IEEE 802.11 Procedures

Cisco.com

Dave Halasz and Nancy Cam-Winget
December 2002

Disclaimer

- **This presentation is an informal presentation on IEEE 802.11 procedures and the status of IEEE 802.11i draft 3.0.**
- **It should not be interpreted as coming from IEEE 802.11 or as a position statement from IEEE 802.11.**

What is IEEE 802.11 ….

From http://grouper.ieee.org/groups/802/11/main.html

- IEEE 802.11 is a standards working group on wireless local area networks
- The working group is a part of IEEE LMSC (LAN MAN Standards Committee) formerly called IEEE Project 802
- IEEE LMSC reports to the Standards Activity Board (SAB) of the IEEE Computer Society.

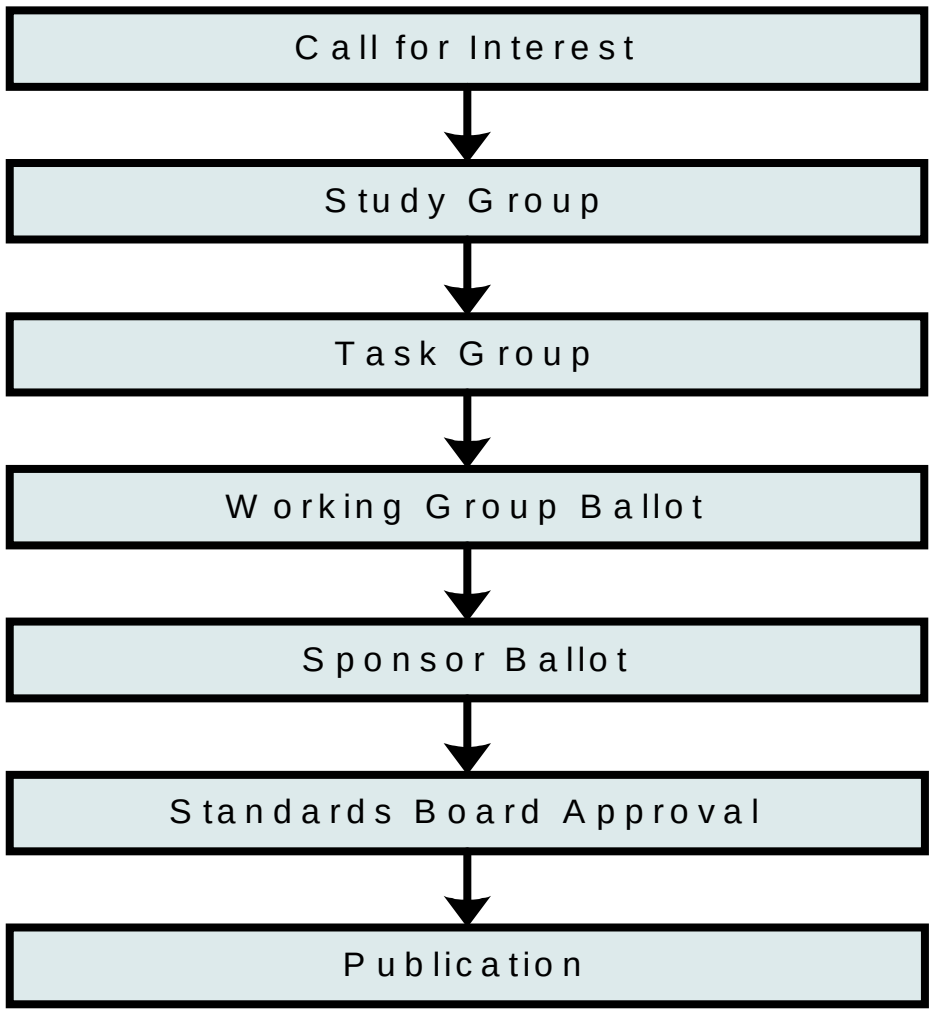
IEEE 802.11Mechanics

- **Open Forum: anyone can attend.**
- **Though recommended no IEEE membership is required**
- **Voting: limited to voting members.**
  - **Voting membership rights is gained by participating in at least 2 plenary meetings out of 4 consecutive plenary meetings**

References

- **About 802.11 & How to participate:**
  - **http://grouper.ieee.org/groups/802/11/main.html**
- **00/331 IEEE 802.11 Working Group Rules (Stuart Kerry, Chair - P802.11, Philips)**
- **Operating rules of IEEE project 802, LAN MAN Standards Committee (LMSC)**

Overview of the Project Process



Call for Interest and Start of Study Group

- **Study group creates a Project Authorization Request (PAR) and Five Criteria:**
  - **Broad Market Potential**
  - **Compatibility (with IEEE Standard 802.11)**
  - **Distinct Identity**
  - **Technical Feasibility**
  - **Economic Feasibility**
- **In July of 1999, IEEE 802.11 had a study group meeting for people interested in enhancing the IEEE 802.11 MAC for QoS and Privacy**

Task Group history

- **In March of 2000, TGe was created to,**
  - **“enhance the 802.11 Medium Access Control (MAC) to improve and manage Quality of Service, provide classes of service, and enhanced security and authentication mechanisms.”**
- **The scope of TGe is bound by the PAR of TGe**
- **John Fakatselis (Intersil), Dave Halasz (Cisco) were co-Chairs of TGe**

Task Group history continued

- In March of 2001, the TGe PAR was split into TGe (QoS) and TGi (Security)
  - TGi acted independently in May of 2001
- TGi PAR:
  - Enhancements to the current 802.11 MAC to provide improvements in security.
- Dave Halasz remains Task Group Chair of TGi
- John Fakatselis remains TGe Chair

Working Group Letter Ballot

- Conduct ballot on draft
- Resolve comments from WG ballot
- Iterate to closure

- Need 75% yes to proceed to Sponsor Ballot

TGi Working Group Letter Ballot history:

- **Draft 1.0 went to LB in March 2001**
- **Draft 2.0 went to LB in March 2002**
- **Draft 3.0 went to LB in December 2002**

Sponsor Ballot

- **Form ballot pool**
- **Obtain approval to go to Sponsor Ballot from 802.11 WG & 802 EC (Executive Committee)**
- **Submit draft for Sponsor ballot**
- **Resolve comments**
- **Iterate to closure**

Standards Board Approval

- Obtain approval for submission from WG 802.11 and 802 EC
- Check for Intellectual Property Rights requirements
- Submit to RevCom and IEEE Standards Board for approval

Publication

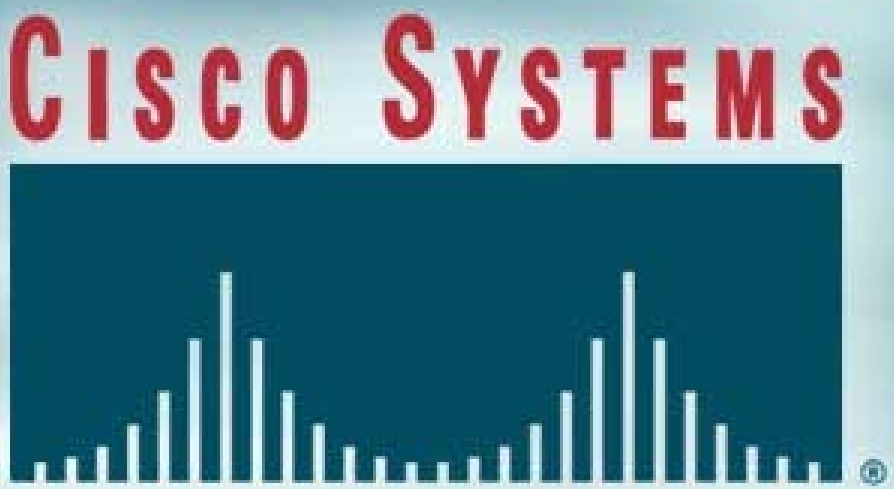
- **Support IEEE editor in preparation for publication**

Current TGi status

- **Letter Ballot for draft version 3.0 soon**
- **TGi draft version 3.0 available for public purchase (review):**
  - **http://standards.ieee.org/reading/ieee/std/lanman/**
  - **IEEE P802.11i/D3.0 Unapproved Draft Supplement to Standard for Telecommunications and Information Exchange Between Systems—LAN/MAN Specific Requirements—Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Specification for Enhanced Security**

IEEE 802.11 2003 Meetings

- *January 12-17: Ft Lauderdale, Fla*
- **March 9-14: Dallas, Tx**
- *May 11-16: Singapore*
- **July 20-25: San Francisco, Ca**
- *September: TBD*
- **November 9-14: Albuquerque, NM**


Cisco Systems

802.11i Status

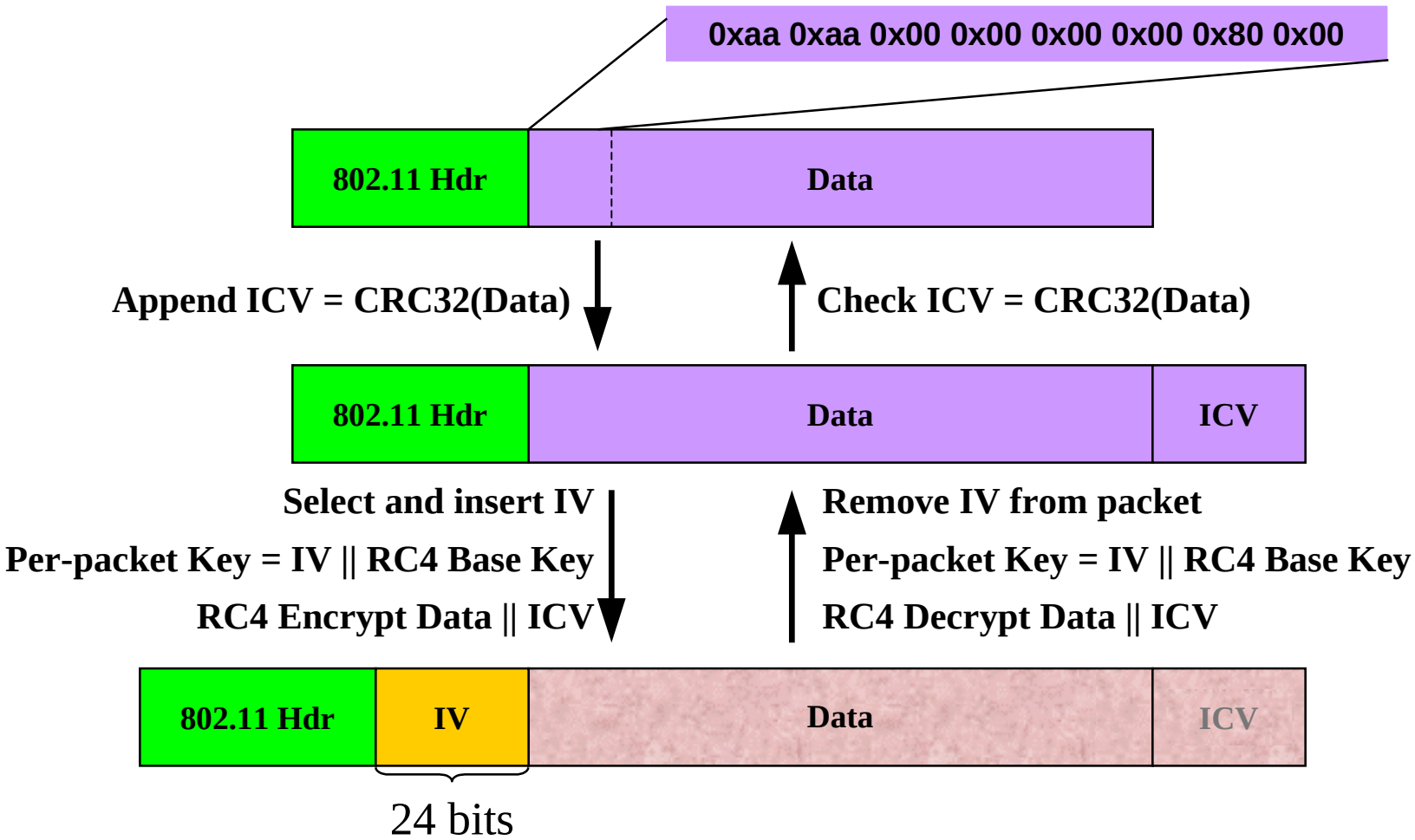
Current 802.11 Security

- **IEEE Std 802.11-1999 defines Wireless Equivalent Privacy (WEP)**
  - **Protocol intended to effect privacy…**
  - **…because anyone with a radio receiver can eavesdrop!**
- **WEP's Goals:**
  - **Create the privacy achieved by a wired network**
- **WEP has been broken!**
  - **Walker (Oct 2000), Borisov et. al. (Jan 2001), Fluhrer-Mantin-Shamir (Aug 2001)**

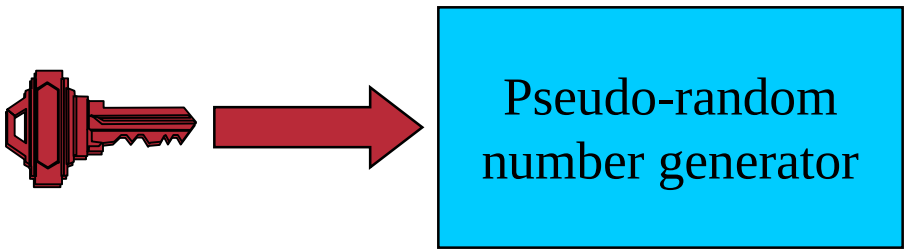
Legacy Security Issues

- **WEP doesn’t work (old news)**
  - **Key reuse allows data recovery without encryption key**
  - **Utilizes encryption improperly**
  - **No protection against replay attacks**
  - **Forgery of encrypted messages trivial**
- **802.11 Authentication doesn’t work (old news)**
  - **Trivial to steal authentication credentials**

How does WEP work?



RC4 cipher review…



"key stream" byte ***b***

Plaintext data byte
p

$\oplus$

Ciphertext data byte
$c = p \oplus b$

Decryption works the same way: $p = c \oplus b$

Thought experiment: what happens when p_1 and p_2 are encrypted under the same "key stream" byte ***b***?

$$c_1 = p_1 \oplus b \qquad c_2 = p_2 \oplus b$$

Then: $c_1 \oplus c_2 = (p_1 \oplus b) \oplus (p_2 \oplus b) = p_1 \oplus p_2$

Collision attacks

• WEP expands each RC4 key into 2^{24} per-packet keys ⇒ data can be recovered if IV is ever repeated with same key ⇒ RC4 key must be changed at least every 2^{24} packets or data is exposed through IV collisions!

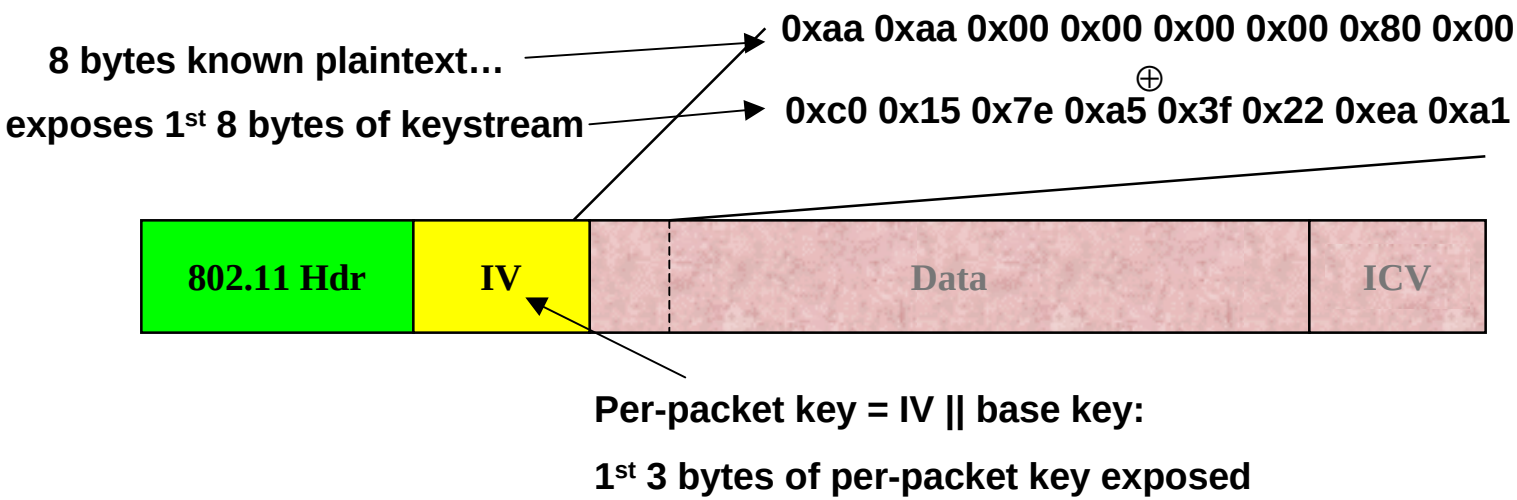
Some implemented IV selection strategies:

• Random: Collision probability $\boldsymbol{P_n}$ two packets will share same IV after $\boldsymbol{n}$ packets is $\boldsymbol{P_2} = 1/2^{24}$ for $\boldsymbol{n} = 2$ and $\boldsymbol{P_n} = \boldsymbol{P_{n-1}} + (\boldsymbol{n}-1)(1-\boldsymbol{P_{n-1}})/\ 2^{24}$ for $\boldsymbol{n} > 2$.

- ❑ 50% chance of a collision exists already after only 4823 packets!!!

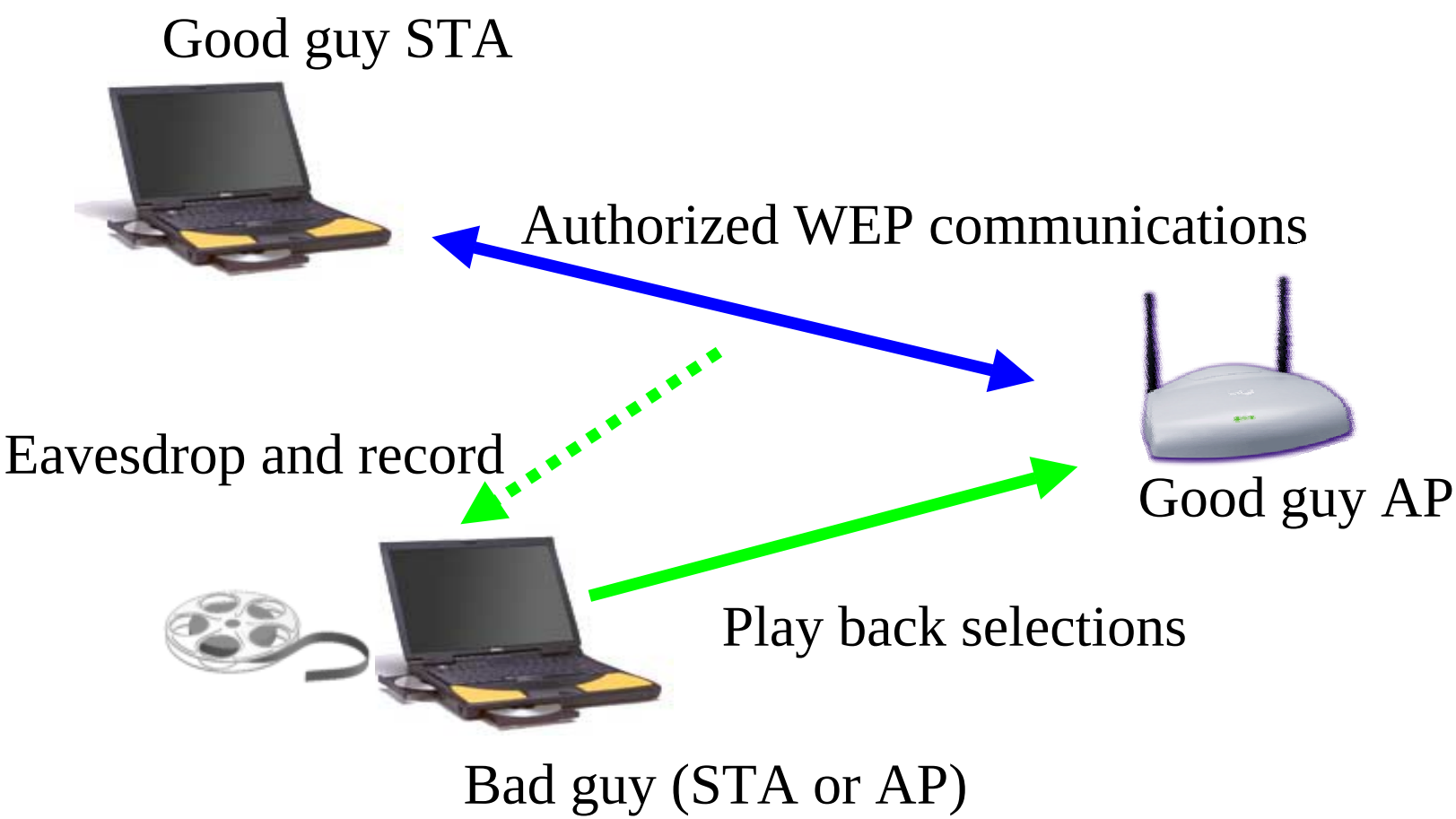
• Increment from 0: Collision probability = 100% after ***two*** devices transmit

Weak Key attack

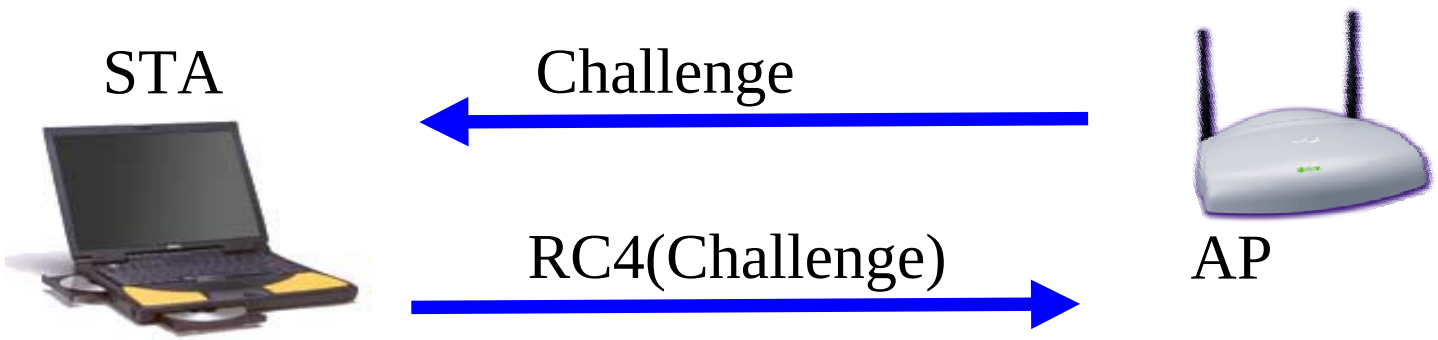


- Class of RC4 ***weak keys*** exists where patterns in the 1st 3 bytes of key causes corresponding patterns in 1st few bytes of the generated RC4 key stream.
- For each packet, use IV and exposed key stream to identify potential weak keys
- Iterate over potential weak keys from a sequence of packets until the RC4 base key is found

Replay attack

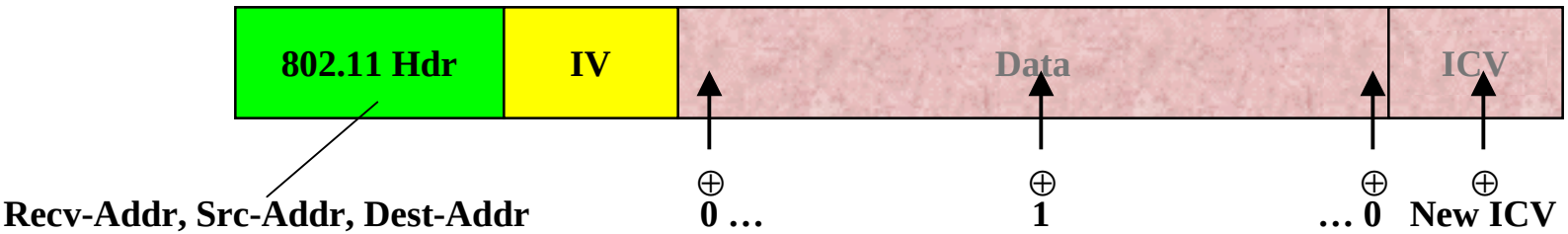


How does WEP authentication work?



Authentication key stream = Challenge ⊕ RC4(Challenge)

Forgery attacks



- Sample Attack 1:
  - ❑ Recv-Addr, Src-Addr, Dest-Addr are all unprotected
  - ❑ On packets from a STA to the AP, corrupt the Dest-Addr
  - ❑ The AP will decrypt data and send it to the forged destination
- Sample Attack 2:
  - ❑ create a blank message with same number of data bytes
  - ❑ Flip some bits and compute the ICV
  - ❑ XOR resulting bit-flipped message + ICV into captured message

Problem statement

- Enterprises want protected campus access.
- Home users want to block unauthorized access.
- Everyone wants to stop unauthorized usage of their networks—particularly illegal activities!
- Users want to know they are connecting to a trusted access point instead of an imposter.
- Everyone wants to prevent credential theft.
- Everyone wants security without user complexity.
- Everyone wants a balance between ease of use and risk management.

802.11i Goals

- **Security for Infrastructure**
- **Relies on 802.1X EAP for authentication, authorization and key management**
- **Adopts AES based encapsulation: CCMP**
- **Requires authentication servers for central authentication/authorization**