

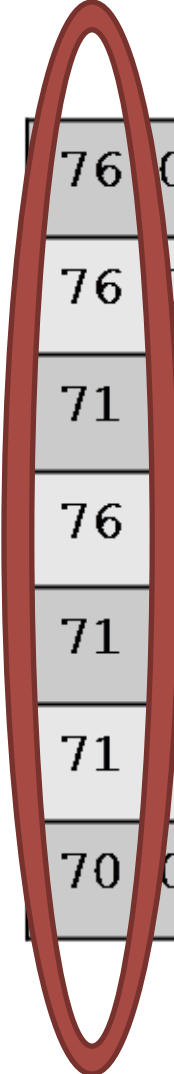
Most Common Cryptography Mistakes

4/7/2014

Encrypted credit card numbers

76	06	93	93	2b	8f	4b	c6	ec	e2	b3	d7	a1	09	f7	
76	06	9a	95	27	84	4f	c1	ef	e2	bb	df	a5	0a	f3	
71	01	9a	93	2b	85	41	ca	e2	e9	ba	df	a0	01	fa	26
76	05	9d	99	2b	84	4a	ca	e8	e1	b7	d7	a5	08	f4	
71	04	98	98	22	8b	49	c0	ed	e1	b0	d7	a8	08	f6	22
71	05	93	94	22	8d	4a	c7	eb	e5	b0	df	a8	09	f3	23
70	02	9d	93	23	8c	4f	c4	e2	e8	bb	d0	a7	08	f6	20

Encrypted credit card numbers



76	06	93	93	2b	8f	4b	c6	ec	e2	b3	d7	a1	09	f7	
76	06	9a	95	27	84	4f	c1	ef	e2	bb	df	a5	0a	f3	
71	01	9a	93	2b	85	41	ca	e2	e9	ba	df	a0	01	fa	26
76	05	9d	99	2b	84	4a	ca	e8	e1	b7	d7	a5	08	f4	
71	04	98	98	22	8b	49	c0	ed	e1	b0	d7	a8	08	f6	22
71	05	93	94	22	8d	4a	c7	eb	e5	b0	df	a8	09	f3	23
70	02	9d	93	23	8c	4f	c4	e2	e8	bb	d0	a7	08	f6	20

ASCII: ..., '3' = 0x33, '4' = 0x34, '5' = 0x35, ...

Encrypted credit card numbers

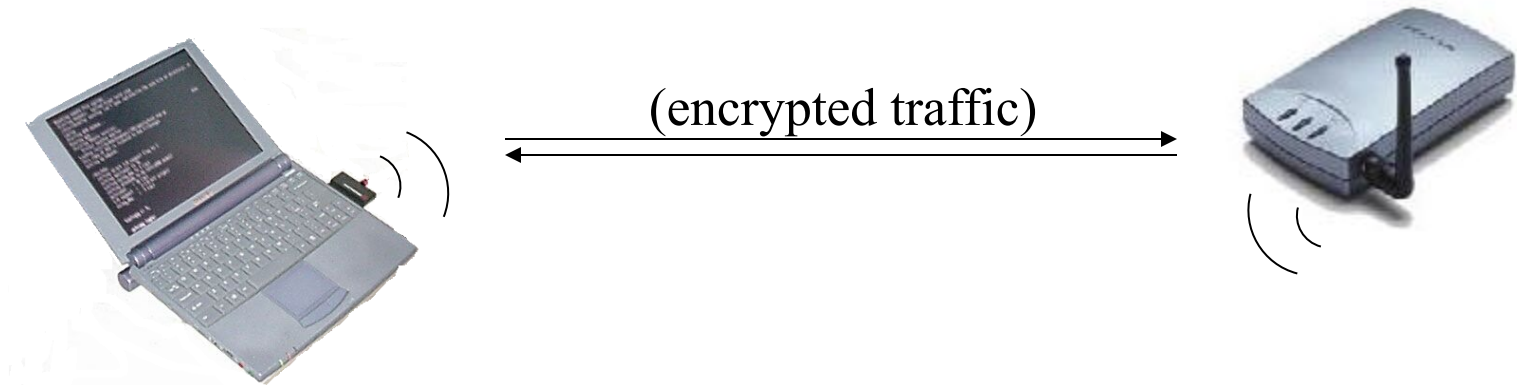
76	06	93	93	2b	8f	4b	c6	ec	e2	b3	d7	a1	09	f7	
76	06	9a	95	27	84	4f	c1	ef	e2	bb	df	a5	0a	f3	
71	01	9a	93	2b	85	41	ca	e2	e9	ba	df	a0	01	fa	6
76	05	9d	99	2b	84	4a	ca	e8	e1	b7	d7	a5	08	f4	
71	04	98	98	22	8b	49	c0	ed	e1	b0	d7	a8	08	f6	2
71	05	93	94	22	8d	4a	c7	eb	e5	b0	df	a8	09	f3	23
70	02	9d	93	23	8c	4f	c4	e2	e8	bb	d0	a7	08	f6	20

ASCII: '0' = 0x30, ..., '7' = 0x37, '8' = 0x38, '9' = 0x39

#7: Don't re-use nonces/IVs

- Re-using a nonce or IV leads to catastrophic security failure.

WEP



- Early method for encrypting Wifi: WEP (Wired Equivalent Privacy)
 - Share a single cryptographic key among all devices
 - Encrypt all packets sent over the air, using the shared key
 - Use a checksum to prevent injection of spoofed packets

WEP - A Little More Detail

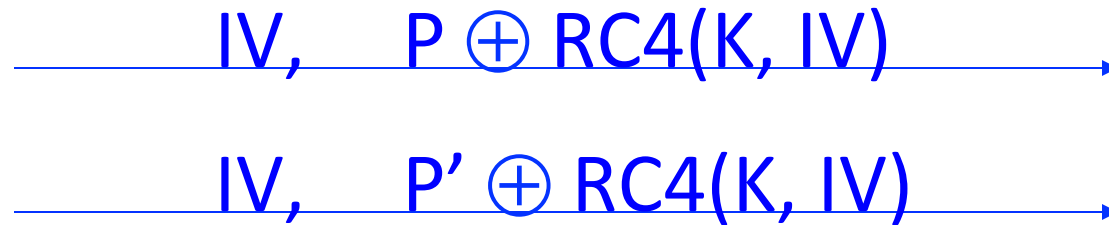


→ $IV, P \oplus RC4(K, IV)$ →



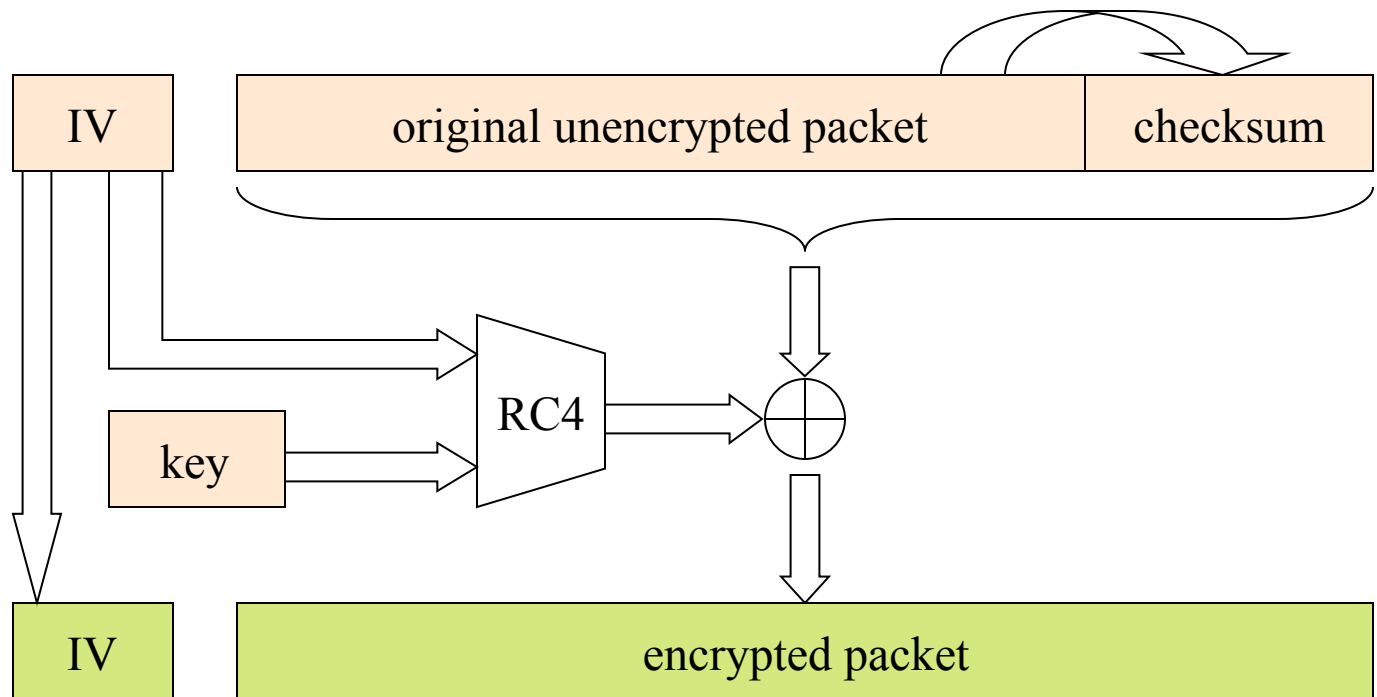
- WEP uses the RC4 stream cipher to encrypt a TCP/IP packet (P) by xor-ing it with keystream ($RC4(K, IV)$)

A Risk of Keystream Reuse



- In some implementations, IVs repeat.
 - If we send two ciphertexts (C, C') using the same IV , then the xor of plaintexts leaks ($P \oplus P' = C \oplus C'$), which might reveal both plaintexts
- Lesson: Don't re-use nonces/IVs

WEP -- Even More Detail



Attack #2: Spoofed Packets

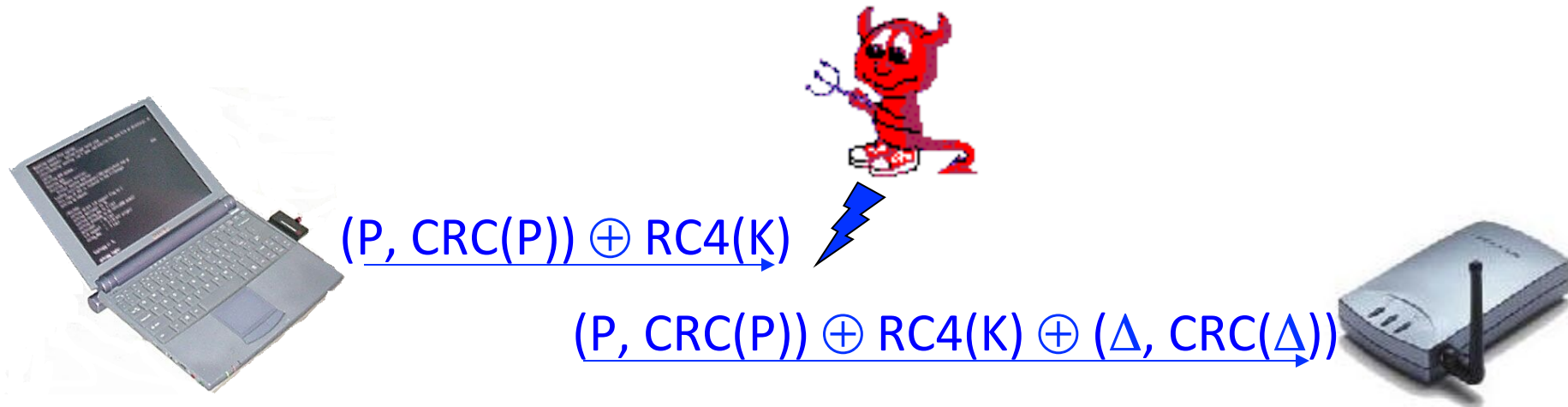


$IV, (P, CRC(P)) \oplus Z$



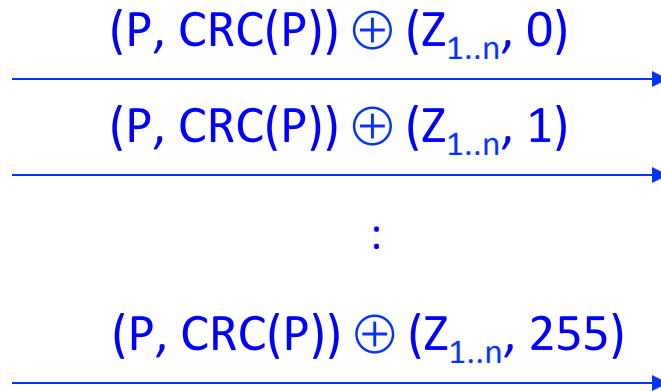
- Attackers can inject forged 802.11 traffic
 - Learn $Z = RC4(K, IV)$ using previous attack
 - Since the CRC checksum is unkeyed, you can then create valid ciphertexts that will be accepted by the receiver

Attack #3: Packet Modification



- CRC is linear
 - ⇒ $\text{CRC}(P \oplus \Delta) = \text{CRC}(P) \oplus \text{CRC}(\Delta)$
 - ⇒ the modified packet $(P \oplus \Delta)$ has a valid checksum
- Attacker can tamper with packet (P) without breaking RC4

Attack #4: Inductive Learning

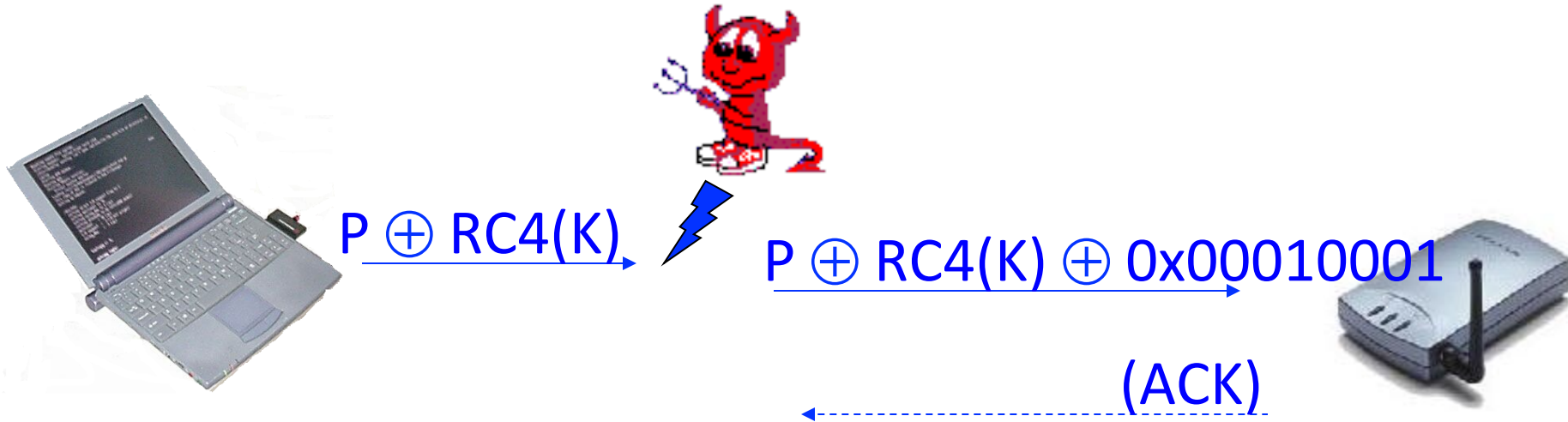


(pong)



- Learn $Z_{1..n} = \text{RC4}(K, IV)_{1..n}$ using previous attack
- Then guess Z_{n+1} ; verify guess by sending a ping packet $((P, \text{CRC}(P)))$ of length $n+1$ and watching for a response
- Repeat, for $n=1,2,\dots$, until all of $\text{RC4}(K, IV)$ is known

Attack #5: Reaction Attacks



- TCP ACKnowledgement returned by recipient
 - ⇔ TCP checksum on modified packet ($P \oplus 0x00010001$) is valid
 - ⇔ $wt(P \& 0x00010001) = 1$
- Attacker can recover plaintext (P) without breaking RC4

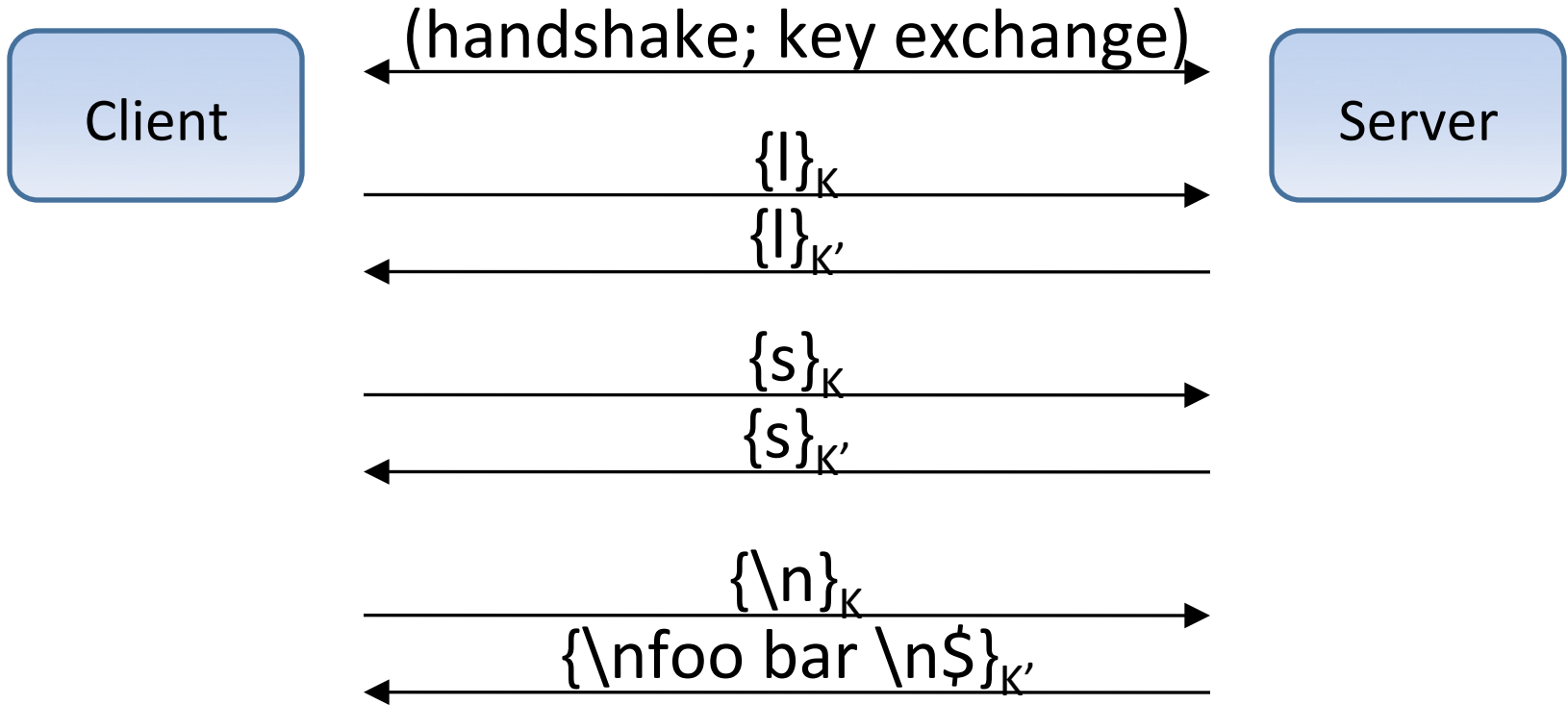
#7: Key Re-use

- Don't re-use keys for both encryption and authentication.
- Don't re-use keys for both encryption and signing.
- Don't use same key for both directions.

#8: Traffic Analysis is Still Possible

- Encryption doesn't hide sender, recipient, length, or time of message. (“meta-data”)

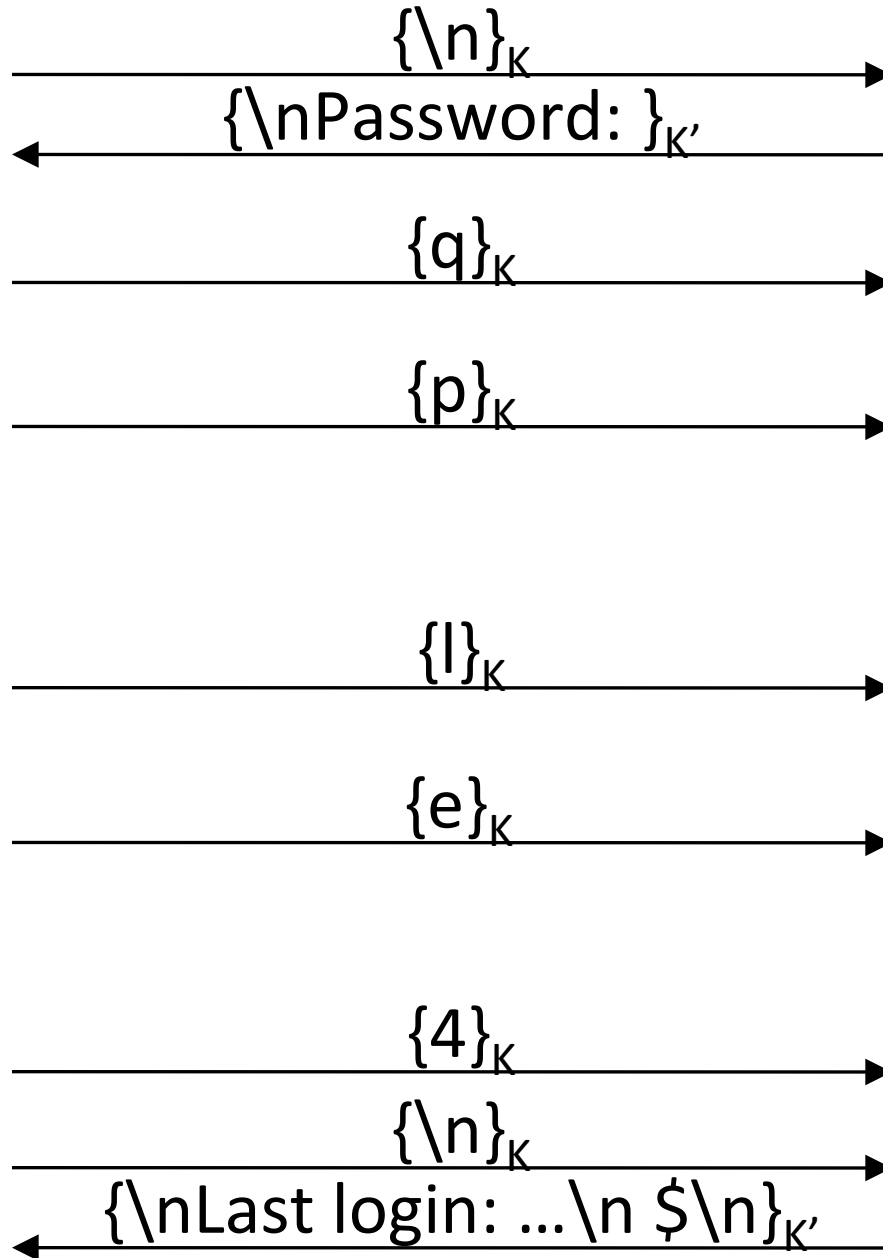
SSH



SSH

Client

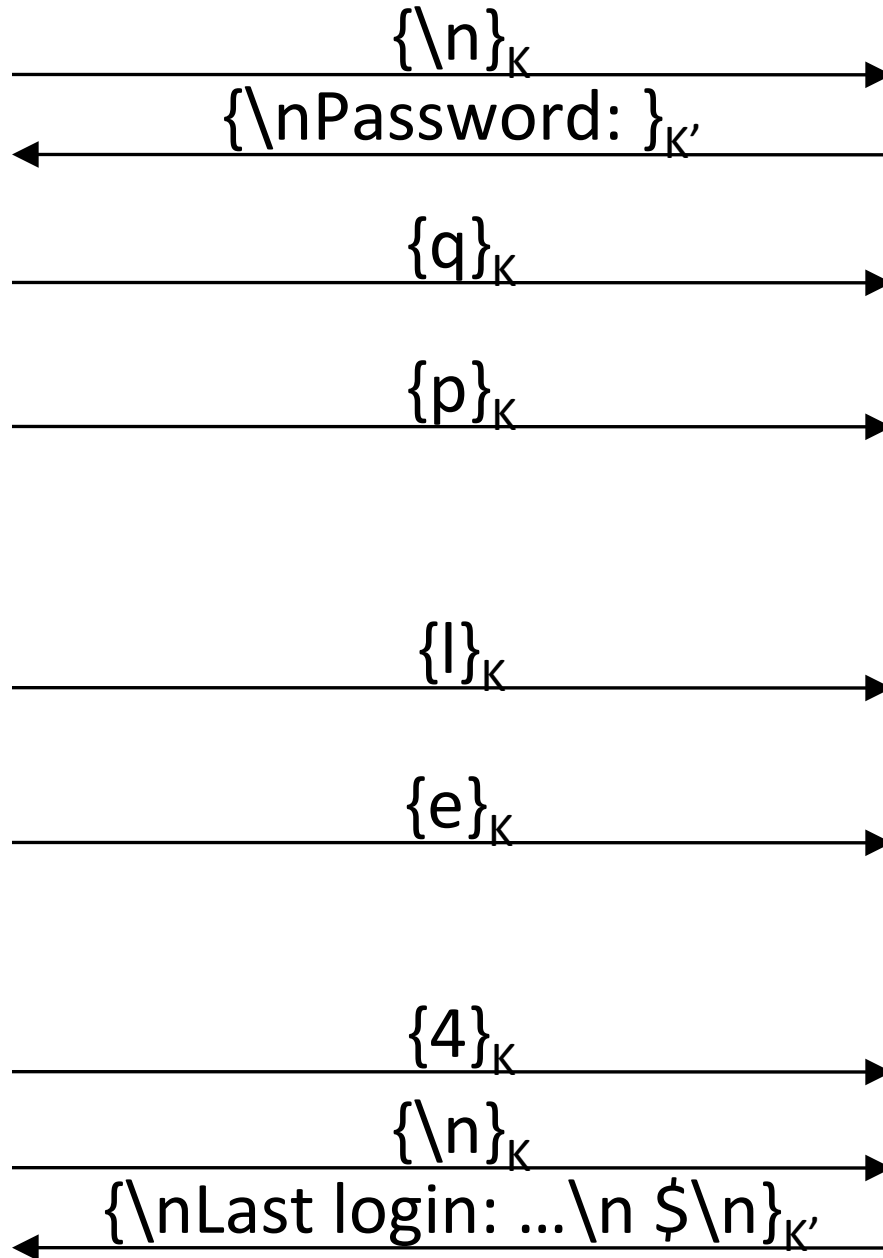
Server



SSH

Client

Server



Reveals time between keystrokes. This leaks partial information about the password!

Lessons Summarized

- Don't design your own crypto algorithm.
- Use authenticated encryption (don't encrypt without authenticating).
- Use crypto-quality random numbers.
- Don't derive crypto keys from passphrases.
- Be secure by default.
- Be careful with concatenation.
- Don't re-use nonces/IVs. Don't re-use keys for multiple purposes.
- Encryption doesn't prevent traffic analysis ("metadata").

Meta-Lessons

- Cryptography is hard.
- Hire an expert, or use an existing system (e.g., SSL, SSH, PGP).
- But: Most vulnerabilities are in applications and software, not in crypto algorithms.

Securing Internet Communication: TLS

CS 161: Computer Security

Prof. David Wagner

April 7, 2013

Today's Lecture

- Applying crypto technology in practice
- Goal #1: overview of the most prominent Internet security protocol
 - **SSL/TLS**: transport-level (process-to-process) on top of TCP
 - Secures the web via HTTPS
- Goal #2: cement understanding of crypto building blocks & how they're used together

Building Secure End-to-End Channels

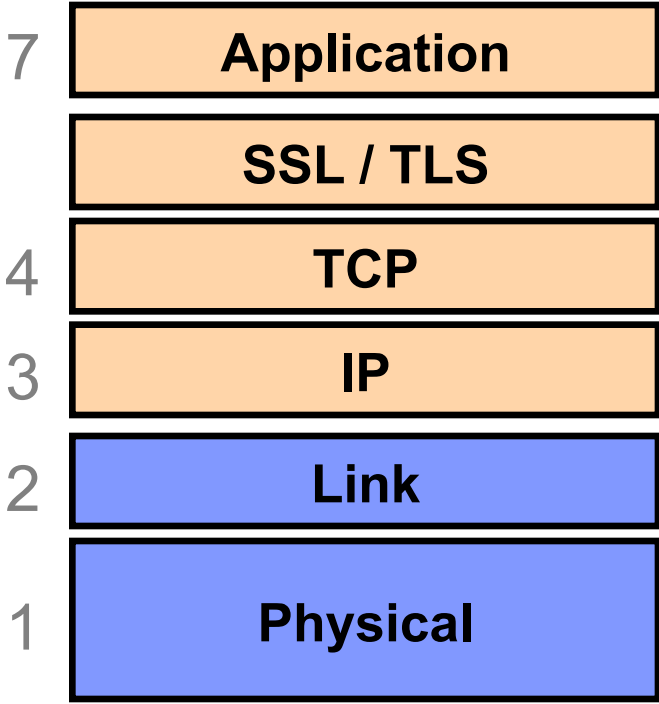
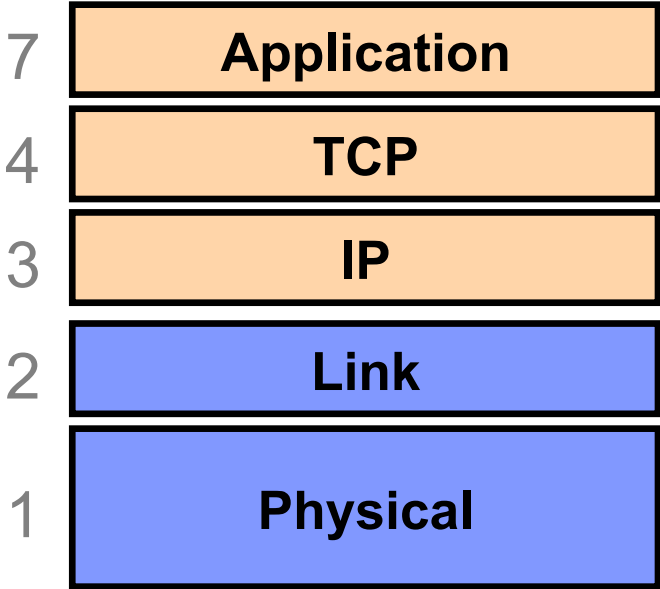
- *End-to-end* = communication protections achieved all the way from originating client to **intended** server
 - With no need to trust intermediaries
- Dealing with threats:
 - Eavesdropping?
 - **Encryption** (including session keys)
 - Manipulation (injection, MITM)?
 - **Integrity** (use of a MAC); *replay protection*
 - Impersonation?
 - **Signatures**

(What's missing?
Availability ...)

Building A Secure End-to-End Channel: SSL/TLS

- SSL = *Secure Sockets Layer* (predecessor)
- TLS = *Transport Layer Security* (standard)
 - Both terms used interchangeably
- Notion: provide means to secure *any* application that uses TCP

SSL/TLS In Network Layering



Building A Secure End-to-End Channel: SSL/TLS

- SSL = *Secure Sockets Layer* (predecessor)
- TLS = *Transport Layer Security* (standard)
 - Both terms used interchangeably
- Notion: provide means to secure *any* application that uses TCP
 - Secure = encryption/confidentiality + integrity + authentication (of server, but *not* of client)
 - E.g., puts the ‘s’ in “https”

Regular web surfing - http: URL

The image shows a screenshot of the Amazon.com website in a browser window. The browser's address bar shows the URL <http://www.amazon.com/>, which is circled in orange. An orange arrow points from the text 'Regular web surfing - http: URL' to this address bar. The website header includes the Amazon logo, a greeting 'Hello. Sign in to get personalized recommendations. New customer? Start here.', and a navigation menu with links for 'Your Amazon.com', 'Today's Deals', 'Gifts & Wish Lists', and 'Gift Cards'. On the right side of the header, there are links for 'Your Account' and 'Help', both circled in orange. An orange arrow points from the text 'But if we click here ...' to the 'Your Account' link. Below the header is a search bar with the text 'All Departments' and a 'GO' button. To the left of the search bar is a vertical menu with 'Shop All Departments' and various product categories like 'Books', 'Movies, Music & Games', etc. The main content area features a large advertisement for the Kindle e-reader, with the text 'Kindle You'll Do a Double Take. Reads Like Real Paper, Even in Bright Sunlight.' and a 'Learn more' button. To the right of the Kindle ad is an image of a wooden lounge chair. Below the lounge chair are two smaller promotional boxes: one for 'Strategic Insight' and another for 'Warm Your Feet in UGG'.

Amazon.com: Online Shopping for Electronics, Apparel, Computers, Books, DVDs & more

<http://www.amazon.com/>

Most Visited Latest Headlines NY Times Google News Daily Weather 294 United Traffic Papers US9 IMC CSET Google Maps RSS Movies

Amazon.com: Online Shopping for...

amazon.com Hello. [Sign in](#) to get personalized recommendations. New customer? [Start here](#). **FREE 2-Day Shipping, No Minimum Purchase: See details**

Your Amazon.com Today's Deals [Gifts & Wish Lists](#) [Gift Cards](#) [Your Account](#) [Help](#)

Shop All Departments Search All Departments GO Cart Wish List

Books > Movies, Music & Games > Digital Downloads > Kindle > Computers & Office > Electronics > Home & Garden > Grocery, Health & Beauty > Toys, Kids & Baby > Clothing, Shoes & Jewelry > Sports & Outdoors > Tools, Auto & Industrial >

Kindle
You'll Do a Double Take.
Reads Like Real Paper,
Even in Bright Sunlight.

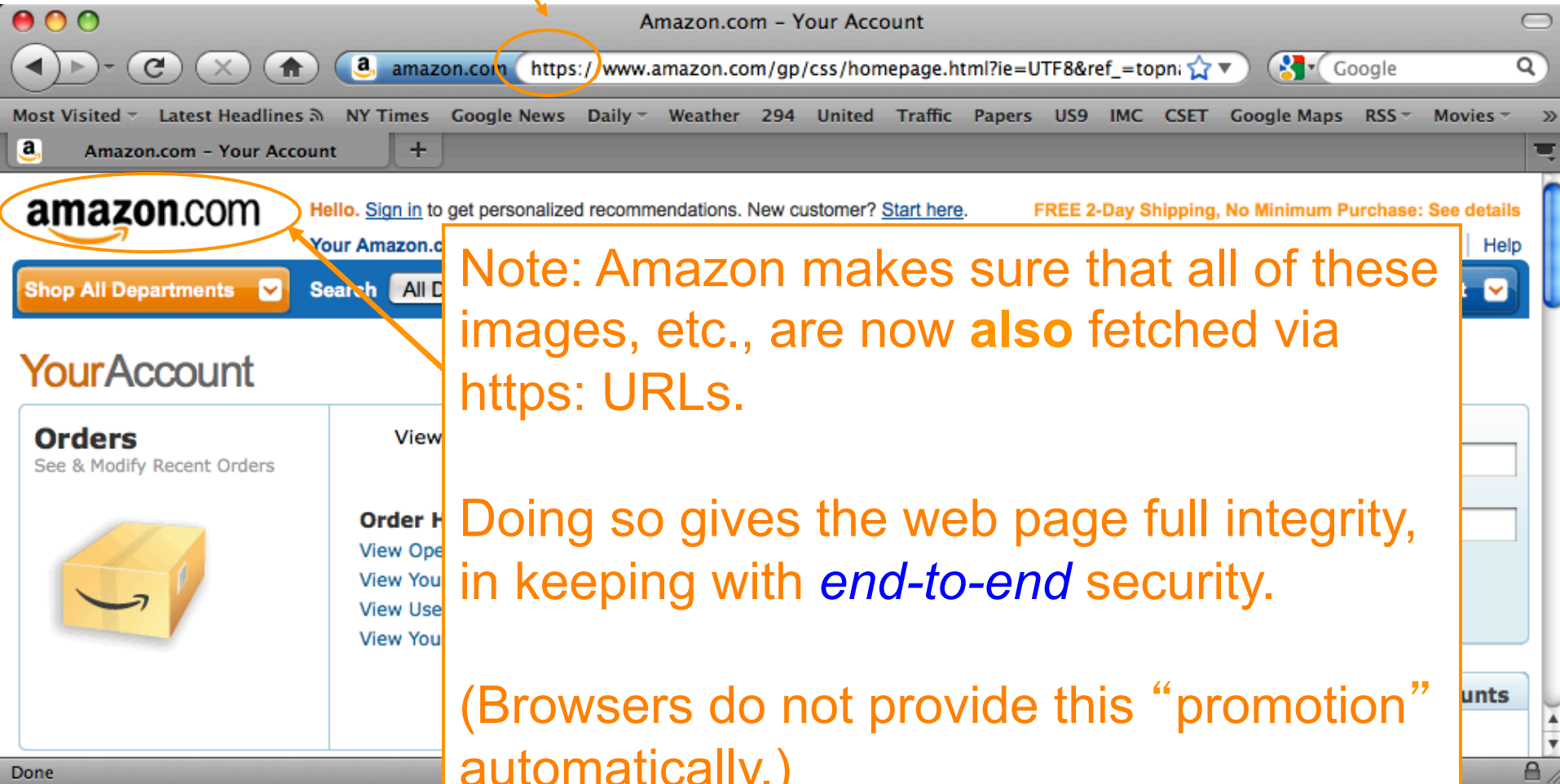
[Shop now](#)

What's your Pay Phrase? **"Strategic Insight"** is still available! [Claim yours](#)

Warm Your Feet in UGG
These twin-faced, breathable sheepskin [UGG](#) boots keep your feet warm and cozy at any time of year. Multiple styles and colors.

Transferring data from spe.atdmt.com...

Web surfing with TLS/SSL - https: URL



The image shows a screenshot of a web browser displaying the Amazon.com website. The browser's address bar shows the URL <https://www.amazon.com/gp/css/homepage.html?ie=UTF8&ref=topn>, with the **https://** portion circled in orange. An arrow points from the text box above to this circled portion. The browser's title bar reads "Amazon.com - Your Account". The page content includes the Amazon logo (circled in orange), a search bar, and a "Your Account" section with an "Orders" subsection. A yellow box with an Amazon logo is visible in the "Orders" section. The browser's status bar at the bottom shows "Done".

Note: Amazon makes sure that all of these images, etc., are now **also** fetched via https: URLs.

Doing so gives the web page full integrity, in keeping with *end-to-end* security.

(Browsers do not provide this “promotion” automatically.)

Basic idea

- Browser (client) picks some symmetric keys for encryption + authentication
- Client sends them to server, encrypted using RSA public-key encryption
- Both sides send MACs
- Now they use these keys to encrypt and authenticate all subsequent messages, using symmetric-key crypto

