

Asymmetric Cryptography

Lukasz Pater CMMS Administrator and Developer



EDMS 1373428

Agenda

Introduction

- Why do we need asymmetric ciphers?
- One-way functions
- RSA Cipher
- Message Integrity
- Examples
 - Secure Socket Layer
 - Single Sign On
- Conclusion





Introduction

Challenge: How perfect strangers can send each other encrypted messages?

Powerful Idea: Public-key encryption!



Diffie, Hellman, Merkle [1976]



Rivest, Shamir, Adleman [1977]



Introduction

- Symmetric Cryptography
 - Requires that sender and receiver know shared secret key
- Asymmetric Cryptography radically different approach



- Sender and receiver do not share the same key
- Public encryption key known to all
- Private decryption key know only to the receiver

2014 Lukasz Pater

CFR

One-way functions

Most functions are invertible; for any f(x) = y, there is an f¹(y) = x (e.g. division, multiplication, DES)

•
$$f(x) = 2 \cdot x, f^{-1}(x) = x / 2 \dots$$

- A function which is easy to compute in one direction, but difficult to compute in the other, is called *one-way function*
 - Polynomial factorization, hashing, modular arithmetic, ...
 - One-way function that can be easily inverted with additional knowledge (
 is known as *trapdoor one-way function*

$$f(x) \dots easy$$

$$f^{1}(x) \dots hard$$

$$f^{1}(x, \bigcirc \cdots) \dots easy$$
Domain Range

2014 Lukasz Pater

One-way functions and cryptography

- Public key encryption is based on the existence of trapdoor one-way functions
 - Encryption, done with the public key (____), is very easy
 - Decryption is computationally hard (factorization of large numbers, discrete logarithm problem)
 - Knowledge of the private key () "opens the trapdoor", making inversion easy



One-way functions and cryptography

- Public key encryption is based on the existence of trapdoor one-way functions
 - Encryption, done with the public key (____), is very easy
 - Decryption is computationally hard (factorization of large numbers, discrete logarithm problem)
 - Knowledge of the private key () "opens the trapdoor", making inversion easy



RSA (Rivest, Shamir, Adleman)

- RSA is the most well-known and common public key cryptosystem
- Basic notation: a key pair (e,d,N) contains two keys:
 - (e,N) is the public key, (d,N) is the private key
 - Let RSA be the encryption function and 'ABC' plaintext message



RSA Algorithm

- RSA's security is based on modular arithmetic
 - x mod n; remainder of x when divided by n (5 mod 2 = 1)
 - p and q are relatively prime if their greatest common divisor is 1
 - p and q are multiplicative inverse when $(p \cdot q = 1 \mod n)$

RSA algorithm

- Pick two large prime numbers p and q, let $N = p \cdot q$
- Select small integer e that is relatively prime to (p-1)(q-1)
- Find d, the multiplicative inverse of e mod (p-1)(q-1)
- (e,N) is the public key, to encrypt compute $C = M^e \mod N$
- (d,N) is the private key, to decrypt compute $M = C^d \mod N$



RSA Algorithm / Example

Pick two large prime numbers p and q, let N = p • q

Select small integer e that is relatively prime to (p-1)(q-1)

Find d, the multiplicative inverse of e mod (p-1)(q-1)

- (e,N) is the public key, to encrypt compute M^e mod N
 - (3,33) is the public key, **2**³ mod 33 = **8**
- (d,N) is the private key, to decrypt compute M^d mod N
 - (7,33) is the private key, 8⁷ mod 33 = 2

TFR

Strengths of RSA

- Why is RSA secure?
 - Suppose you know the public key (e, N), $N = p \cdot q$
 - The security of RSA is dependent on the assumption that it's difficult to determine the private key d from (e,N)
 - Essentially need to find factors of N without knowing p and q
 - Factoring is thought to be computationally hard (no proof!)
- Some statistics for the fastest known factoring algorithm

Key Size	Size MIPS-years required to factor				
512 bits	30,000				
1024 bits	300,000,000,000				
2048 bits	300,000,000,000,000,000				

TER

Message Integrity

- Allows communicating parties to verify that received messages are authentic
 - Content of the message has not been altered
 - Source of the message is who/what you think it is
- Message Digests
 - A Hash function H() that takes as input an arbitrary length message and outputs a fixed-length string – message digest



Message Integrity

- Allows communicating parties to verify that received messages are authentic
 - Content of the message has not been altered
 - Source of the message is who/what you think it is
- Message Digests
 - A Hash function H() that takes as input an arbitrary length message and outputs a fixed-length string – message digest



FR

2014 Lukasz Pater

Digital Signatures

- Cryptographic technique analogous to hand-written signatures
 - Sender digitally signs the digest of the document () with his/hers private key (), establishing that he is the owner



Certification Authorities

- Certification Authority (CA<u>m</u>) binds public key to particular entity, for example: to Bob
 - Bob provides "proof of identity" to the CA
 - CA creates certificate binding Bob to his public key
 - Certificate () containing Bob's public key () digitally signed by CA's private key () says: "This is Bob's public key"



Secure Socket Layer (SSL)

- TCP provides reliable end-toend service
- TCP with SSL provides reliable and secure end-to-end service
 - HTTPS: HTTP over SSL
 - Subsequently became Internet standard know as TLS
 - Provides message integrity (hash functions) and message confidentiality (symmetric encryption with shared secret key)



Secure Socket Layer (SSL)



2014 Lukasz Pater

Single Sign On (SSO)

Scenario during typical work day (at CERN)

- Sign in for an absence request
- Sign in to subscribe to one of the technical trainings
- Sign in to order a book from the library
- Sign in ...

					Search					12
< ►	(đ) 🖻 (+ 🗖)	ttps 🔒 cta	.cern.ch/	cta2/f?p=1	10:9:20423	3259869	7748::::X_ST	ATUS,XS_COURSE	N C Re	ader 🛛 🔘
m III	WCF rest seentors.co	m Apple	iCloud	Facebook	Twitter	Yahoo!	Wikipedia	Informations *	Divers *	+
M	Catalogue									
IR Trainir	ng Website							França	is Print	Logout
	Language	Leadersh	lp	Personal Comm	Dev &	Safety		Technical	Tech M	gmt
Welcome	to the CERN Training Cata	ilogue. Plea	ise use the	e form below	to search a	mong the	307 available	e courses.		
Course o	r Competency				Programme	Technie	al		\$	Has Upcomin
// cour	ses found. Please select o	ne from the	results be	NOW.						
»Inform:	ation technologies									
*Inform:	ation technologies						Language	Next Session	Duration	,
×Inform Agile Inf	ation technologies rastructure & Puppet for Se	ervice Mana	igers: getti	ing started		E	L <i>anguage</i> Inglish	Next Session 11-Jun-14	Duration 1 day	On ava
×Inform Agile Inf Agile Pre	ation technologies rastructure & Puppet for Sr pject Management with Sc	ervice Mana rum	igers: getti	ing started		E	L <i>anguage</i> Inglish Inglish	Next Session 11-Jun-14 06-May-14 to 07- May-14	Duration 1 day 2 days	On ava
×Informa Agile Inf Agile Pro Business	ation technologies rastructure & Puppet for Sr zject Management with Sci s Objects Basic	ervice Mana rum	igers: getti	ing started		E	anguage inglish inglish inglish or irench	Next Session 11-Jun-14 06-May-14 to 07- May-14 to be scheduled	Duration 1 day 2 days 2 days	On ava On ava to t
»Informa Agile Inf Agile Pro Business Business	ation technologies rastructure & Puppet for Sr oject Management with Scr s Objects Basic s Objects Universe Design	ervice Mana rum er	igers: getti	ing started		E	anguage inglish inglish inglish or rench inglish or rench	Next Session 11-Jun-14 06-May-14 to 07- May-14 to be scheduled to be scheduled	Duration 1 day 2 days 2 days 2 days	On ava On ava On ava to t
*Informa Agile Inf Agile Pri Businesa Businesa Businesa	ation technologies astructure & Puppet for Sr gloct Management with Sci o Objects Basic o Objects Universe Design o Objects advanced	ervice Mana rum er	igers: getti	ing started		E E F F E F F	Language inglish inglish or rench inglish or rench inglish or rench	Next Session 11-Jun-14 06-May-14 to 07- May-14 to be scheduled to be scheduled to be scheduled	Duration 1 day 2 days 2 days 2 days 1 day	On ava
*Informa Agile Inf Agile Pri Business Business C++ Par	ation technologies rastructure & Puppet for Sr sjoct Management with So s Objects Basic s Objects Universe Design s Objects advanced t1 - Handa-On Introduction	ervice Mana rum er	igers: getti	ing started		E E F F F F F F F F F F F F F F F F F F	Language inglish inglish or rench inglish or rench inglish or rench inglish	Next Session 11-Jun-14 06-May-14 to 07- May-14 to 07- May-14 to be scheduled to be scheduled to be scheduled	Duration 1 day 2 days 2 days 2 days 1 day 4 days	On ave On ave On ave to t 2 m nee On per
»Informa Agile Inf Agile Pri Business Business C++ Par C++ Par	ation technologies rastructure & Puppet for Sr sjoct Management with So s Objects Basic s Objects Universe Design s Objects advanced 11 - Hands-On Introduction 12 : Object-Oriented	ervice Mana rum er	igers: getti	ing started		E E F E F E E F E E F F E E F F	Language inglish inglish or rench inglish or rench inglish or rench inglish or rench	Next Session 11-Jun-14 06-May-14 to 07- May-14 to 107- May-14 to 107- to be scheduled to be scheduled to be scheduled to be scheduled	Duration 1 day 2 days 2 days 2 days 1 day 4 days 3 days	On ava On ava On ava On ava On ava On ava On ava On ava On ava On ava On ava On ava On ava On ava On ava On ava On ava On Ava On Ava On Ava On Ava On Ava On Ava On Ava On Ava On Ava On Ava On Ava On Ava On Ava On On Ava On On On Ava On On On On On On On On On On On On On
*Informa Agile Inf Agile Pri Businesa Businesa C++ Par C++ Par C++ Par	ation technologies rastructure & Puppet for Sr joct Management with Srci s Objects Basic s Objects Universe Design s Objects advanced 11 - Hands-On Introduction 12: Object-Oriented 13: Hands-On Generic Pro	ervice Mana rum er n	n C++ and	ing started		E E E F E E F E E E E E E E E E E E E E	Language inglish inglish or inglish or inglish or inglish or inglish or inglish or inglish	Next Session 11-Jun-14 06-May-14 to 07- May-14 to 107- May-14 to 107- to be scheduled to be scheduled to be scheduled to be scheduled	Duration 1 day 2 days 2 days 2 days 1 day 4 days 3 days 2 days	On ava
*Informa Agile Inf Agile Pri Business Business C++ Par C++ Par C++ Par	ation technologies anstructure & Puppet for Sir joed Management with Sor is Objects Basic S Objects Universe Design 11 - Hands-On Introduction 12: Object-Onented 13: Hands-On Geneiro Pro- 14: Hands-On Programmin	ervice Mana rum er n igramming i igramming i	ngers: getti n C++ anc Guide	ing started		2 E E F E E E E E E E E E E E E E E E E	Language inglish inglish or rench inglish or rench inglish or rench inglish or rench inglish inglish	Next Session 11-Jun-14 06-May-14 to 07- May-14 to be scheduled to be scheduled to be scheduled to be scheduled to be scheduled	Duration 1 day 2 days 2 days 2 days 1 day 4 days 2 days 2 days 2 days	On On On On On avia to t The On On On On On Avia On Avia On On Avia On On Avia On On On Avia On On On On On On On On On On

		Absen	ce Request							
I N (2) (2) (+	🍯 https 🔒 edh.cei	n.ch/Document/C	laims/LeaveRequest					Ċ		
WCF rest seen	tors.com Apple IC	oud Facebook	Twitter Yahoo! W	ikipedia	Infor	matio	ns 🔻	Dive	rs v	
EDH - Hom	e (Lukasz Piotr PATER			Absence R	eques	st				+
T Absence	Request		06		5	6	2			
Absence	request						2)			
v			Attach Pr.Vi	ew Sg	nd	1	telp			
			Fields w	ith asteris	(6.(*));	are m	Con	fiden	itial od mu	Urg st be fill
ated by Lukasz Pi	tr PATER (GS-A	SE-EDS) Tel: 7	77858 169407 on	12 04 20	114			ory or	ru mu	
Salos by Eukasz Fi		oc 200) rei. i		.2.34.20						
plicable administrati	ve procedure: "Le	ave at CERN:	OVERVIEW"							
General Informati	on									
Poquestor *:					4000				TAF	
Requestor :	Lukasz Piotr PATER (C	S-ASE-EDS)	r 1	Cern ID:	1096	515, 3	statu	is: S	IAF	
show values in:	8 Hour Days :									
Balance					© Ap	ril - O	4.20	14 😋	Ð	
D -1	I Francisco	0	Development	Mo	Tu	Wo	Th	Fr	80	Su
Balances	Forecast	Current	Previous		1	2	3	4	5	6
Annual	22.00	7.00	8.00	7	8	9	10	11	12	13
				14	15	16	17	18	19	20
				21	22	23	24	25	26	27
Holiday				28	29	30				
Other										
Absence periods										
				1.0.1						
Absence Type		Start Date	En	d Date		1.0.0		Du	1 00	n
Annoai ceave a		25.04.201	• <u>06:30</u> = Ш	25.04.20	1.4		:50	-		
										3.4
	Click here to	add a new line	item +Add						Λpp	'y



2014 Lukasz Pater

FRI

Single Sign On (SSO)

Multi sign on is troublesome

- Is it possible to just sign-on once to perform all the actions?
- Single sign-on can be used to answer that question
- SSO delegates the authentication to centralized service



Single Sign On / How does it work?

- Identity Provider (IP): the system that asserts information about a subject (by issuing a ticket
)
- Service Provider (SP): the system that relies on the information supplied to it by the Identity Provider (in the issued ticket)
- 1) User opens a web page
- 2) SP redirects to IP
- 3) User logs in
- IP issues a ticket and redirects to SP
- 5) SP validates the ticket



Single Sign On (SAML) Ticket

<t:RequestSecurityTokenResponse> <t:Lifetime> <wsu:Created>2014-04-08T13:11</wsu:Created> Iukaszpater — bash — 65×29 <wsu:Expires>2014-04-08T23:11</wsu:Expires> lpatermac:~ lukaszpater\$ openssl x509 -in sso.crt -text Certificate: </t:Lifetime> Data: Version: 3 (0x2) Serial Number: 2d:88:23:bd:00:00:00:00:00:30 <saml:Attribute AttributeName="UPN"> Signature Algorithm: sha256WithRSAEncryption Issuer: DC=ch, DC=cern, CN=CERN Certification Authority lukasz.piotr.pater@cern.ch Validity </soml:Attribute> Not Before: Nov 8 08:38:55 2013 GMT Not After : Jul 29 09:19:38 2023 GMT <saml:Attribute AttributeName="CommonName"> Subject: DC=ch, DC=cern, OU=computers, CN=login.cern.ch Subject Public Key Info: lpater Public Key Algorithm: rsaEncryption RSA Public Key: (2048 bit) </saml:Attribute> Modulus (2048 bit): 00:a7:ab:75:0b:44:86:94:b7:5d:2f:63:3e:96:d7: df:1a:2a:13:9c:34:f7:7b:3b:4e:c6:50:3d:6c:01: <ds:Signature> ae:bc:1f:3f:46:3c:a6:f1:e9:fa:f8:44:fd:6e:83: 34:d8:2c:a8:47:95:69:9f:c8:84:95:75:56:71:c0: <ds:SignatureValue> 04:c4:f2:10:12:ae:f4:0f:a2:cf:7b:ce:af:6f:eb: 58:86:e2:8f:78:b7:ee:20:23:7d:67:44:8c:43:87: nChTR2/k8ltpJTAuAmnsBkt04.... fe:e7:bb:e4:eb:50:a8:d7:fb:b0:ff:c9:0f:bd:79: 72:77:e0:22:f0:3b:27:fc:6d:21:a4:7e:bb:6c:12: </ds:SignatureValue> 3d:54:e4:0a:7e:92:6a:72:57:12:26:e4:a5:50:1e: <X509Certificate> 4f:25:f7:ef:31:4a:6b:db:d0:74:79:1c:7c:2c:a1: 67:20:76:c3:20:b4:ae:ea:75:5b:14:b7:1a:76:d5: MIIIEjCCBfaaAwIBAaIKLYajv.... 88:8d:b6:2f:a0:aa:2b:5e:0d:c9:ea:ea:ed:93:3f: b3:10:37:98:31:3b:c0:e9:91:8e:15:ff:d7:cb:97: </X509Certificate>

</ds:Signature> </t:RequestSecurityTokenResponse>

FRI

R

SSO / Advantages and Disadvantages

Advantages

- Reduces the chance of forgetting your password. By having your one-set master password
- Very reach API
- Less code to maintain for the web master
- Single Sign Out
- Disadvantages
 - The SSO Identity Provider is highly-critical
 - Bad for a multi-user computer, especially if the user stays logged in all the time



Conclusions

- Asymmetric encryption was introduced to complement the inherent problem of the need to share the same key in symmetric ciphers
 - Symmetric encryption algorithms can be extremely fast
 - Public key algorithms are orders of magnitude less efficient than symmetric key encryption
 - Use public key cryptography just to exchange the key!
- Public key certificates allow the secure communication between services and client applications
- Single Sign On enables to access multiple related, but independent software systems



Questions & Answers



