

Kerberos + Android

A Tale of Opportunity

Platform Decisions

The Statistics



Why Go Mobile?



80%

of the world's population now has a mobile phone.

(5 Billion Phones)



Why Go Mobile?



Of those 80%,

1.08 Billion

are smartphones.



Why Go Mobile?



In the US:

the ratio is even higher, with smartphones making up **40%** of all mobile phones.



OK, well why Android?





Android?

Reason 1: US Market Dominance



Android?

Reason 2: Consumer Popularity

- **100 million** activated Android devices (now 400,000 / day)
- **200,000 apps** in Android Market (4.5 billion activations to date)
- **310 devices** available to consumers (112 countries)



Android?

Reason 3: Developer Popularity

• **450,000 developers** building for the platform!





Android.

Meaning?

- Opportunity for increased Kerberos visibility
- **Useful** for Android and Kerberos developers
- **Fun** to see where the community takes it



Our Plan

What we wanted to do.





We wanted to fill a missing gap.

1. Port Kerberos **libraries** to Android

2. Port some C-based Kerberos client apps to Android





Goals

We wanted to spark community involvement.

3. Build a sample **Android NDK App** (with a simple **GUI**)





Action!

What we did.



1. Crypto Implementation



Crypto Added new CyaSSL crypto implementation

Kerberos crypto options:
 CyaSSL, OpenSSL, NSS, built-in



yass

Crypto Added new CyaSSL crypto implementation







2. Porting



Android Port

Kerberos Libraries + CyaSSL ➡ Android.

Cross-compiled libraries for Android

Created shell script for easy reproduction by developers



3. Android Application



Simple sample NDK project

Home Screen

- Single screen
- Uses JNI
- Wrapper around native client apps





Simple sample NDK project

kinit

• Gets a ticket using specified principal





Simple sample NDK project

klist

• Lists our tickets



Simple sample NDK project

kvno

• Gets a service ticket for the entered principal





Simple sample NDK project

klist after kvno

Verify that we got a ticket



Simple sample NDK project

kdestroy

• Clear our ticket cache





Notes

- Uses a keytab instead of passwords
- <u>Storage locations</u> have been chosen for convenience

— Can be easily modified to what the developer needs

— Currently at /data/local/kerberos



License Type

• Application code will remain under the MIT license



4. GSS-API Wrapper





Java Wrapper

• Provide Java bindings for developers to use

Uses SWIG framework

• Wrapper around native Kerberos GSS-API library

(Contains functionality found in gssapi.h)





Java Wrapper

2 example clients:

- Android client functionality
- Stand-alone Java app for desktop use



GSS-API

Integrated into sample app.

Example Client

- Est. context with example server
- Send wrapped message, verify returned sig. block (gss_wrap, gss_verify_mic)
- Repeat #2, but with gss_seal, gss_verify
- Misc. API tests and exit.





GSS-API

Integrated into sample app.

Example Server

- Est. context with client
- Receive and unwrap a message from the client
- Generate & send signature block for received message



What's happening next?



Look to the Community.

Availability

Code will be linked from both MIT and yaSSL websites

Kerberos: The Network Authentication Protocol	(a)	
• What is Karbarne?		Support Forums
What is Activity Announcements	N1-	
Security Advisories	Masses Home About Products Da	ownload License Blog Docs Community Contact
Kerberos Version 4 End of Life Announcement		
Kerberos Releases		
Current release: <u>krb5-1.10</u>		
Maintenance release: <u>krb5-1.9.3</u>	Embedded SSL Library	A CONTRACTOR OF
Maintenance release: <u>krb5-1.8.6</u>	Embedded OOL Eibrary	
• Kerberos for Windows: <u>ktw-3.2.2</u>	for Applications, Devices, and the Cloud	
Historical releases of MIT KrDS		LA LA ALL ALL ALL
Down Sources and binaries from MIT	Providing secure communication for smart devices on automobiles, routers,	
Release in testing	applications, IP and mobile phones, the cloud, and much more.	
The krd5-current Snapshots (for developers only)		
 krb5-1.6.4-beta1 		
Documentation	Does your Application or Device Need SSL?	
 Documentation for the latest release 		
 How do the new US export regulations affect Kerberos? 	The CyaSSL embedded SSL library is a lightweight C-language-based SSL/TLS library targeted at embedded and RTOS	
 Papers about the Kerberos protocol 	environments primarily because of its size, speed, and featu	ire set. It works seamlessly in regular desktop and
Kerberos Y2K statement	enterprise environments as well. CyaSSL supports the industry standards up to the current TLS 1.2 level, is up to 20 times smaller than OpenSEL offers a simple ADI an OpenSEL compatibility layer. DTLS cuprent is backed by the	
The MIT Kerberos Team	robust CTaoCrypt crypto library, and much more.	insise comparishing layer, bres support, is backed by the
Contact Information		
Other Research		
Mailing lists	OUR PRODUCTS	WHERE ARE WE USED?
 comparation protocols kerberns newsamin 		
USC/SI Kerbens Page	yaSSL focuses on creating embedded security	Curious about where yaSSL products are used? To learn
 Oak Ridge National Laboratory's "How to Kerberize your Site" 	software. Current products include the CyaSSL	more about specific areas which are currently using our
	embedded SSL library and the yaSSL Embedded Web	products, please visit our Case Studies page.
	vaSSI's products are dual licensed under both the	
Recent News	GPLv2 as well as standard commercial licensing.	
Accent fields		
Old news is archived	To learn more about yaSSL and the CyaSSL embedded	
GREATER AND AND A	SSL library, please read our About Us page, or visit a	
06 Feb 2012 - krb5-1 9 3 is released	respective product page.	
The ktp5-1.9.3 source release is now available.	DECENT LICENTO	
	RECEIVE RIGHLIGHTS	Linux Journal, May 2011, Security Issue
06 Feb 2012 - krb5-1.8.6 is released	valid recently publiched an in-death walkthrough in	SCORT
	yessurecency published an in-depth waikthrough in Linux Journal about installion an alternate Java SSI	Linux Journal Website
The krb5-1.8.6 source release is now available.	Provider in the Android operating system. Read the	
	and a person of a person of a person of a person of the pe	



Look to the Community.

PR Activity / Visibility

- Blog posts
- Forum posts
- Press releases
- GitHub
- Mailing lists
- etc...



Other ideas or thoughts?



References

Statistics

- http://ansonalex.com/infographics/smartphone-usage-statistics-2012-infographic/
- http://www.go-gulf.com/blog/smartphone
- http://blog.nielsen.com/nielsenwire/online_mobile/40-percent-of-u-s-mobile-users-own-smartphones-40percent-are-android/
- Google I/O 2011: <u>http://www.google.com/events/io/2011</u>

Project Locations

Kerberos: <u>http://web.mit.edu/kerberos/</u> CyaSSL: <u>http://www.yassl.com/</u>

- Android NDK App: <u>https://github.com/cconlon/kerberos-android-ndk</u>
- GSS-API Java Wrapper: <u>https://github.com/cconlon/kerberos-java-gssapi</u>





