

Mobile Web Security

A Moving Target

Alex Stamos and Chris Clark

iSEC Partners



Agenda

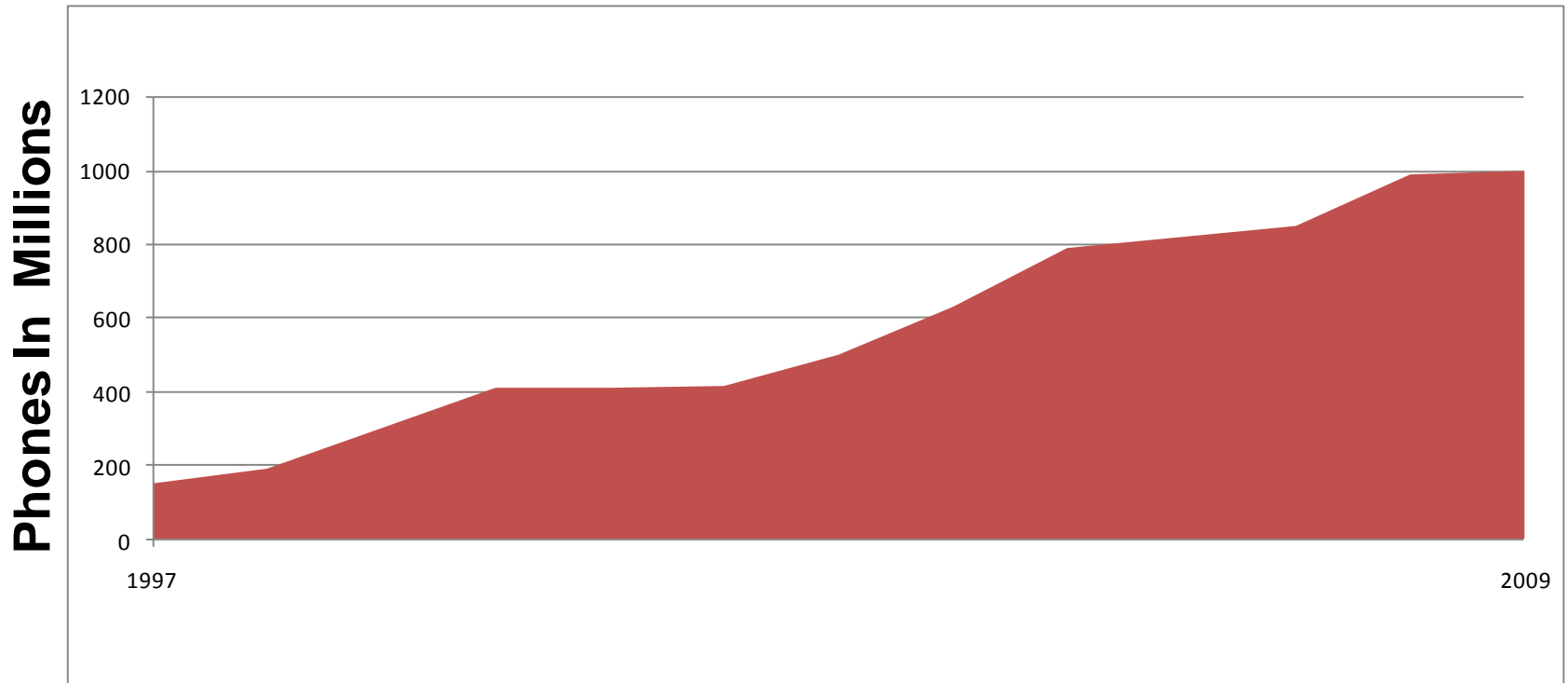
- The Mobile Revolution
- Security Challenges
- Securing the Mobile Web
- To Dos

Special Thanks

- Chris Clark
 - Will be speaking to more technical depth at RSA this year
 - Focus on thick client apps and OS security
- Rich Cannings
 - Android Security Manager
- Entire Android Team

The Mobile Revolution

Mobile Phone Ownership



From Gartner

Modern Smartphones

- Phone/E-Mail/Texting
- Rich Web Browsing
- Media Player
- Flash Memory
- Office Suite Support
- **Custom Applications**
- Wi-Fi
- Edge/3G Data
- Bluetooth
- GPS
- Desktop Synchron

Major Smartphone Platforms

- Symbian
- Windows Mobile
- iPhone
- RIM (Blackberry)
- Android

- Palm coming back?

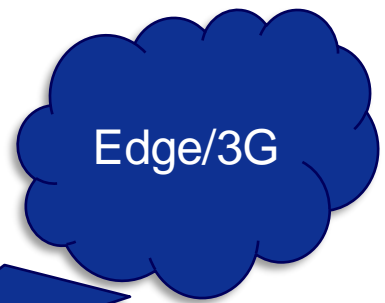
The Business Trend

- What used to be a solid two markets...



- Is getting all complicated





Flash Memory



Desktop Sync

Mobile Applications

- 20,000+ iPhone Apps (and Counting)
- 18,000 Windows Mobile Apps
- 10,000 Symbian Apps
- 2,300+ Android Apps
- ??? Blackberry Apps
- MANY Web Applications Optimized for Mobile

These Trends Will Continue

- Sexier Devices
- Younger Generation
- F500 Acceptance
- Multi-Environment Phones
- Unlimited Data Plans
- Every Provider Pushing an App Store

Security Challenges

What is security?

- Not the PC or server model
 - Single User
 - High-Value Info
 - Low-Value Apps
 - Availability and power are key
- Availability robustness against local attackers is ignore in most desktop and server OSes

Who is mobile security serving?

- User
 - Privacy of personal information
 - Availability of service
 - Pay services
- Carrier
 - Control over competing apps (Skype)
 - Reduce traffic impact, support costs
- Application Developer
 - DRM
 - Protection from other apps

Security Decisions

- The result of the competing needs...
 - Wildly different control points
 - Varying levels of user control
 - Much more complicated idea of “secure”
- At least Linux, OS X, and Windows have the same idea of security

The Airline Pocket

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

Hardware Limitations

- Screen Size
- Poor Keyboards
- Limited Bandwidth
- CPU
- OS Capabilities

* CPU and OS are less of an issue today

Regulations



User Identification

- Must be Available Immediately
- One Handed Interface
- Many more prompts on a daily basis than a PC
- Not easy to extend with biometrics

Software Distribution & Updating

- Desktop Installation
- Flash Memory or Browser Sideload
- AppStore Purchase
 - Fascist policies might help security
 - Again, who is security serving?

Patch Distribution Challenges

- Indirect Customer Relationship
- Patching is hard
 - Carriers are anti-patch
 - FCC might be anti-patch
- Long Update Lag
 - Have to assume some users on 1.0 forever
- Some OSes support many platforms
 - Drivers/HAL not in control of OS company
 - Building patches for many devices

Unsafe Languages

- Windows Mobile (C/C++)
- iPhone (Objective-C)
 - Has C Constructs, overflows
- Symbian (Symbian C++)
 - C++ with more Complex Memory Management

Desktop Heritage



















































- Android, Palm Pre, and iPhone are based on desktop architectures
- Vulnerabilities found in the desktop OS are likely to appear in the mobile versions
- May not be as exploitable
 - Other protections could have an impact
- E.g. First iPhone Vuln found by fuzzing Safari

Vulnerabilities



BlackBerry
BlackBerry
BlackBerry
BlackBerry
BlackBerry

symbian OS
symbian OS
symbian OS
symbian OS
symbian OS

	Windows Mobile				
	Windows Mobile				
	Windows Mobile				
	Windows Mobile				
	Windows Mobile				
	Windows Mobile				
	Windows Mobile				
	Windows Mobile				
	Windows Mobile				
	Windows Mobile				

More to Come

- Targeted by Security Community
- CanSecWest
 - Although Pwn2Own was a washout. Why?
- Asian & European Research
- Commercial Spy Products

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

Mobile Web Browsers

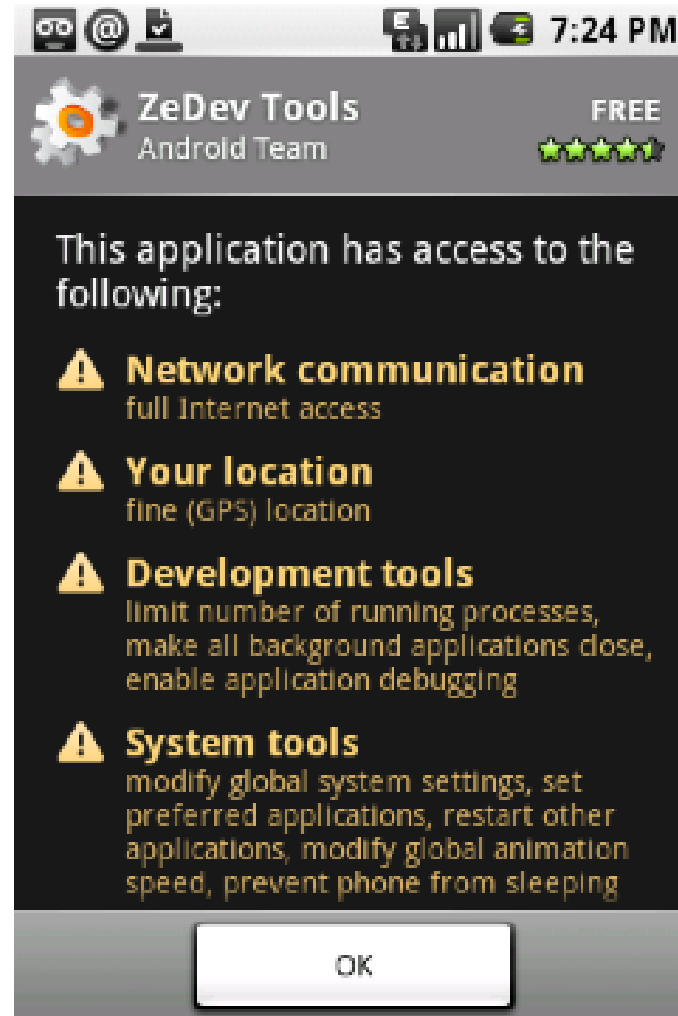
- Common problem: bad security UX



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

Mobile Web Browsers

- It's difficult to communicate complicated security ideas



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

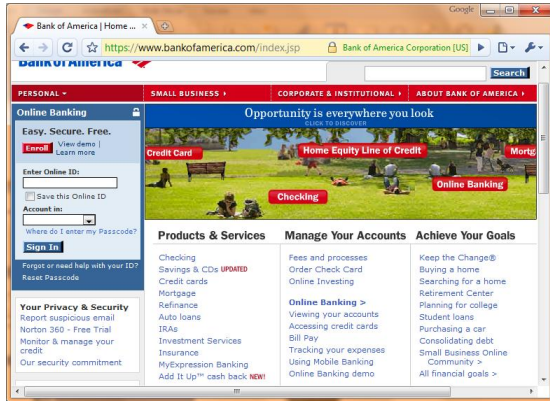
- Most mobile sites use www. creds
- Bad idea
 - Users downgrade their credentials
 - Mobile phishing is still easier
 - Eliminates ability for per-browser auth
- One option:
 - Shorter “mobile PIN” for m.*
 - Limited functionality with this PIN

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:



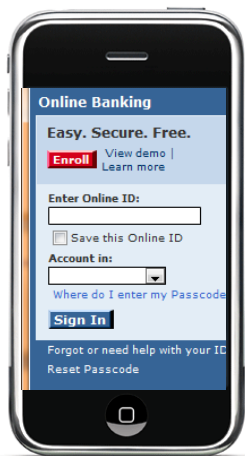
User, Pass +
Request for PIN



One time PIN



www.bank.com



One Time PIN



Crypto Key



Key(Request)



m.bank.com

Choices

- So should I build a thick app? Big question this week...
- From a security perspective, thick apps help with:
 - Authentication
 - Fraud analytics
 - Should be infrequent re-installs
 - Crypto
 - You control it
 - No reliance on ancient browsers
- 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

ToDos

For Enterprise

For Developers

For Web Developers

For Enterprises

- Define a Mobile Application Security Policy
- Set Application Security Policy for Users
 - Are App Stores Allowed?
- Build Secure Line of Business Applications
- Create a unified model for mobile interaction with customers
 - Don't mix m. with /mobile or different domains

For Developers

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

For Web Developers

- Try to build web portals that do not decrease overall security
 - Limited functionality
 - Do not compromise on SSL or using proper domains
- Authentication is hard
 - Don't use www password
 - Thick mobile apps help this
- Don't make phishing easier
 - Don't send links in email
 - Don't confuse users

Questions?

alex@isecpartners.com

cclark@isecpartners.com