Carnegie Mellon

Mechanisms to Mitigate Wireless Privacy Threats

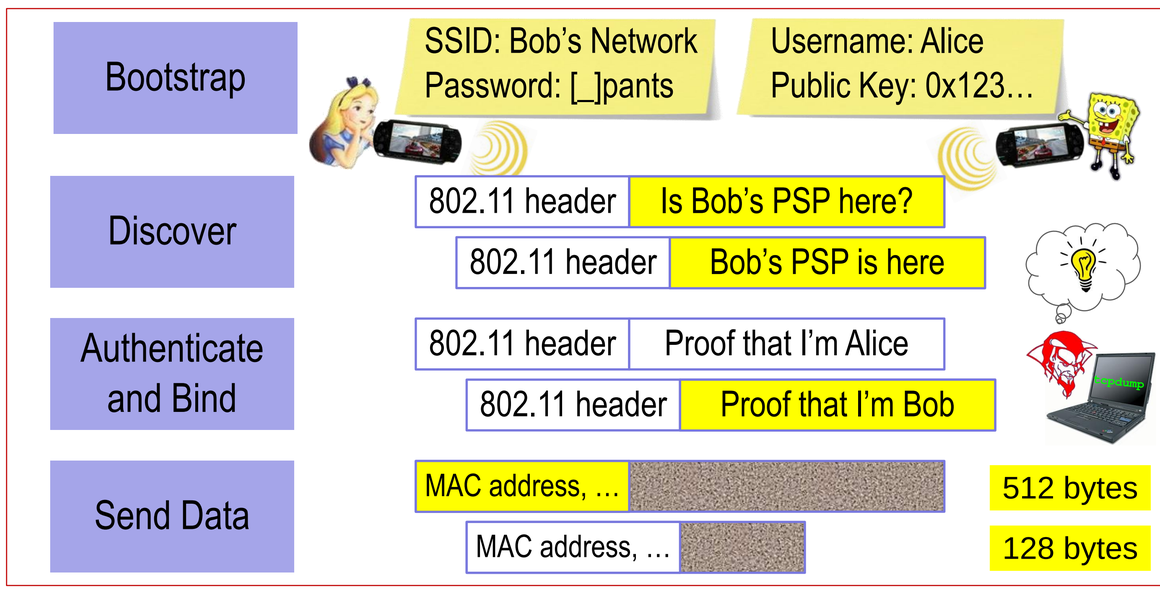
Jeffrey Pang <jeffpang@cs.cmu.edu>
http://www.cs.cmu.edu/~jeffpang

Problem: existing protocols leak information

Best security practices still expose identifiers, credentials, and packet sizes/timings to third parties, enabling attacks:

- **Location tracking**: identifiers can be linked over time
- **User profiling**: info can be cross-indexed with databases
- **Side-channel analysis**: sizes/timing reveals packet contents

Greenstein, *HotOS* '07; Pang, *MobiCom* '07; Pang, *HotNets* '07; Jiang, *MobiSys* '07; Sapanos, *Usenix Security* '07; www.bluetoothtracking.org; ...

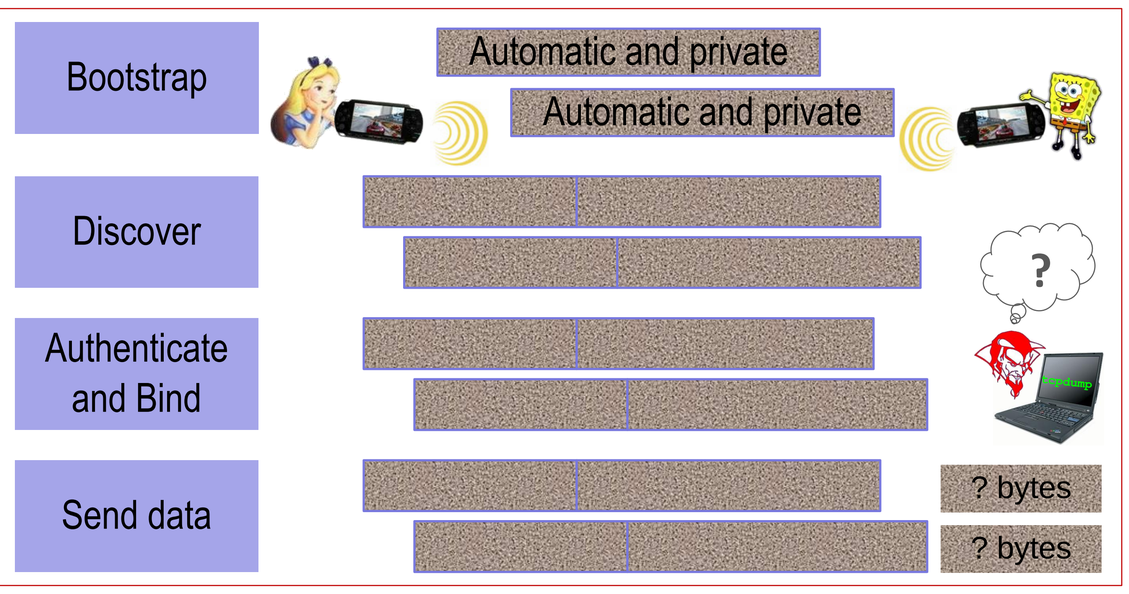


Goal: obsure everything from third parties

Three essential protocol changes to prevent attacks:

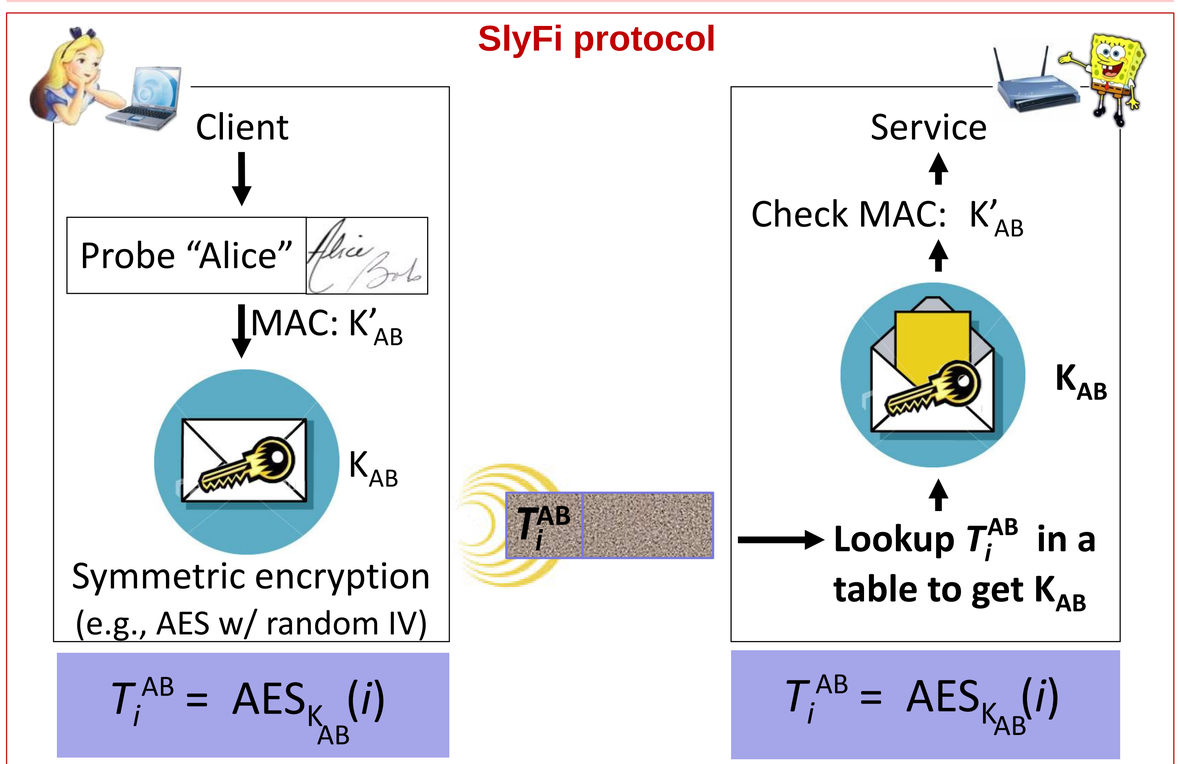
1. Obscure all transmitted bits during all protocol phases
2. Obscure packet sizes/timing that act as side-channels
3. Obscure and automate bootstrapping of keys to prevent communication with untrusted third parties

1. *MobiSys* '08; 2. *CMU Thesis Proposal* '08; 3. *HotNets* '07



SlyFi: obscures all transmitted bits

- **Problem**: Third parties can use unencrypted bits such as addresses to track and profile users. How can devices efficiently process packets without addresses?
- **Idea**: Sender and receiver agree on sequence of tokens beforehand; attach one token to each packet



Details: How do sender and receiver synchronize *i* ?

- Discovery/binding messages: infrequent and narrow interface ⇒ short term linkability is O.K.

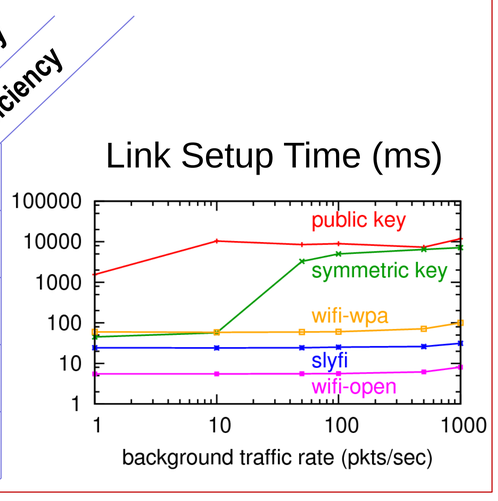
$$T_i^{AB} = AES_{K_{AB}}(i) \qquad \text{where } i = \lfloor \text{current time}/5\ \text{min} \rfloor$$

- Data messages: only sent on established connections ⇒ expect receiver to get most messages

$$T_{iAB} = AES_{K_{AB}}(i) \qquad \text{where } i = \text{transmission \#}$$

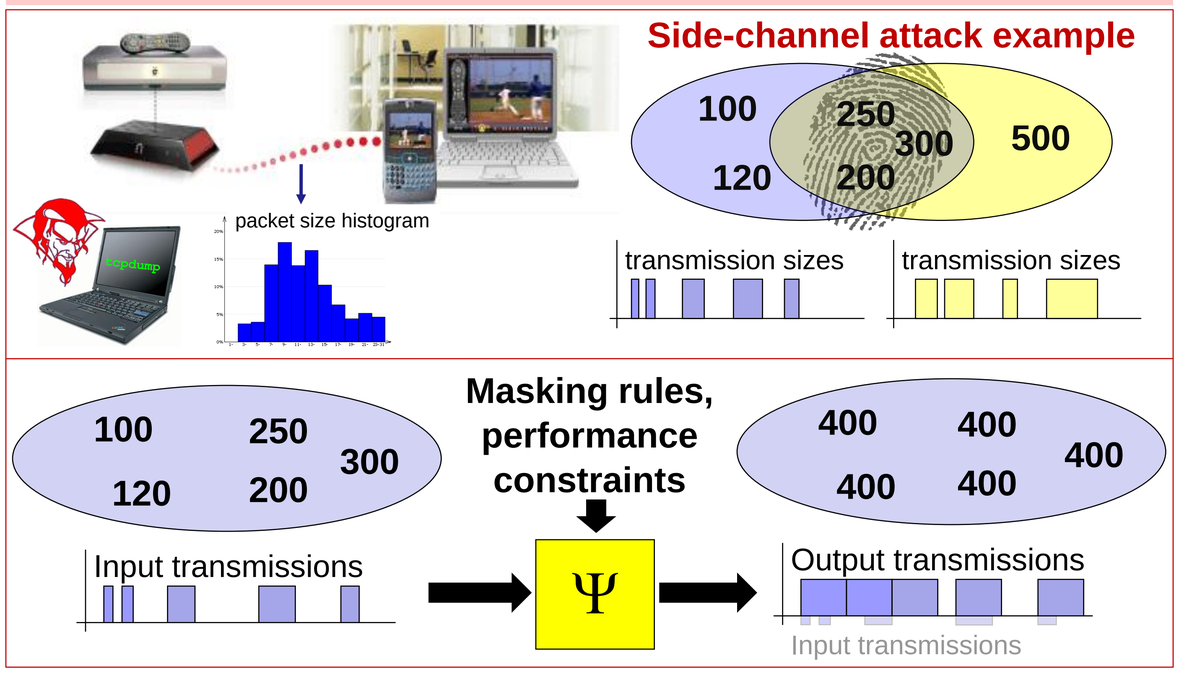
- Performs as well as WPA and has stronger security

	Confidentiality	Authenticity	Integrity	Unlinkability	Efficiency
802.11 WPA	Data Only	Data Only	Data Only	⊘	✓
MAC Pseudonyms	⊘	⊘	⊘	Long Term	✓
Encrypt Everything	✓	✓	✓	✓	⊘
SlyFi: Discovery	✓	✓	✓	Long Term	✓
SlyFi: Data	✓	✓	✓	✓	✓



Sudare: obscures side-channel leaks

- **Problem**: Packet sizes and timings reveal sensitive contents in encrypted packet streams (identity, videos…)
- **Idea**: Framework for masking side-channel leaks using signature-like rules for packet padding and cover traffic



Tryst: obscures & automates bootstrapping

- **Problem**: Clients often need to communicate with new devices. How does a client know who to trust?
- **Idea**: Leverage transitive trust relationships and device reputation to automatically bootstrap keys