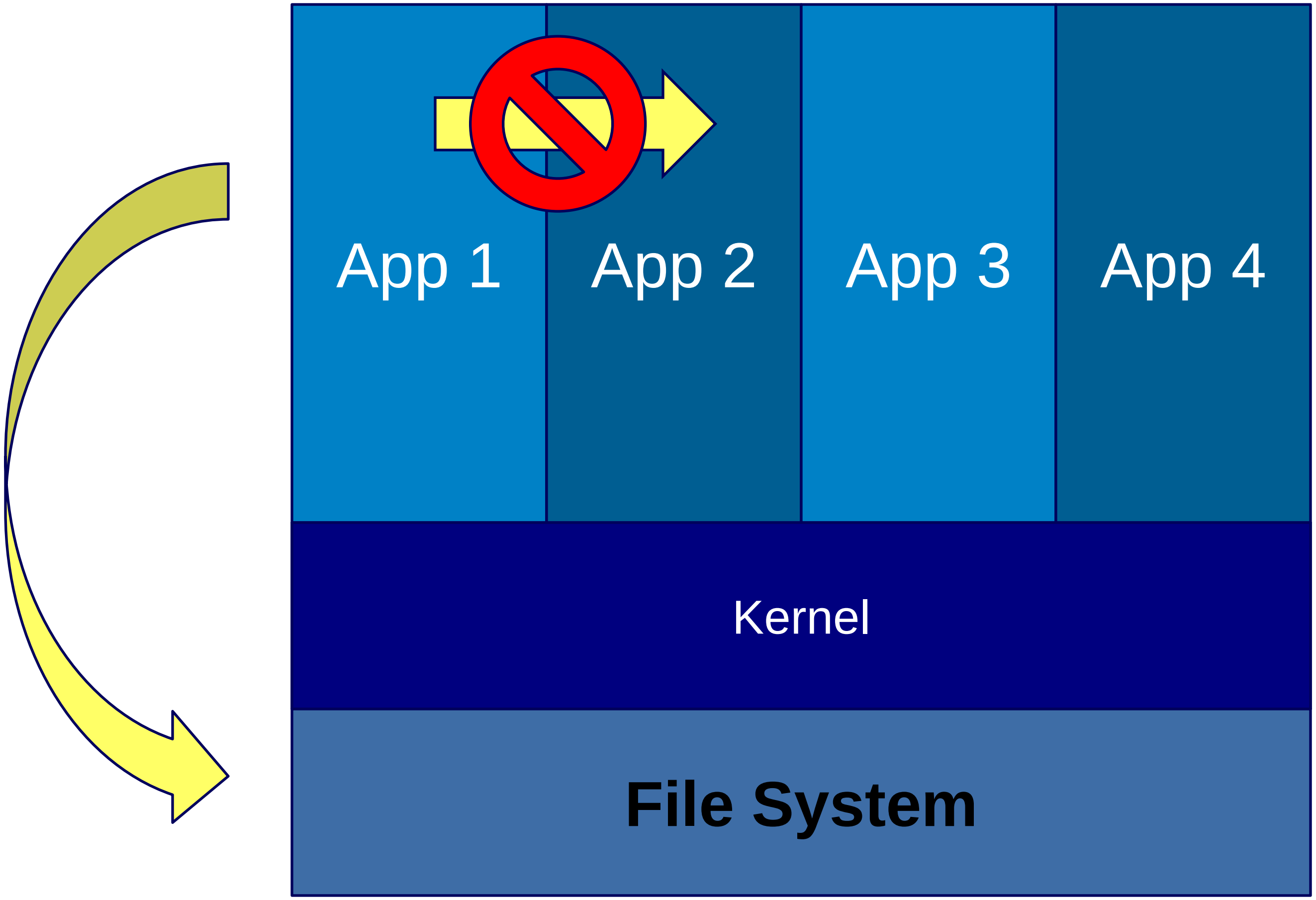
Pros

- Easy to Understand
- Easy to Test

Cons

- No Exploit Containment
- User can’t Make Granular Choices

Windows Mobile



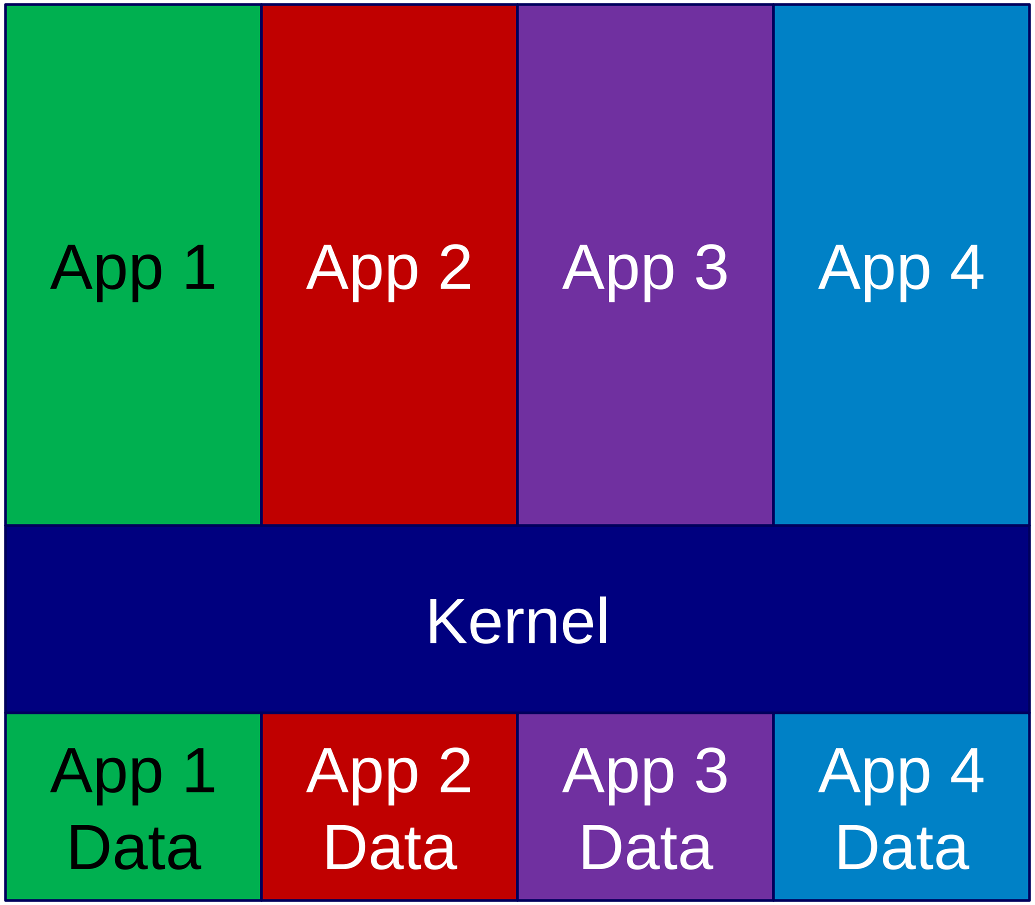
Blackberry

- J2ME Based
  - MIDP 2.0 with modifications
  - Class based security
- No Raw Device Access
- Web Services and Web Based Models

Security Opportunities

- More Granular Permissions
- Sandboxed Applications
- Reduced Attack Surface
- Give Users Control of Data

iPhone



App 1

App 2

App 3

App 4

Kernel

App 1 Data

App 2 Data

App 3 Data

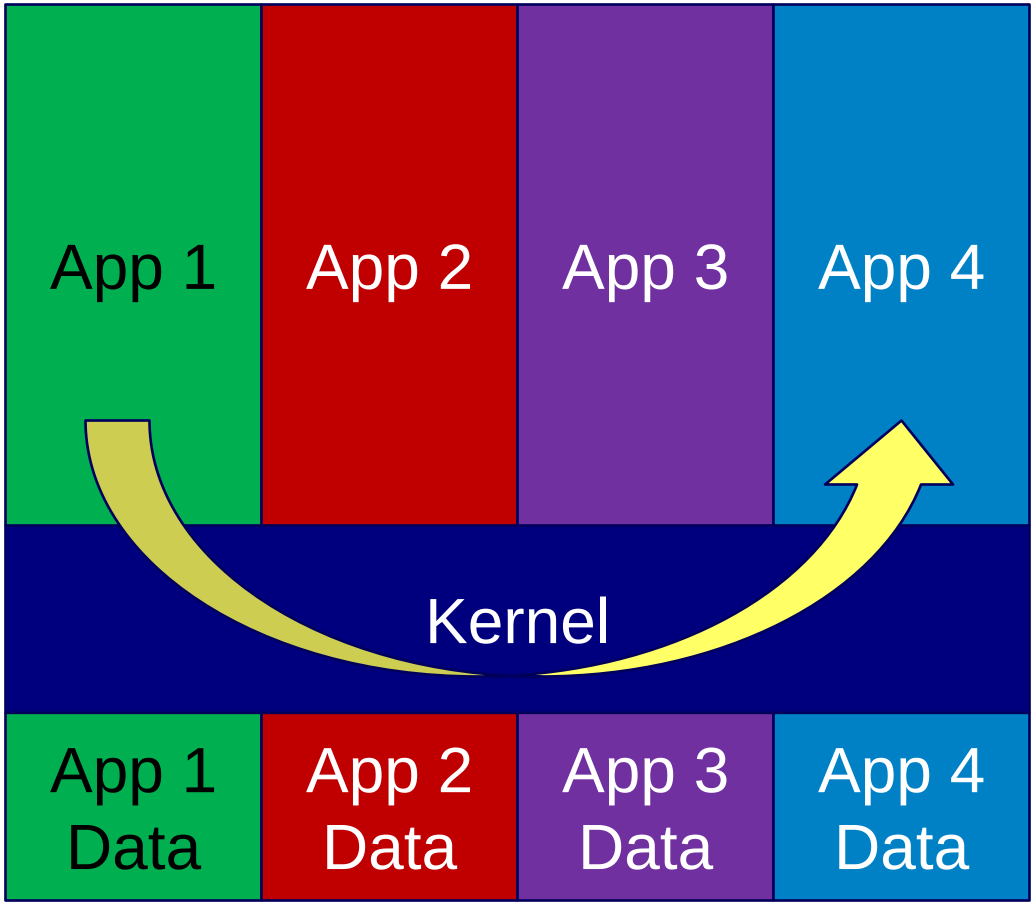
App 4 Data

iPhone

- One Distribution Method
- Strict AppStore Policy
- Non-Technological Policy Enforcement

Application Store is a Security Barrier

Android & Symbian

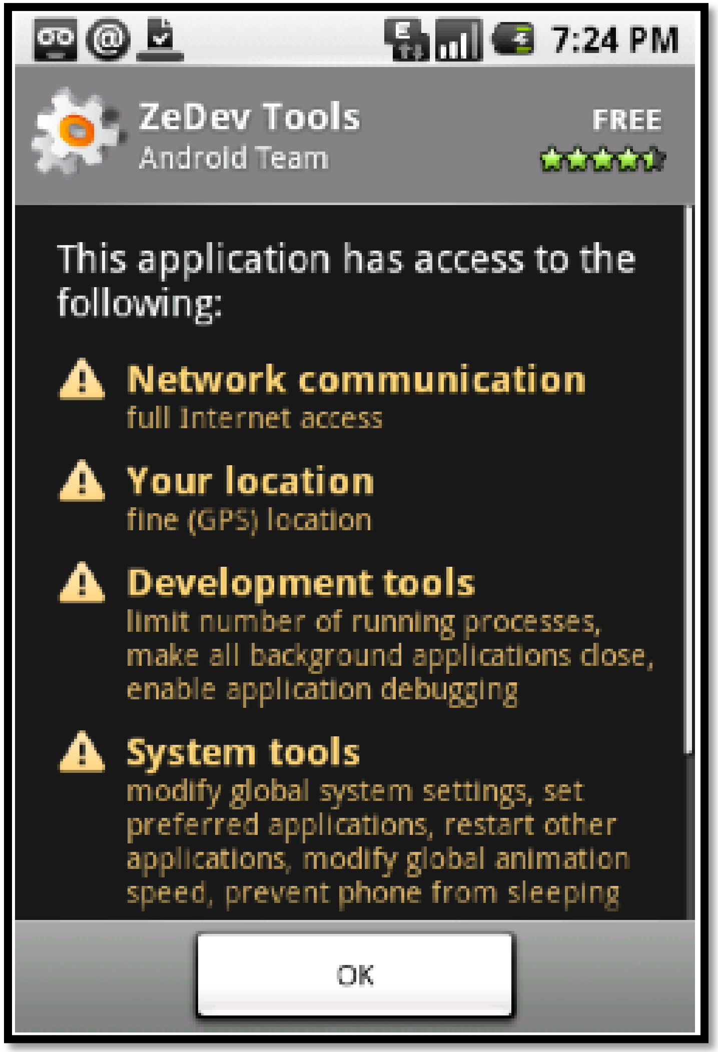


iSEC PARTNERS

Benefits

- Extensible to Custom Data Types
- Users Have Control
- Same-Developer Sandbox
  - An Office Suite is Possible
  - Attack Surface Increased

Challenges



ZeDev Tools
Android Team

FREE

This application has access to the following:

⚠ **Network communication**
full Internet access

⚠ **Your location**
fine (GPS) location

⚠ **Development tools**
limit number of running processes, make all background applications close, enable application debugging

⚠ **System tools**
modify global system settings, set preferred applications, restart other applications, modify global animation speed, prevent phone from sleeping

Android Market

- Self-Signed Certificates
- Community Reputation
- No Unsigned Code Allowed

Application Store is a Minor Security Barrier

Technical Comparison

Feature	**Blackberry**	**WinMo 6.x**	**iPhone 2.2.1**	**Android**
Enterprise Mail and Calendar	🟩	🟩	🟩	🟥
Remote Wipe	🟩	🟨	🟨	🟥
Side-Load Applications	🟨	🟨	🟥	🟩
Application Sandbox	🟩	🟥	🟨	🟩
User permission UI	🟩	🟩	🟥	🟩
App Signing	🟩	🟩	🟩	🟩
Browser	🟨	🟩	🟩	🟩

Technical Comparison

Feature	**Blackberry**	**WinMo 6**	**iPhone 2.2.1**	**Android**
Application Language	🟩	🟨	🟨	🟩
Permission Model	🟥	🟥	🟨	🟩
App Buffer Overflows	🟩	🟨	🟥	🟩
OS Buffer Overflow Protections	🟩	🟩	🟩	🟩
Signature Required?	🟥	🟥	🟩	🟩

Securing the Mobile Web

Mobile Web Browsers

Mobile Portal Mistakes

Choosing Thick or Thin

Mobile Web Browsers

Mobile browsers are pulled in two ways:

- Simple
  - Speed over low-bandwidth
  - Rendering on small screens
  - Better user experience without scrolling
  - BB Browser, Feature Phones,

- Compatible
  - Renders like desktop
  - AJAX support (JS and XHR)
  - Plugins?
  - Mobile Safari, Android, Opera Mini

Mobile Web Browsers

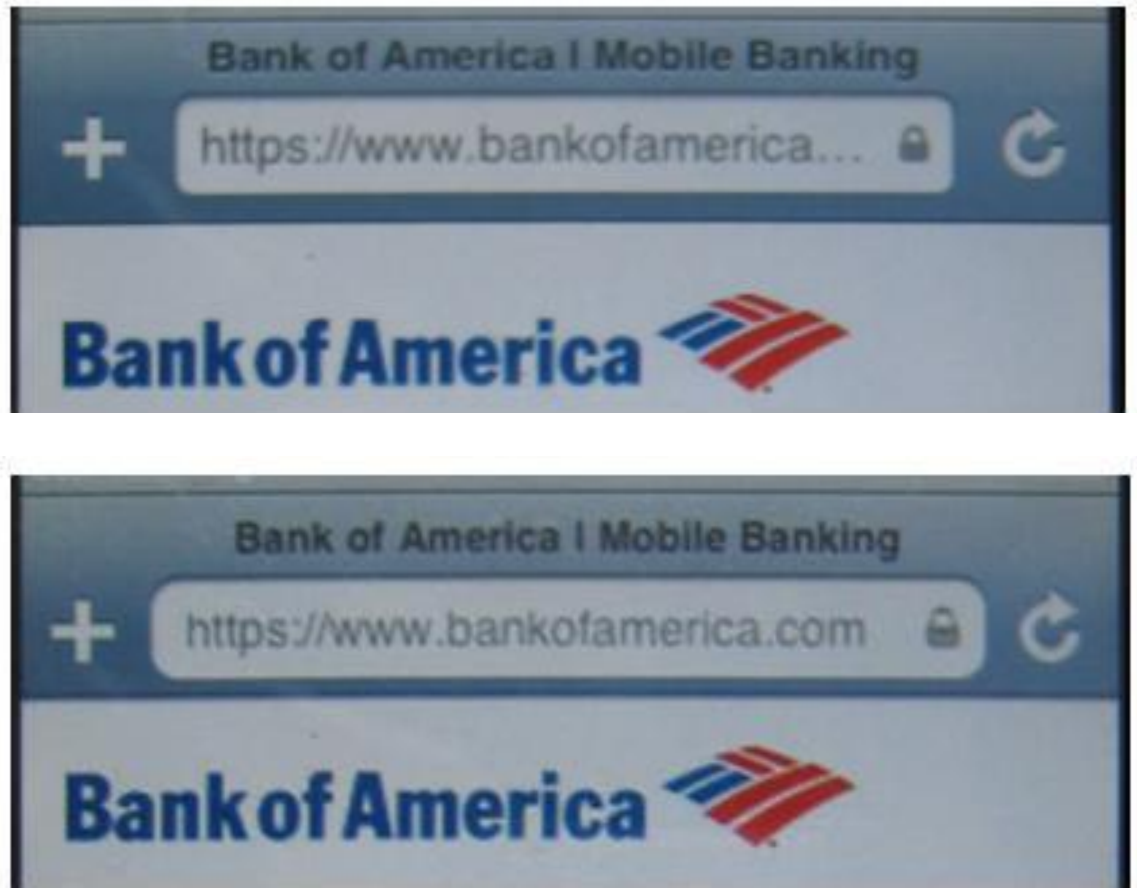
- Simple
  - Pros
    - Less attack surface
    - No JS
  - Cons
    - Proxied TLS, W-TLS
    - Bad Security UX

Mobile Web Browsers

- Compatible
  - Pros
    - More professional security work
    - Real TLS
  - Cons
    - Full browser bugs might port
    - Much more complex
    - Too much WebKit
    - Still bad security UX

Mobile Web Browsers

- Common problem: bad security UX



Bank of America | Mobile Banking

https://www.bankofamerica...

Bank of America

Bank of America | Mobile Banking

https://www.bankofamerica.com

Bank of America

iPhish. Yuan Niu, Francis Hsu, and Hao Chen @ UC Davis

Mobile Portals

- Multiple Internet Presences
- Both are on the Internet
  - Generally both will “accept” connections from both types of browsers
  - We generally pen-test mobile sites from desktops
- Common Real World Result:
  - Primary website highly secured
  - Mobile site unprotected

Common Mobile Portal Mistakes

- Using a different SLD
  - Bank.mobilecorp.com
  - Mobilecorp.com/bank

- Massively sets back fight against phishing

- Users need to be taught to:
  - Only go to your SLD
  - Use HTTPS
  - Not click on email links

- Use one standard for the Enterprise
  - I like m.*

Common Web Portal Mistakes

- Poor Crypto Practices
  - You do not want to allow for proxied TLS
  - W-TLS, old phones, Opera Mini
  - Need to blacklist old browsers by User-Agent

- Do not mix HTTP/HTTPS
  - Mobile phones are always on insecure networks
  - Even desktop browsers handle this poorly

Mobile Web - Authentication

- Most mobile sites use www creds

- Bad idea
  - Users downgrade their credentials
  - Mobile phishing is still easier
  - Eliminates ability for per-browser auth

- One option:
  - Shorter “mobile PIN” for m.*
  - Limited functionality with this PIN

Mobile Web - Authentication

- Mobile sites destroy best anti-fraud weapon, user analytics

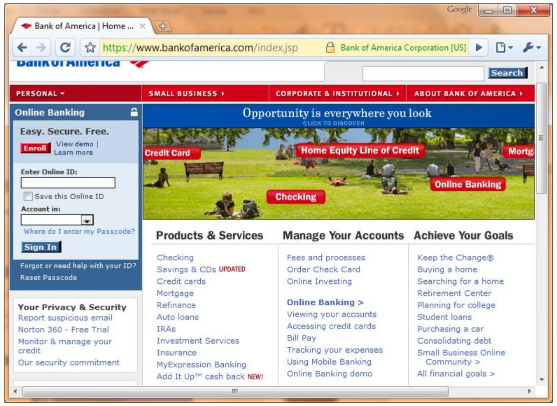
- For example, the iPhone:
    - Roaming AT&T IP
    - Same User-Agent
    - Much more difficult geo-location

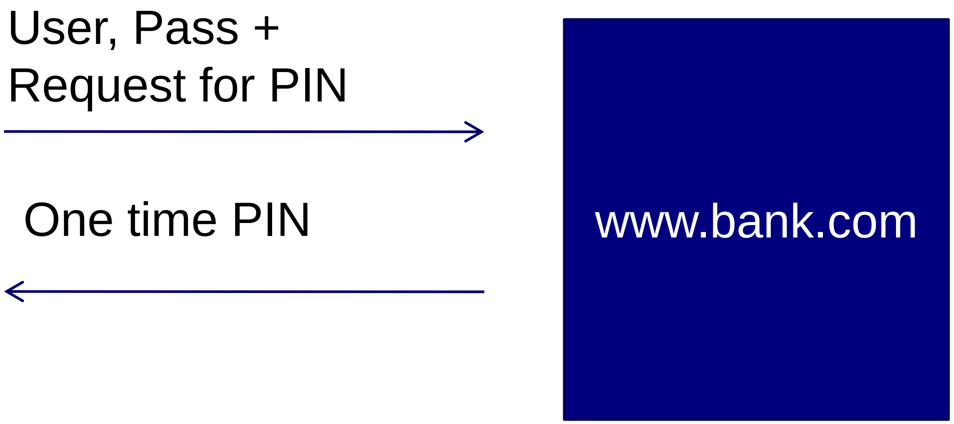
- Many browsers don't support persistent cookies

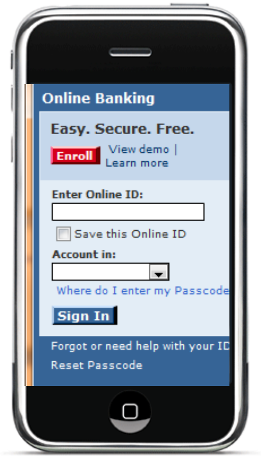
- No flash cookies

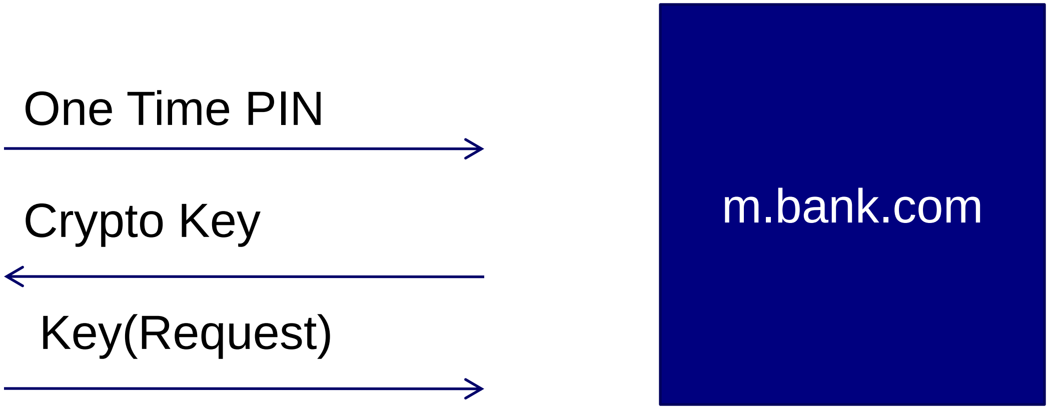
Authentication

- This problem is much easier with a thick app:









iSEC PARTNERS

Choices

- So should I build a thick app? Big question these days…

- From a security perspective, thick apps help with:
  - Authentication
  - Fraud analytics
  - Crypto

- Thick client apps can introduce flaws, so you need to be mindful
  - Still, the sandbox on phones is better
  - Most phones have anti-overflow technologies

Actions

For Enterprises

- Define a Mobile Application Security Policy
- Set User Application Security Policy
  - Are App Stores Allowed?
- Build Secure Line of Business Applications
- Create a Unified Model for Mobile Interactions
  - Don’t mix “m.” with /mobile or .mobi domains
- Be firm on enforcing access to your network from random devices

For Developers

- Define Security Assertions for Users
- Define Threats
    - Lost Phone
    - Network Attacks
- Create Limits
    - E.g. Read-only Mobile Endpoints
- Apply Secure Development Guidelines
- Test on Real Devices

For Mobile Web Developers

- Disallow Older Browsers
- Do Not Decrease Overall Security
  - Tightly-Scope Functionality
  - Use SSL and Proper Domains
- Strong Authentication
  - Unique Authentication for Mobile Sites
- Don’t Make Phishing Easier
  - Keep Links out of Email
  - Maintain Clear Message

Questions?

alex@isecpartners.com