NEXT-GENERATION AUTHENTICATION IN WI-FI

Matthew Gast

September 22, 2014

The next 60 minutes

This talk is not about 802.11ac

Agenda

- Security property review
- PSK security analysis
- What comes next?

SECURITY REVIEW

Let's talk about hackers

(Yeah, I still miss it)

Types of attacks

- Passive attack
- Active attacks
- Dictionary attacks
- Denning-Sacco attack

Passive attacks

- **General flow**
  - Capture something from the protocol
  - Do "stuff" with it – analyze, compute, store
- **May learn a shared secret itself (e.g. AirSnort)**
- **May learn enough to break the protocol**
- **Usually must get close enough to be seen while taking action (sitting in the parking lot)**

Active attacks

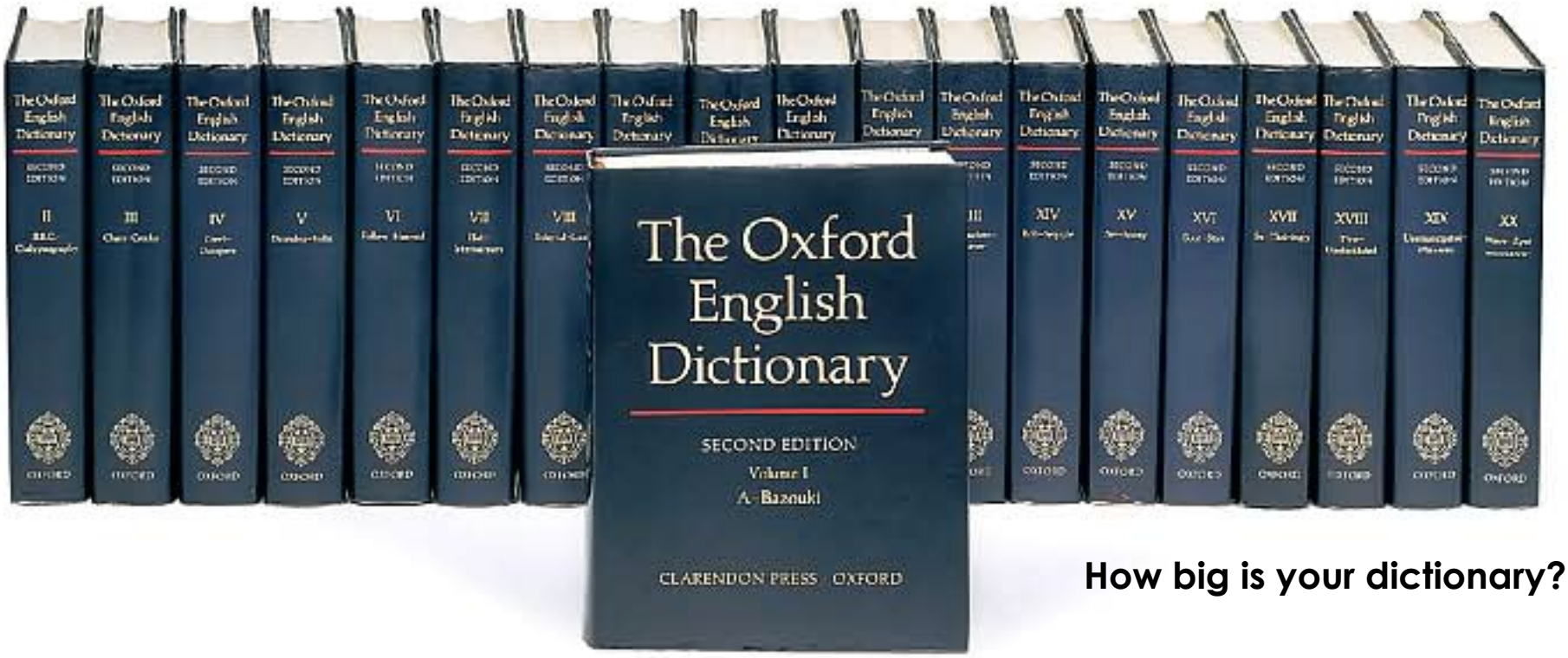
- **Be the device you want to be!**
- **Impersonate "honest" devices by**
  - Stealing keys
  - Man-in-the-middle
  - Protocol fuzzing
- **Definitely must decloak to fire frames**

Active attacks

- **Be the device you want to be!**
- **Impersonate "honest" devices by**
  - Stealing keys
  - Man-in-the-middle
  - Protocol fuzzing
- **Definitely must decloak to fire frames**

Dictionary attacks

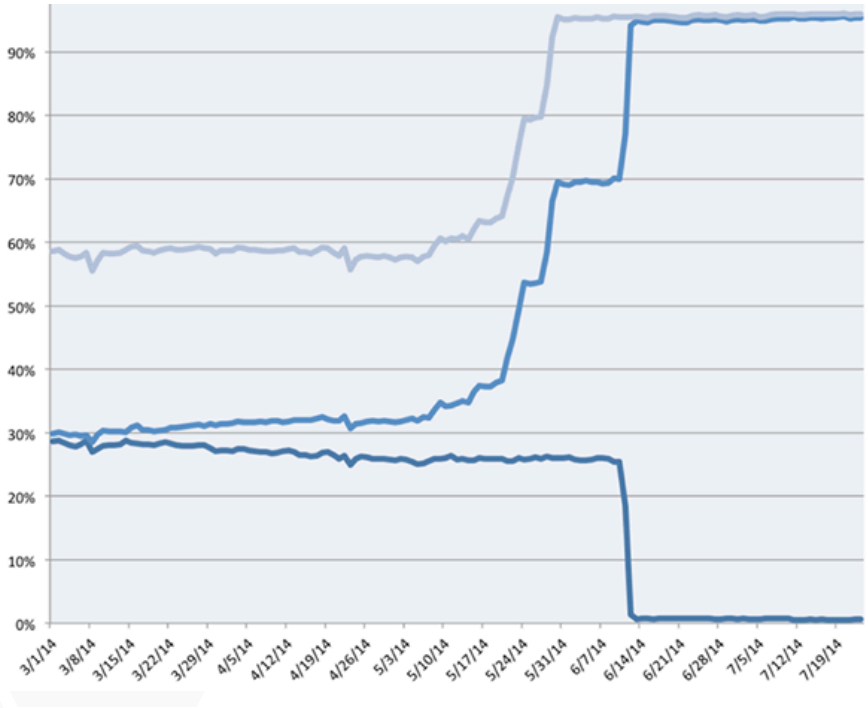
- **Run through all candidate secret keys**
  - Possibly enhanced by rainbow tables
- **Some implementations may rate-limit attempts**



How big is your dictionary?

Denning-Sacco attack

- **Flow**
  - Record session X
  - Wait for the time to be right
  - Replay session X to get on-line
- **Moral #1: Timestamp the protocol somehow**
- **Moral #2: The importance of <u>forward secrecy</u>**
  - Sometimes called Perfect Forward Secrecy (PFS)
  - More computation now, but benefits later
  - If you break run X of the protocol, it should not help you in the future



A question?

Let's look at Wi-Fi

- In large-scale environments, 802.1X is deployed by IT department (or self-service tools)
- But what if you don't have the ability to configure 802.1X?

Yuck! We need passwords

- **Pros: passwords are simple, and people understand how to use them**
  - Just put in the password and go!
  - Can add additional steps with new APIs for additional factors
- **Cons: simple**
  - People pick names of pets or children
  - Often need long passwords to have any security value ("sufficient entropy")
  - Re-use across systems
  - And WPA-Personal (PSK) is just awful

How does WPA-Personal stack up?

- **Password robustness: No "salt" in the handling of passwords, so it is possible to try all passwords reasonably quickly**
  - From November 2003! http://wifinetnews.com/archives/2003/11/weakness_in_passphrase_choice_in_wpa_interface.html
- **Offline dictionary attacks: capture the authentication exchange, and start computing on it**
  - Many tools implement this, for example http://www.willhackforsushi.com/Cowpatty.html and http://aircrack-ng.org/
  - GPUs can accelerate this up to 4000 passwords/sec
  - Amazon cloud: $0.85/min for 250,000 passwords/sec (improved since 2011)
- **Perfect forward secrecy? Heck no! Get the key, and you're in forever (or at least until the key changes)**

How does WPA-Personal stack up?

- **Password robustness: No "salt" in the handling of passwords, so it is possible to try all passwords reasonably quickly**
  - From November 2003! http://wifinetnews.com/archives/2003/11/Major_weakness_in_passphrase_choice_in_wpa_interface.html
- **Offline dictionary attacks: capture the authentication exchange, and start computing on it**
  - Many tools implement this, for example http://www.willhackforsushi.com/?page_id=50 and http://aircrack-ng.org/
  - GPUs can accelerate this up to 4000 passwords/sec
  - Amazon cloud: $0.80/hr for 250,000 passwords/sec (improved since 2011)
- **Perfect forward secrecy? Heck no! Get the key, and you're in forever (or at least until the key changes)**

BADLY!

The traditional way of making passwords better

- **Oddly, it's usually to make them harder to remember**

(example collected from the Internet)

The traditional way of making passwords better

- **Should not be easily defeated by small pieces of paper**

SO WHAT ARE WE DOING ABOUT IT?

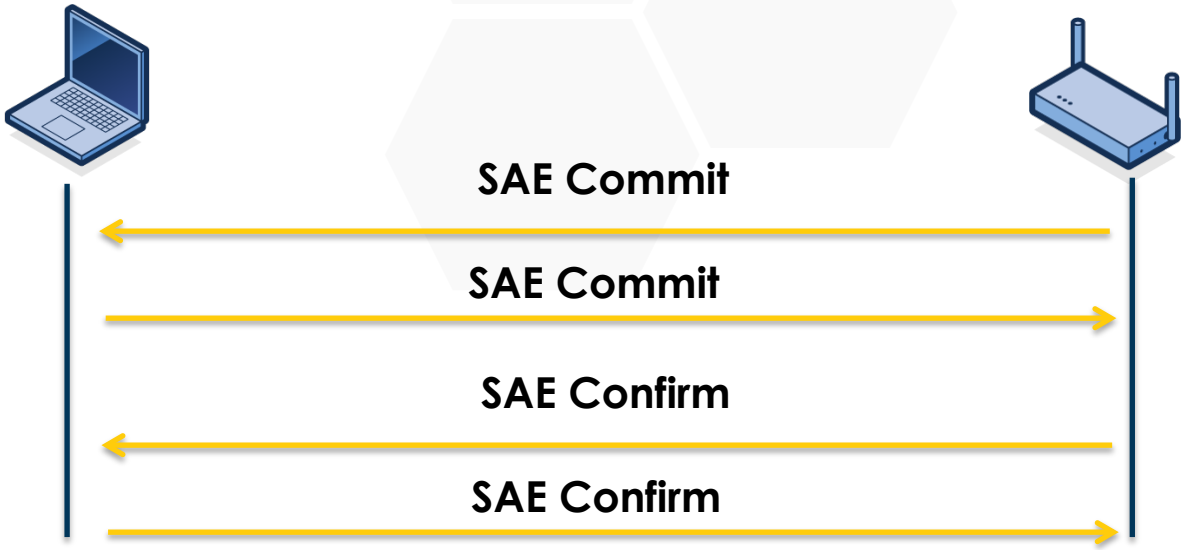
What kinds of fixes does PSK need?

- **Stop dictionary attacks**
  - Allow better passwords
  - Handle passwords better
- **Implement forward secrecy (it's about time)**

- **Stop passive observation attacks (more like Ipsec than WEP)**
- **Stop flooding attacks**

Enter SAE = "Simultaneous Authentication of Equals"

- **Originally defined in 802.11s (mesh extensions)**
  - Same goal as all cryptographic protocols: share a key between two devices
- **Basic protocol design: commit and then confirm**
  - Either side can commit at any time
  - After both sides commit, one party confirms
  - After both sides confirm, the protocol is complete



SAE cryptographic fundamentals

- **Key exchange: Diffie-Hellman cryptography**
  - Either cyclic group or elliptic curve
  - Many curves to choose from: NIST curves (FIPS 186-3), Brainpool curves (RFC 5639)
  - Lightweight – actually better than PSK for computation!
- **Diffie-Hellman exchanges are not authenticated unless it is designed on top of the crypto**
  - SAE adds authentication based on the password
  - Actually a transform of the "password equivalent" (PE)
- **Important addition: "anti-clogging" protection to stop flooding attacks**

SAE Commit

random -> rnd-A, mask-A
scalar-A = (rnd-A + mask-A) mod q
element-A = PE $^{-mask-A}$

random -> rnd-B, mask-B
scalar-B = (rnd-B + mask-B) mod q
element-B = PE $^{-mask-B}$

Shared Secret!

(PE $^{scalar-M}$ * element-M) $^{rnd-A}$ mod p = (PE $^{scalar-A}$ * element-A) $^{rnd-M}$ mod p

SAE Confirm

KCK | MK = KDF (Shared Secret, "stuff", (scalar-A + scalar-M) mod q)

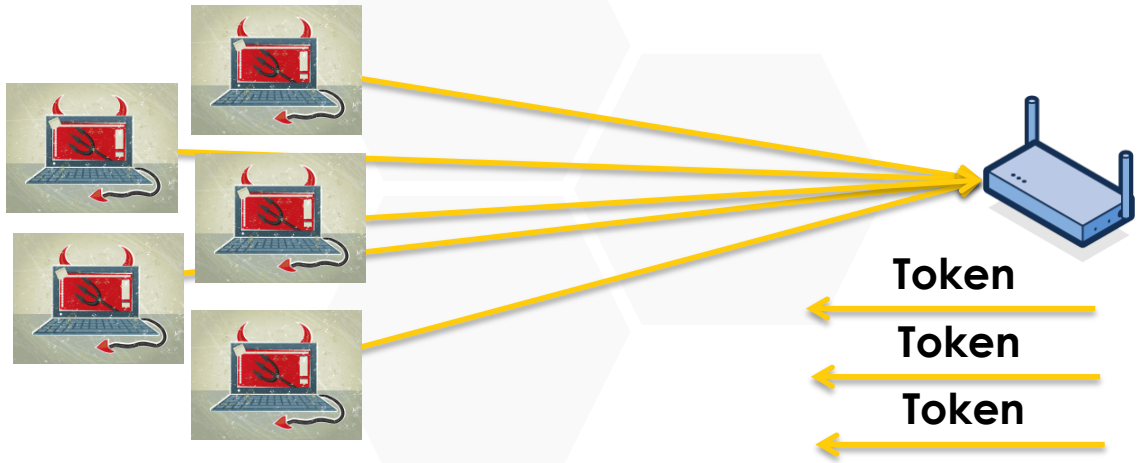
confirm-A = H(KCK, scalar-A | scalar-M | element-A | element-M)

confirm-M = H(KCK, scalar-A | scalar-M | element-A | element-M)

Master Key-based exchange is used to ensure confirmation
Two parties begin using new keys

Anti-clogging

- **When lots of sessions are pending, a peer will start issuing tokens needed to continue the exchange**
  - › Attackers can't generate tokens without doing work
  - › Tokens limit the number of pending sessions



The password of the future

- This is the future of password-based security in Wi-Fi
- Transition: support both PSK & SAE simultaneously
- The end goal: SAE is how we do passwords

THANK YOU!

@MatthewSGast

mgast (at) aerohive (dot) com