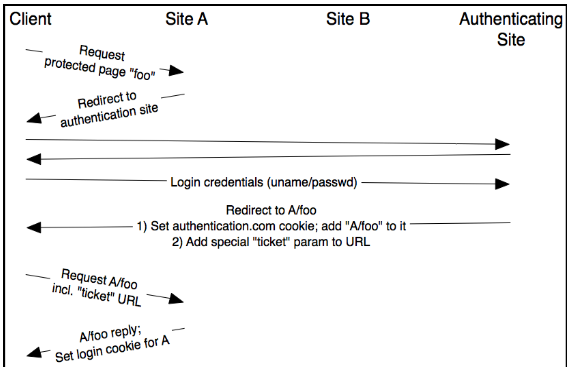
Lecture 5
Sessions (cont'd) + Security

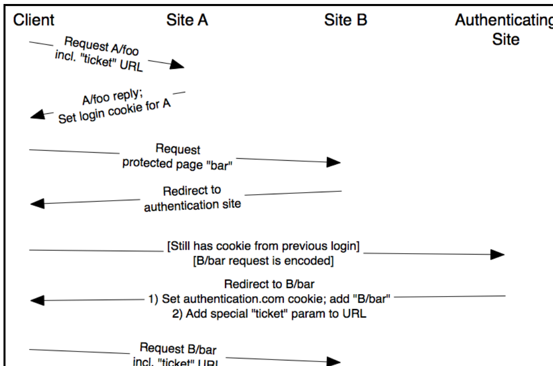
Single Signon

- Can we log into many systems at once?
- Many problems:
  - If site A redirects to B for login, how will B redirect back to A?
  - How to communicate cross-site login-status via cookies?
  - Log user out of all sites at once?

2



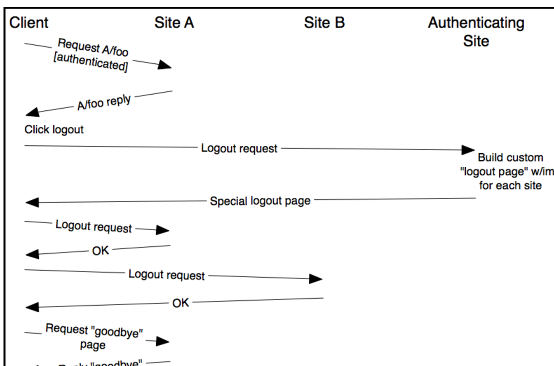
3



4

What about logout?

5



6

Next: Security

- Security Goals
- Threats & Defenses
- Encryption
- Secure connections
- Secure servers

7

Security Goals

- Lots of different dimensions to Web security
  - Confidentiality/Privacy
  - Data Integrity
  - Service Integrity (availability)
  - Authenticity
  - Non-repudiation

8

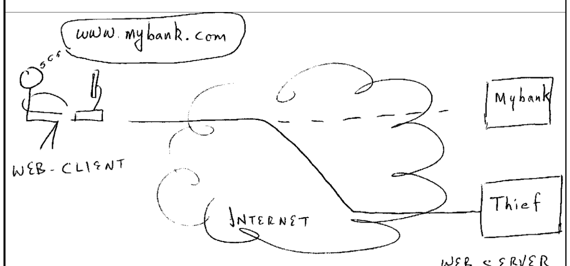
Threads/evil techniques

- Masquerading: pretend to be someone else
- Address spoofing: pretend to be somewhere else
- Eavesdropping: listen in on comm
- Man-in-the-middle: manipulate comm
- Replay: record and use comm data later
- Physical: steal the post-it with password

9

Examples

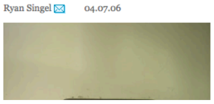
- Client-side masquerading obvious



10

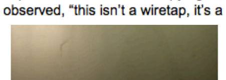
Whistle-Blower Outs NSA Spy Room

Ryan Singel 04.07.06



AT&T provided National Security Agency eavesdroppers with full access to its customers' phone calls, and shunted its customers' internet traffic to data-mining equipment installed in a secret room in its San Francisco switching center, according to a former AT&T worker cooperating in

The evidence also shows that the government did not act alone. EFF has obtained whistleblower evidence [PDF] from former AT&T technician Mark Klein showing that AT&T is cooperating with the illegal surveillance. The undisputed documents show that AT&T installed a fiberoptic splitter at its facility at 611 Folsom Street in San Francisco that makes copies of all emails, web browsing, and other Internet traffic to and from AT&T copies to the NSA. This copying includes both domestic and international Internet activitie observed, "this isn't a wiretap, it's a country-tap."



AT&T's central office on Folsom Street in San Francisco houses a secret room that allows the National Security Agency to monitor phone and internet traffic, according to former AT&T technician-cum-whistle-blower Mark Klein. View Slideshow

On Wednesday, the EFF asked the court to issue an injunction prohibiting AT&T from continuing the alleged wiretapping, and filed a number of documents under seal, including three AT&T documents that purportedly explain how the wiretapping system works.

According to a statement released by Klein's attorney, an NSA agent showed up at the San Francisco switching center in 2002 to interview a management-level

Client	Man-in-the-Middle	Server
Request "info" w/ uname/passwd →		
	Remember uname/passwd	
	Request "info" w/ uname/passwd →	
	← Reply "info"	
	Note that login succeeded	
← Reply "info"		

Examples

- Replay attack
  - Record good conversation, then replay to masquerade as one party
  - E.g., record the uname/passwd, then replay it to authenticate in the future
- How vulnerable is TCP to replay-attack hijacking?
- Man-in-the-middle?

13

Defenses

- Authentication
  - A party establishes identity to others
  - Usually requires credentials
    - ID badge
    - Passport
    - Password
  - In real world, assymmetric relationships mean one-sided authentication
  - On Web, no social clues to indicate identity; all parties must authenticate
  - Makes masquerading impossible

14

Defenses

- Non-repudiation
  - A party to transaction cannot later deny it
  - In real-world, we use signatures
  - On Web, can you repudiate a login?
- Authorization
  - Granting privileges to authenticated parties
  - A policy is a spec of authorization rules
- A mechanism is the system by which a security policy is implemented
  - Most fundamental is encryption
  - Encryption != security

15

Encryption

- Cryptography vs cryptanalysis
- Encryption applies a reversible fn to some piece of data, yielding something unreadable
- Decryption recovers the original data from the unreadable encryption-output
- The encryption/decryption algorithm assumed known; the *key* is secret

16

Encryption (2)

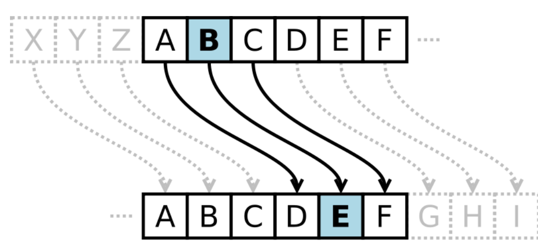
- Plaintext string s
- Encryption key K_{enc}
- Decryption key K_{dec}

- Encrypt s with K_{enc} to obtain ciphertext $K_{enc}(s)$
- Decrypt $K_{enc}(s)$ with decryption key K_{dec} to reobtain s
- $K_{dec}(K_{enc}(s)) = s$

17

A Brief History

- **Caesar cipher** rotates alphabet by 3



18

A Brief History

TAKE THE ROAD TO ROME   plaintext

↓ ↓ ↓ ↓ ↓

WDNH WKH URDG WR URPH   ciphertext

19

Substitution Ciphers

- No need to shift 3 chars
  - You could do 2! Or even 4!
- You also don't have to shift the alphabet at all. Just arbitrary 1:1 mapping of alphabet chars, using a *substitution table*
- All of these are vulnerable to frequency analysis
  - Letter
  - Word
  - Common phrases

20

Polygram Cipher

- Translate n-grams, not chars

plaintext	ciphertext
AAA	QWE
AAB	RTY
AAC	ASD

- How big is substitution table?
  - A^n entries, where A is size of alphabet
  - A=26,n=3; 17576 entries
  - A=100,n=6; 1T entries
- Still vulnerable, but requires more text

21

Substitution Rules

- Don't store table explicitly; derive table rows using substitution rule
  - E.g., ***s* XOR *k***, where k is *key*
  - Remember: security level depends on size of key
  - Key of len *b* => 2^b possible keys

22

Substitution Rules

- XOR "flips a bit" for input bits that correspond to key's "1"
  - Correspond to a 0? No change

```
0000000001010101    plaintext
1011010010011100    key
1011010011001001    XOR
```

- Encrypted string should ideally show no pattern for frequency analysis attack
- Use key long enough to make ciphertext appear random

23

Substitution Rules (2)

- What's the right size key?
  - Who is trying to break the scheme?
  - 3GHz CPU => 300 inst for possible key test
  - 1 sec, 10M keys
  - 1 day, 1T keys
  - 60-bit key takes 100 CPUs 3 years
- Is that good enough?
- Also, use statistical techniques to determine ideal key length

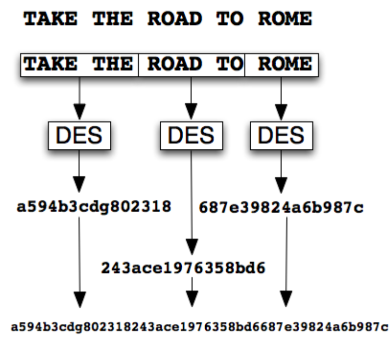
24

Data Encryption Standard

- DES is a block cipher with 56-bit key
  - 64-bits at a time
  - Perform 16 rounds of encryption, w/std. permutations of keys and data
  - DES is not secure
- Data xmitted in 64-bit blocks, each may be coded independently

25

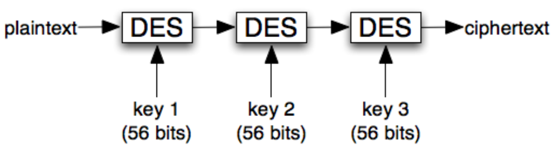
DES in 64-bit blocks



26

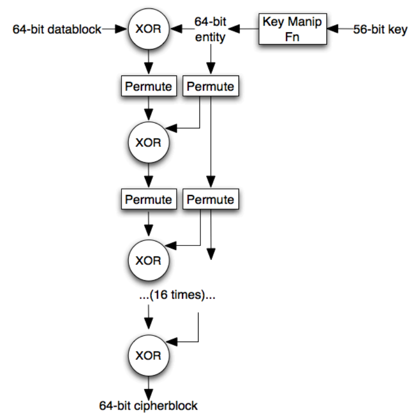
Triple DES

- Triple-DES is 168 bits
- Break the key into 3 parts



- DES' bit-logic techniques make it fast

27



28

Key Management

- Encryption depends on everyone having the same key
- Key distribution is the weak link
  - Hard to distribute
  - Vulnerable to key theft
- What we've been discussing is best called *symmetric encryption*
  - Only kind from 5000BC to 1976
- Assymmetric, or public-key encryption, uses two keys
  - One of the greatest achievements of CS

29